BlockDom Requirements Analysis

George Giamouridis

November 2021

BlockDom is a public blockchain network, meaning that all participants can read it and use it to carry out transactions but also if everyone can participate in the process of creating the consensus participants can join at any time without any restrictions [1]. The blockchain is responsible for handling different types of domain names (TLDs) and serving users requests. BlockDom differs from traditional blockchain as it does not use or maintain any cryptocurrency for the needs of the transactions.

1 Implementation Requirements

1.1 The Network

BlockDom blockchain follows the sharding technique, meaning that the blockchain is partitioning into smaller committees, each of these processes a disjoint set of transactions [2]. As a result, BlockDom can be considered as a collection of autonomous sub-blockchains, each of it operating on its own. Each committee maintains a ledger where blocks with transactions are stored in it. Those transactions are related only to this sub-blockchain, and they do not have any relationship with any other sub-blockchain. Although sub-blockchains are fully autonomous and have nothing to do with each other, they are able to exchange data through smart contracts.

All sub-blockchains must be designed in such a way that they can store a specific amount of TLDs and an unlimited number of domains names assigned to them. When a new node will be assigned to a sub-blockchain, it will synchronize the ledger of this sub-blockchain and will be responsible for validating transactions only within this sub-blockchain.

1.2 Nodes

In blockchain networks, nodes follow the P2P architecture, according to which nodes are defined as heterogeneous distributed resources which are connected by a network [3] and having the same rights and responsibilities. In BlockDom blockchain nodes will be assigned with **roles**. There will be two different node roles. The **Full Node** and the **Seeder**.

A Full Node will be a regular node participating in a sub-blockchain and maintaining its ledger. This node will be able to verify new transactions and propagate them to the network. A Full Node will be connected to other nodes in the same sub-blockchain according to the flat topology of the P2P architecture. This node will be also able to making new transactions and broadcasting them to the sub-blockchain. Full Nodes will have the ability to join and leave anytime.

A Seeder node will be a long-running, stable node that is listed in the BlockDom client as a *seed node*. Each Seeder will maintain the following data:

- The blockchain (ledger) of the sub-blockchain
- A record with the current status (active nodes) of the sub-blockchain

Each sub-blockchain will have a Seeder node. When a new node (full-node) joins the sub-blockchain, the Seeder will be responsible for establishing a TCP connection between the new node and some active network's nodes [4]. Seeders are also responsible for maintaining the ledger of the sub-blockchain in case there are no active full-nodes in it [5].

1.3 Transactions

A transaction will be originated whenever a user registers a new domain to the blockchain. Each transaction will contain the domain-IP pair as shown in listing 1, and will be stored in a unique block inside a sub-blockchain.

```
{
    domain : "google.com"
    IP     : "217.160.0.201"
}
```

Listing 1: Transaction

When the transaction is successfully propagated to the whole network, it will then be mined by a full-node, appended to a block and finally recorded on the sub-blockchain. Once the block with the transaction is appended to the blockchain it will be permanent part of this sub-blockchain, but it can be accessed by any node in any sub-blockchain through by using a smart contract.

1.4 The Blockchain

BlockDom blockchain will be consisted of multiple-smaller-autonomous sub-blockchains. Each of these blockchains will be an order back-linked list of blocks that contains transactions. Blocks will be linked to each other by referring to the previous block of the chain. Each block inside the blockchain will be identified by a unique hash (block header), which will be generated by using the SHA256 hashing algorithm. Each block will be referred to its parent (previous block) through the previous block hash. All the linked blocks will create a chain going back all the way to the Genesis block, which will be the initial block of

each sub-blockchain.

A block will be a data structure that stores transactions. While most popular blockchains like Bitcoin and Ethereum store multiple transactions within a block, BlockDom would be able to store only one transaction per block. This is because blocks in BlockDom have to be accessed fast by the smart contracts in order to spot the requested domain.

1.5 Smart Contracts

Smart contract is an essential part of the BlockDom blockchain. As long as different types of TLDs are stored in different sub-blockchains, each of them should be able to exchange data. There are 3 processes for which smart contracts are needed:

1. Assigning a node to a sub-blockchain
2. Registering new domains
3. Requesting domains

Assigning a node to a sub-blockchain is the first process that will occur when a new node is joining the network. The smart contract should be able to identify the most appropriate sub-blockchain (according to some criteria) in which the new node will be assigned.

Searching domain names and generating DNS requests will be the main BlockDom's functionality. Similarly to traditional DNS, this smart contract should be responsible for getting the domain name that the user has requested and translated into an IP address. The contract searches through the sub-blockchain to find the corresponded IP for the requested domain.

A transaction will be originated whenever a node adds a new domain in the blockchain. If the contract that searches the sub-blockchain returns an NXDOMAIN code (the domain name which is thus denied and all the names under it do not exist [6]), the registration contract should be able to refer to the traditional DNS servers, retrieve the IP address and register it to the BlockDom blockchain. in case the requested domain is not registered even in the traditional DNS, the contract should be able to generate the domain-IP pair for this domain and register it to the blockchain.

1.6 Consensus

Still working on it...

2 Security Requirements

- **Anonymity**: In traditional DNS, an ISP is responsible for handling the DNS requests of the user. Thus, user's activity is tracked by the ISP. The

proposed model should be able to replace the ISP (which acts as a central party) with a decentralized network which handles requests anonymously.

- **Security:** In terms of security, traditional DNS doesn't meet all the requirements of the CIA triad:
  - Confidentiality: Apart from the DNS servers, DNS records are also stored in user's cache memory. Although cache can be accessed only by the owner of the machine, there are several attacks through with an adversary can gain unauthorized access to the user's machine and therefore to the cache memory.
  - Integrity: DNS integrity is threatened by various popular attacks that aim to manipulate the records (e.g., DNS spoofing modifies the domain-IP pair and redirects users to malicious websites).
  - Availability: DNS availability is mainly threatened by DoS-based attacks like "DNS flooding". DNS service cannot ensure that the servers will be always available, as DoS attacks are likely to occur.
- **Performance:** Traditional blockchains require from users to synchronize the whole ledger and therefore the sync process takes a long time. Furthermore, a big (in terms of data storage size) ledger makes the searching process more complex and slow. The proposed decentralized — blockchain-based DNS should be able to handling the data in such way, that fundamental functionalities like synchronization and searching would be executed efficiently.

3 Data Handling Requirements

Blockchain networks are designed in such way that data can only be appended in them, but not deleted or modified. A minor change affects the whole blockcahin and breaks the chain.

It is very usual that the domain name of a website can be changed or deleted. As long as traditional DNS is. centralized systems, modification and deletion are easy to happen. Therefore, when a change occurs to a domain, the servers are updated accordingly. However, in BlockDom data modification and deletion is impossible to happen as we mentioned earlier that those operations are not taking place in blockchain networks. That means that whenever a domain changes, the ledger is unable to be updated.

References

[1] Dominique GUEGAN, "Public blockchain versus private blockhain," May 2017. [Online]. Available: https://halshs.archives-ouvertes.fr/halshs-01524440/document

[2] Gang Wang, Zhijie Jerry Shi, Mark Nixon, Song Han, "Sok: Sharding on blockchain," October 2019. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3318041.3355457

[3] Riidiger Schollmeier, "A definition of peer-to-peer networking for the classification of peer-topeer architectures and applications," 2002. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=990434

[4] Andreas Antonopoulos, "Mastering bitcoin," 2010. [Online]. Available: https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf

[5] bit2me ACADEMY, "What is a seed node?" July 2020. [Online]. Available: https://bit.ly/3sz0y2G

[6] S. Bortzmeyer, S. Huque, "Nxdomain: There really is nothing underneath," November 2016. [Online]. Available: https://www.hjp.at/(en)/doc/rfc/rfc8020.html