Tencent

Tencent Cloud Blockchain

Privacy-Preserving Data Sharing on Blockchain via TEE

- A case study on Tencent Cloud Blockchain

Midas (Tencent Billing Platform)

Tencent Cloud Blockchain

ZHANG Tao

Content

Tencent Cloud Blockchain

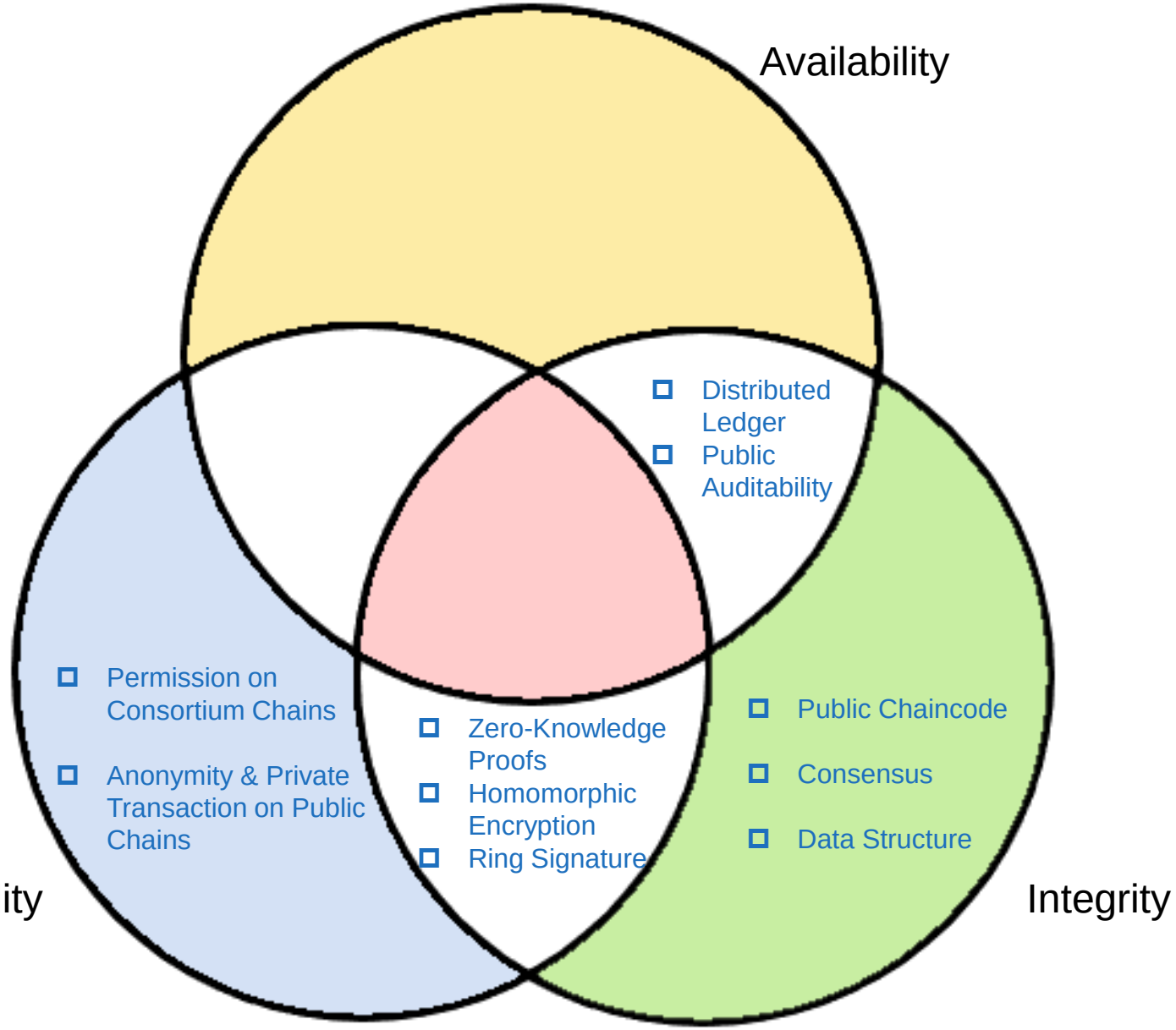
- Blockchain & its privacy issues
- Trusted execution environment (TEE)
- TEE-enhanced Blockchain
  - Design of Shuliantong, a TEE-enhanced blockchain platform provided by Tencent Cloud
- Application Scenarios for Shuliantong

ITU-T SG17 passed “Security Requirements for Smart Contract Management”, X.srscm-dlt

Blockchain & Its Security

Tencent Cloud Blockchain

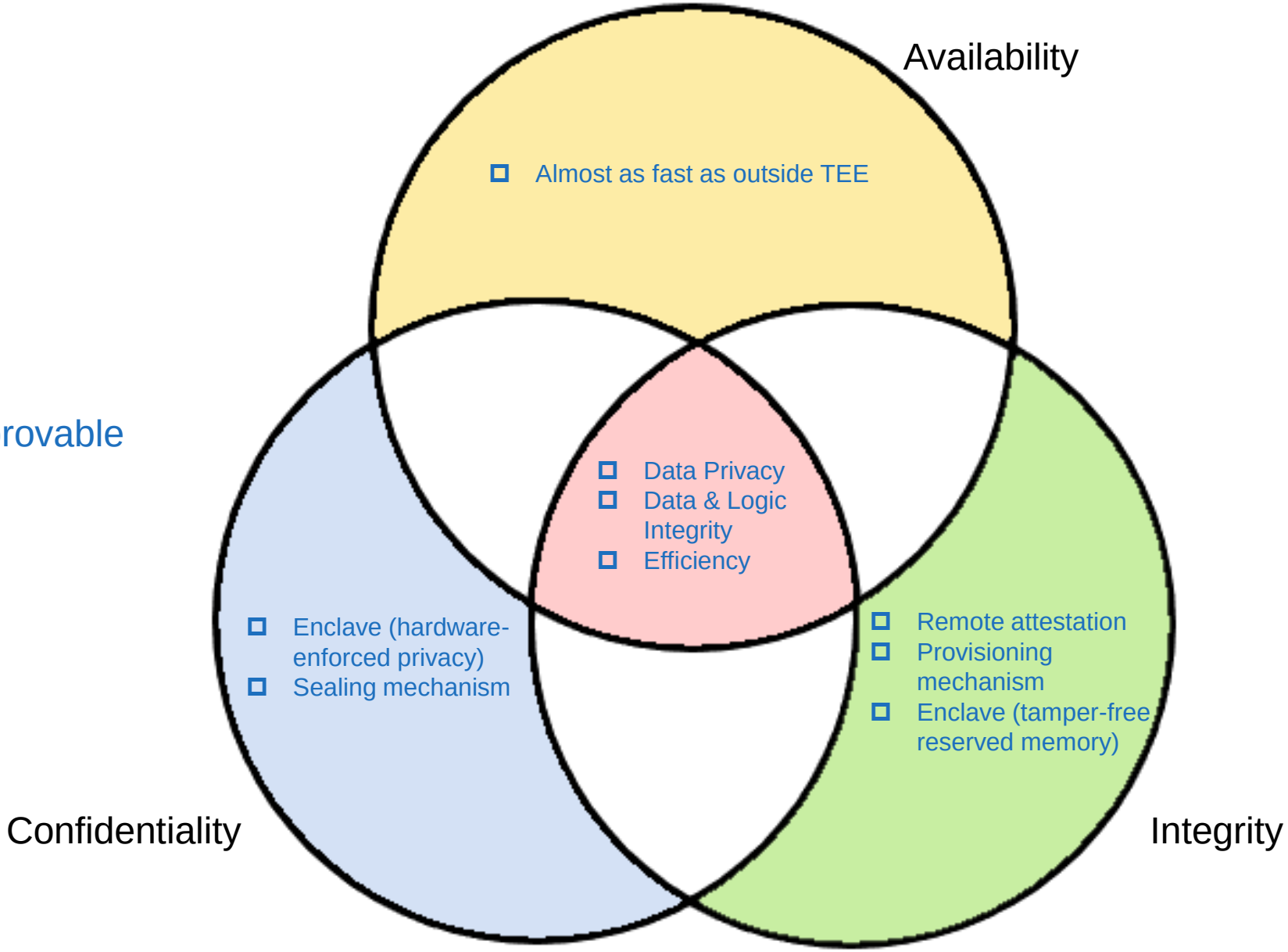
- Minimum Data Privacy
  - Data on the chain is public to chain participants
- Data & Logic Integrity
  - Chaincodes are public
  - Consensus
  - Blockchain data structure
- Efficiency
  - Crypto algorithms are resource-consuming



TEE (SGX) for Privacy and Integrity

Tencent Cloud Blockchain

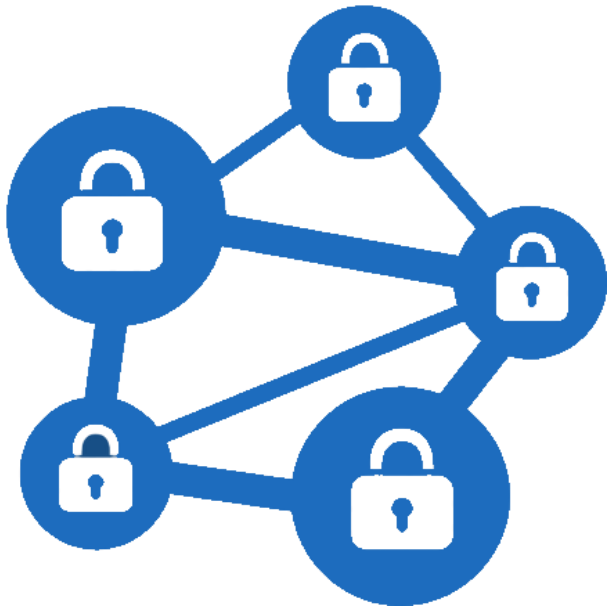
- Data Privacy
- Data & Logic Integrity
- Efficiency
- Hardware-enforced & Not provable



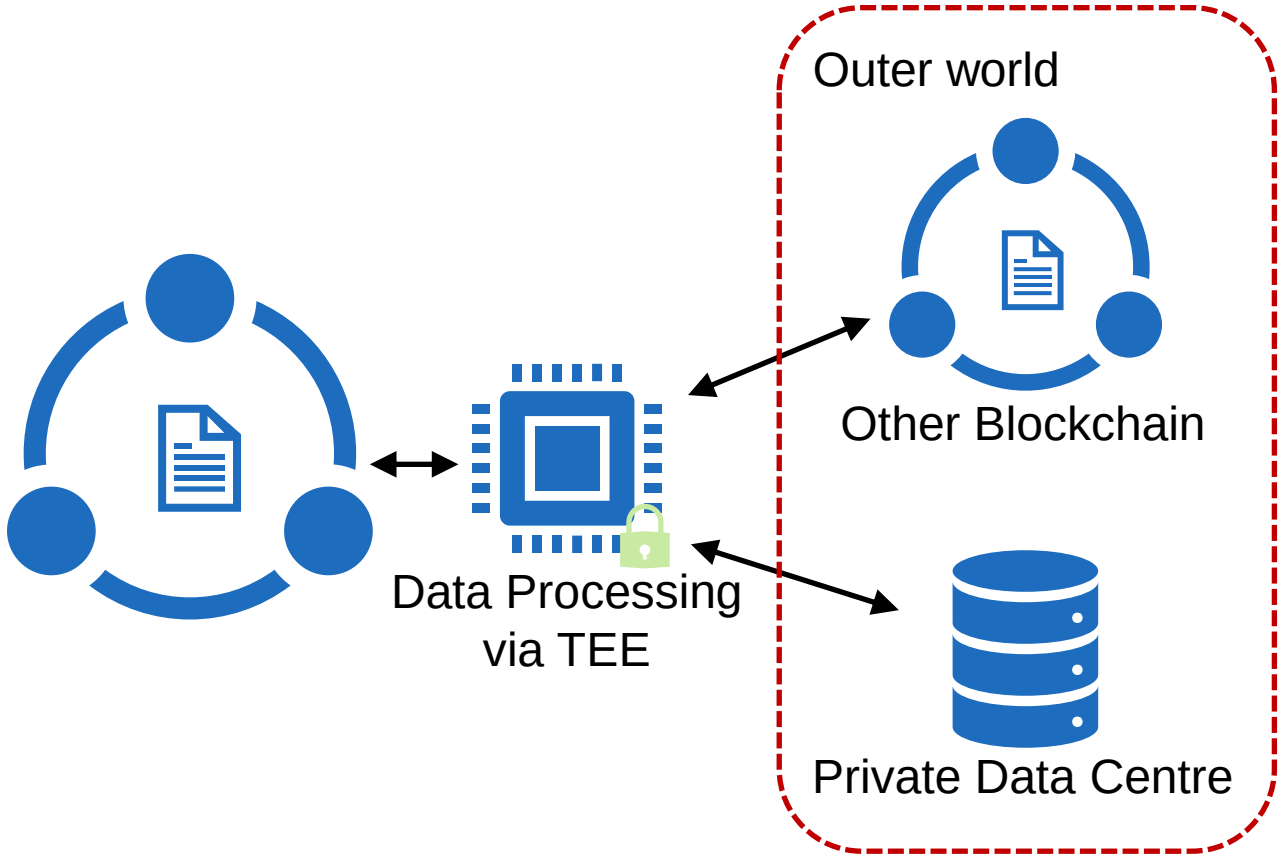
TEE-Enhanced Blockchain

Tencent Cloud Blockchain

- Execute chaincode with TEE
  - Data is confidential
  - Processing procedure is publicly auditable

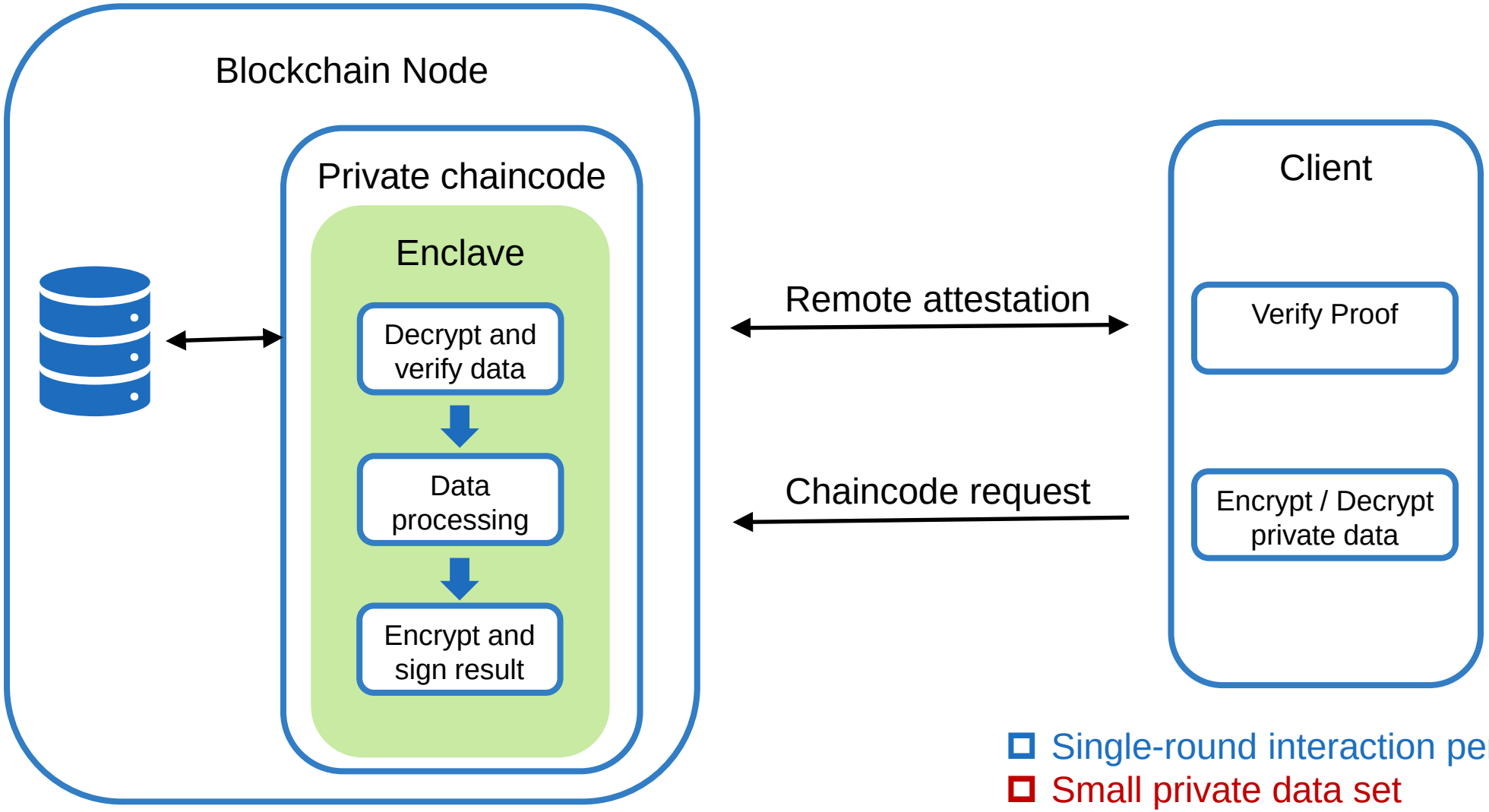


- Process private data from outer world



TEE-enhanced Chaincode

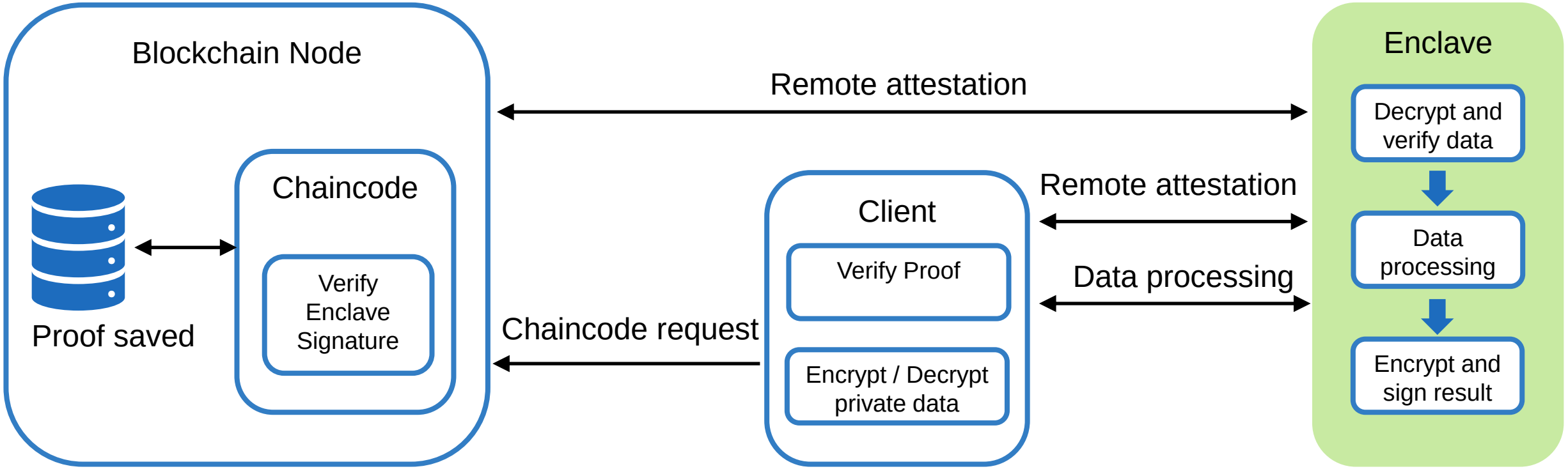
Tencent Cloud Blockchain



- Single-round interaction per task
- Small private data set
- Deterministic algorithm in TEE (Consensus-compatibility)

TEE as an Off-chain Service

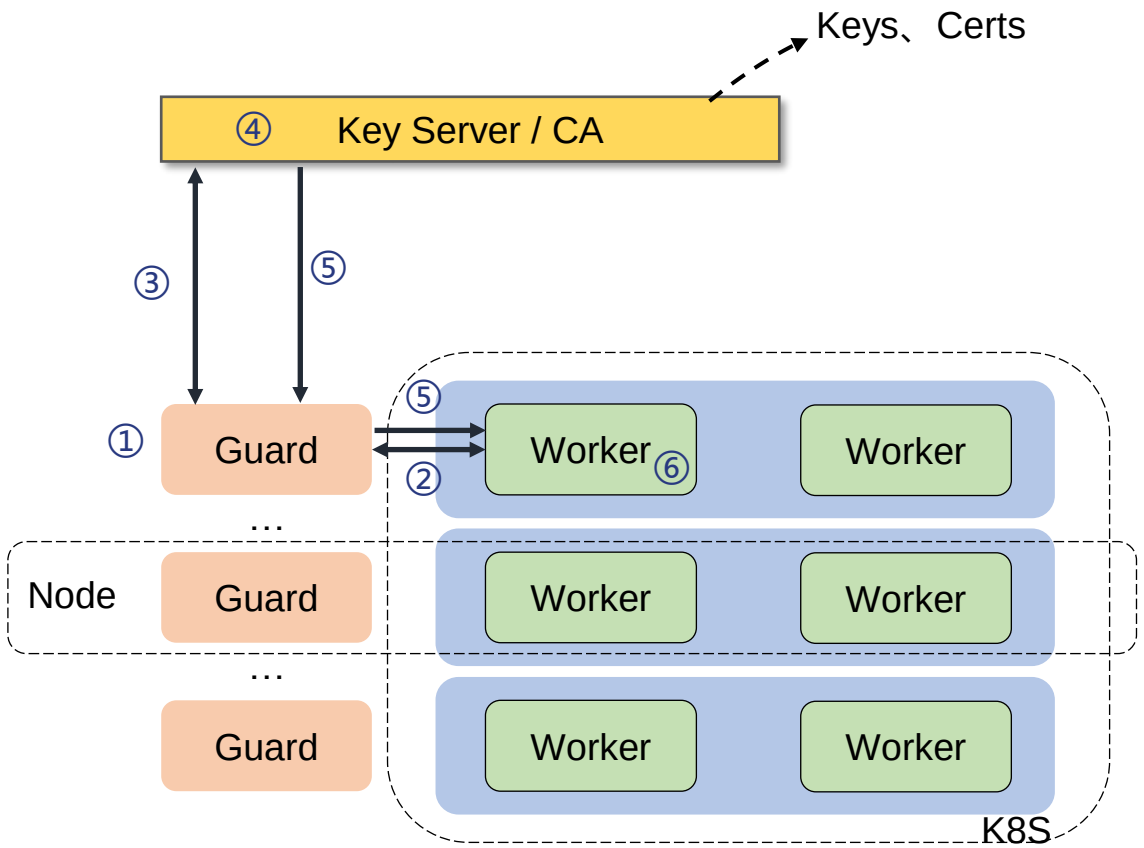
Tencent Cloud Blockchain



- Large private data set
- Randomized algorithm in TEE
- Multiple-round interactions per task

TEE Cluster

Tencent Cloud Blockchain



P.S. Key Server, Guards, and Workers are all SGX Enclaves

① Each node has a Guard enclave deployed.

② Guard and local Workers conduct local attestation. Worker sends its CSR to Guard.

③ Guard signs CSR, conducts bidirectional remote attestation with Key Server, and sends the signed CSR to Key Server.

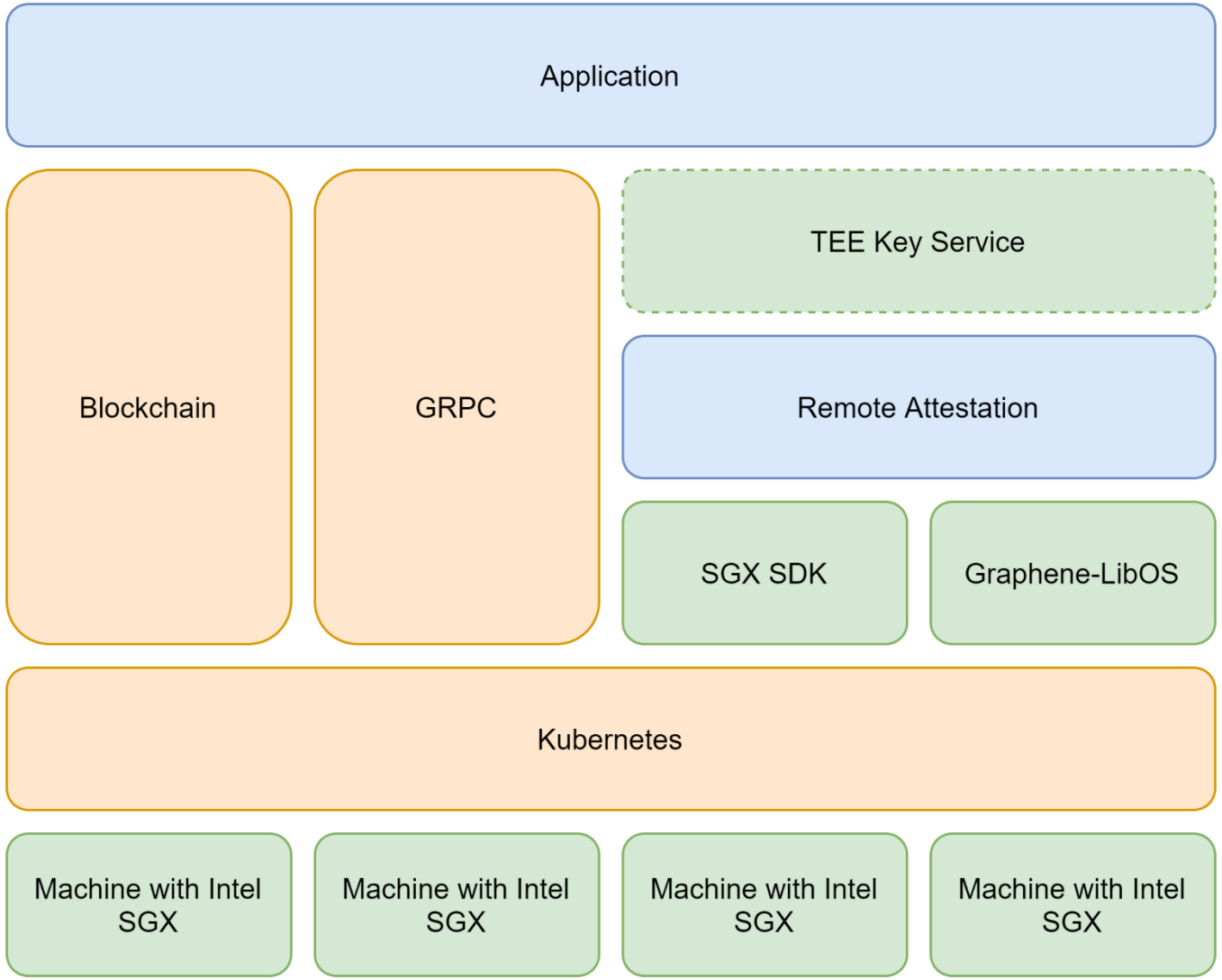
④ Key Server verifies Guard's signature, and issues a certificate on CSR.

⑤ Key Server returns certificate and encryption / decryption key to Guard. Guard forwards these to Worker

⑥ Worker can manage application data with the key received from Key Server, and use its own Seal Key to manage this key.

Structure Diagram of Shuliantong

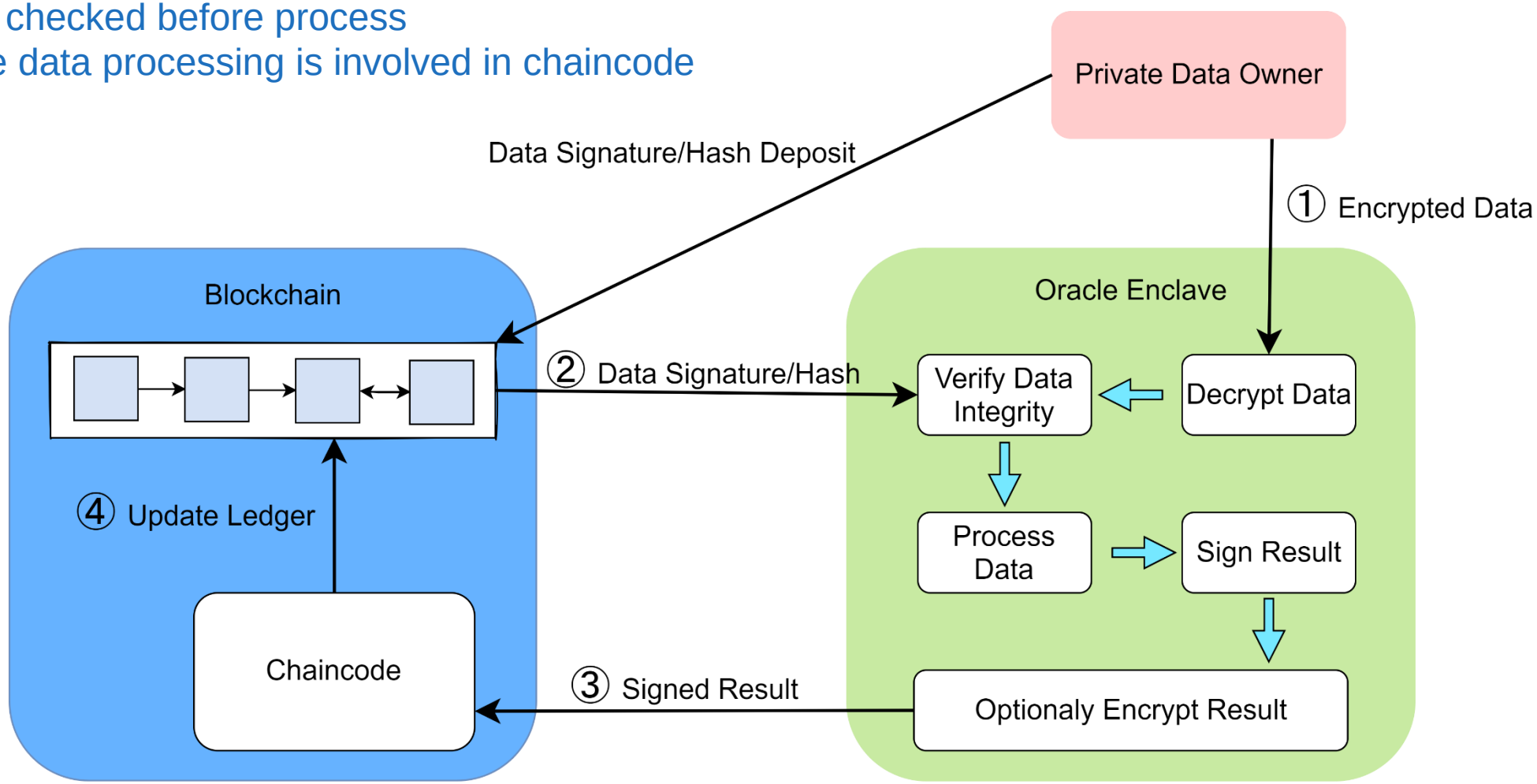
Tencent Cloud Blockchain



TEE as Oracle for Blockchain

Tencent Cloud Blockchain

- Store sensitive data off-chain privately
- Deposit data signature/hash into the ledger when data is generated of updated
- Data integrity is checked before process
- Result of private data processing is involved in chaincode



Cross-Chain Interoperation

Tencent Cloud Blockchain

1. Client send cross-chain request to Chain 1

2~4. Gateway send chaincode invocation request, subscribe events for this request

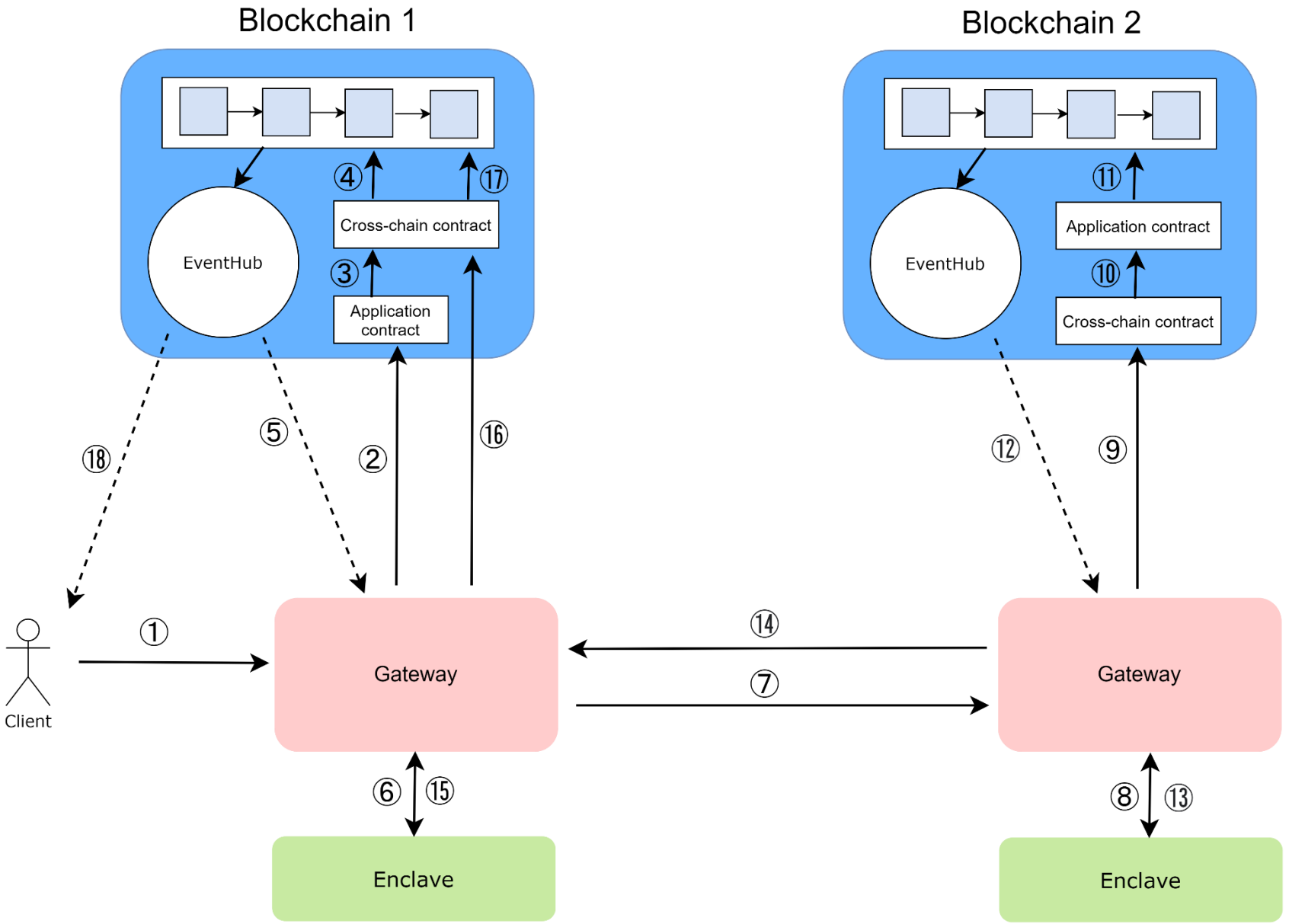
5. Gateway gets notification for completion of chaincode

6~8. Enclave verify the notification, and sends a corresponding request to Chain 2

9~11. Same as 2~4

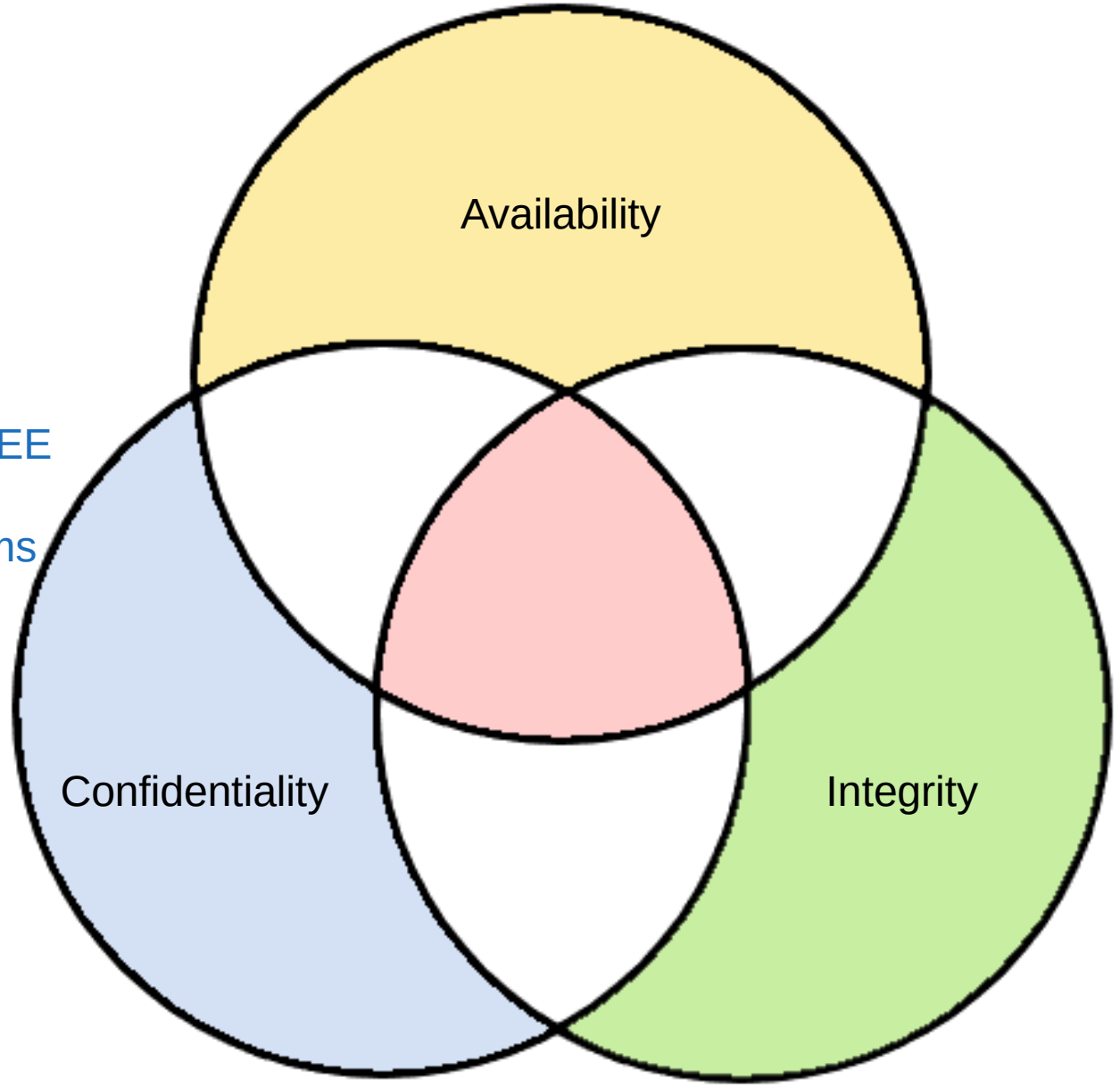
12~15. Same as 6~8

16~18. Finalize the state of cross-chain operation, and notify Client



Summary

- Balanced
  - Confidentiality:
    - Reserved memory by TEE
  - Integrity:
    - Blockchain mechanism
    - Tamper-free environment by TEE
  - Availability:
    - Avoid complex crypto algorithms



Tencent

Tencent Cloud
Blockchain

Thank you!