



Blockchain-based crossdomain IIoT identity authentication

Rui Tian, Ph.D.

Director of Research

Chaincomp Technologies Co., Ltd (中科物缘)

rui.tian@chaincomp.net

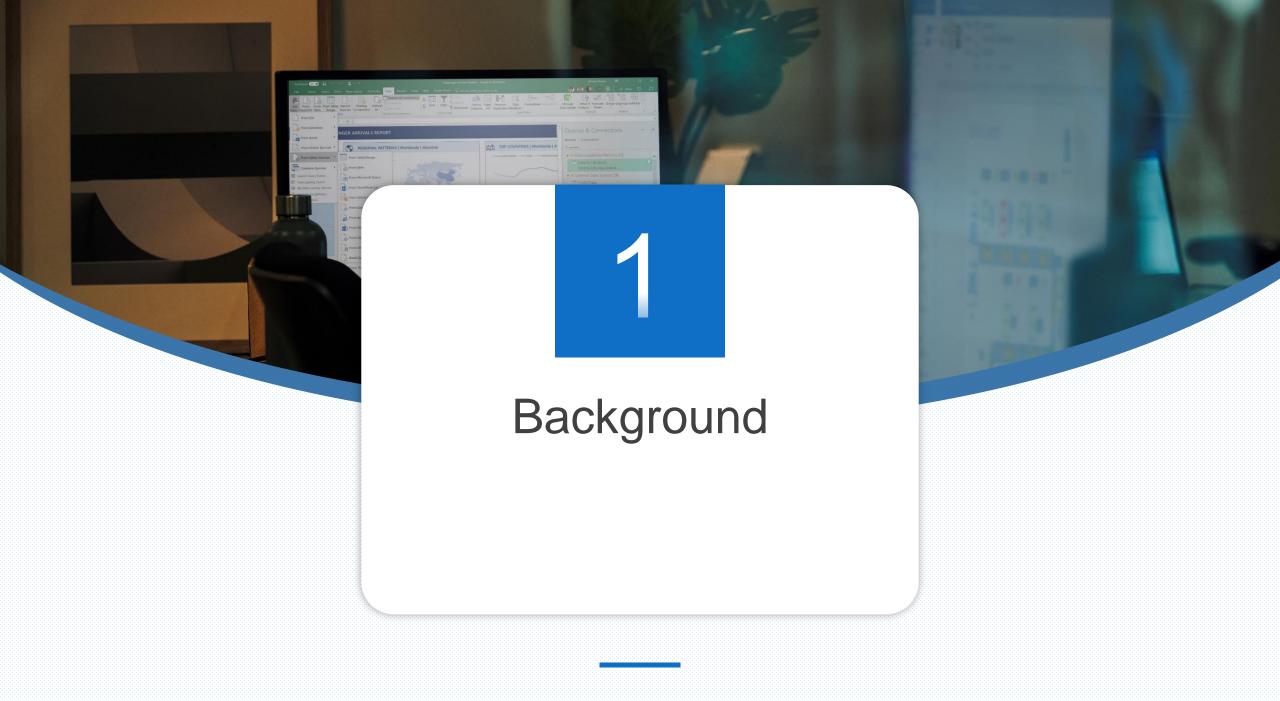




1 Background

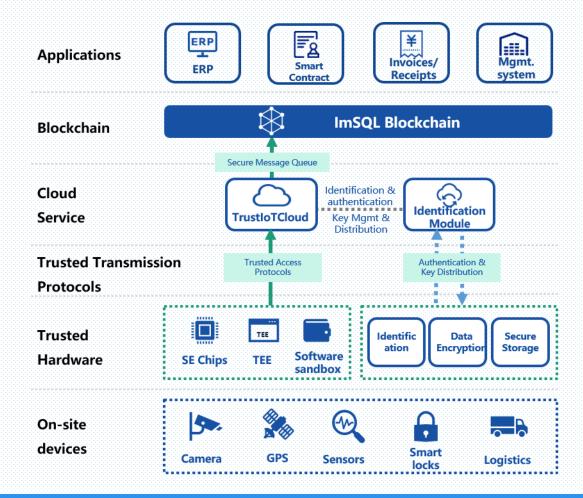
3 Our Solution 2 Related Works

4 Performance Evaluation



Ġ Chaincomp - Blockchain of IoT Architecture 🔞 中科物编

ImSQL[™] Storage Blockchain, EdgeTrust[™] and TrustloTCloud[™] for Trusted IoT Management



	2020-02-04	10:08:55 早期二					R #	inin 🔻 🛛 Eng
mSQL监管服务	ImSQL监管服务 / 在RC	14						
移带点	USER GATEWAY							
gua								
	user-gate-way-pr	rod 🔍 👼						
耐医块	p.	118.24.42.205						
党行为	520	52002						
	DATA NODE							
	prod-node4 .	WS	prod-node3 .	ws.	prod-node2 😐	ŦS	prod-node7 🔹	要多
		119,27,191,213		119.27.191.213	IP.	119.27.191.213	IF.	132,232,213,81
		50004	100 C	50003	80	50002	100 C	50007
	磁盘容量	49.1568		498.15.045	税应会量	49.1558	延生安量	49,1538
	信盤劇寺古里	28.0708	巡察前午容量	26.0708	國直到中容量	26.07GB	經黨原本容量	32,3258
	内容	7.6368	大臣	7.6368	内存于	7.63GB	四存	7,63G8
	空闲内厅	0.73646	全局内存	0.1.008	全部的行	0.1.858	空闲内存	0.12040
	内存占用率	0.25%	内存占用率	0.25%	内存占用率	0.23%	内容占用率	0.21%
	prod-node1	東多	prod-node6 .	更多	prod-node5 .	更多		
		In	nSQL	Mgn				
		In	nSQL	Mgn				
•		In	nSQL	Mgn		6 5044		-28
0 10 10 10 10 10 10 10 10 10 10 10 10 10		In 1	nSQL	Mgn		€ 50% 2 © 7 ²		-228
	1472	In	nSQL	Mgn	Control 2008	क ²⁰⁰⁴ 7	100 100 100	-29
		In	nSQL	Mgn	InSOL 2008 InSOL 200	2054 x 20554 x 20554 x 20554 x 20554 x 20554 x 20554 x 205552 x 2055552 x 205552 x 2055552 x 2055552 x 205552 x 2055552 x 2055552 x 2055	100	-228
		In	nSQL	Mgn	Control 2008	2054 x 20554 x 20554 x 20554 x 20554 x 20554 x 20554 x 205552 x 2055552 x 205552 x 2055552 x 2055552 x 205552 x 2055552 x 2055552 x 2055	Re Markey (Markey Constant)	-128 201 No. 101 101 201 No. 101 101
		In	nSQL	Mgn	Image: 100 and	COLOR 1/2 5 100 COLOR 1/2 5 100 COLOR 1/2 5 100 COLOR 1/2 5 100 COLOR 1/2 5 100		-120 -120
			nSQL	Mgn	Impos uses Second State Second State <td>COLOR 1/2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2</td> <td></td> <td></td>	COLOR 1/2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2		
1		In	nSQL	Mgn	Processe	COLOR 10 C	Bo Mathematical Statistical Statis Statiste Statistical Statiste Statistical Statistical Statistic	-100 101 00 00 00 101 00 00 00 101 00 00 101 00 100 00 100 1
			nSQL	Mgn	Impos uses Second State Second State <td>COLOR 1/2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2</td> <td></td> <td>40- 40 00 00 00 00 40 00 00 00 00 40 00 00 00 40 00 00 50 00 00 50 00 00 50 00 5000 5000 5000 5000 5000 5000 5000 5000 5000000</td>	COLOR 1/2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2		40- 40 00 00 00 00 40 00 00 00 00 40 00 00 00 40 00 00 50 00 00 50 00 00 50 00 5000 5000 5000 5000 5000 5000 5000 5000 5000000
			nSQL	Mgn	Processe		Bo Mathematical Statistical Statis Statiste Statistical Statiste Statistical Statistical Statistic	
1			nSQL	Mgn	Image: second	Constant Constant	BC	
PRO AN			nSQL	Mgn		CONTRACT CONTRACT CONTRACT CONTRACT CONTRACT	B B	
PRO AN			nSQL	Mgn		Company C		-
PRO AN			nSQL	Mgn			B B	
Part of Ar			nSQL	Mgn			Re Re Re Re Re Re Re Re Re Re	
Part of Ar			nSQL	Mgn			Fe Se	
Part of Ar			nSQL	Mgn			Re Re Re Re Re Re Re Re Re Re	
Part of Ar			nSQL	Mgn			Fe Se	

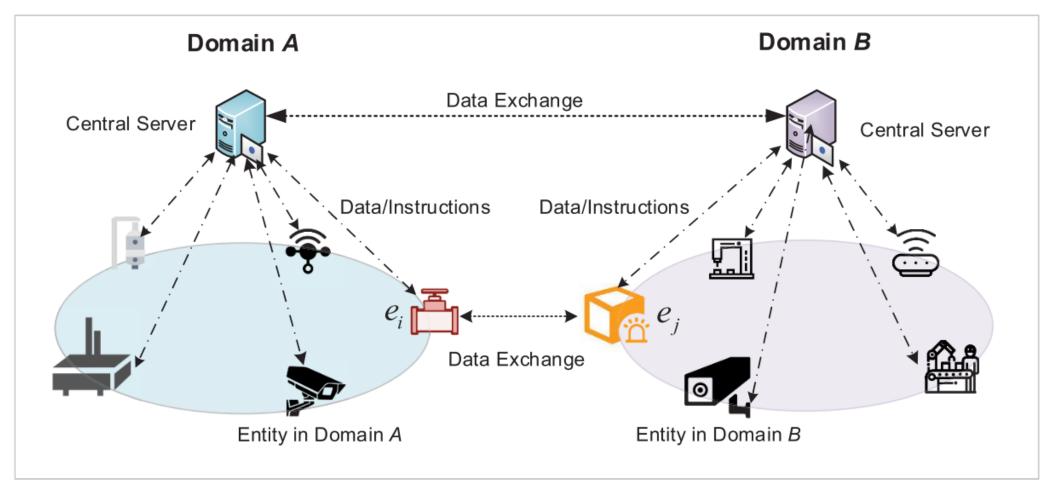
Trusted IoT Module



Background – Industrial IoT Application



Cross-domain identity authentication



🔄 Background – Public Key Systems



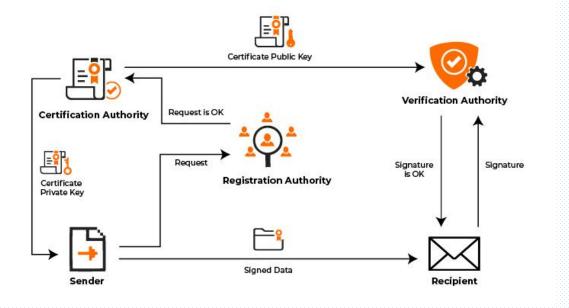
Signer(ID)

Sign:

 $\sigma = PH(ID) + H(M,...)$

PKI (Public Key Infrastructure)

ID PKC (Identity-based public key cryptography)



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



KGC

"master" public key

master-private key

Require private-key

Return master private-key(ID)

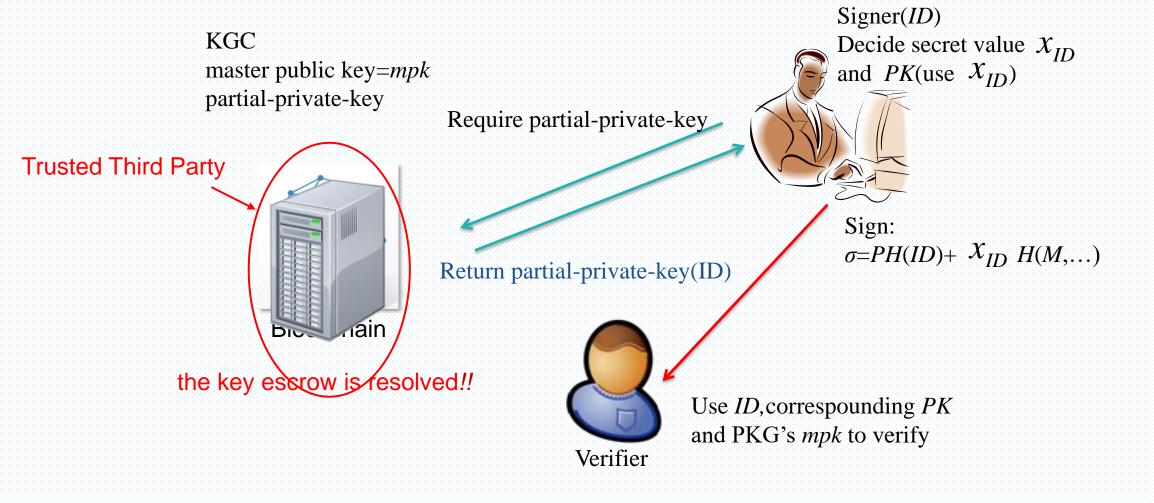
Assume the KGC completely trusted!!

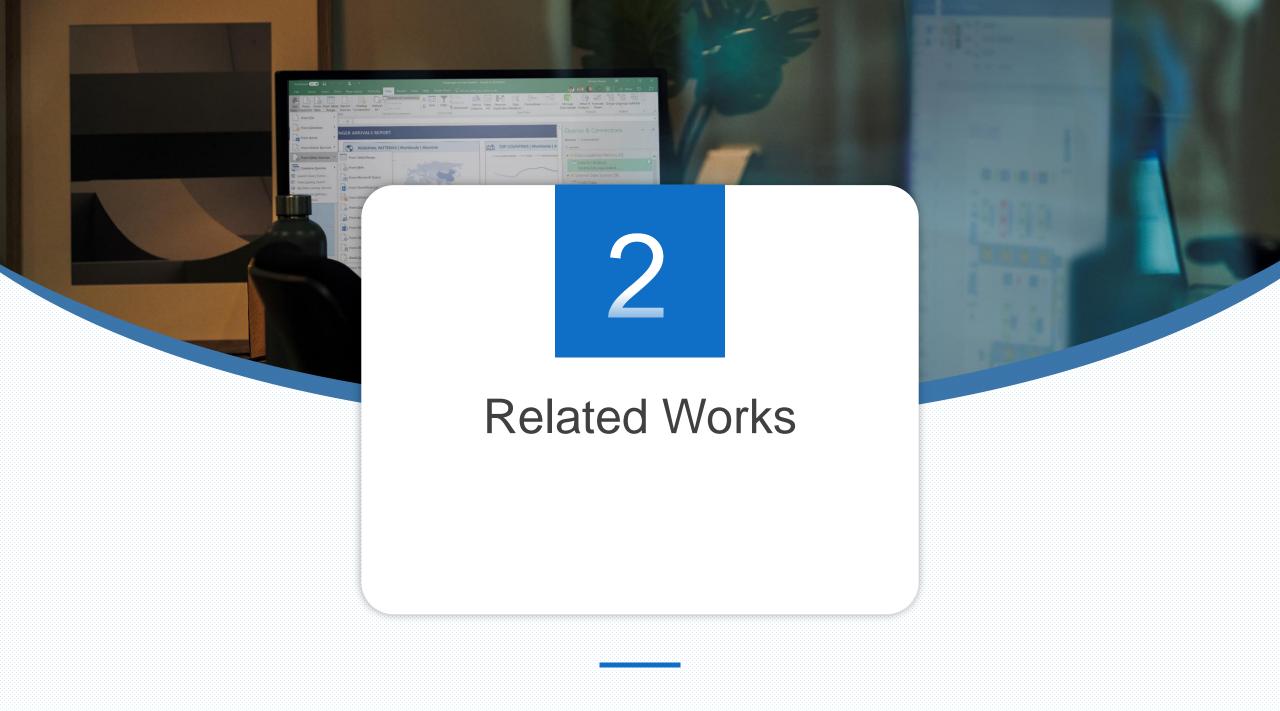
Use *ID* and PKG's *public key* to check Verifier

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

合 Background – Public Key Systems (Cont.)

CL-PKC(Certificateless public key cryptography)

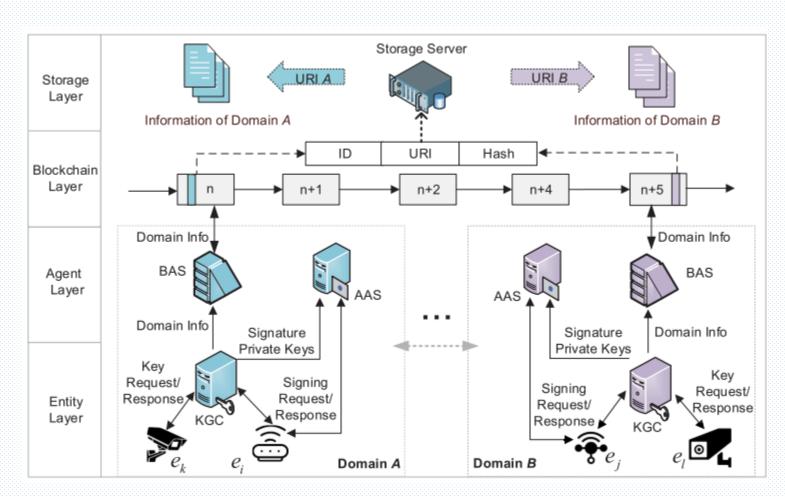








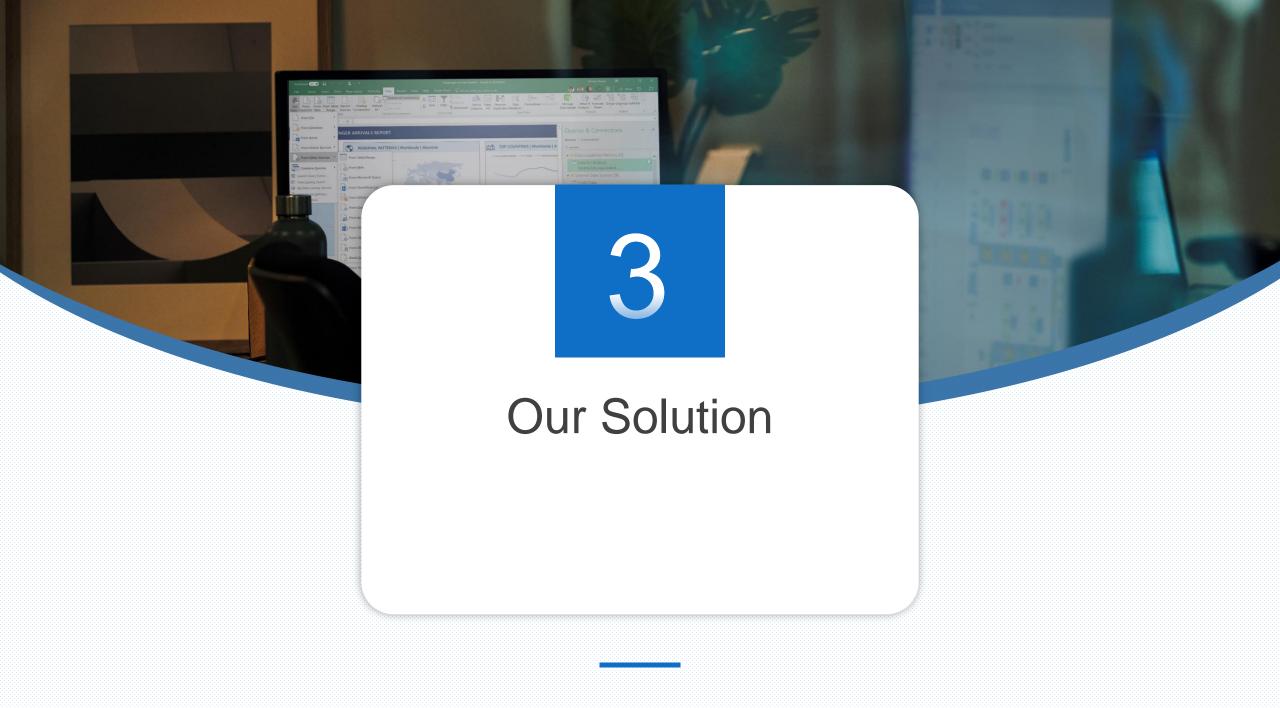
M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchainassisted secure device authentication for cross-domain industrial iot," IEEE Journal on Selected Areas in Communications, vol. 38, no. 5, pp. 942–954, 2020.







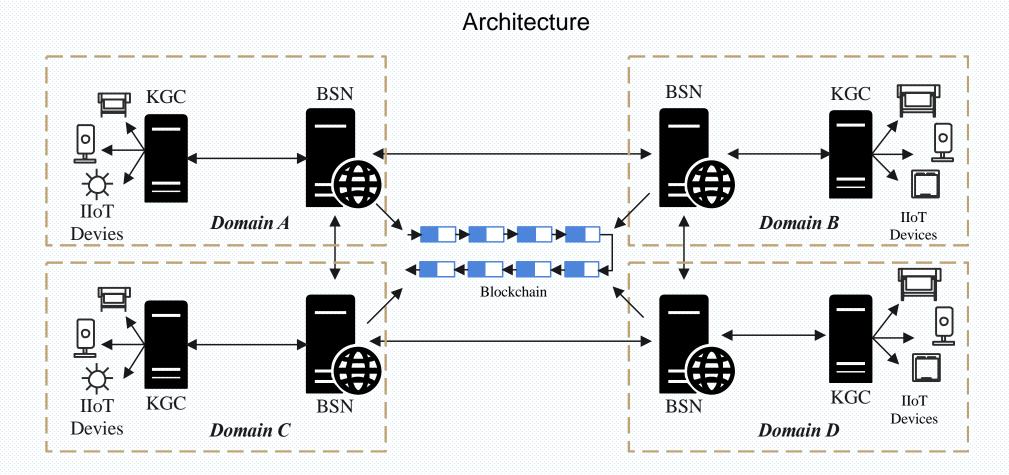
Internet Z. Cui, X. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid WSN_n blockchain-based identity authentication scheme for multi-... WSN wsn," IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 241–251, 2020. Link 4 _ink Link2 Link3 I cluster head node 🐵 :Base station 🛄 :End user Crdinary node Ordinary node A Local blockchain Public blockchain Cluster head B OID Ordinary node B Cluster head A OID End user Base station Request_of_Registration Verify by smart WSN WSN 3 Local Local contract and store Allow access to local block chains Request_of_Registration Blockchain 4 Blockchain 3 node information erify timeliness Trigger smart contract Verify by smart contract and store low access to cluster network node information Request_of_Connection Public Trigger smart contract and select Blockchain blockchain for verification -----Message of Confirm Credential of Authentication, Signed, Verify Verify Local Credential of Authentication_B,Sighed_b Local Blockchain1 Blockchain 2 Establishing secure communication WSN 2 WSN Ask for permission Permission Request of Connection Message of Confirm Message of Confirm Cluster node Base Station Credential of Authenticationuser, Signeduc Verify Credential of Authentication_B,Signed_B Verify Establishing secure communication



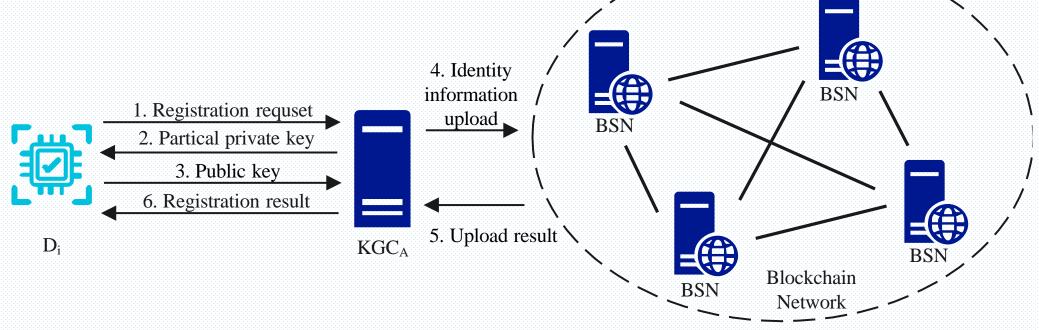
合 Blockchain-based IIoT Identity



Authentication



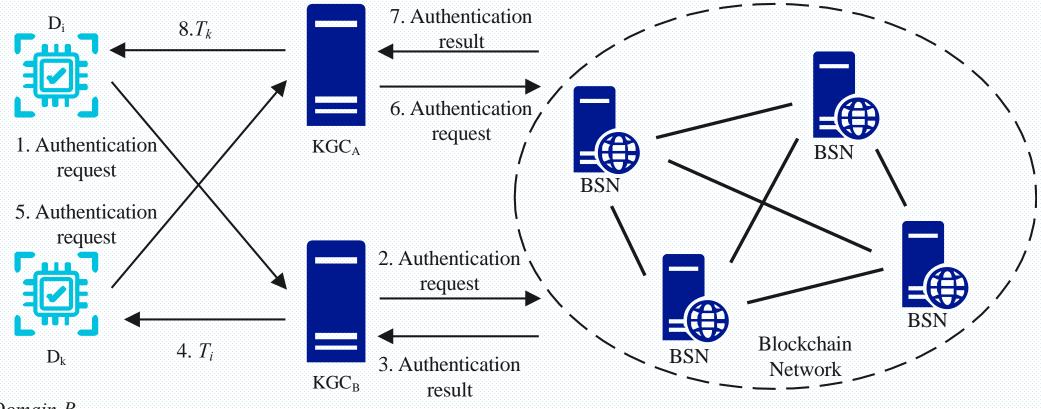
Initialization and Registration Process



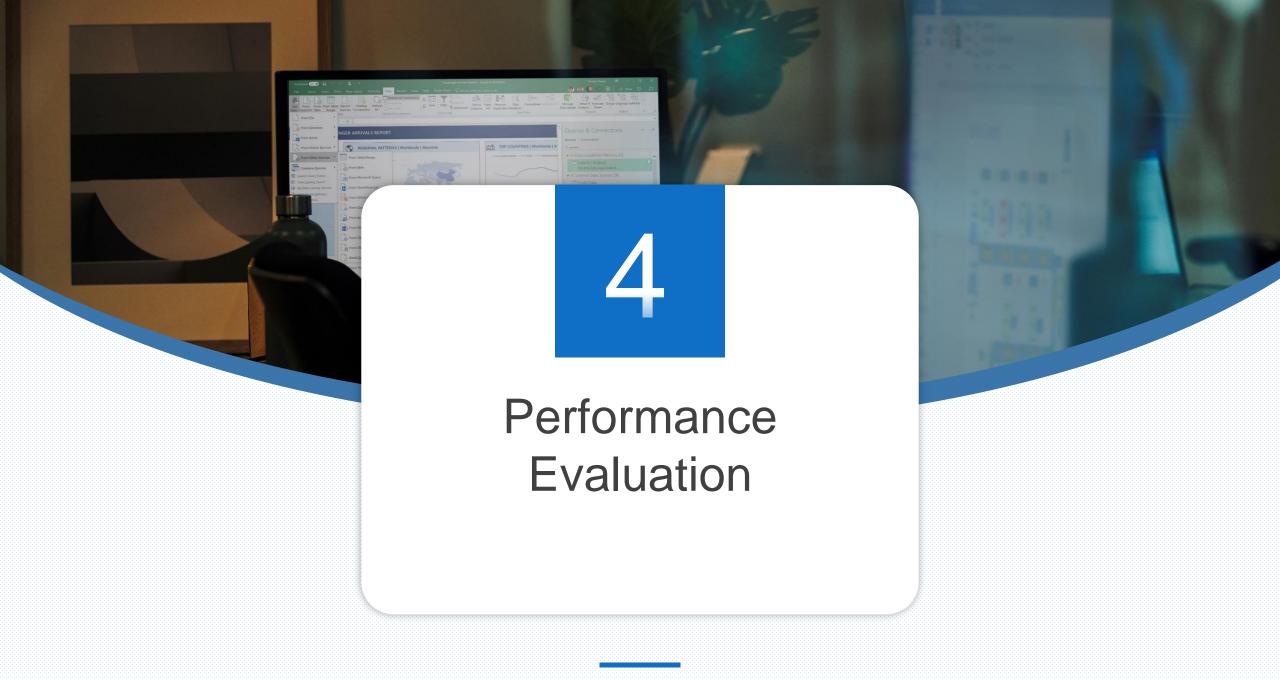
Identity Authentication Process



Domain A

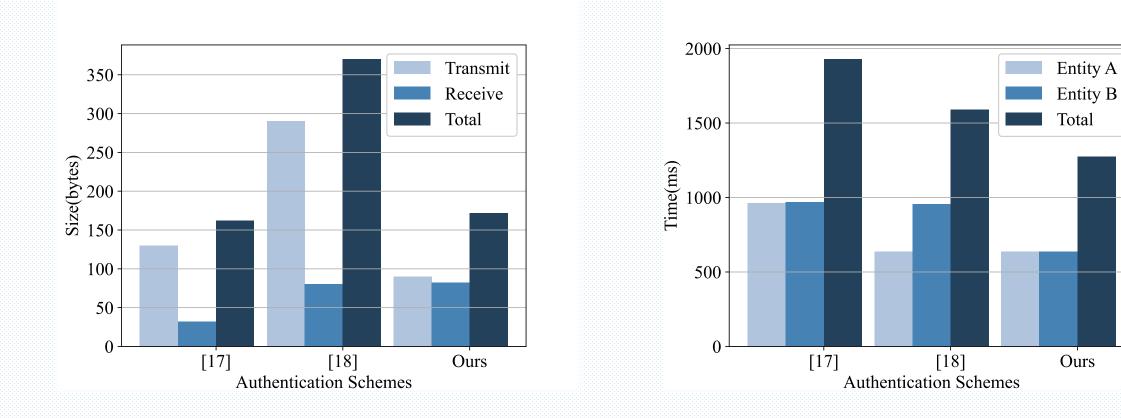






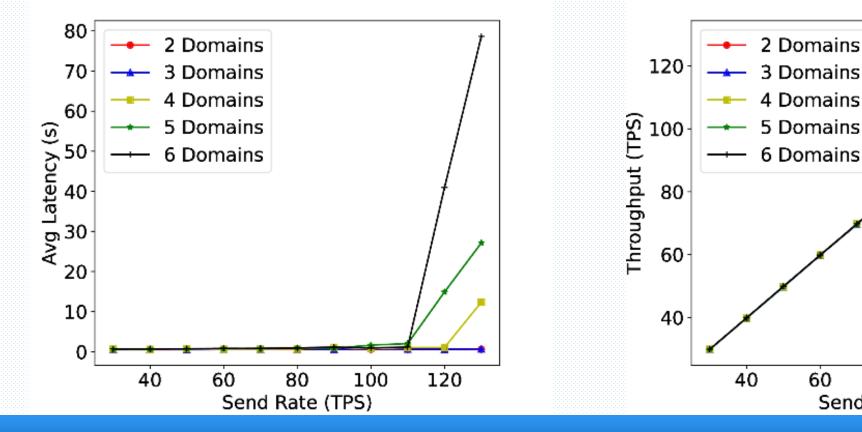


- The cost of completing an identity authentication and key agreement is about 150 bytes
- The total delay of the process is about 1200ms.



Performance Evaluation

- When the rate of authentication requests is **below 100TPS**, the delay is close ZERO. ٠
- As TPS increases, the delay and throughput performance are constrained by the ٠ performance of the underlying blockchain.



Tests carried out on Fabric Implementation

80

Send Rate (TPS)

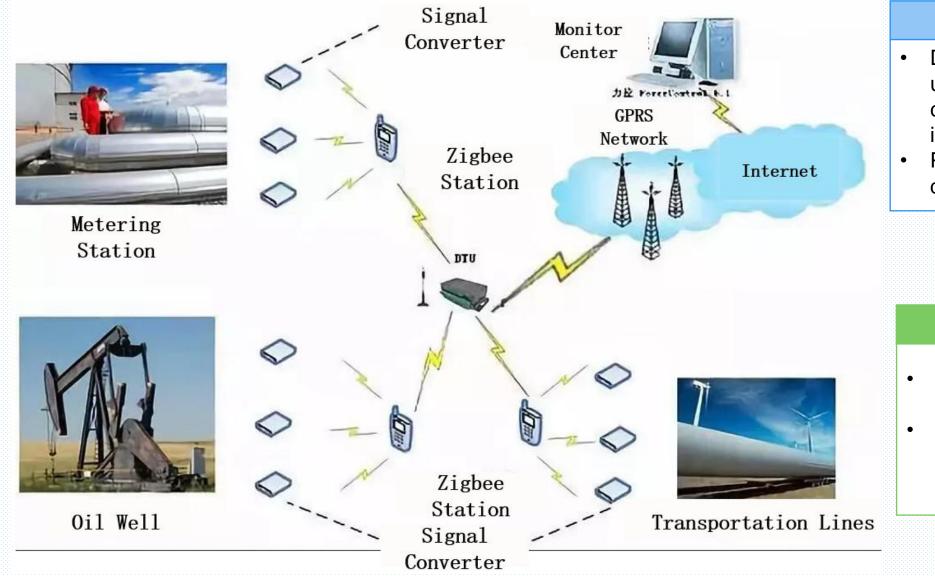
100

120

60

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

