


Speedup of Information Propagation on Blockchains

----Final Report

曹晋

515030910536

2018.05



Outline

- Background
- Related Work
- Proposal
- Experimental results & Conclusion

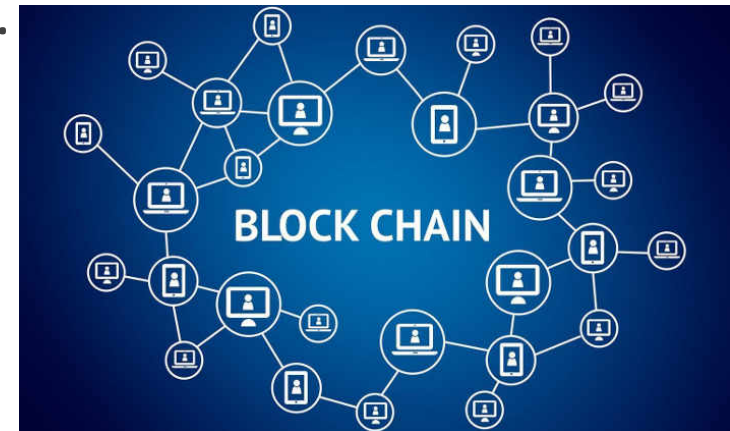
Outline

- Background
- Related Work
- Proposal
- Experimental results & Conclusion

Background

- What is blockchain?

- A continuously growing list of records, called blocks, which are linked and secured using cryptography.
- An intelligent peer-to-peer network for identifying, disseminating and documenting information with distributed database.



Background

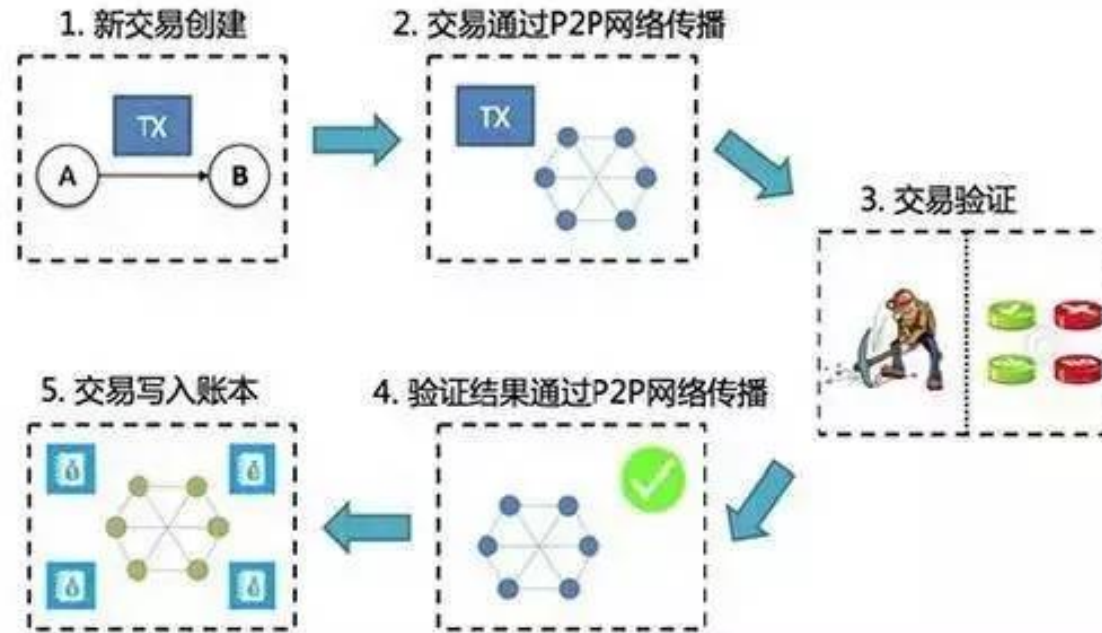
- What are the characteristics of the blockchain?
 - Decentralized
 - Unmodifiable
 - Transparent
 - Collectively maintained
 - Reliable

Background

- What is Bitcoin?
 - A peer-to-peer encrypted digital currency
 - Each valid transaction is recorded in the blockchain

Background

- The procedure of recording a transaction



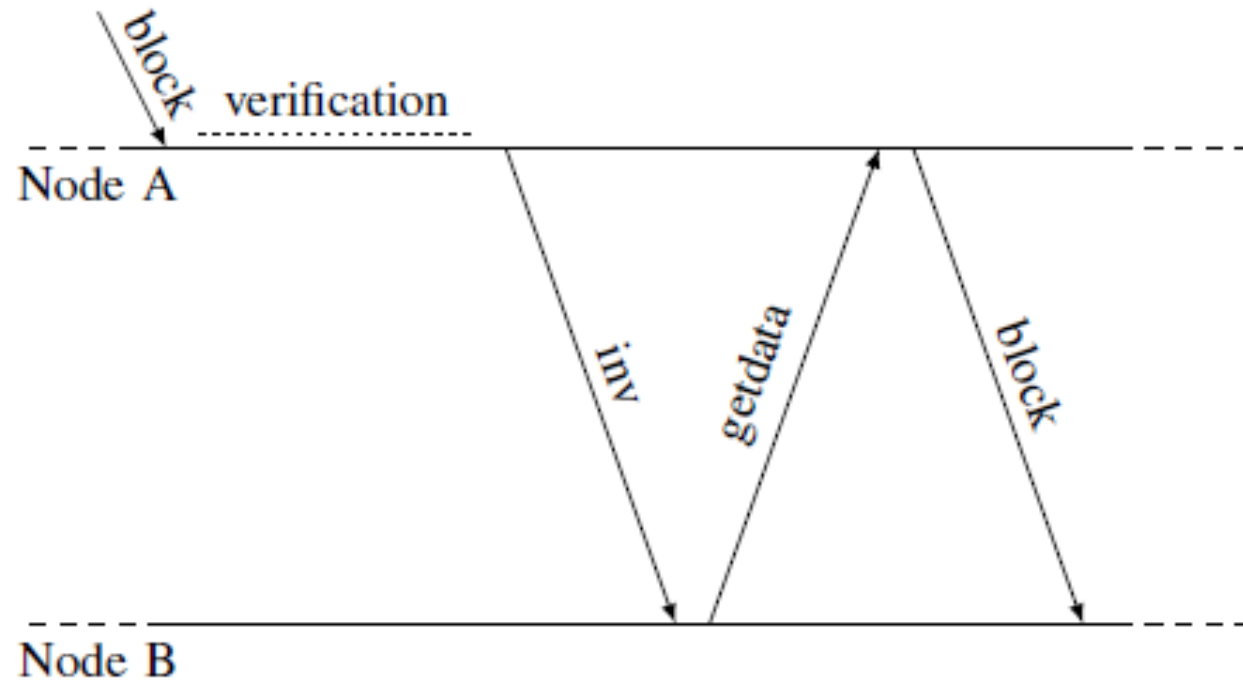
区块链的分布式记账

Outline

- Background
- Related Work
- Proposal
- Experimental results & Conclusion

Related Work

- The basic propagation process



Related Work

- The existing problem
 - Before forwarding the block to the next node, a verification time (correlated to the size of block) is needed
 - Every transaction is broadcast at least twice before being written into the ledger
 - Longer propagation time usually means larger probability of forks

We should speed up information propagation!

Related Work

- Method I : Minimize verification in a single node

The verification can be divided into two phases:

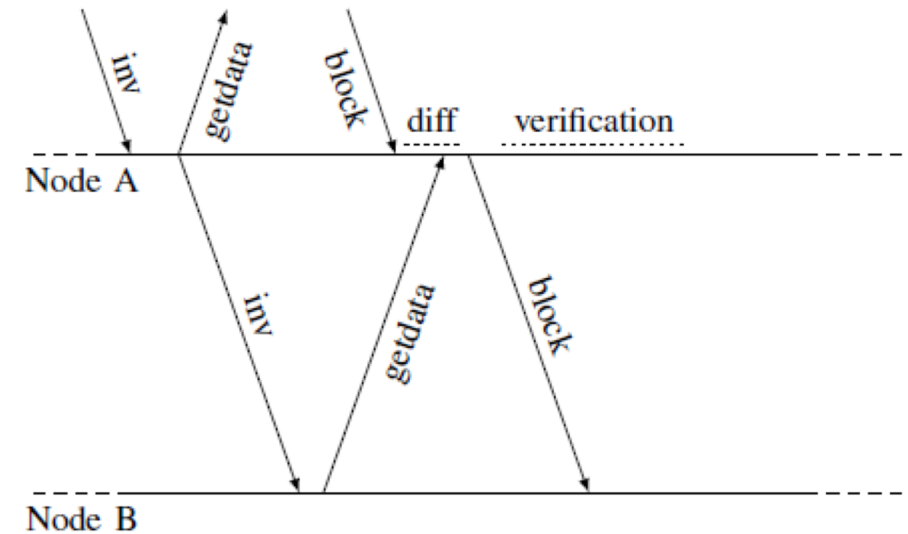
- An initial difficulty check
- A transaction validation

The block can be relayed to the neighbors, as soon as the difficulty has been checked and before the transactions has been verified.

Little improvement if implemented only by single node.

Related Work

- Method Π : Pipelining block propagation in a single node
 - The *inv* message is forwarded immediately
 - The verification is split into two phases



Little improvement if implemented only by single node.

Related Work

- Method III: Connectivity increase

The method of information propagation in the blockchain network is pretty similar to randomized rumor spreading. So it should be useful to minimize the distance between any two nodes. A feasible way is try to connect more nodes in the network creating a star sub-graph that is used as a central communication hub.

High bandwidth requirements.

Related Work

- Method IV: Reduce redundant propagation

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

Hard to judge the current leader. May only be feasible with PoS mechanism.

Outline

- Background
- Related Work
- **Proposal**
- Experimental results & Conclusion

Proposal

- Test the propagation time for a new transaction/block based on the current model. Verify the correctness of the propagation method.
- Try to generalize method I and Π to all nodes in the network. Evaluate the result by testing the propagation time and number of forks.
- Change the connectivity of the network. Find the relationship between connectivity and propagation time(# forks). Balance high bandwidth and high latency.

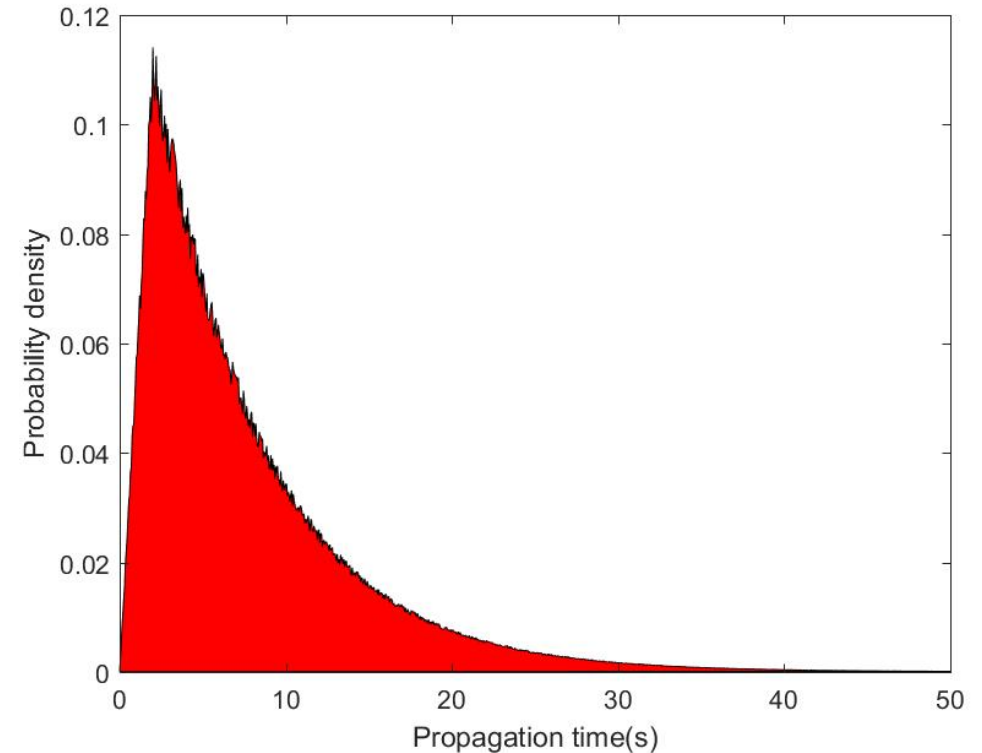
Outline

- Background
- Related Work
- Proposal
- Experimental results & Conclusion

Experimental results

- Simulation result

As expected, the proportion and propagation time shows an exponential decay relationship and is similar to Poisson distribution. It indicates that the basic propagation method is correct.

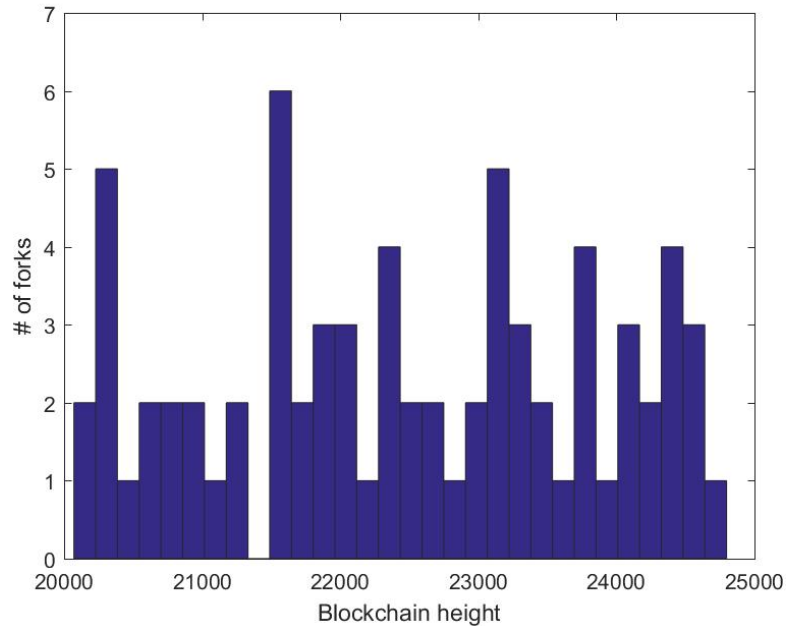


Experimental results

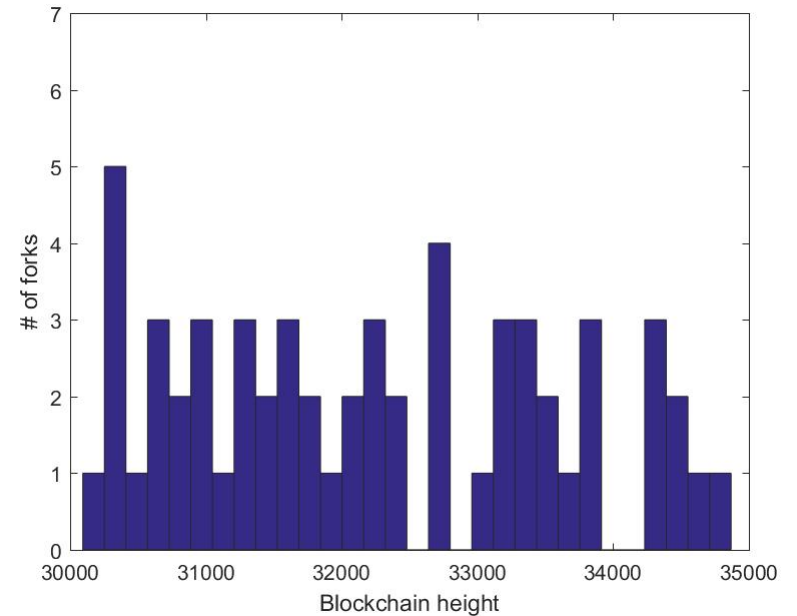
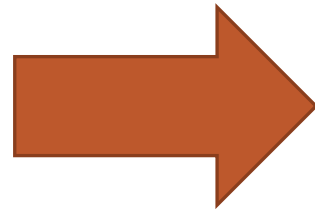
- Generalization of method I and II

Since method II is based on I, it is more effective to consider them together. I tested the number of forks in 5,000 blocks with the pipelining modifications. Comparing it with the original case, an effective improvement can be seen. There were 58 blockchain forks (the original is 72) and the fork rate was 1.16%, with a 19.44% improvement.

Experimental results



Histogram of blockchain forks from height 20,000 to 25,000 with original protocol



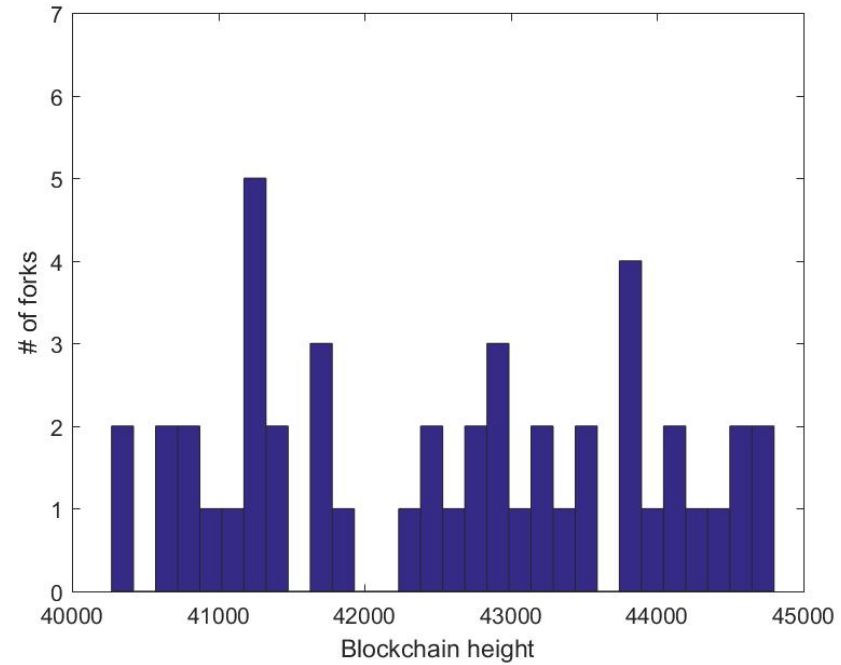
Histogram of blockchain forks with pipelining modifications

Experimental results

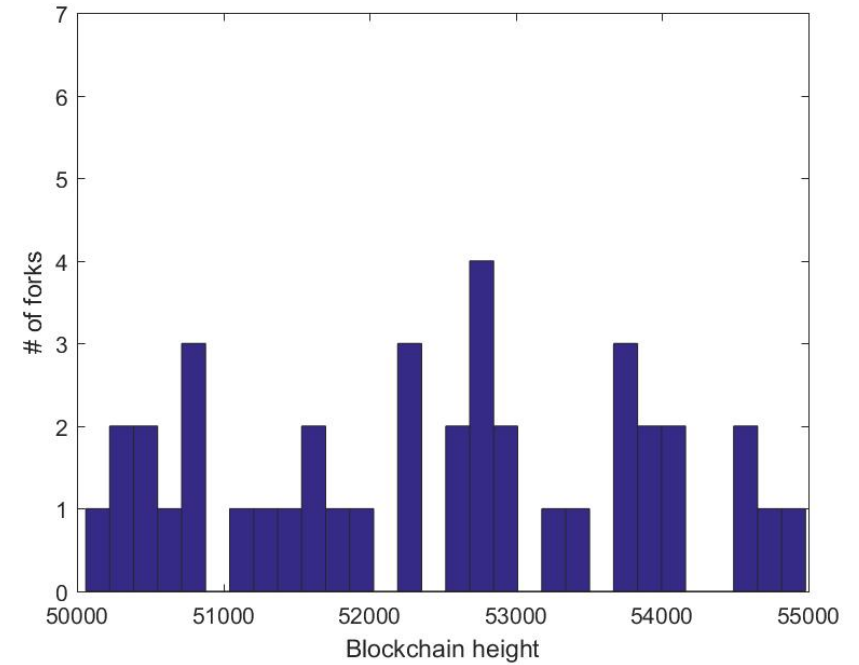
- Change the connectivity

The most influential problem is the remote distance between the origin of a transaction or a block and the nodes. To minimize the distance between any two nodes I attempted to connect to every node in the network creating a star sub-graph that is used as a central communication hub, speeding up the propagation of inv messages, blocks and transactions. It should speed up information propagation but also suffer higher bandwidth.

Experimental results



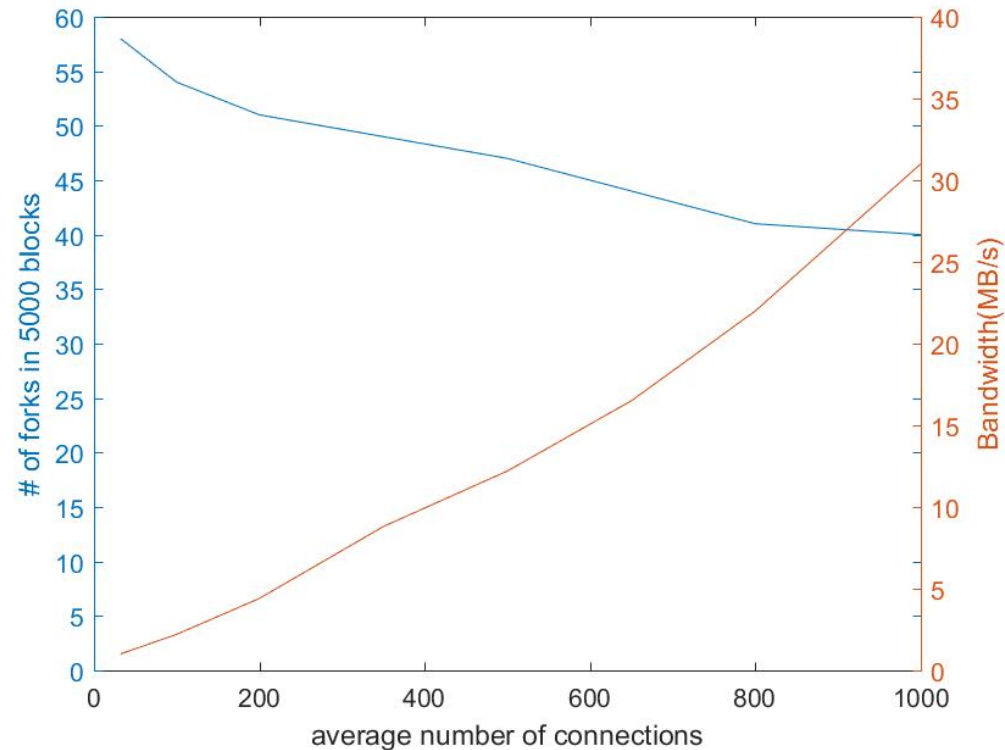
500 connections



1,000 connections

Experimental results

- Relationship between fork rate and bandwidth



Conclusion

- As blockchain forks are symptomatic for an inconsistency in the ledger replicas, it is important that the nodes in the network are aware about them.
- Some changes were done to the current Bitcoin protocol that reduce the risk of a blockchain fork. The measurements show a visible improvement and also the bottleneck due to bandwidth.
- However, the root cause of the problem maybe intrinsic to the way information is propagated in the network. To find more efficient method with more advanced propagation strategy will be a challenging task.

References

- 1. Alqassem I, Svetinovic D. Towards Reference Architecture for Cryptocurrencies: Bitcoin Architectural Analysis[C]// Internet of Things. IEEE, 2015:436-443.
- 2. Ersoy O, Ren Z, Erkin Z, et al. Information Propagation on Permissionless Blockchains[J]. 2017.
- 3. Turner A, Irwin A S M. Bitcoin transactions: a digital discovery of illicit activity on the blockchain[J]. Journal of Financial Crime, 2017:00-00.
- 4. Decker C, Wattenhofer R. Information propagation in the Bitcoin network[C]// IEEE Thirteenth International Conference on Peer-To-Peer Computing. IEEE, 2013:1-10.

Thanks!