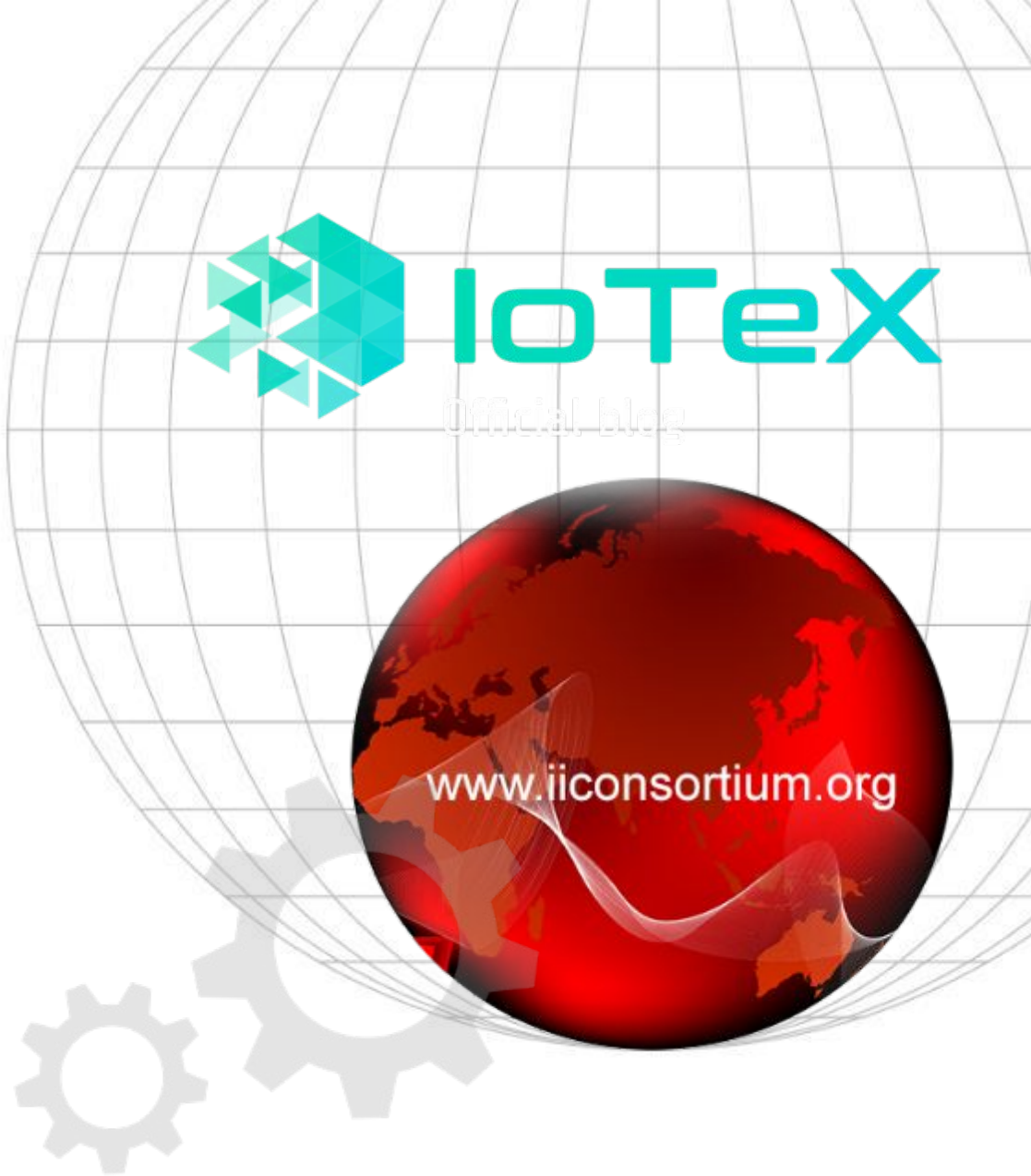
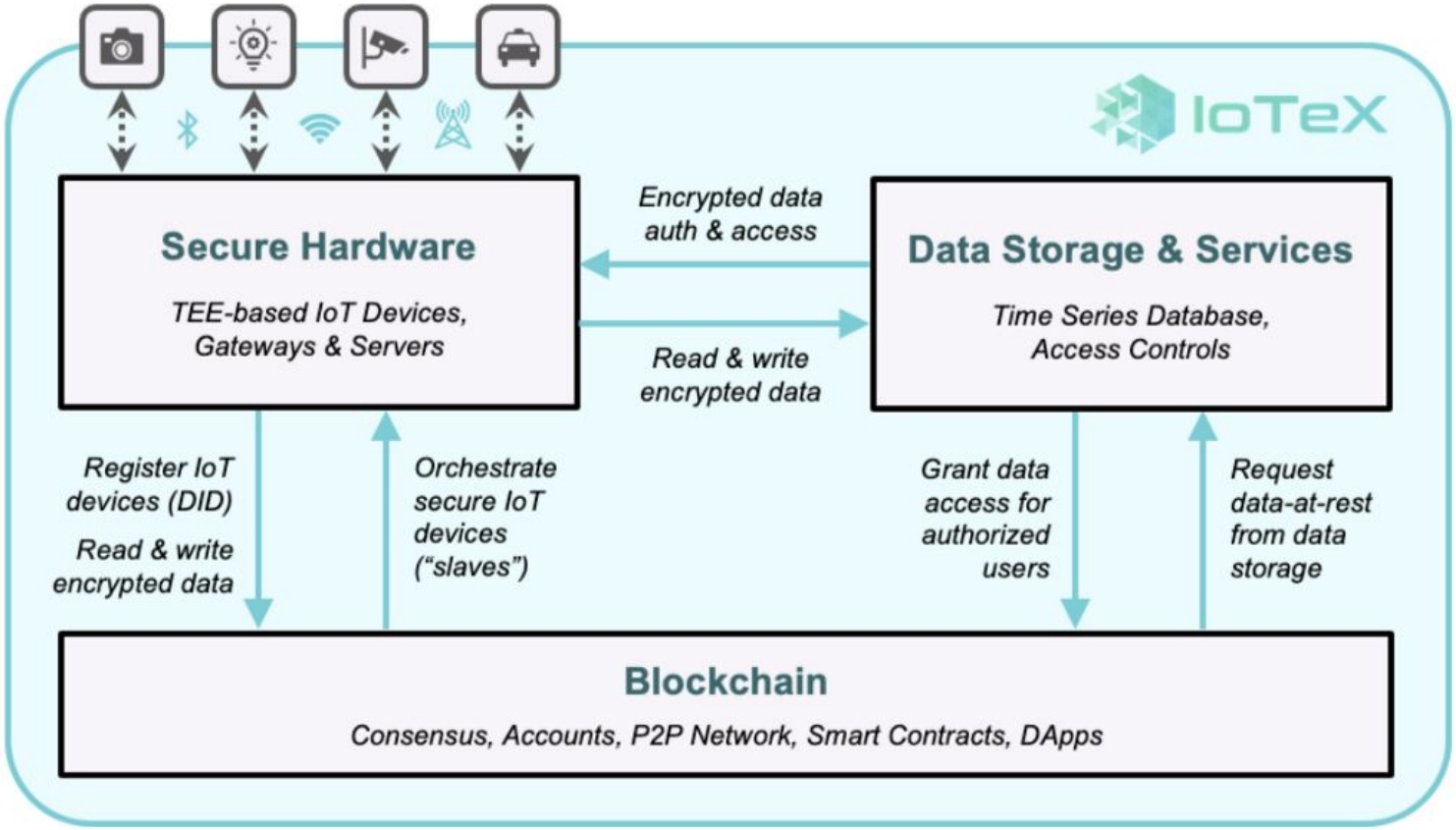


Decentralized Ledger Based Authentication Framework for Industrial Internet of Things (DIoTA)

Xinxin Fan, Ph.D., CISSP
IoTeX

Join work with Lei Xu, Lin Chen, Zhimin Gao, Taeweon Suh, and Weidong Shi

IoTeX Overview



- Founded in 2017
- Funded on January 2018, **50+** institutional investor globally
- **30** global team members in Silicon Valley, China, India and Singapore
- **Mainet Alpha** went live on April 2019
- **30+** IoT partners, **60+** delegates and **200K+** community members

Unlock the Potential of Internet of Trusted Things on a Global Scale!

Content restricted to IIC Members
Not for External Publication

Data Authentication Challenges in IIoT Systems

- An IoT system usually involves a large number of devices
- An IoT device usually has limited computation capability and power supply
- IoT devices might be owned and managed by multiple parties
- Decentralized ledger technology provides a new way to protect authenticity of the data collected by IoT devices in a collaborative environment.

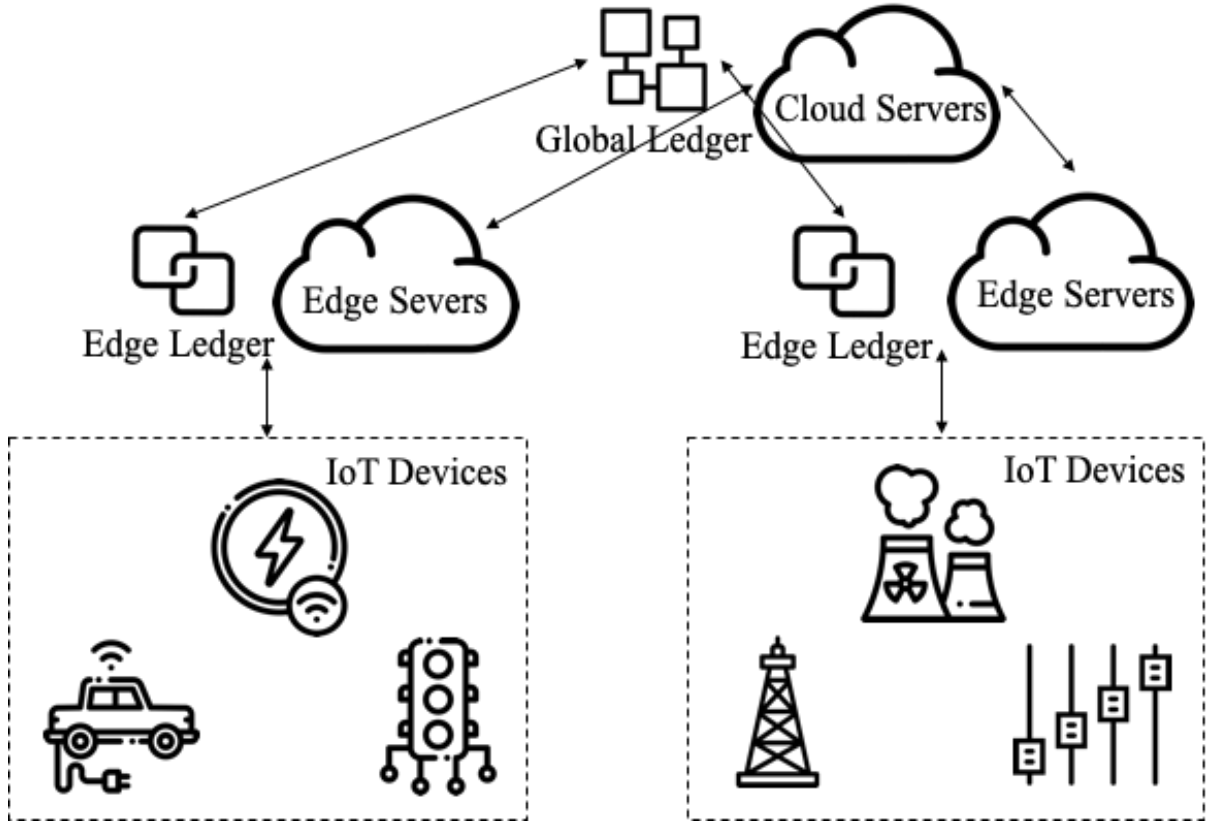
Content restricted to IIC Members
Not for External Publication

Permissioned Ledger

- Formed by a set of known transacting parties
- Validation is controlled by a selected set of nodes
- Specialized verifiers can be added with the agreement of the current members
- Created to maintain compatibility with existing applications
- Ledgers replicate the high degree of transparency and accountability

Content restricted to IIC Members
Not for External Publication

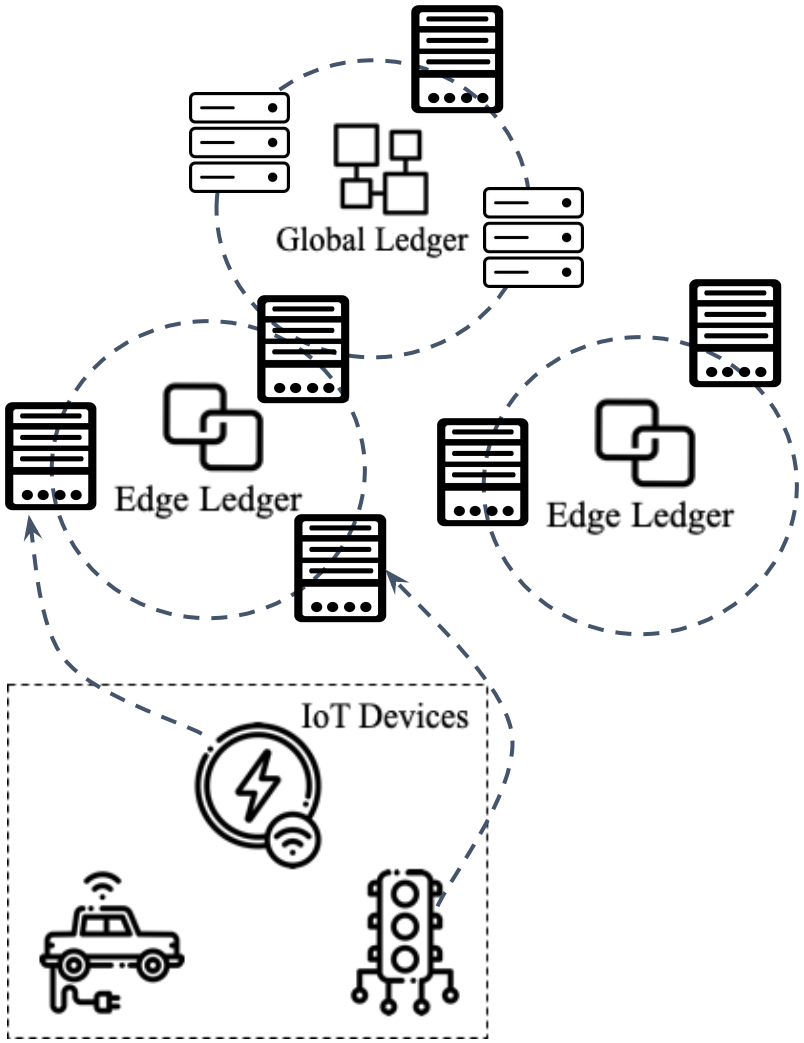
System Architecture of DIoTA



- Layered decentralized ledger architecture:
  - Edge ledger
  - Global ledger
- Each edge ledger only serves a subset of IoT devices
- The global ledger connects all edge ledgers to facilitate occasional cross-ledger data exchange
- Cloud and edge servers store IoT data and are not fully trusted

Content restricted to IIC Members
Not for External Publication

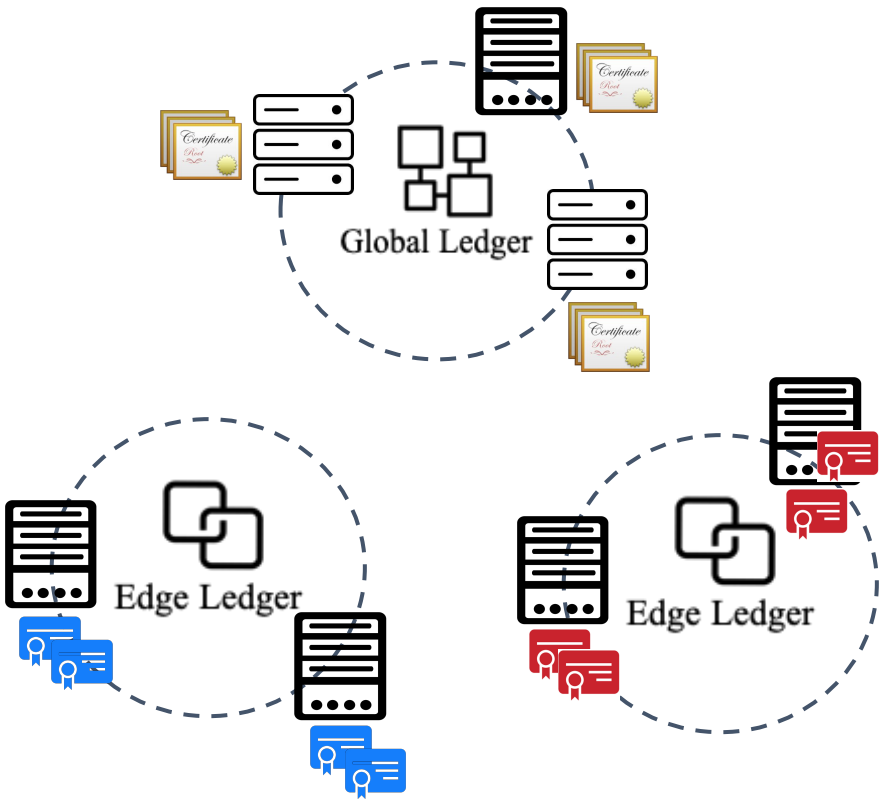
Connection of Different Components



- Edge ledger nodes can be deployed on the edge (e.g., IoT gateway)
- Different edge ledgers are not directly connected with each other
- Global ledger is maintained by a group of nodes that is usually sit in the cloud
- An edge ledger and the global ledger can share some nodes for connection
- Each IoT device locally keeps a list of edge ledger nodes for reliable connection

Content restricted to IIC Members
Not for External Publication

Certificate Management

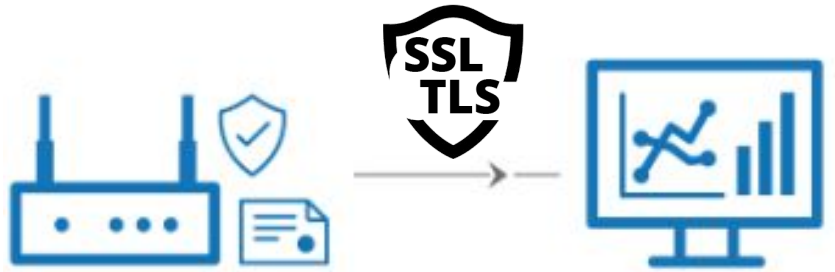


- Each IoT device has a device certificate issued by a CA and registered with the edger ledger
- All ledger nodes' certificates are stored in each edger ledger and the global ledger
- A certificate revocation is performed by generating a revocation transaction on the corresponding ledger(s)
  - The revocation of device certificates is managed by the edge ledger
  - The revocation of a ledger node's certificate is broadcasted to all the ledgers in the system

Content restricted to IIC Members
Not for External Publication

IoT Data Authentication - Basic Idea

- Two major interaction models in IoT systems:
  - request/reply model
  - publish/subscribe model
- SSL/TLS can be utilized to protect the data authenticity in transmission
- The energy required to maintain the SSL/TLS connection is not negligible for IoT devices.
- A **lightweight** data authentication protocol is highly desirable.
- DIoTA **minimizes** the use of expensive public-key cryptography operations.
- Motivated by the idea of Time Efficient Stream Loss-tolerant Authentication (**TESLA**)



Content restricted to IIC Members
Not for External Publication

IoT Data Authentication - Authentication Schema

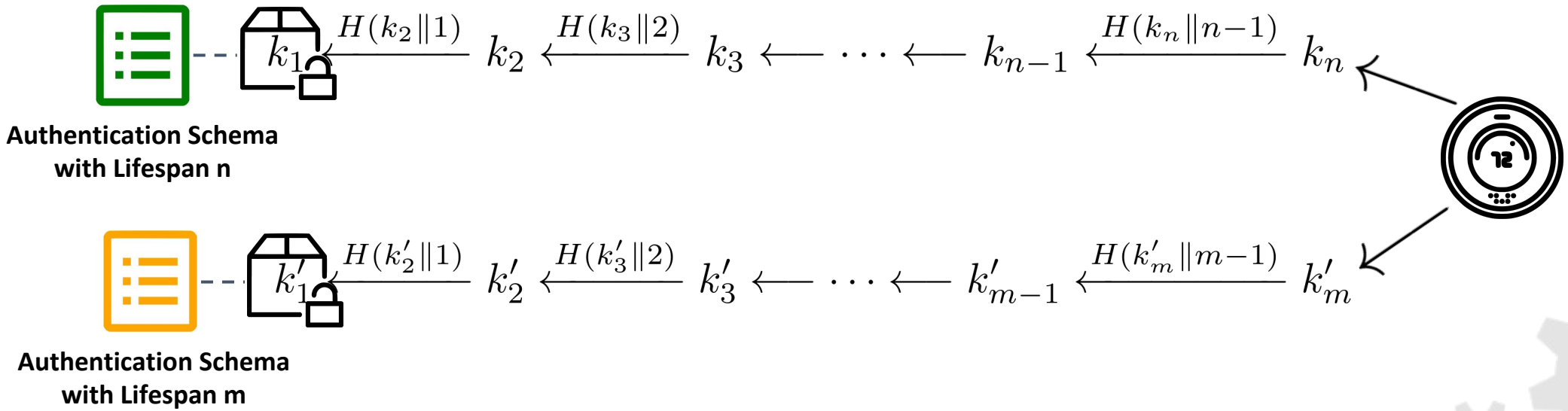
Field Name	Description
Sender	Certificate of IoT device
Data Unit	Unit of data transmission (e.g., 1KB, 1MB, etc.)
Data Authentication Mechanism	Message authentication code (e.g., HMAC, CMAC, etc.)
Key Information	Committed key for data authentication
Key Updating Frequency	Number of data units authenticated by the key
Schema Lifespan	Number of times the key can be updated

- The IoT device submits its data authentication schema together with a digital signature to its edge ledger
- The end user of data can obtain the schema information from the edger ledger.

Content restricted to IIC Members
Not for External Publication

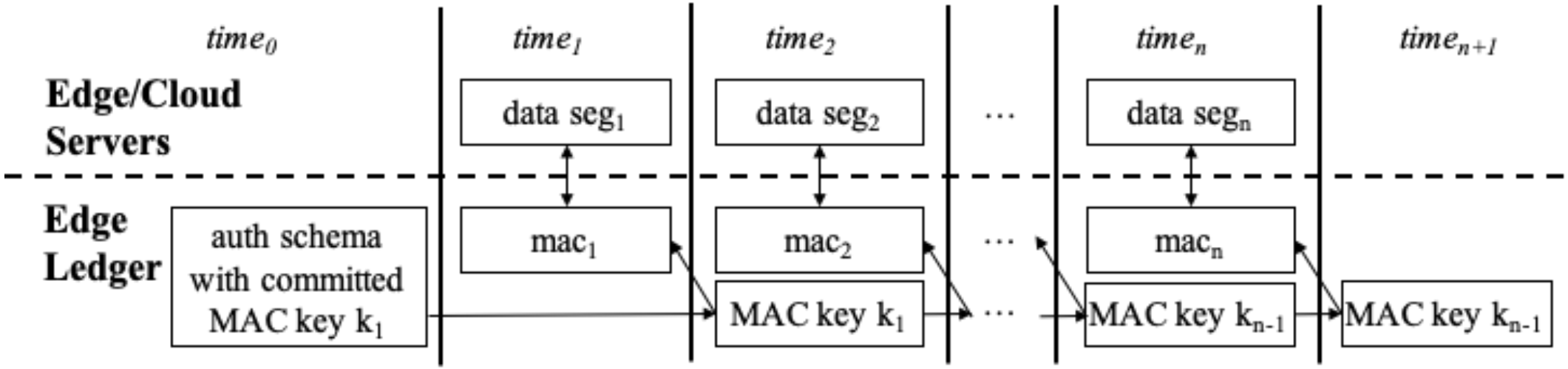
IoT Data Authentication - Key Management

- An IoT device generates a single digital signature for a data authentication schema
- The ‘Key Information’ field will be updated after the ‘Schema Lifespan’
- A hash chain is utilized to generate a number of keys for data authentication
- The length of the hash chain is determined by the ‘Schema Lifespan’ field



Content restricted to IIC Members
Not for External Publication

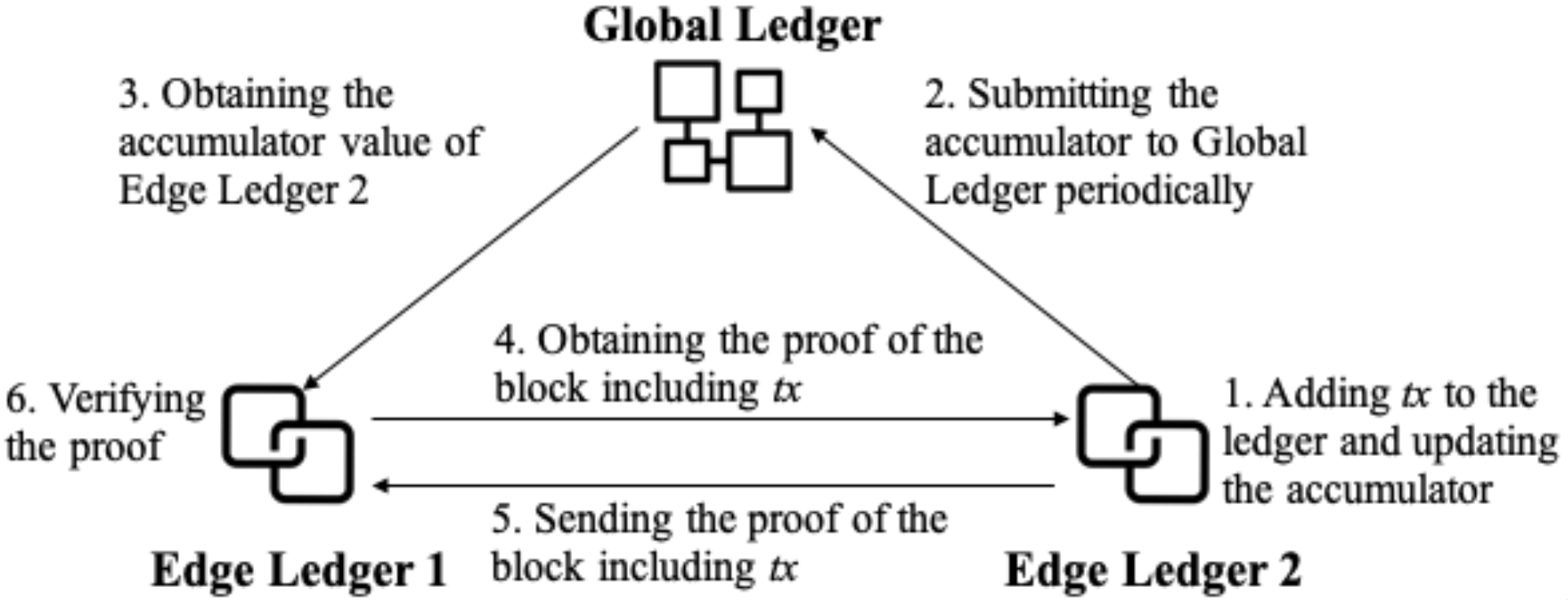
IoT Data Authentication - Data Verification and Storage



- The data from IoT devices are collected and stored by edge/cloud servers
- DIoTA is responsible for managing and verifying authenticity information
- When the data segment seg_t is sent and stored by edge/cloud servers, the corresponding edge ledger cannot verify its authenticity immediately
- The authenticity protection key is provided by the IoT device in time period $t+1$

Content restricted to IIC Members
Not for External Publication

Cross-Ledger Information Exchange



- **Cryptography Accumulator**: A one-way membership function which answer a query to whether a potential candidate is a member of the set without revealing the individual members of the set.

Content restricted to IIC Members
Not for External Publication

Performance Analysis

IoT Device

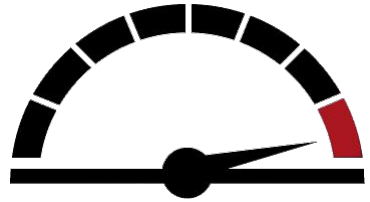
- Generate data authentication schema
- Generate MAC keys
- Generate MACs

Edge Ledger Node

- Process local transactions
  - Number of IoT devices connected
  - Schema lifespan

Global Ledger Node

- Track the updates of each edge ledger
  - Number of edger ledger connected
  - Aggregation factor (i.e., how often updates occur)



Content restricted to IIC Members
Not for External Publication

Security Analysis

- **Confidentiality of authentication key**: The hiding feature of the commitment scheme guarantees the confidentiality of the first authentication key

- **Forward/Backward Security**: Assume that the key k_t is disclosed to the attacker
  - Forward security is guaranteed by the immutability of the decentralized ledger
  - Backward security is guaranteed by the one-wayness of the cryptographic hash function

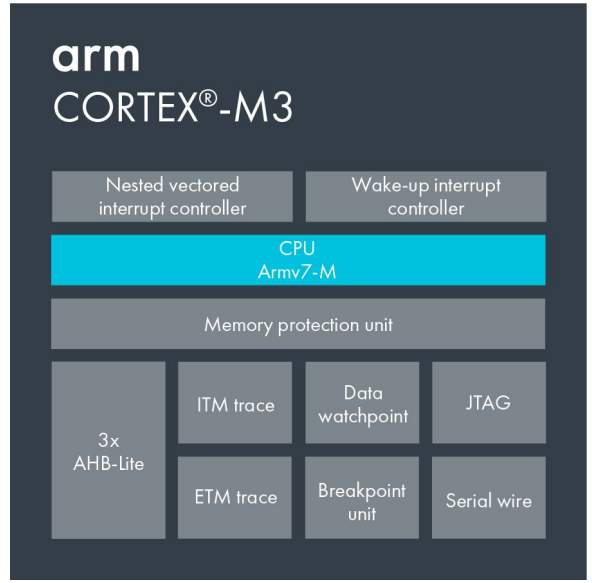
- **Device Compromise**: The attacker can forge all the future messages, but not historical data

$$k_1 \longleftarrow \cdots \longleftarrow k_t \longleftarrow \cdots \longleftarrow k_n$$

Content restricted to IIC Members
Not for External Publication

Implementation - IoT Device

Algorithm	Input Size	Time
AES-CMAC-256	1024 Bytes	0.9 ms
SHA-256		0.6 ms
ECDSA (secp256k1)		130 ms for generation 488 ms for verification



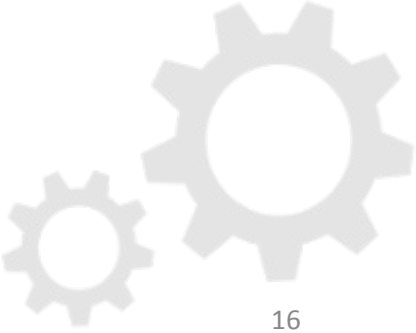
- **NXP LPC1768**
  - ARM Cortex-M3 @96MHz
  - 512KB Flash, 32KB RAM

Content restricted to IIC Members
Not for External Publication

Implementation - Edge/Global Ledger

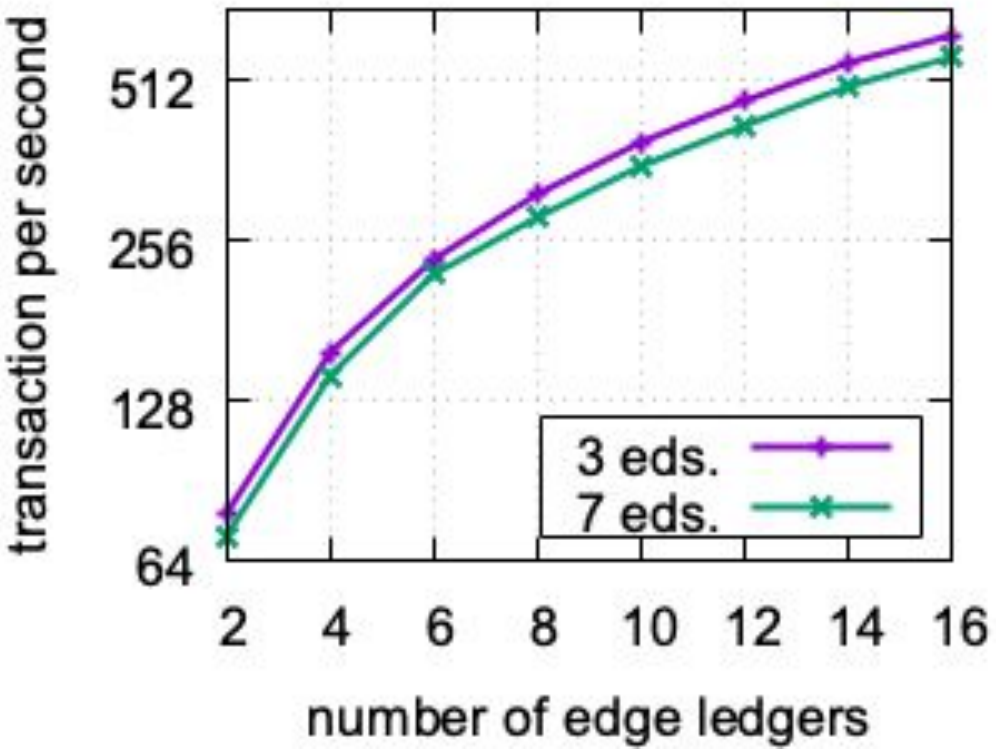
- Three types of nodes in Hyperledger Fabric: peers, endorsers, and orderers
- The lifecycle of a transaction:
  a. A peer initializes a transaction and sends it to all endorsers in the ledger
  b. A endorser checks validity of the transaction and signs it
  c. A peer collects all endorsements from endorsers, puts them together with the transaction, and submits it to oderers
  d. An orderer checks whether the transaction satisfies the pre-defined endorsement policy, packs it to a block, and appends to the ledger via a consensus protocol
- The edge ledgers and the global ledger are implemented as different channels
- One or more peers of an edge ledger is enrolled to the global ledger for overcoming the limitation of channels in Hyperledger Fabric

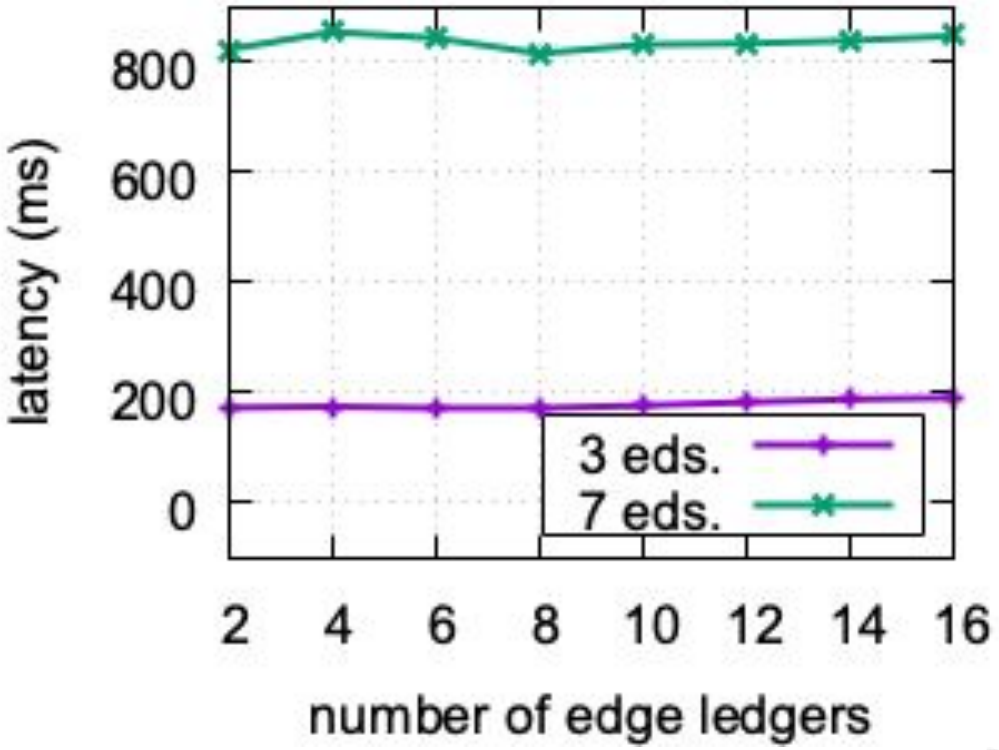
HYPERLEDGER FABRIC



Content restricted to IIC Members
Not for External Publication

Experiment Results - Transaction Processing

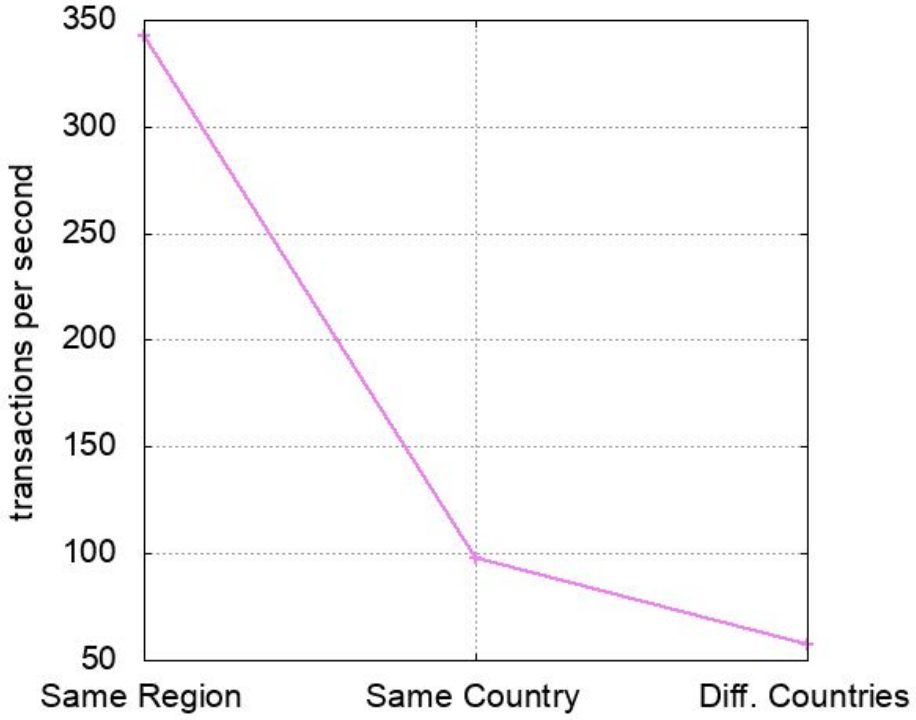


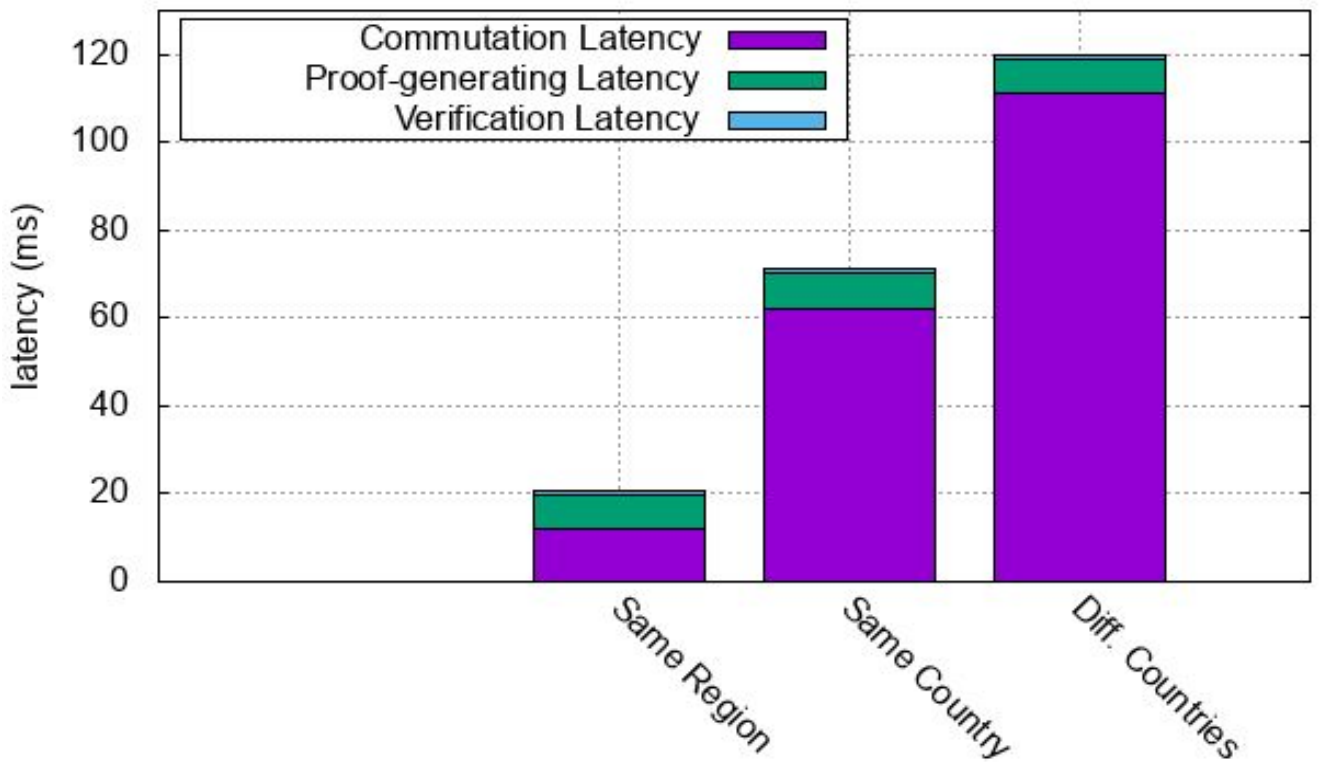


- The transactions include submission of the new authentication schema, key updating operations, and MACs uploading.

Content restricted to IIC Members
Not for External Publication

Experiment Results - Cross-Channel Queries





- The data user is served by an edge ledger that is different from the edge ledger that serves the IoT devices

Content restricted to IIC Members
Not for External Publication

Q&A

Xinxin Fan

Head of Cryptography

IoTeX

IoTeX
xinxin@iotex.io
https://www.iotex.io/

LET'S BUILD DECENTRALIZED FUTURE TOGETHER!

Content restricted to IIC Members
Not for External Publication

INDUSTRIAL INTERNET CONSORTIUM
USE OF INFORMATION - TERMS, CONDITIONS & NOTICES

AUTHORS AND LEGAL NOTICE

Copyright© 2019 Industrial Internet Consortium, a program of Object Management Group, Inc. *("OMG").*

All copying, distribution and use are subject to the limited License, Permission, Disclaimer and other terms stated in the Industrial Internet Consortium Use of Information – Terms, Conditions & Notices, as posted *at* http://www.iiconsortium.org/legal/index.htm*#use_info*. If you do not accept these Terms, you are not permitted to use the document.