Communication Analysis in a Private Blockchain

Libo Feng，Hui Zhang, W. T. Tsai

Beihang University

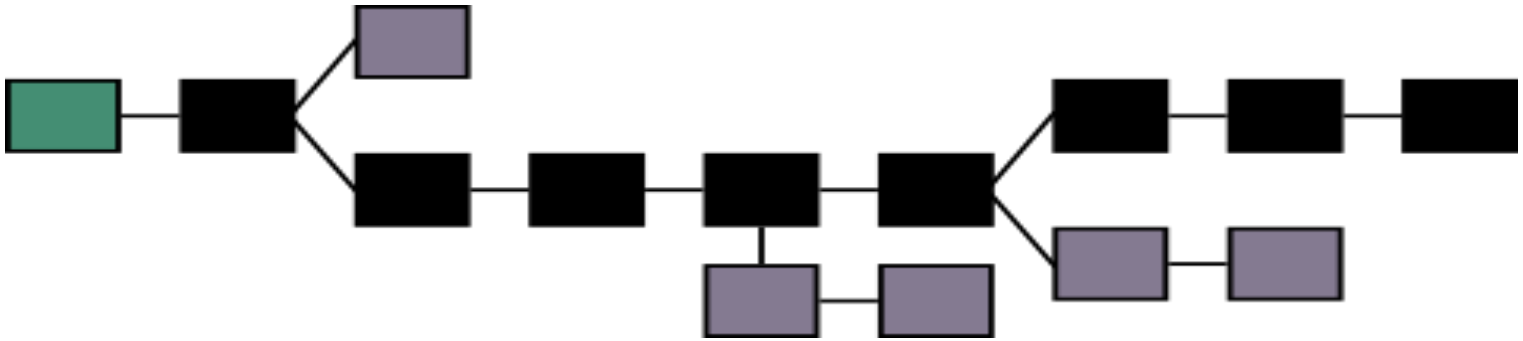
北京航空航天大學 BEIHANG UNIVERSITY

1. Introduction
2. Blockchain Operations
3. Communication Analysis
4. Framework Design
5. Traffic Analysis
6. Conclusion

Introduction

北京航空航天大學 BEIHANGUNIVERSITY

- **Blockchain is a new research topic, it is one enabling technologies to increase trust. Because of the decentralist characteristics of blockchain, the server broadcasts a block when it is generated. Furthermore, the blockchain needs to perform consensus protocol such as Paxos protocol as a part of Byzantine General problem. When there is a large amount of data flows into the blockchain, the performance of the broadcast communication can be an issue.**

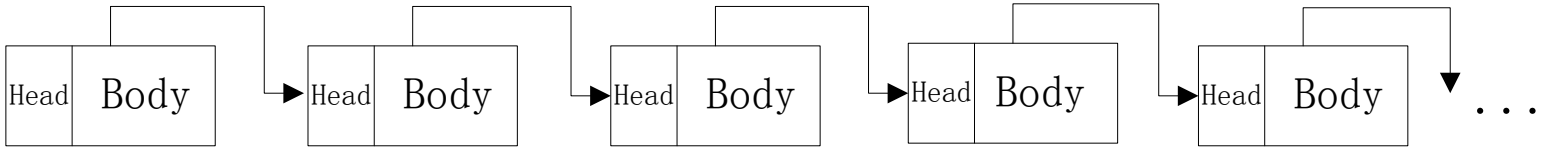


Blockchain Operations

北京航空航天大學 BEIHANG UNIVERSITY

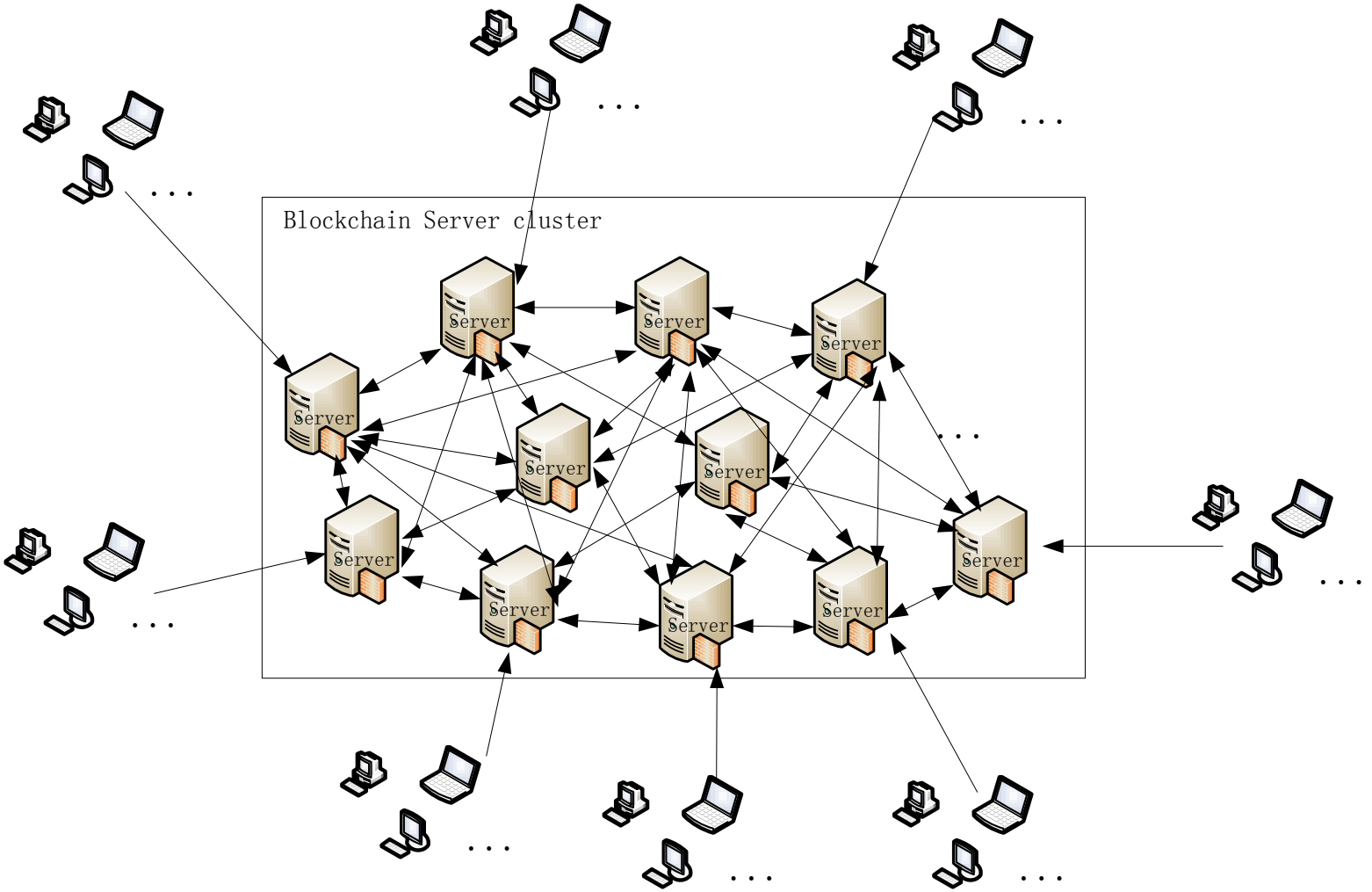
- Decentralization
- Blockchain can be public or private, and private blockchains have more security.
- If the application needs to process a large amount of data, such as NASDAQ (100K transactions per s), it may be necessary to have a cluster of servers.
- The cluster is essentially a distributed processing system. For each of the blockchain server is an autonomous machine, independent of other servers, but they work in cooperative manner.

Communication Analysis



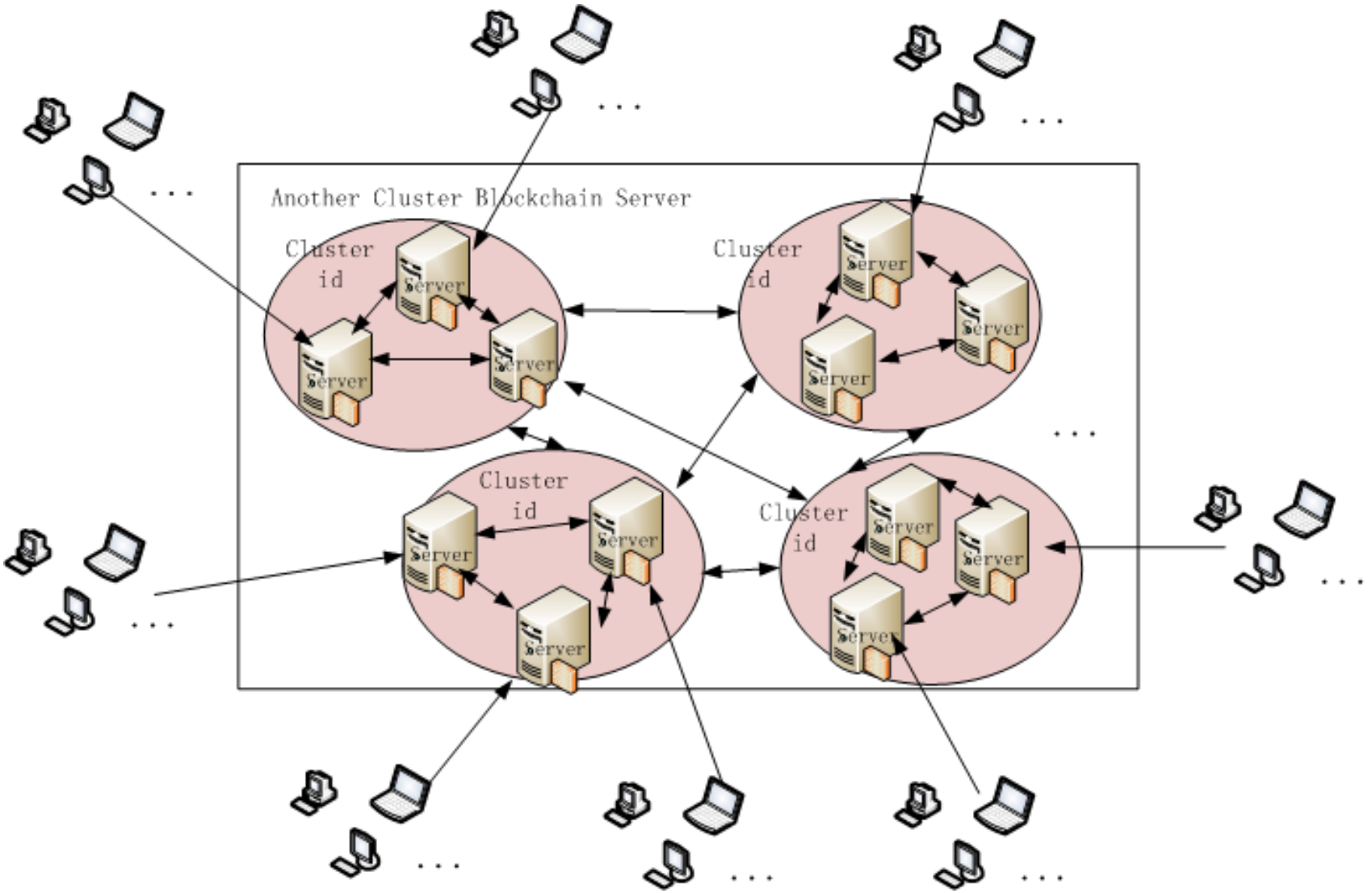
- **It is a linked list, and it runs on top of a server cluster. With a server cluster, multiple machines may be running concurrently.**

Server Cluster in a Trusted Environment

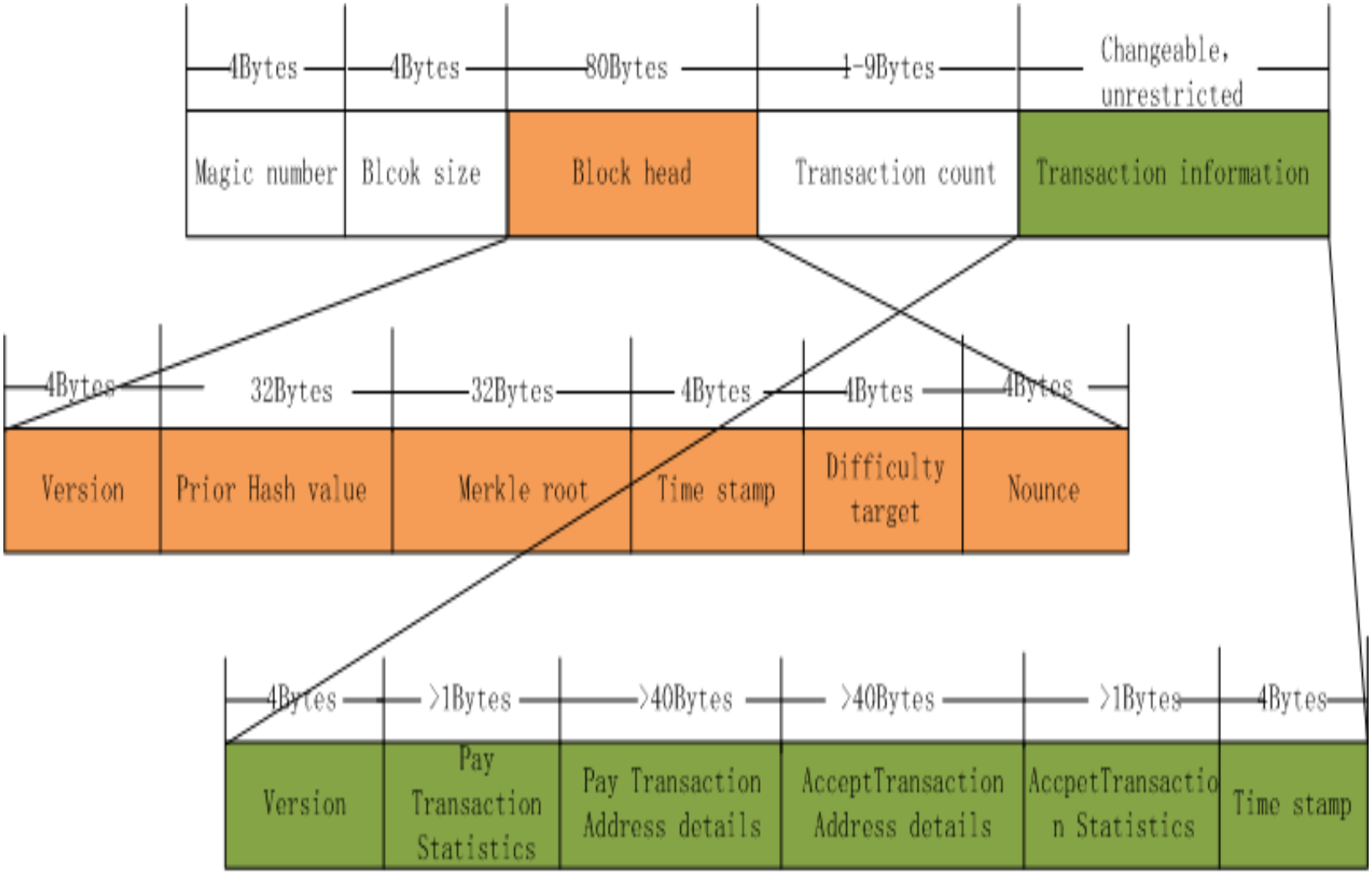


Untrusted Environment

北京航空航天大學 BEIHANGUNIVERSITY



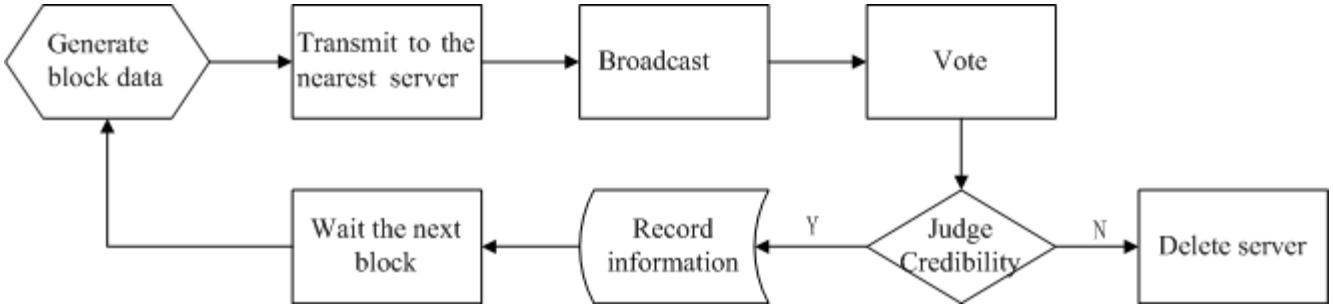
Structure of a block



- **Cluster server can be divided into two types. The first kind, all the blocks of the chain between the server to form a cluster, each server broadcast to the whole network. Second, the use of clustering in the form of each of the three servers or more to form a small cluster, cluster internal first broadcast communications, to confirm the credibility of each member. When all the servers in the cluster are credible, then broadcast between the clusters.**
- **The Second ways can significantly reduce the amount of communication. See the next section of the calculation process.**

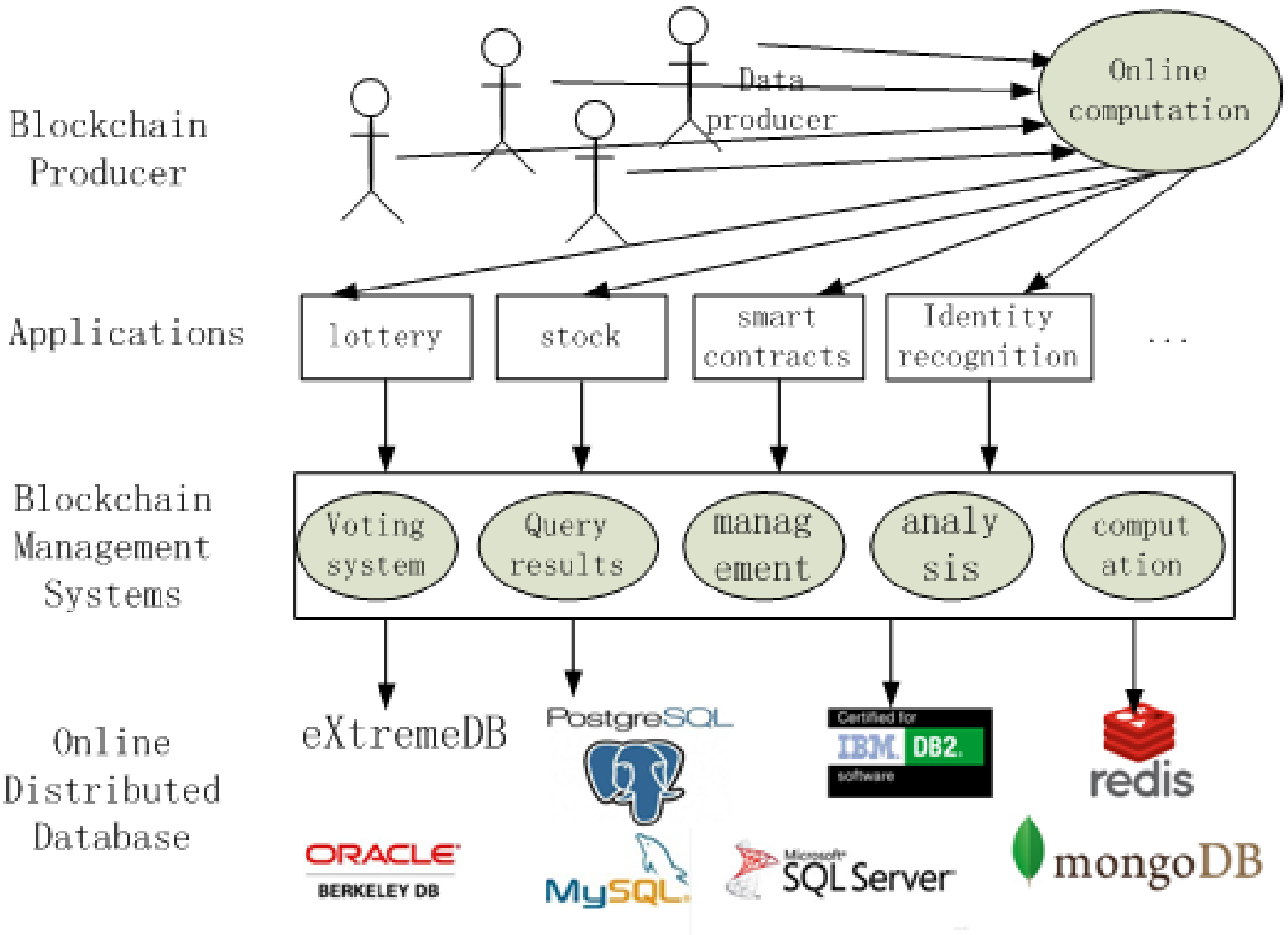
- **There is a strong trust mechanism among them. Servers that do not meet the trust mechanism are isolated. Voting mechanism can solve this. When there is a new block reaching, each cluster server vote, and record the voting information. When the voting results are consistent, it is believed that the blockchain server is trusted. Then accept the block to join. When the voting results are not consistent, the server which has the less votes will be removed from the server cluster. Ensure the credibility of the server.**

Overall Process



- **Step 1: Generate block data**
- **Step 2: Transmit to the nearest blockchain server through the Internet**
- **Step 3: Server broadcast the message in the cluster**
- **Step 4: Server vote using a consensus protocol**
- **Step 5: Calculate the server's trust index**
- **Step 6: Insert the trust index into the blockchain and record related information or delete the server with low trust**
- **Step 7: Wait for the next block**

Framework Design



Timing Analysis

北京航空航天大學 BEIHANGUNIVERSITY

- Generate a block, in the guest networks
- Transfer time in the Internet of a block. It is related with distance , internet speed and so on.
- Process time in the servers, including encryption address generation and so on.
- Broadcast time in the server cluster.
- Voting time of all the servers in the cluster.
- Write in time to the cluster

$$T_{total} = T_{generate} + T_{vote} + T_{calculate}$$

Traffic Analysis

北京航空航天大學 BEIHANGUNIVERSITY

- Under the first structure, the size of each block is *k*, the number of the cluster server is *n*, when the block is broadcast, the assumption is a one-way broadcast, and no longer broadcasts to his server, then the required number of broadcast is *n** (*n*-1) /2, and the total amount of broadcast data is *k***n** (*n*-1) /2.

Traffic Analysis

北京航空航天大學 BEIHANGUNIVERSITY

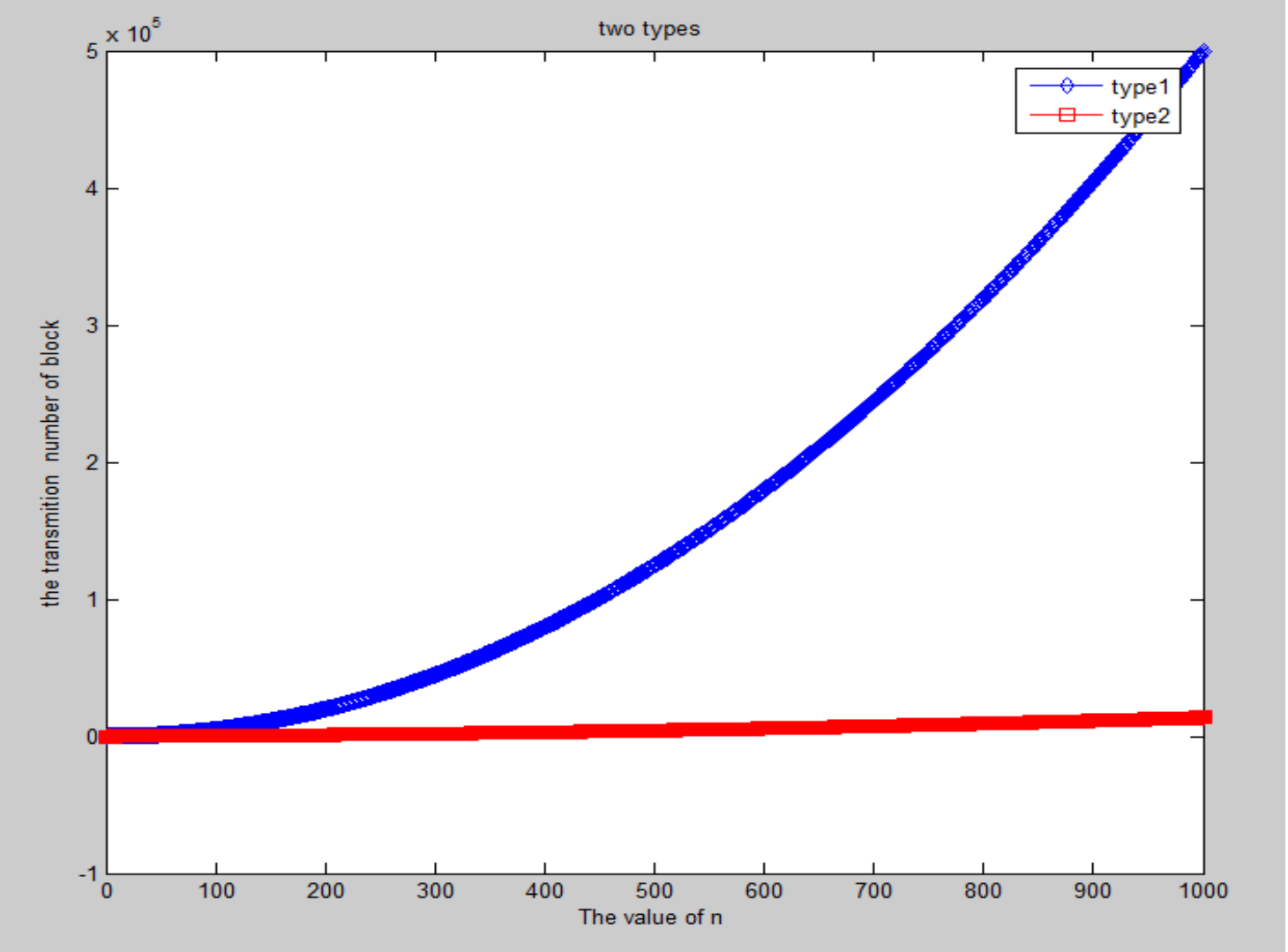
- In the second structure, using the method of clustering, the cluster size is *m*, then the total number of clusters is *n/m*.
- Within the cluster, the number of blocks is $m*(m-1)*\frac{1}{2}$
- The number of inter cluster broadcast is $\frac{n}{m}(\frac{n}{m}-1)*\frac{1}{2}$
- So the total amount of block communication is

$$m*(m-1)*\frac{1}{2}*\frac{n}{m}+\frac{n}{m}(\frac{n}{m}-1)*\frac{1}{2}$$

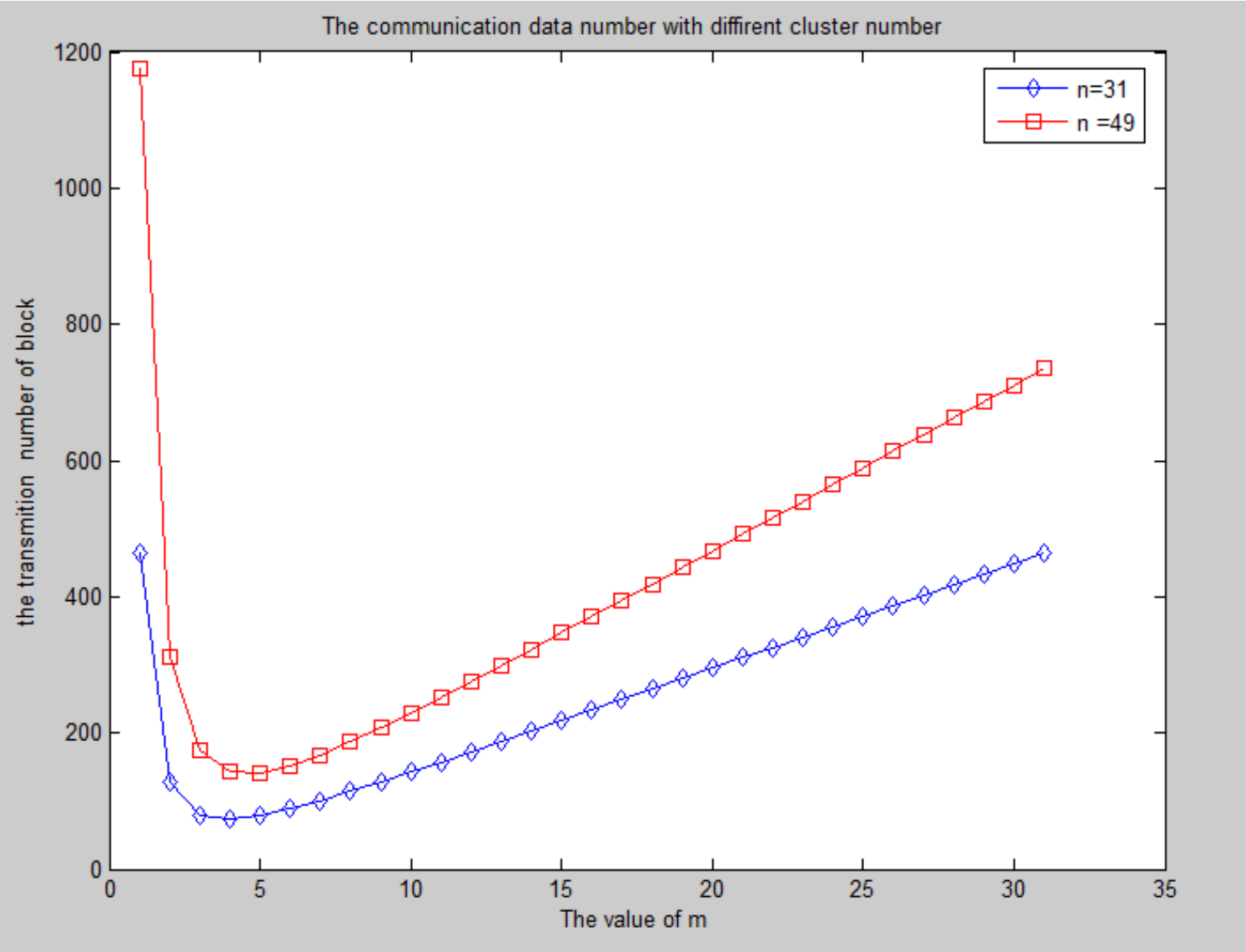
- The total amount of broadcast data is

$$f(m)=\frac{1}{2}*(\frac{n^2}{m^2}-\frac{n}{m}+nm-n)*k$$

Traffic Analysis



Performance Analysis



Conclusion

北京航空航天大學 BEIHANGUNIVERSITY

- **Under *n*=31 and *n*=49 we can find that the best number of a cluster is *m*=4 and *m* =5**

- **With the rapid increase of *n*, the second type can decrease the communication.**

Conclusion

北京航空航天大學 BEIHANGUNIVERSITY

- **This paper analyzes the structure of the blockchain and two kinds of structure of the server deployment. Then summarize the work flow of the blockchain and design the framework. In the end, the paper analyzes the communication volume of two kinds of structures, and proves that the clustering service structure can effectively reduce the amount of communication.**

Future work

北京航空航天大學 BEIHANGUNIVERSITY

- **In the area of the transaction information, when there is a large data storage, such as certificates, pictures, copyright, video and other information, it will cause a great deal of communication in the block server. This is a focus that we research next.**

Thank you!

2015.10.21