Routing in Blockchain P2P Overlay Networks

Student ID & Name & Login User Name

1214448 YueyuanZhang YUEYUANZ

Catalog

1. Identification Info

On a macro level, blockchain has three basic characteristics, distributed storage, P2P network and consensus mechanism. Therefore, blockchain is naturally one of the most widely used scenarios for P2P overlay networks, such as the unstructured overlay network used in Bitcoin and the structured overlay network used in Ethereum. At the same time, routing is widely used in bookkeeping and payment transactions. In the process of collecting data, different papers try to improve the current routing mechanism from different angles, and provide different design ideas and improvement schemes. This project attempts to sort out the internal relations of these journal papers and compare the advantages and disadvantages of routing mechanisms.

2. Introduction to the Topic

Major applications for blockchain include cryptocurrencies, cross-border payment and settlement, and other applications where a degree of privacy and reliability is required.

The improvement of routing mainly includes the following aspects:

2.1 Adjusting routing table coverage

Classical P2P networks cannot operate routing mechanisms and lookups on existing networks, because routing tables are often updated at high frequency and in large quantities, and peer discovery mechanisms are poor [1] (Naik et al., 2020). How to modify the coverage structure of dynamic routing table, so that it can find the peer with as few hops as possible, and how to manage the routing table efficiently and make it as easy to maintain as possible have become a thinking direction.

2.2 Optimizing routing algorithm

The complexity of the algorithm design is that it involves more than just the widest path or maximum flow. Each path has a certain time delay constraint, each directional communication needs to reduce interference, and the dynamic network and channel monotonicity caused by concurrency problems. Specifically, a distributed algorithm needs to be designed, with each node having its own knowledge; timeliness and availability constraints should be considered in some scenarios; also avoid generating redundant concurrent contending requests [7] (Yu et al, 2018).

2.3 Introduction of new routing protocols

Good routing protocols can improve the overall performance of the network. Most routing protocols are reactive or proactive. However, with the increasing complexity of the network, the traditional routing protocol is not enough to support the security problem, and some nodes may still be attacked by malicious. For example, the traditional Border Gateway Protocol is used to connect the edge routers in adjacent autonomous systems, but the problem is that the mutual trust between autonomous systems will lead to partial or complete attacks on nodes. In view of this, new secure routing protocols can be designed and introduced to prevent data tampering [8] (Saad et al, 2019).

3. Related Work Details

Banno et al. (2021) believe that unstructured coverage networks are inefficient in transmitting information, and that the overlapping layers of structured coverage networks are risky and insecure. Therefore, they propose a semi-structured overlay that applies to overlapping layers and is maintained by a flexible routing table (FRT). FRT consists of two steps: Entry Learning and Entry Filtering. Entry Learning collects node information and Entry Filtering introduces randomization to discard useless information. The relationship between randomness and path length is obtained by using Java simulation experiment. High randomness will lead to longer path length [2].

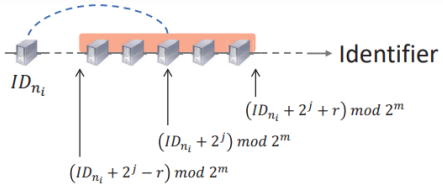

Fig. 2. Neighbor selection in proposed method.

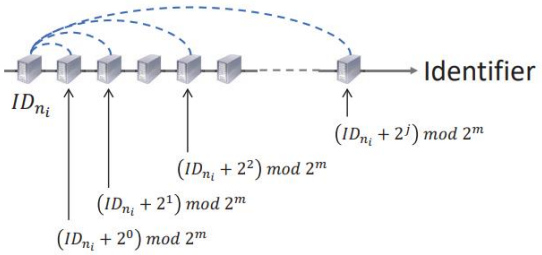

Fig. 1. Neighbor selection in Chord.

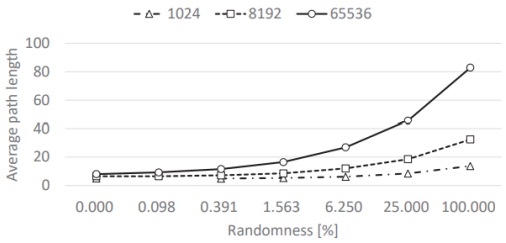

Fig. 3. Trade-off of path length and randomness.

Rohrer et al. (2019) evaluated Kadcast, a novel peer-to-peer protocol network propagated by blockchain. They established a probabilistic model to analyze Kadcast's elastic loss to packets and interruption failures, and confirmed its advantages in terms of delivery performance, broadcast reliability, efficiency and security. Kadcast makes use of the overlapping structure of Kademlia, a UDP-based peer protocol, to enable efficient broadcasting. Kademlia uses a structured overlay network that determines the location of nodes through a binary routing tree. Nodes can traverse the network structure efficiently with a message complexity of $O(log\, n)$. Each node stores a triple (ip_addr, port, ID) and marks

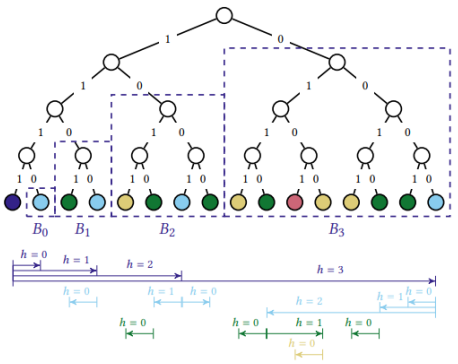

Figure 2: Example broadcast initiated by node 1111 ($\beta = 1$). Colors indicate node distances in the spanning tree, relative to the initiator.

known nodes as k-buckets. Buckets are regularly updated by each node, which enables lightweight overlaid member information management [3].

Wang et al. (2021) designed a blockchain-based lightweight secure routing algorithm for unmanned aircraft swarm systems (UAS) that can identify malicious UAS connections and prevent wiretapping, hijacking, and attack by the operator. They argue that the routing security of the Swarm UAS network is essentially dependent on the HOP selection and needs to be authenticated. Traditional methods use static storage and require a large amount of computing resources to broadcast updated blocks. They adopted a new approach that passively broadcasts the updated blocks, making the attacker require powerful computing resources to pass verification [4].

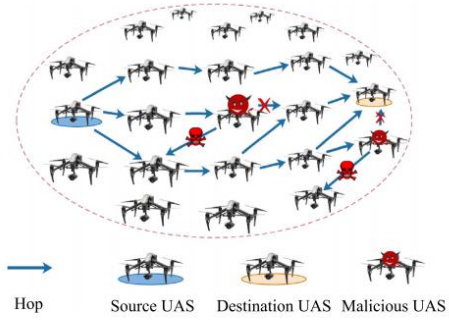

Fig. 1. Attackers in swarm UAS networking.

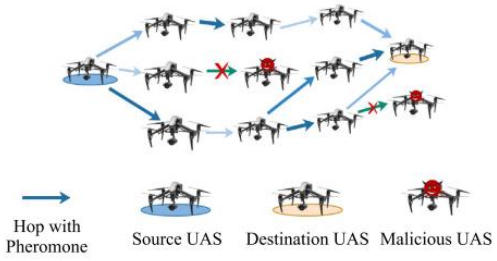

Fig. 2. Security routing of swarm UAS networking.

Tran et al. (2021) evaluated the rapid patching and protocol adjustment of the Bitcoin Core against the Erebus attack and found that there was no simple solution that could effectively respond. They propose a comprehensive defense framework that adds route-aware peer (or RAP) to the simple protocol tweaks available. They also provide an algorithm that outputs the best defense configuration to protect against most Erebus attacks. It gives each node the ability of symmetrical defense. Specifically, it requires each node to obtain the routing knowledge of

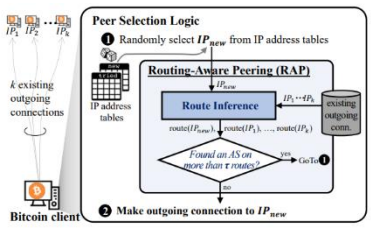

Figure 4: Bitcoin's peer selection logic and routing-aware peering (RAP) improvement. When IP_{new} is chosen for a new outgoing connection, the RAP function checks whether a malicious AS will likely be on the path.

Table 2: A quick comparison between three notable BGP route estimation algorithms in the literature.

Algorithms by Authors	Input Data	Advantages
Mao et al. [37]	AS-level topology and business relationship	Lightweight, minimal dependencies
Qiu et al. [47]	(all above) and BGP feed data	More fine-grained and accurate estimation
Akhoondi et al. [1]	(all above) and estimated AS path lengths	Over-estimation of intermediate ASes

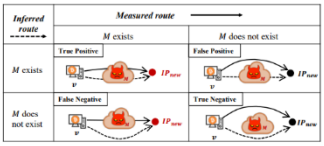

Figure 5: Confusion matrix for evaluating an inferred route from v to IP_{new}, given the potentially malicious AS M.

all peer connections through peer selection algorithm, detect whether there is a malicious autonomous system before making external connections, and refuse to connect to this IP address once it is found [5].

Dotan et al. (2021) review the latest technologies and challenges facing blockchain networks, including topology and neighbor discovery, cross-block and transactional propagation, sharding and off-chain networks. Regarding routing, they review popular payment channel networks (PCNs), which typically use source routing, which specifies the full routing of payments, and explore several ways to adjust scalability, such as using beacon nodes to maintain lists of adjacent channels and beacons. Another example is to use Ad Hoc On-Demand Distance Vector Routing (AODV) to reduce computing and memory overhead. The main challenges for these solutions are how to secure users while using light nodes, how to avoid a single point of failure, and how to pay across multiple paths [6].

4. Comparison of Key Approaches (benefits and disadvantages)

Improvement Approaches	Usage Scenarios	Advantages	Disadvantages
Semi-structured coverage of flexible routing tables	Encryption currency	Communication efficiency & Security	Scalability
A new p2p protocol propagate transactions by broadcasting	EFT(electronic fund transfer)	Lightweight Node Information Management	Security
Secure routing algorithm	Unmanned Aircraft Swarm System (UAS)	Security	Communication Efficiency
Route-aware peers(RAP) implement the defense framework	Bitcoin (BTC)	Security	Communication Efficiency
Use beacon nodes to maintain adjacent channels, adopting AODV protocals	Payment and Settlement	Scalability & Low Transaction Latency	Security

Table1: Blockchain Routing Approaches Comparison

A good routing mechanism should be combined with specific use scenarios to talk about,

in different use scenarios, need to consider the trade-off between various factors, priority to meet what needs, lagging to consider what problems, there is no optimal solution in all aspects. For the above mentioned five blockchain routing mechanism improvement schemes, Table 1 makes a simple use scenario and a comparison of advantages and disadvantages. For example, in the case of cryptocurrency, which involves a large number of network nodes, privacy security is the first thing to be guaranteed; in the case of electronic remittance and payment settlement, communication efficiency and scalability are the most important considerations due to high frequency trading. In addition, in the UAS flight system, it is necessary to avoid the UAS being manipulated and controlled by others, so safety has become the primary consideration.

As Tang et al. (2020) [9] pointed out, the tradeoff between privacy and practicality cannot be optimized by releasing noisy channels in PCNs, and Tradeoff cannot be improved by designing more complex utility indicators. Therefore, among the factors, only some metrics can be optimized, and some performance can be sacrificed or abandoned to better match the actual requirements. Such as prioritizing scalability and reducing security, or prioritizing privacy over communication efficiency.

5. Conclusions and Future Directions

At present, there is no clear conclusion on the routing mechanism of blockchain. Researchers try to put forward new ideas and solutions from various perspectives. Among them, communication efficiency, privacy and security, and scalability are still the most important considerations. With the booming development of various business needs, the future blockchain routing mechanism should be able to deeply integrate with the application scenarios and get close to the functional requirements of products to the greatest extent.

6. References

[1] Naik, A. R., & Keshavamurthy, B. N. (2020). Next level peer-to-peer overlay networks under high churns: a survey. Peer-to-Peer Networking and Applications, 13(3), 905-931.

[2] Banno, R., Kitagawa, Y., & Shudo, K. (2021). Exploiting semi-structured overlay networks in blockchain systems. IEICE Communications Express.

[3] Rohrer, E., & Tschorsch, F. (2019, October). Kadcast: A structured approach to broadcast in blockchain networks. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies (pp. 199-213).

[4] Wang, J., Liu, Y., Niu, S., & Song, H. (2021). Lightweight blockchain assisted secure routing of swarm UAS networking. Computer Communications, 165, 131-140.

[5] Tran, M., Shenoi, A., & Kang, M. S. (2021). On the Routing-Aware Peering against Network-Eclipse Attacks in Bitcoin. In 30th {USENIX} Security Symposium ({USENIX} Security 21).

[6] DOTAN, M., PIGNOLET, Y. A., SCHMID, S., TOCHNER, S., & ZOHAR, A. (2021). Survey on Blockchain Networking: Context, State-of-the-Art, Challenges. Proc. ACM Computing Surveys (CSUR).

[7] Yu, R., Xue, G., Kilari, V. T., Yang, D., & Tang, J. (2018, July). Coinexpress: A fast payment routing mechanism in blockchain-based payment channel networks. In 2018 27th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-9). IEEE.

[8] Saad, M., Anwar, A., Ahmad, A., Alasmary, H., Yuksel, M., & Mohaisen, A. (2019, May). RouteChain: towards blockchain-based secure and efficient BGP routing. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 210-218). IEEE.

[9] Tang, W., Wang, W., Fanti, G., & Oh, S. (2020). Privacy-utility tradeoffs in routing cryptocurrency over payment channel networks. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 4(2), 1-39.