A Blockchain Implementation of Domain Name Service

Ken Cheng

Motivation

- DNS servers must maintain consistent replica
- Users must trust DNS server
- DNS servers are vulnerable to DDoS

Approach

- A zone file is where DNS servers store the (hostname,ip) mapping pairs
- A blockchain powered zone file can guarantee the following properties
- Exact replica across network
- Append-only transaction style update
- Scalability in distributed settings

Problems

- Remember proof of work?
    - Achieving consensus while tolerating malicious users
    - Providing stability as the chain grows
    - PoW is expensive!
- Why would DNS providers compete?
- How to incentivize providers in computing PoW?

Insight

- Why do DNS registrars provide service?
- What if providers must contribute to chain to make money?
- Integrated transaction type
  - Quota transaction
  - Mapping transaction

Transactions

- Quota transaction
  - Earn quota by mining
  - New mapping limited by quota


```
{
        "block_index": 2,
        "node": "6828d92f6e76427a9093197994bd73ab",
        "reward": 10
}
```

Transaction

- Mapping transaction
- Consumes provider's quota


```
{
        "hostname": "www.apple.com",
        "ip": "456.123.123.123",
        "port": "5678"
}
```

Implementation

- Blockchain layer
  - General transaction-storing class
- DNS layer
  - Abstraction of blockchain layer
  - DNS lookup and new entry storing
- Server layer
  - RESTful API providing layer
  - Allows communication between nodes

Demo

Future Development

- RFC compliant packets
- More versatile record types
- Node route message broadcasting