Blockchain-based cross-domain IIoT identity authentication

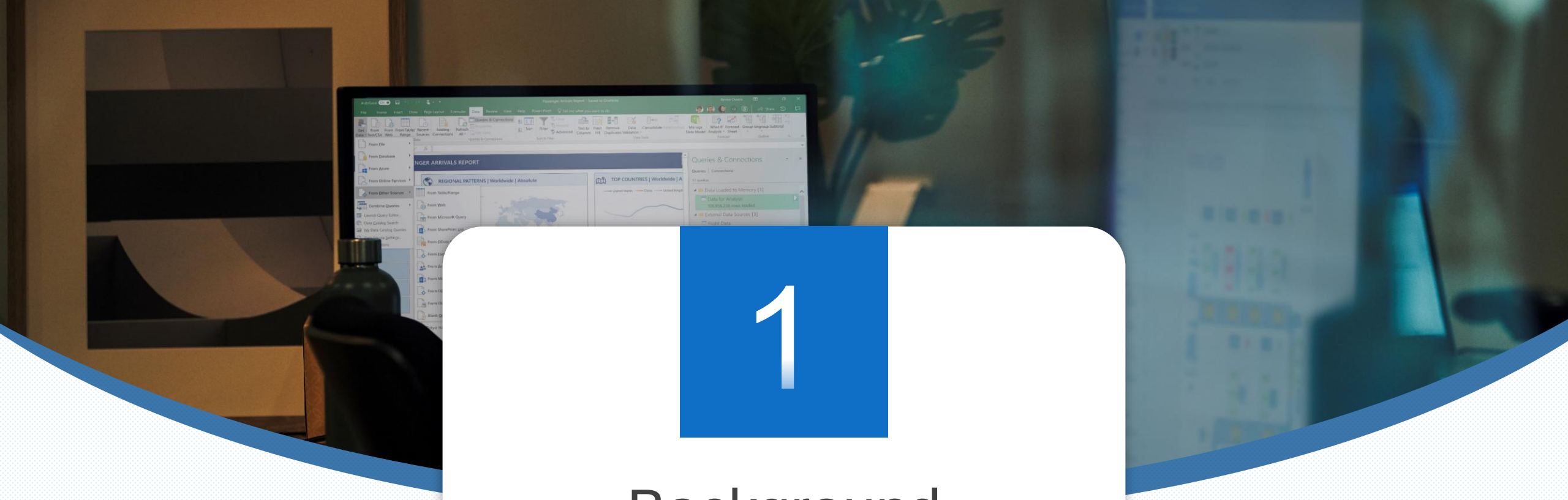
Rui Tian, Ph.D.

Director of Research

Chaincomp Technologies Co., Ltd (中科物缘)

rui.tian@chaincomp.net

CONTENT

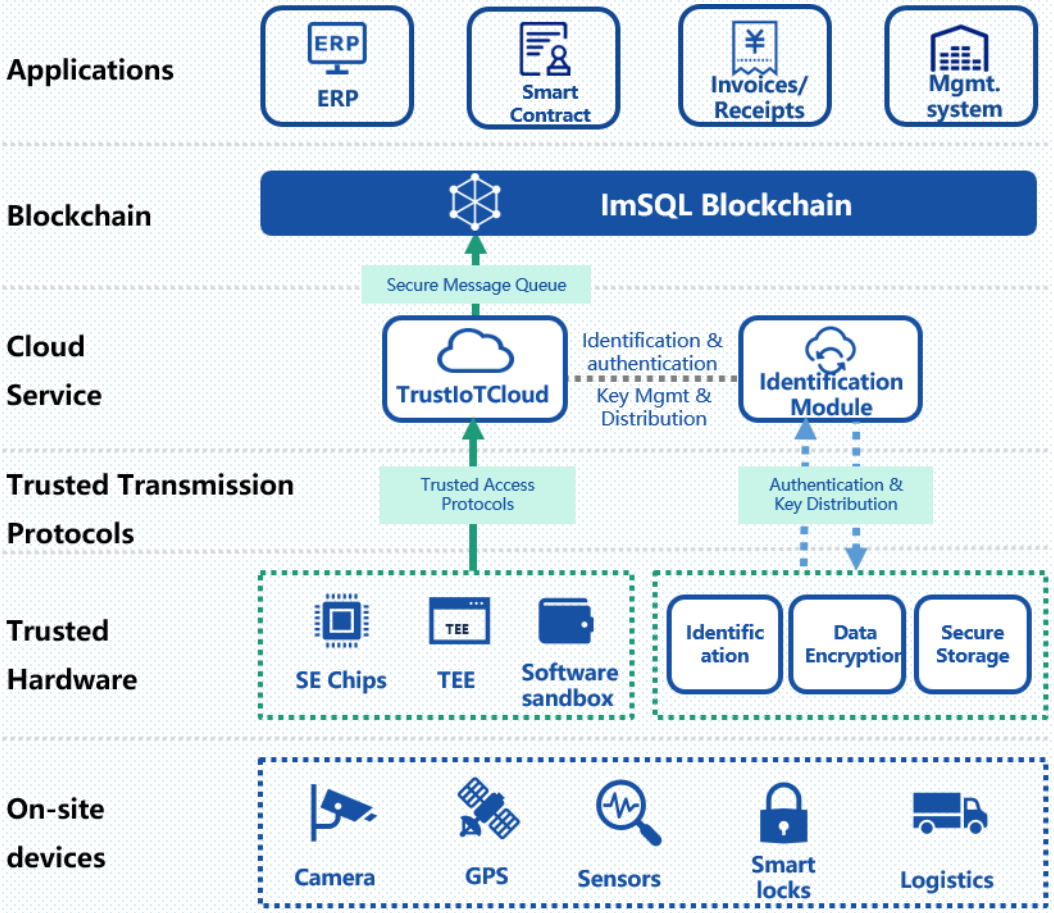


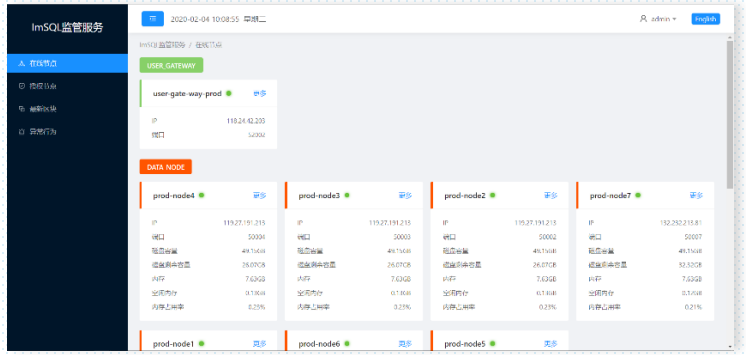
1

Background

Chaincomp - Blockchain of IoT Architecture

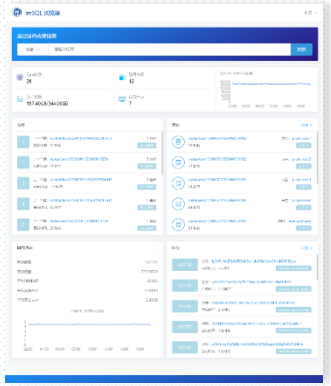
ImSQL™ Storage Blockchain, EdgeTrust™ and TrustIoTCloud™ for Trusted IoT Management





ImSQL Mgmt End

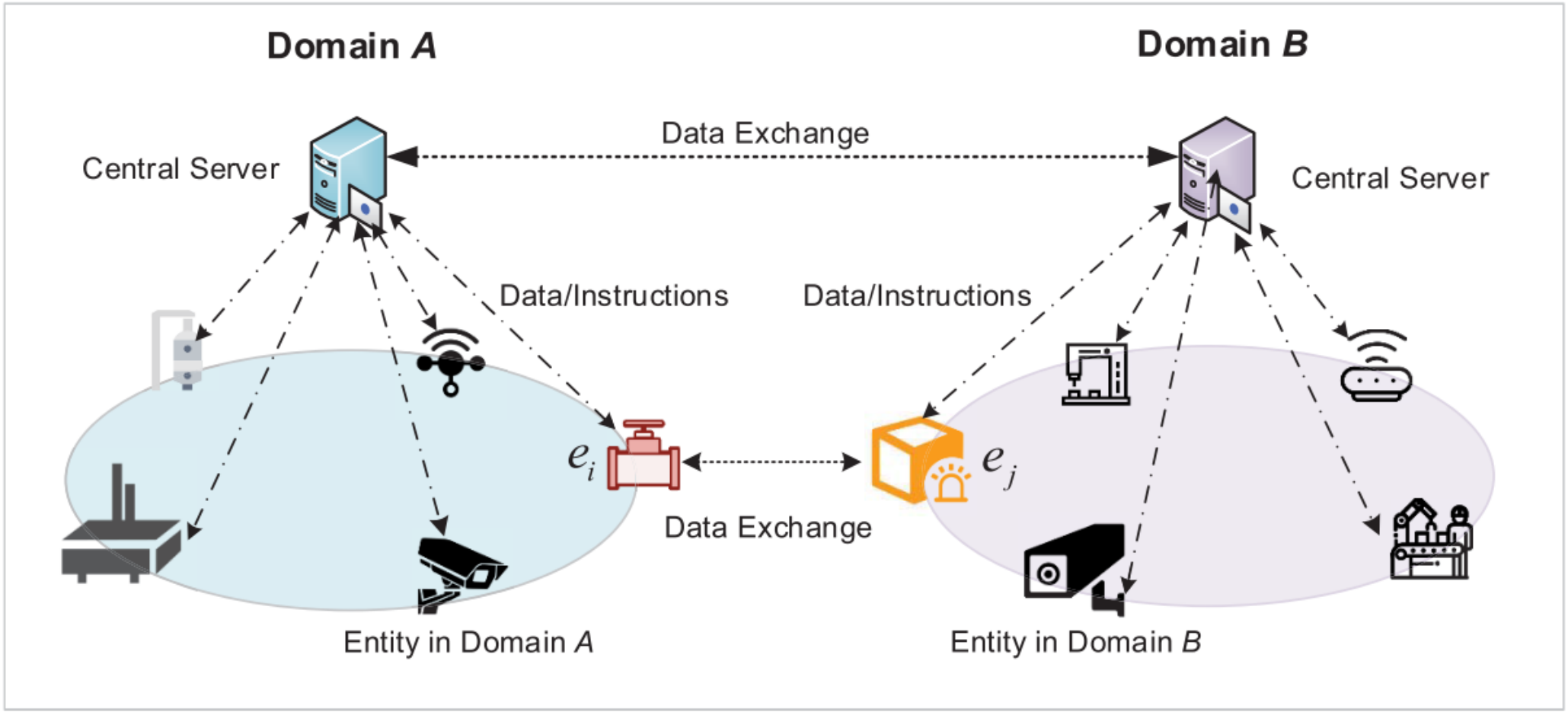
Trusted IoT Module



ImSQL Exploerer

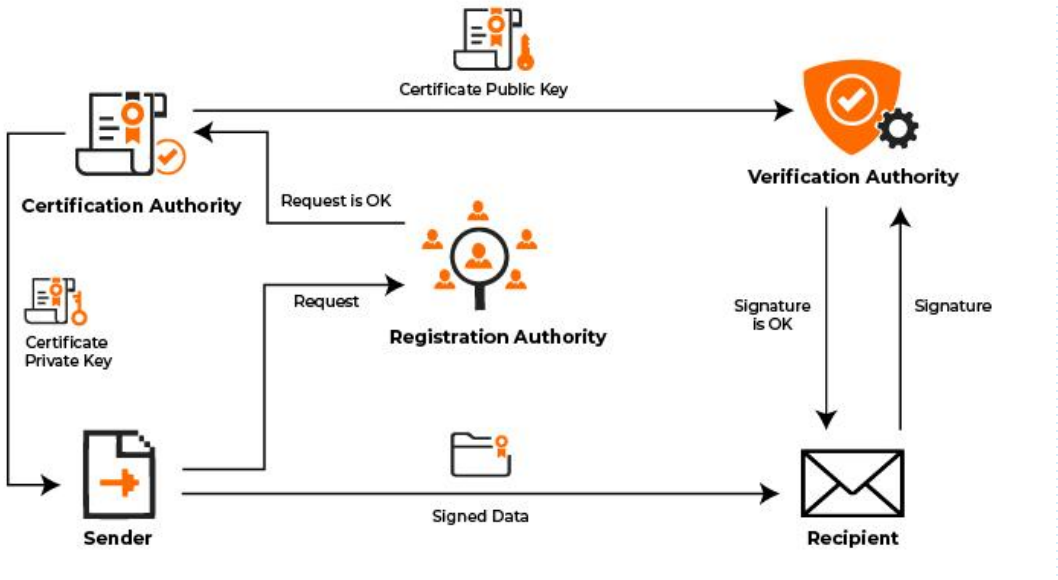
Background – Industrial IoT Application

Cross-domain identity authentication



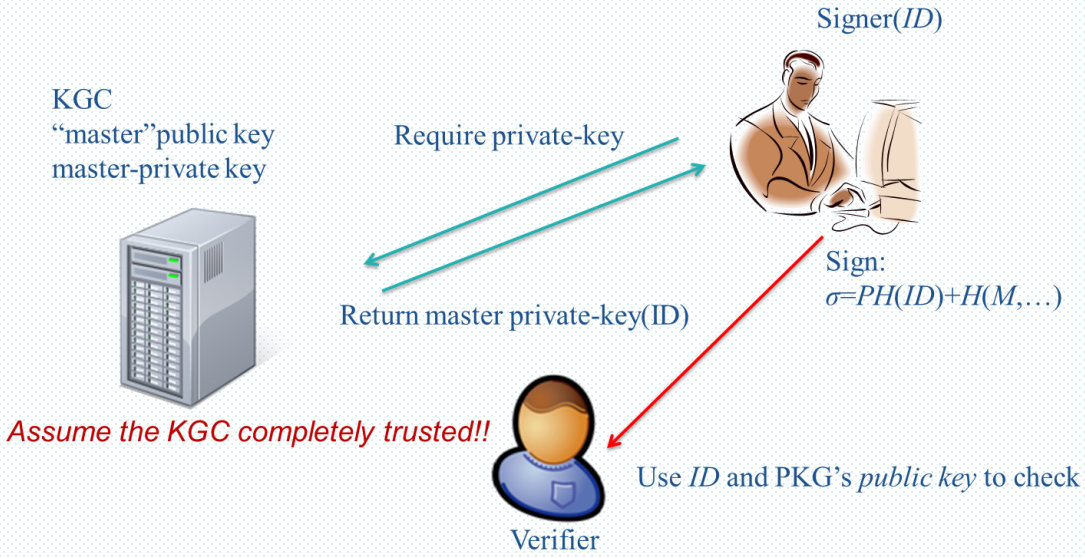
Background – Public Key Systems

PKI (Public Key Infrastructure)



- Bandwidth Overhead
- Verification Time Overhead
- Storage Space
- Energy Consumption
- Centralized CA attacks

ID PKC （Identity-based public key cryptography）



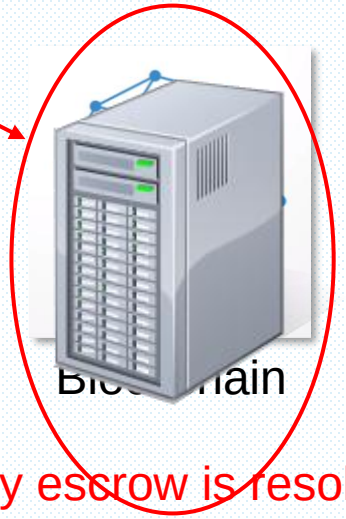
- ~~Bandwidth Overhead~~
- Verification Time Overhead
- ~~Storage Space~~
- Energy Consumption
- Centralized CA attacks

Background – Public Key Systems (Cont.)

CL-PKC(Certificateless public key cryptography)

KGC
master public key=*mpk*
partial-private-key

Trusted Third Party



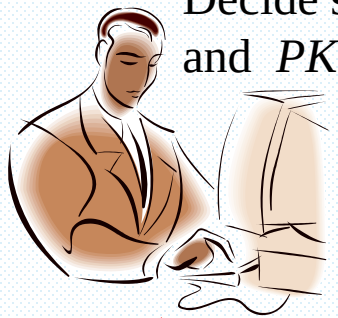
Bl[illegible]hain

the key escrow is resolved!!

Require partial-private-key

Return partial-private-key(ID)

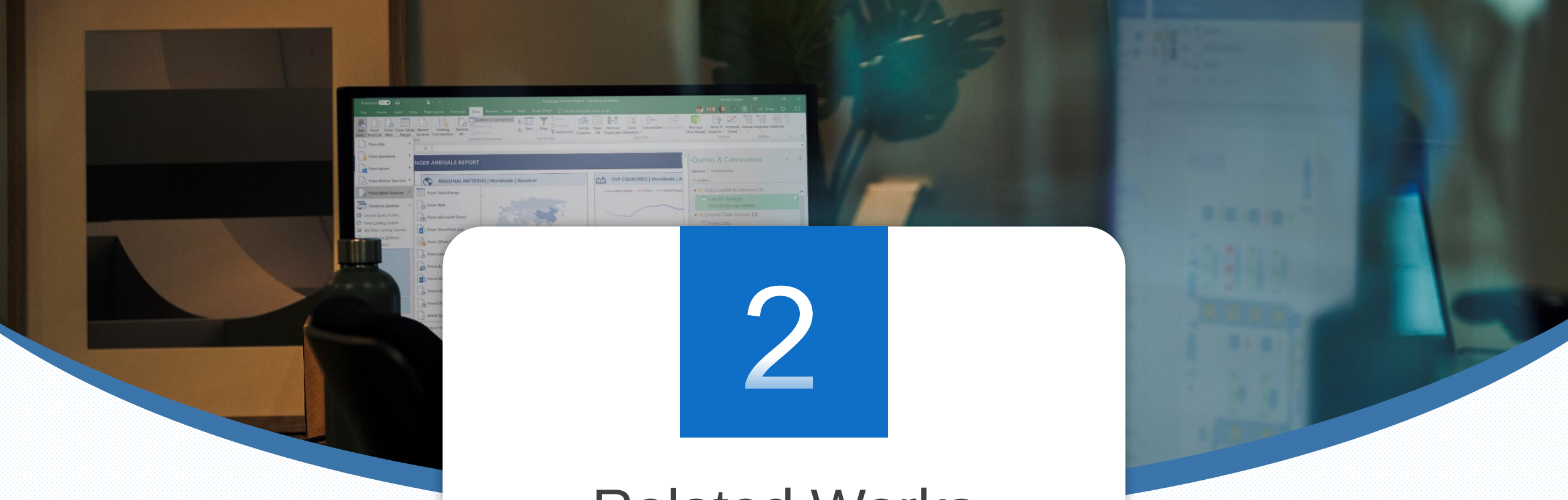
Signer(*ID*)
Decide secret value x_{ID}
and *PK*(use x_{ID})



Sign:
$\sigma = PH(ID) + x_{ID}\, H(M,\ldots)$

Verifier

Use *ID*,correspounding *PK*
and PKG's *mpk* to verify

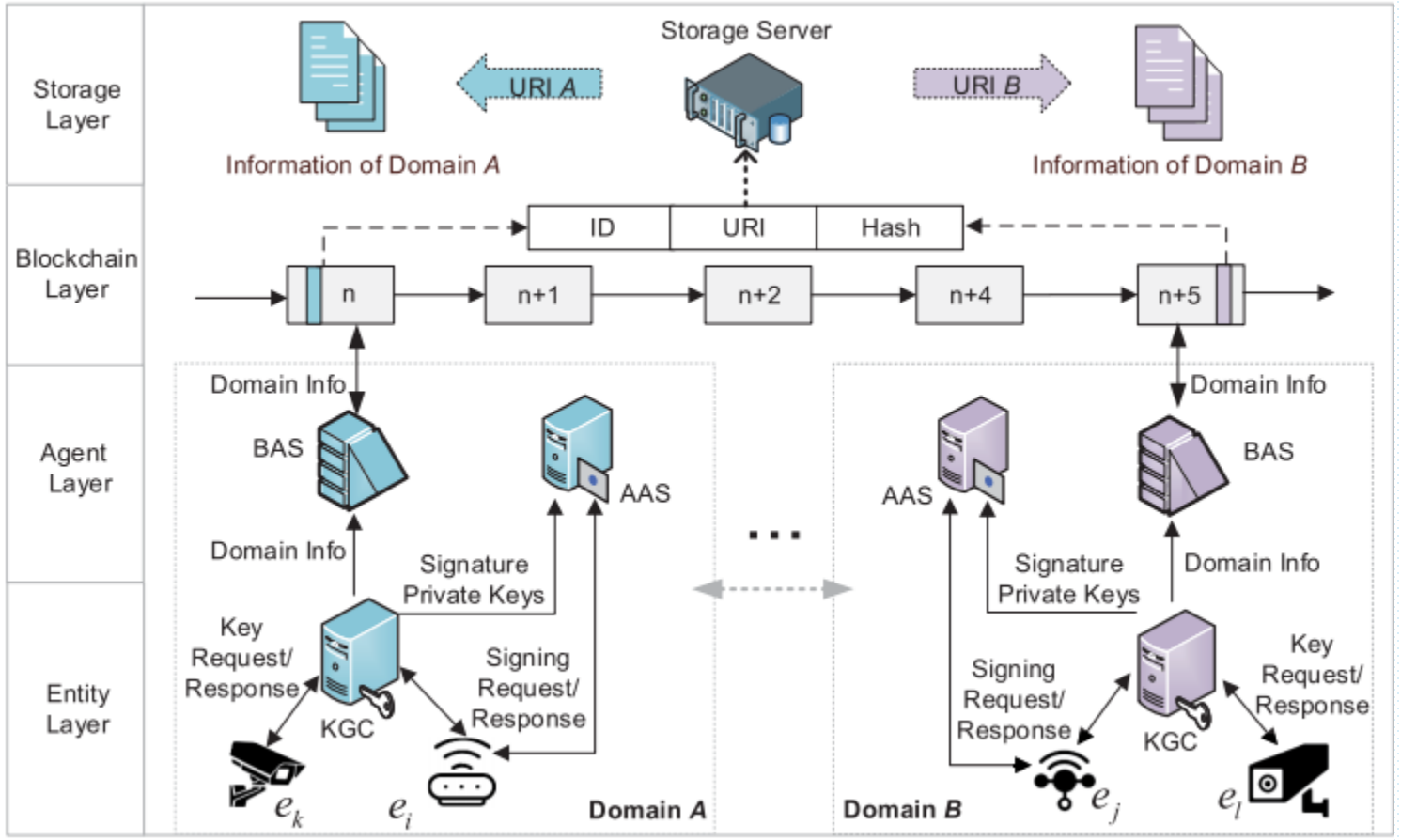


2

Related Works

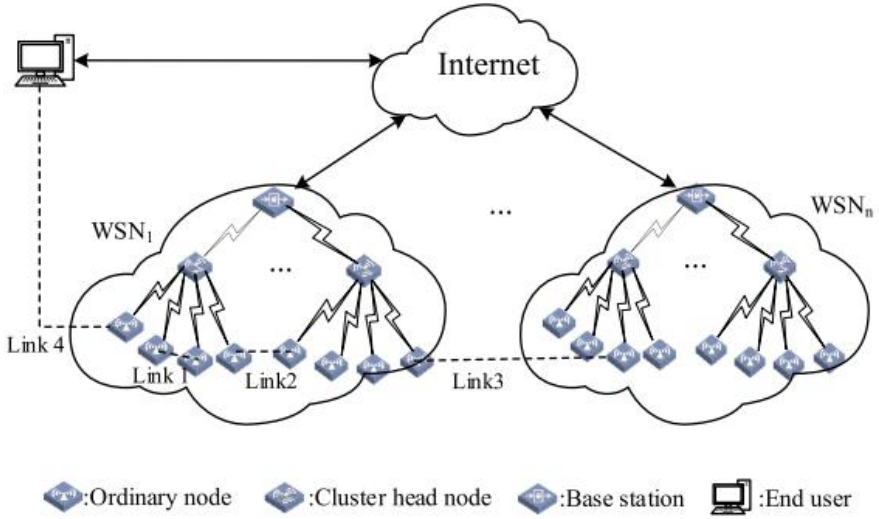
Related Work

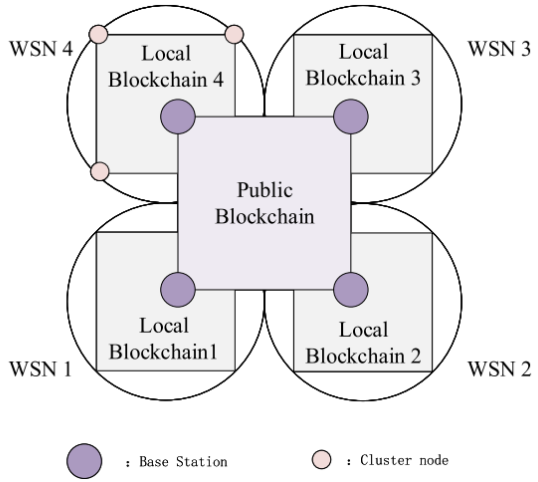
M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchainassisted secure device authentication for cross-domain industrial iot," IEEE Journal on Selected Areas in Communications, vol. 38, no. 5, pp. 942–954, 2020.

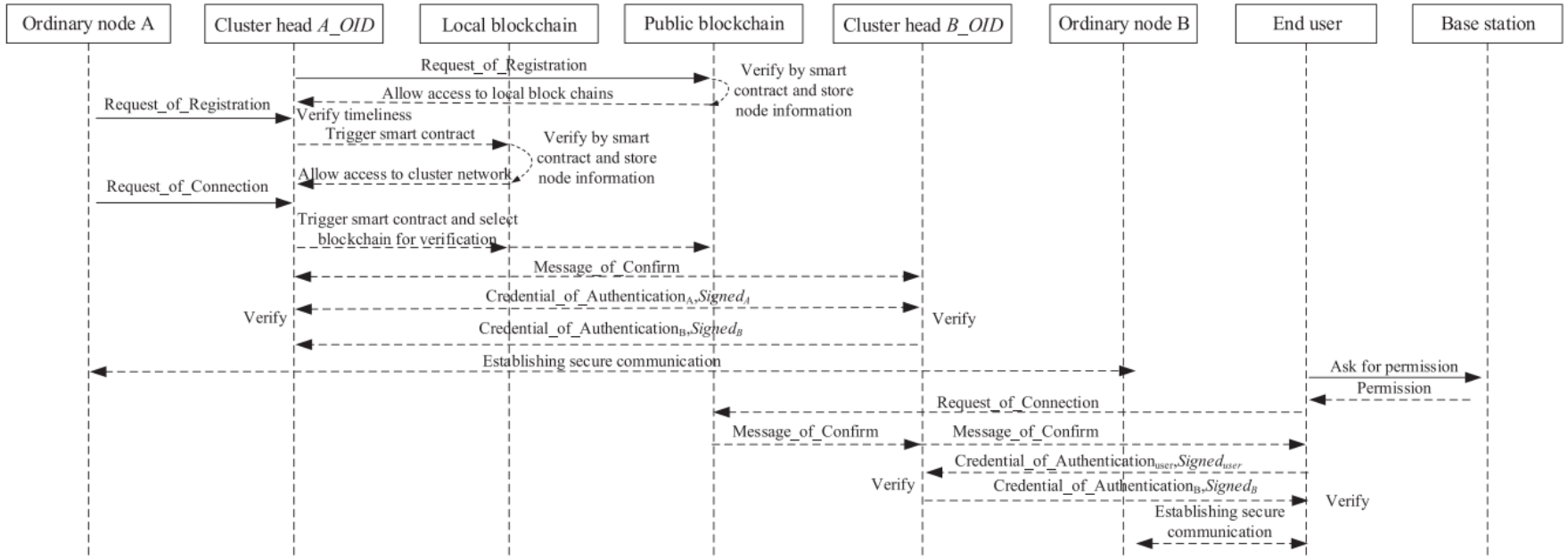


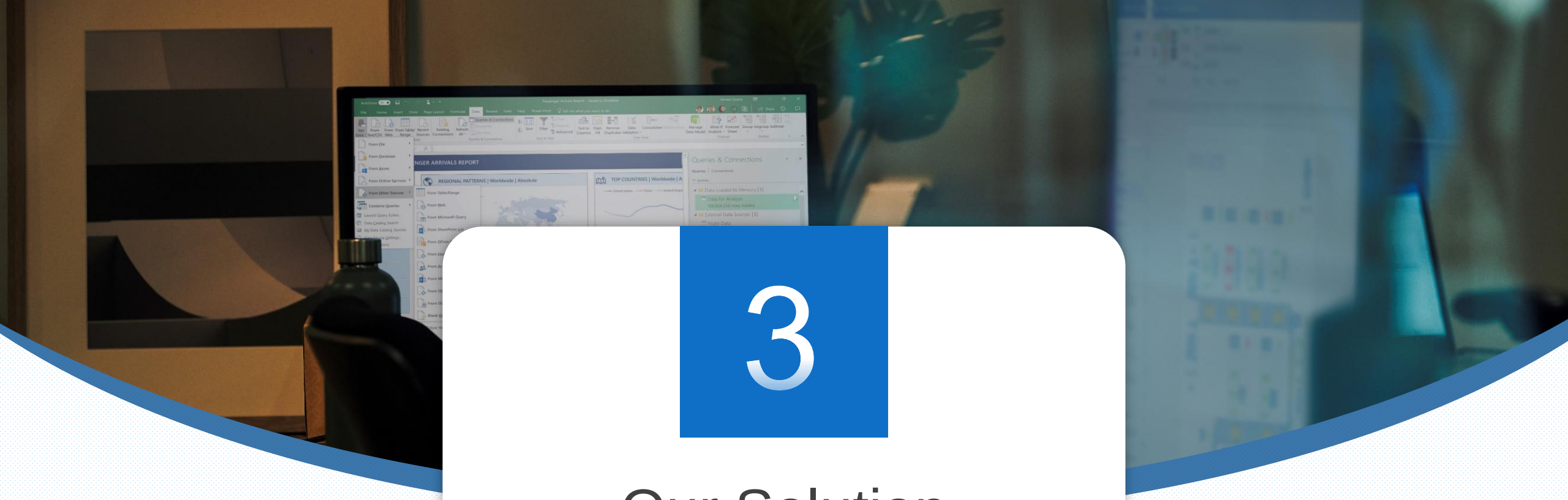
Related Work (Cont.)

Z. Cui, X. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-wsn," IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 241–251, 2020.







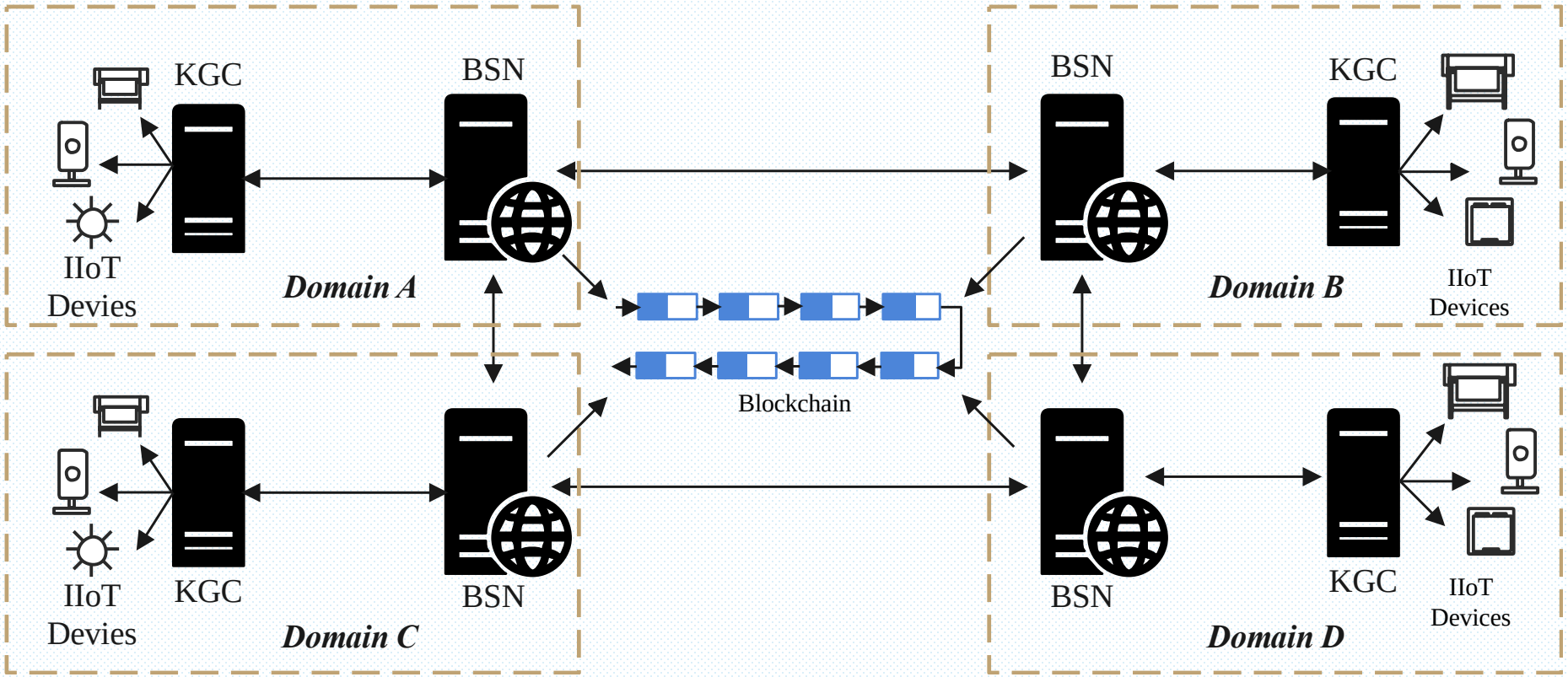


3

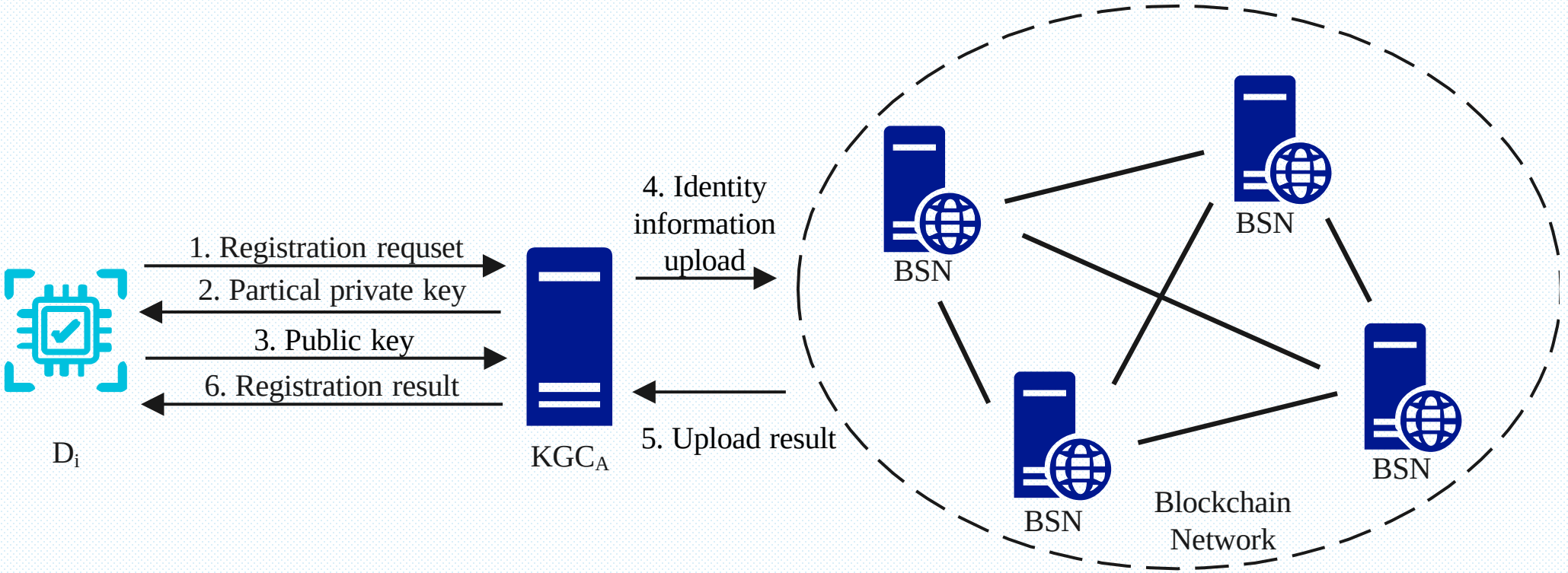
Our Solution

Blockchain-based IIoT Identity Authentication

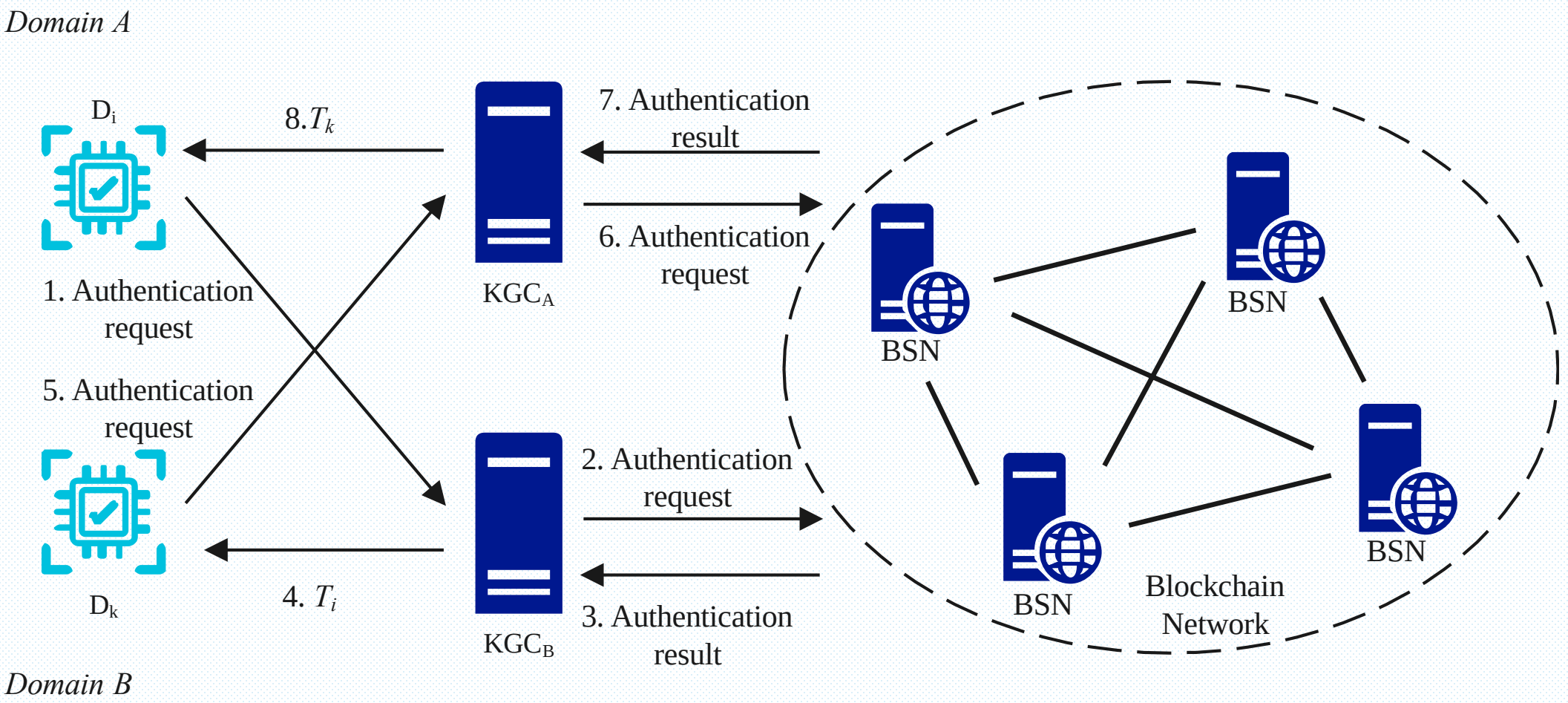
Architecture

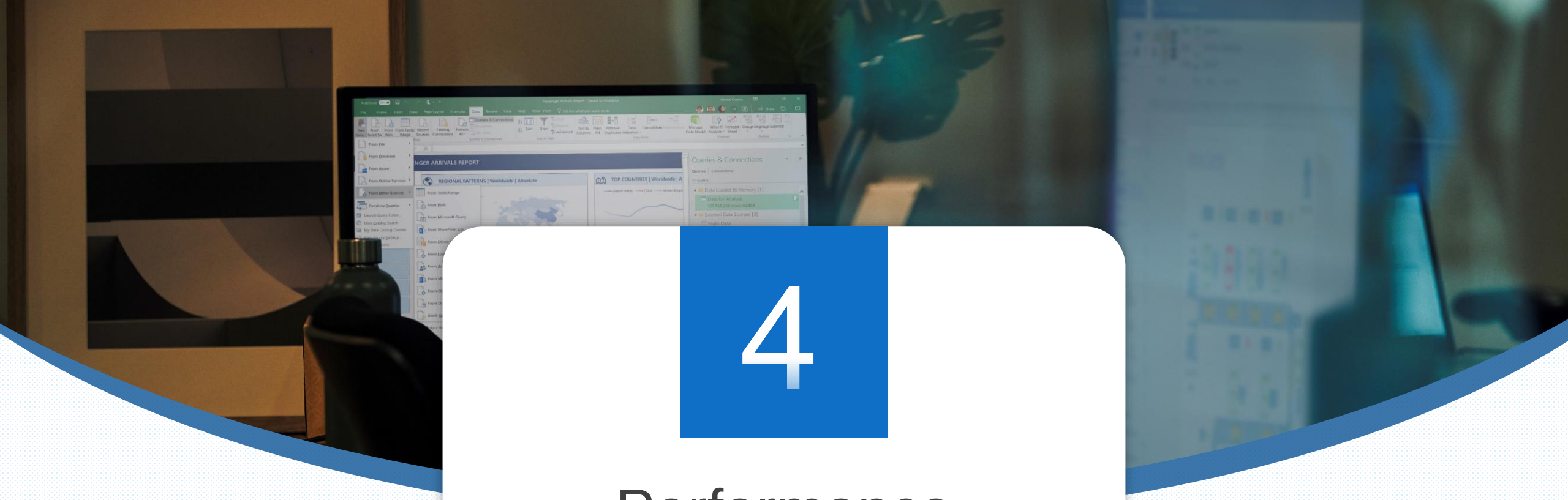


Initialization and Registration Process



Identity Authentication Process



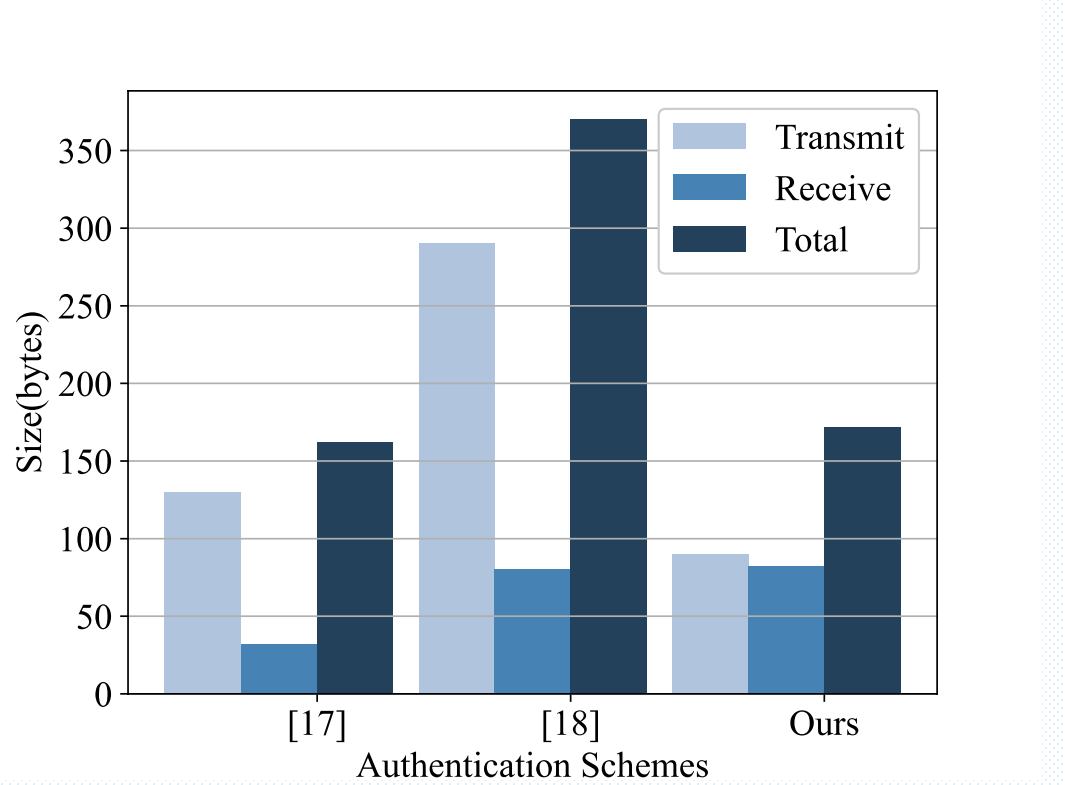


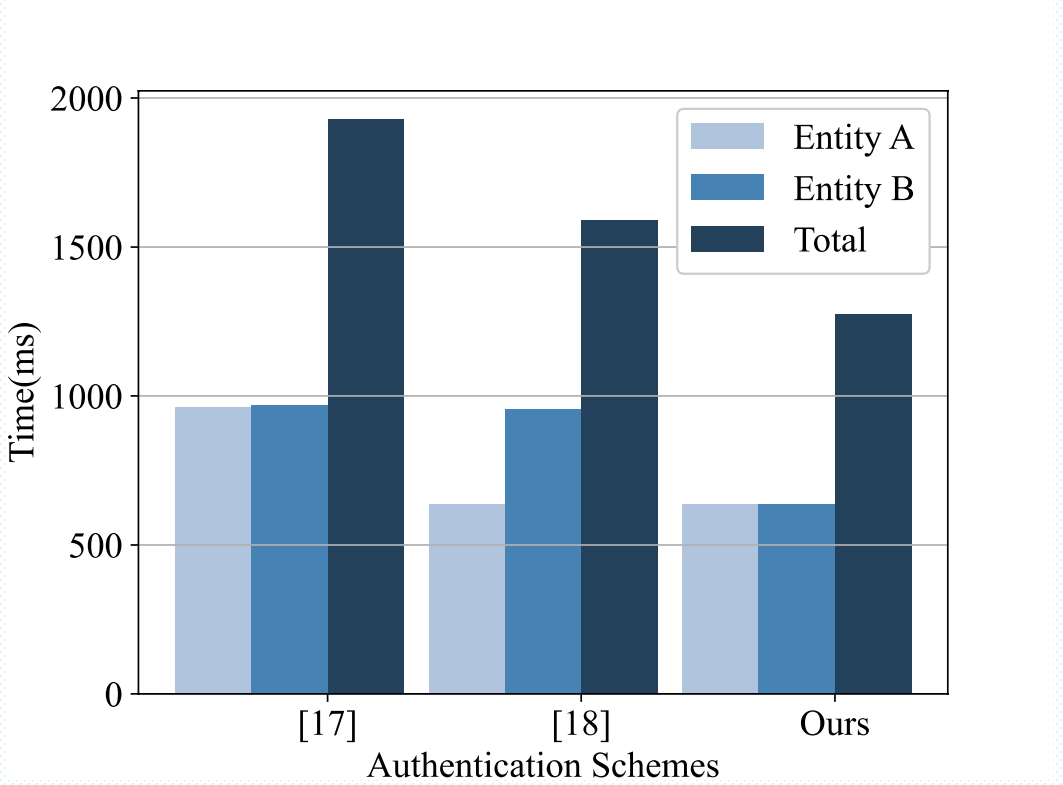
4

Performance Evaluation

Performance Evaluation

- The cost of completing an identity authentication and key agreement is about 150 bytes
- The total delay of the process is about 1200ms.

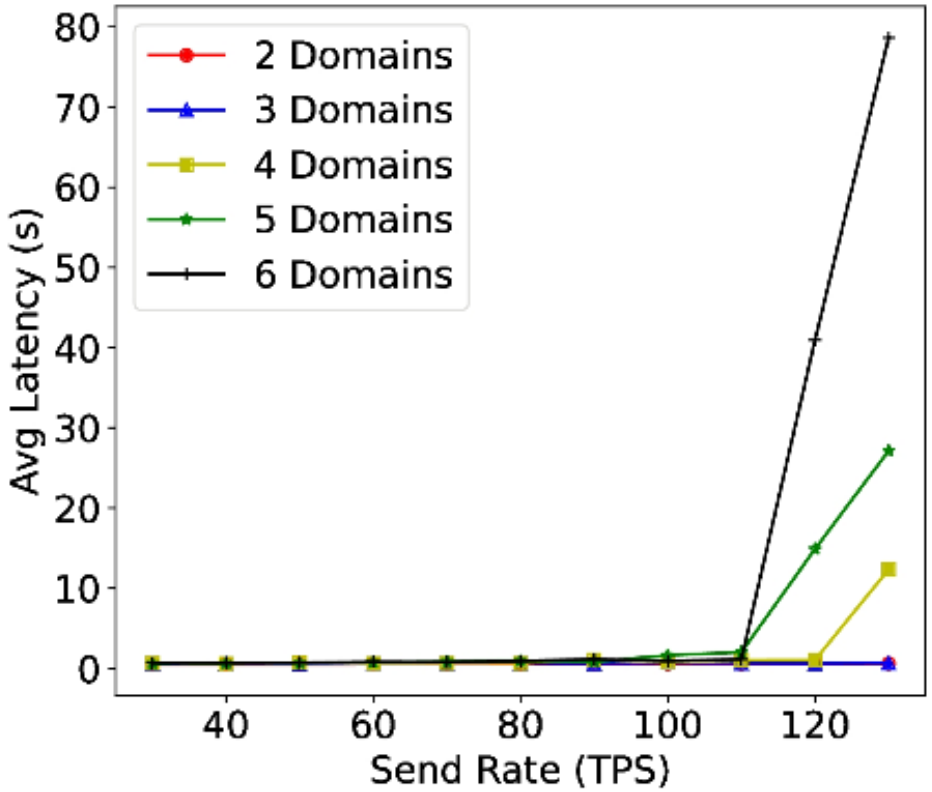


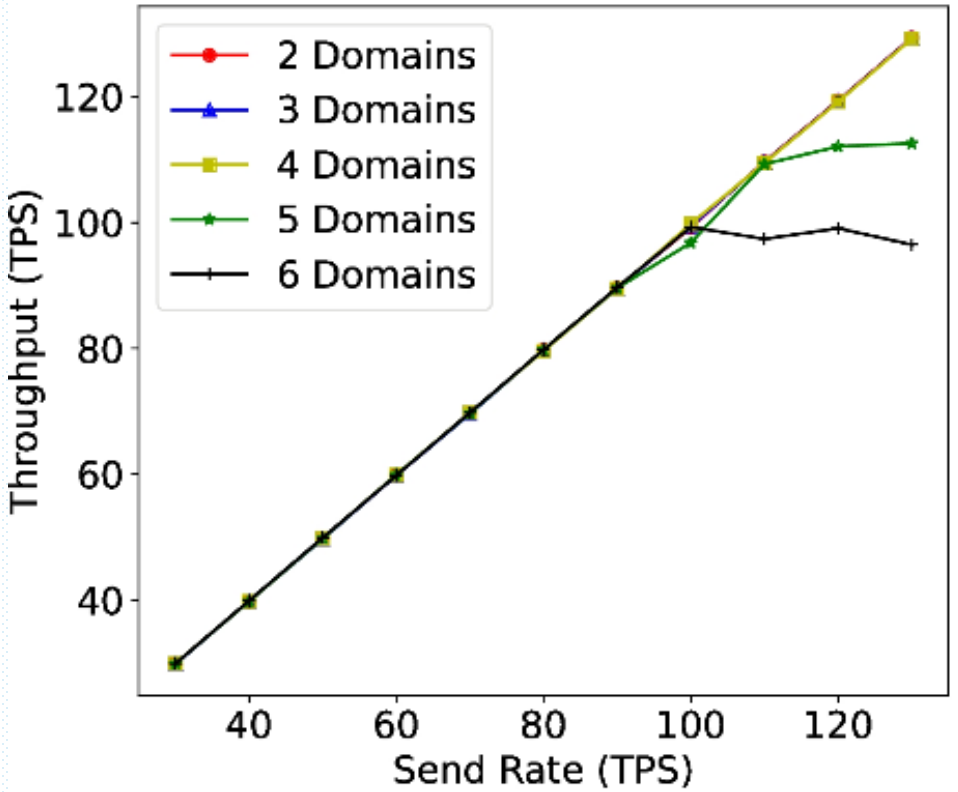


Performance Evaluation

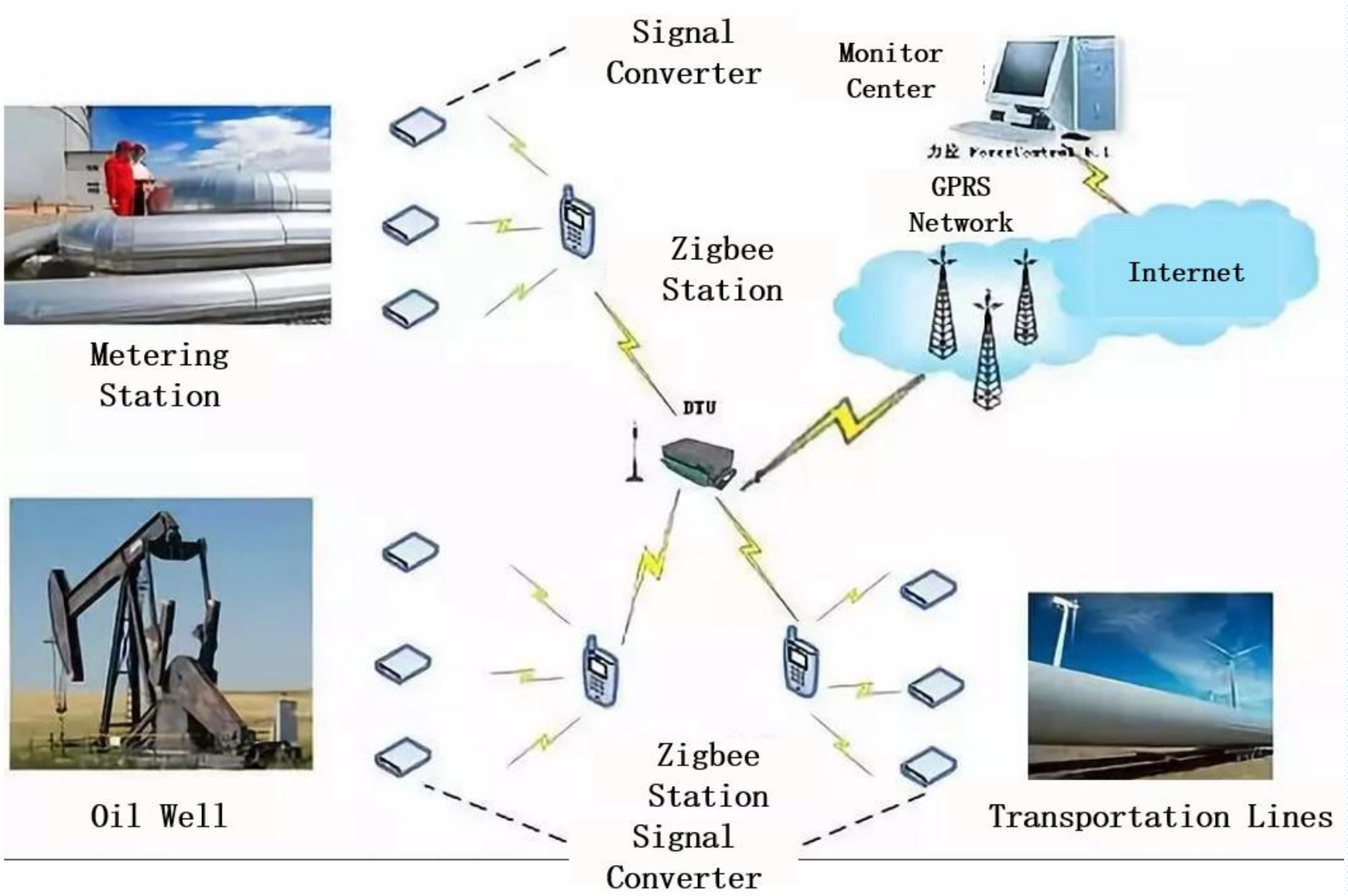
- When the rate of authentication requests is **below 100TPS** , the delay is close ZERO.
- As TPS increases, the delay and throughput performance are constrained by the performance of the underlying blockchain.

Tests carried out on Fabric Implementation





Implementation in Oil Field



Before

- Different departments unwilling to adopt centralized IoT node identity hosting
- Possible fraudulent device identification

After

- Fraudulent free identity of IoT nodes
- Trusted data management along oil filed production

Thanks!

Contact: rui.tian@chaincomp.net