Routing Mechanism And Anonymity In Permissionless Blockchains

su da 515030910045

Abstract

Blockchain technology, as a decentralized and non-hierarchical platform, has the potential to replace centralized systems. Yet, there are several challenges inherent in the blockchain structure.One of the deficiencies of the existing blockchains is a convenient information propagation technique enhancing routing mechanism and anonymity.

I. INTRODUCTION

A blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is ”an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way”. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. This makes blockchains potentially suitable for the recording of events, medical records, and other records management activities, such as identity management, transaction processing, documenting provenance, food traceability or voting.

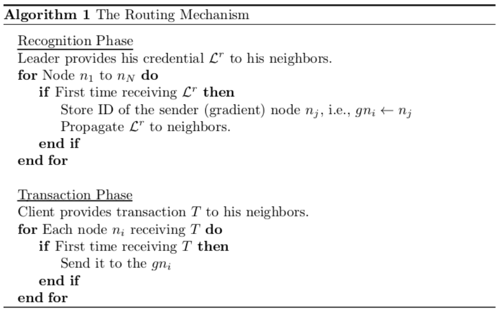
Blockchain was invented by Satoshi Nakamoto in 2008 for use in the cryptocurrency bitcoin, as its public transaction ledger. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has been the inspiration for other applications.[1]

Privacy protection is an important problem in blockchain.We can use bitcoin as an example.In computer science, anonymity refers to an unlinkable pseudonym. The so-called incoherence refers to the inability to associate any two interactions between the user and the system from the perspective of the attacker. In bitcoin, it is obvious that transactions can be associated because users repeatedly use public key hash values as transaction identifiers. So bitcoin is not anonymous.

II. LOCATIONAL PRIVACY IN ROUTING MECHANISM

A. routing mechanism

Protocol[2] as showed in figure 1 and figure 2 can be divided into two parts: Recognition Phase where the routes are determined and Transaction Phase where the transactions are propagated. Instead of sending each transaction to all nodes in the network, it is relayed over the shortest path between the client and the leader. The distance between (almost) any two nodes in a connected graph is dramatically smaller than the size of the network. This is equivalent to cost reduction from O(N) to O(ln N) in a random network of size N. The existing research shows that



Algorithm 1 The Routing Mechanism

```
Recognition Phase
Leader provides his credential $\mathcal{L}^r$ to his neighbors.
for Node $n_1$ to $n_N$ do
    if First time receiving $\mathcal{L}^r$ then
        Store ID of the sender (gradient) node $n_j$, i.e., $gn_i \leftarrow n_j$
        Propagate $\mathcal{L}^r$ to neighbors.
    end if
end for

Transaction Phase
Client provides transaction $T$ to his neighbors.
for Each node $n_i$ receiving $T$ do
    if First time receiving $T$ then
        Send it to the $gn_i$
    end if
end for
```

Fig. 1: 1.png

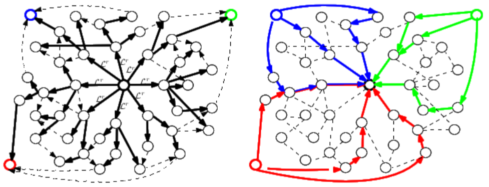


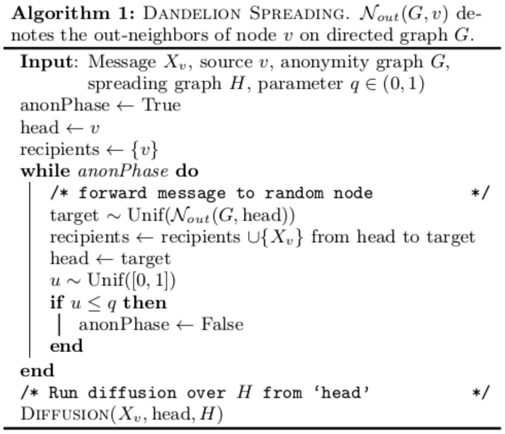
Figure 2: The Routing Mechanism. The left one illustrates the Recognition Phase and connections to the gradient nodes are shown with bold solid lines. On the right, three clients and their transaction paths are presented.

Fig. 2: 2.png

matching public keys and IP addresses can be done by eavesdropping. In this manner, FLTB-based blockchains may exposed to DoS (denial-of-service) attacks against to the round leader. The mechanism in figure 1 does not cause any additional vulnerabilities for DoS-like attacks against the round leader.

B. locational privacy improvement

We can improve the locational privacy via anonymity phase where the message is first forwarded in a line of nodes, then diffused from there[3].The extra cost of anonymity would be a few nodes on the line which is still proportional to the logarithmic size of the network. In particular, we can apply dandelion spreading to the routing mechanism as an anonymous networking policy. Dandelion spreading forwards each message on a randomly-selected line before diffusing it to the rest of the network. Dandelion spreading consists of an anonymity phase and a spreading phase as showed in figure 3. In the anonymity phase, the protocol spreads the message over a randomly-selected line for a random number of hops; in the spreading phase,the message is broadcast using diffusion until the whole network receives the message.



Algorithm 1: DANDELION SPREADING. $\mathcal{N}_{out}(G, v)$ denotes the out-neighbors of node v on directed graph G.

```
Input: Message $X_v$, source $v$, anonymity graph $G$,
       spreading graph $H$, parameter $q \in (0, 1)$
anonPhase ← True
head ← $v$
recipients ← $\{v\}$
while anonPhase do
    /* forward message to random node */
    target ~ Unif($\mathcal{N}_{out}(G, \text{head})$)
    recipients ← recipients $\cup\{X_v\}$ from head to target
    head ← target
    $u \sim$ Unif([0, 1])
    if $u \leq q$ then
        anonPhase ← False
    end
end
/* Run diffusion over $H$ from 'head' */
DIFFUSION($X_v$, head, $H$)
```

Fig. 3: 3.png

III. PROBLEM AND ANALYSIS

In the experimental results of routing mechanism, propagating information to a few of neighbors(precisely the default number of connections of a node) is sufficient. But if the number of neighbors is smaller, can we satisfy the requirement of average shortest path length? What's more, although we don't need all the neighbors to propagate information, how do we choose the neighbors and calculate the probability of each neighbor? Through selecting proper parameter, we can further lower the redundant communication cost. We can use genetic algorithm to find the global optimal solution.

IV. CONCLUSION AND EXPERIENCE

In this project, I learn about much about information propagation in blockchain,such as sybil-attack,gossip protocol. Then I realize there are many problem we need to solve. For example, we need to reduce the redundant communication and improve the privacy protection. Blockchain is a newly-developing technology with great prospects for development. First, we talk about a smart routing mechanism which the redundant communication cost from the size of the network to the scale of average shortest path length.Second, we apply the dandelion spreading to improve the locational privacy. In the future work, the way to stimulate information propagation can be talked about.

V. REFERENCES

[1]https://en.wikipedia.org/wiki/Blockchain.

[2]Oguzhan Ersoy, Zhijie Ren, Zekeriya Erkin, and Reginald L.Lagendijk. Information Propagation on Permissionless Blockchains,2017.

[3]Shaileshh Bojja Venkatakrishnan, Giulia Fanti, and Pramod Viswanath. Dandelion: Redesigning the bitcoin network for anonymity. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 1(1):22, 2017.