Blockchain as an Audit-able Communication Channel

Shigeya Suzuki, Jun Murai

Keio University
Associate Director, Technology Officer, Keio Blockchain Lab

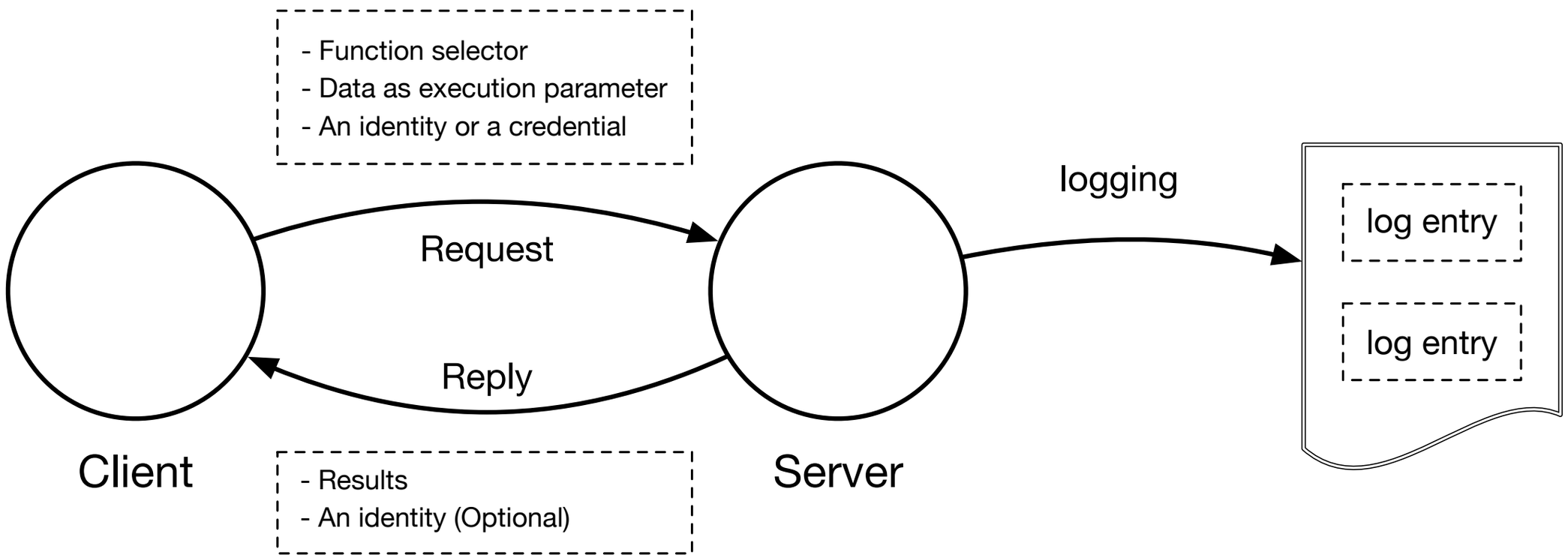
E-mail: shigeya@wide.ad.jp

2018/2/17 @ IRTF DINRG Interim

Outline

- Issues on logging
- Our scheme: Blockchain as a communication channel
- Proof of concept implementation on Bitcoin Blockchain
- Conclusion

Client-Server System and Logging

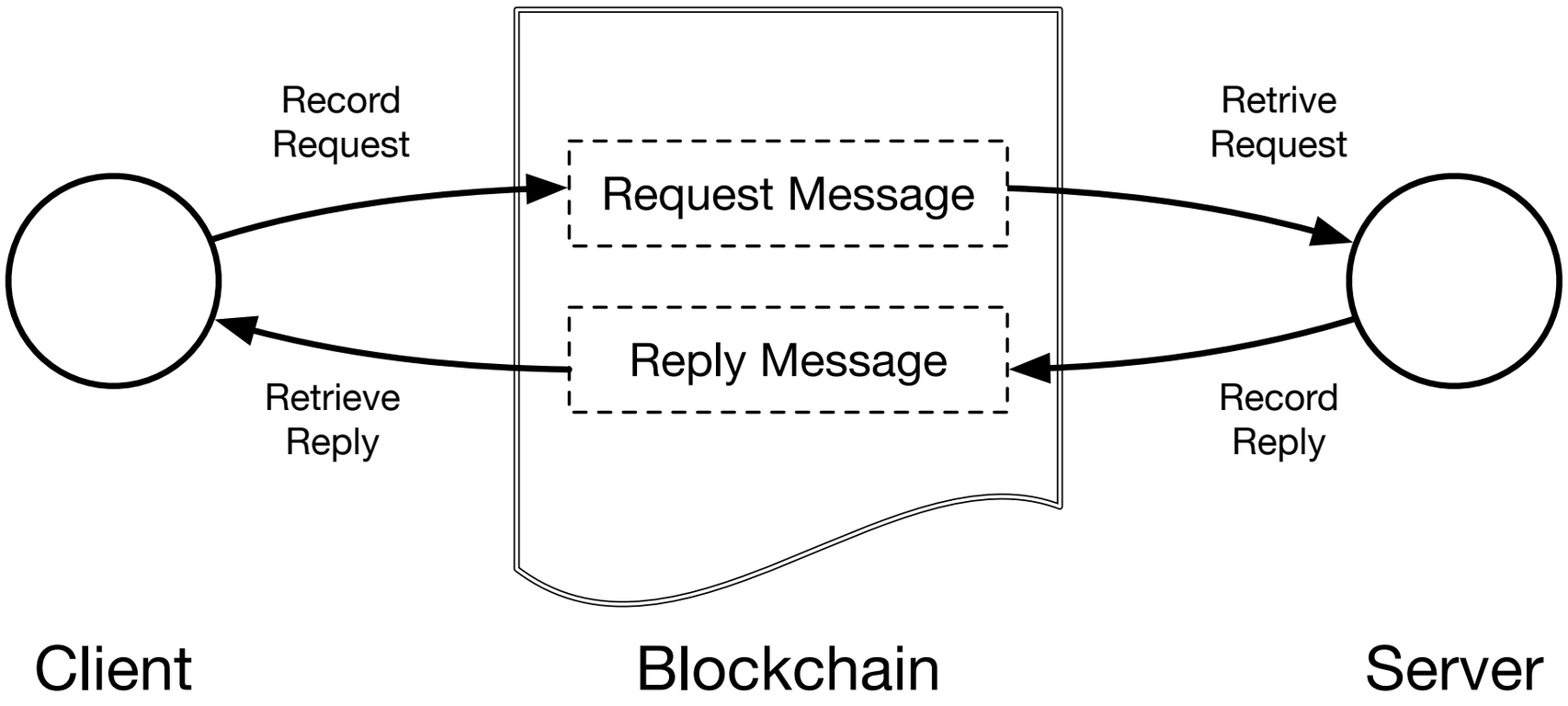


Issues on logging

- Log stored on servers can be tampered / damaged with:
  - Attackers
  - Malicious operators
  - Operational mistake by operators

- Logging server’s general availability problem:
  - Hardware failure

Proposed Scheme:
Blockchain as an audit-able communication channel



Blockchain Requirements for the Proposed Scheme

- Records transactions in chained blocks
  - Sequence of ‘Messages’

- Each transaction may contain extra data area freely used to store the request-reply data
  - Payload in the Messages

- Participating nodes can retrieve the identity of the sender and the receiver of the transaction
  - Source and Destination IDs

- The chain can be accessed by auditors in charge, not necessary, but possibly in public

Applicability of current Blockchain Implementations

- All of three current major Blockchain implementation satisfies the requirements:
  - Bitcoin
  - Ethereum
  - Hyperledger Fabric

Characteristics of Proposed Scheme

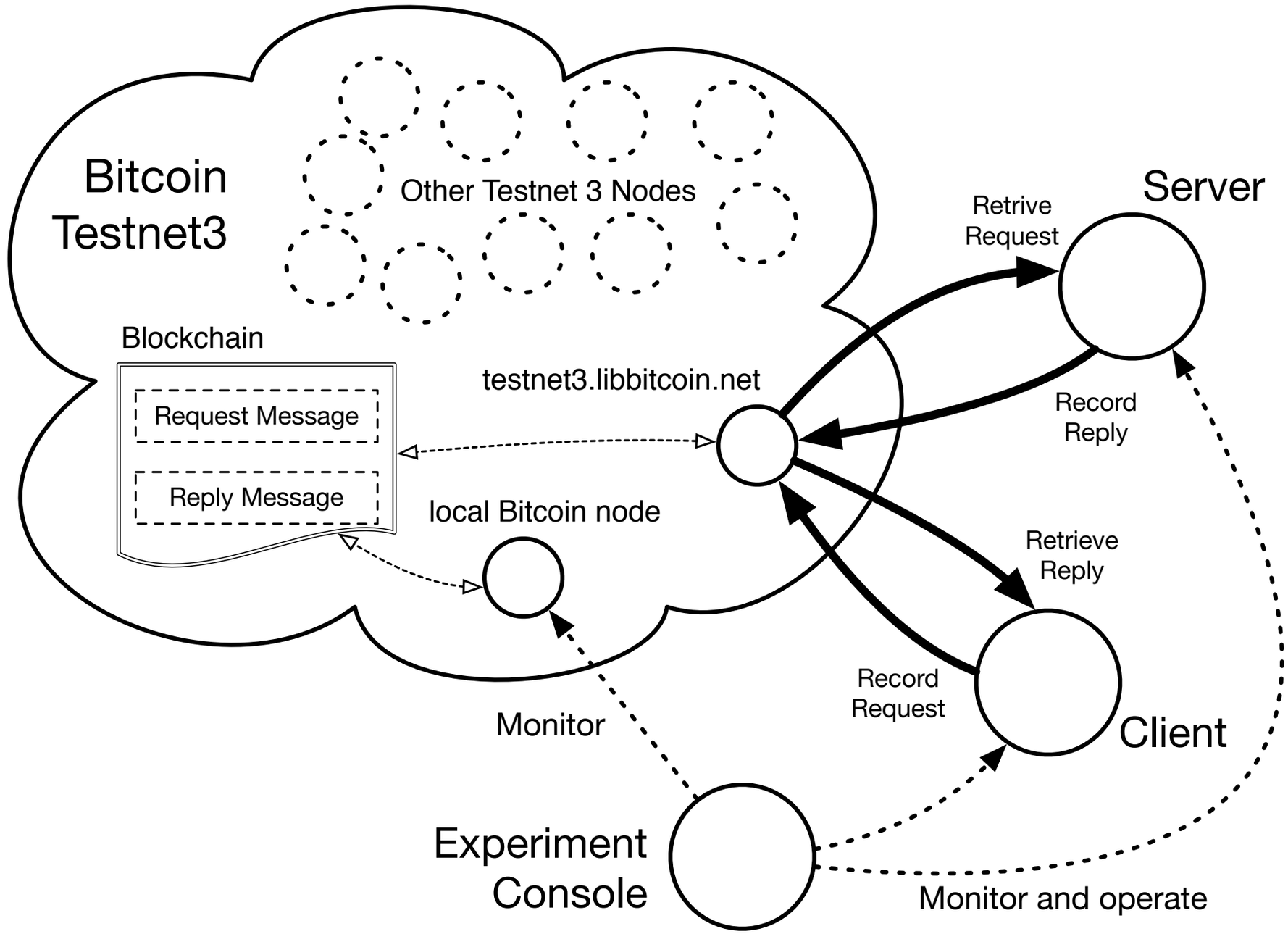
- Highly Available, Modification Resistant and Verifiable Audit
- Lower Visibility of the Node Location on the Network

Proof-of-Concept Implementation

- Implemented on Bitcoin Blockchain
- Experimented with `TestNet3` Bitcoin test network

- Use Bitcoin addresses as node source/destination identifier
- Use Transaction as a message.
  - Transaction’s Payer as the source, Payee as the destination
- Use OP_RETURN script opcode to store payload

Proof of concept experiment



Conclusion

- Proposed to use Blockchain as an audi-table communication channel
- Proof-of-concept using Bitcoin blockchain as basis shown the scheme work as expected
- Two major issues on the scheme: delay and fee
- It is still applicable to a system which has allowance to delay
- To mitigate delay or avoiding fee, suitable blockchain implementation need to be developed
- If these issues resolved, applicability of the system seems good