Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin
National Metrology Institute

Blockchain in Legal Metrology and Inter-NMI Network

Mahbuba Moni, PTB

Outline

- Legal Metrology and Digitalization
- Blockchain and Measurement Applications
- Use case#1: Security and Privacy for Distributed Smart Meter
- Use case#2: PKI for Smart Meters
- Implementation and Results

Legal Metrology and Digitalization

Trends

Increasing numbers of measuring instruments have already a cloud connection.

Require

New solutions to cover the requirements laid down by legal metrology.

Solution

Designing innovative solutions which extend and merge novel technologies.

Blockchain Technology

- Immutable append-only data structure
- Cryptographically linked chain of blocks.
- Platform for distributed systems.
- Smart contracts for automation of workflows.
- Establishing trust among independent parties that do not need to trust each other.

Use-Case #1:

Security for Distributed Smart Meter: Blockchain-based Approach, Ensuring Privacy by Functional Encryption

Yurchenko, A.; Moni, M.; Peters, D.; Nordholz, J.; Thiel, F.
Security for Distributed Smart Meter: Blockchain-based Approach, Ensuring Privacy by Functional Encryption.
In Proceedings of the 10th International Conference on Cloud Computing and Services Science—CLOSER, Prague, Czech Republic, 7–9 May 2020; pp. 292–301.

Current State in Software Verification

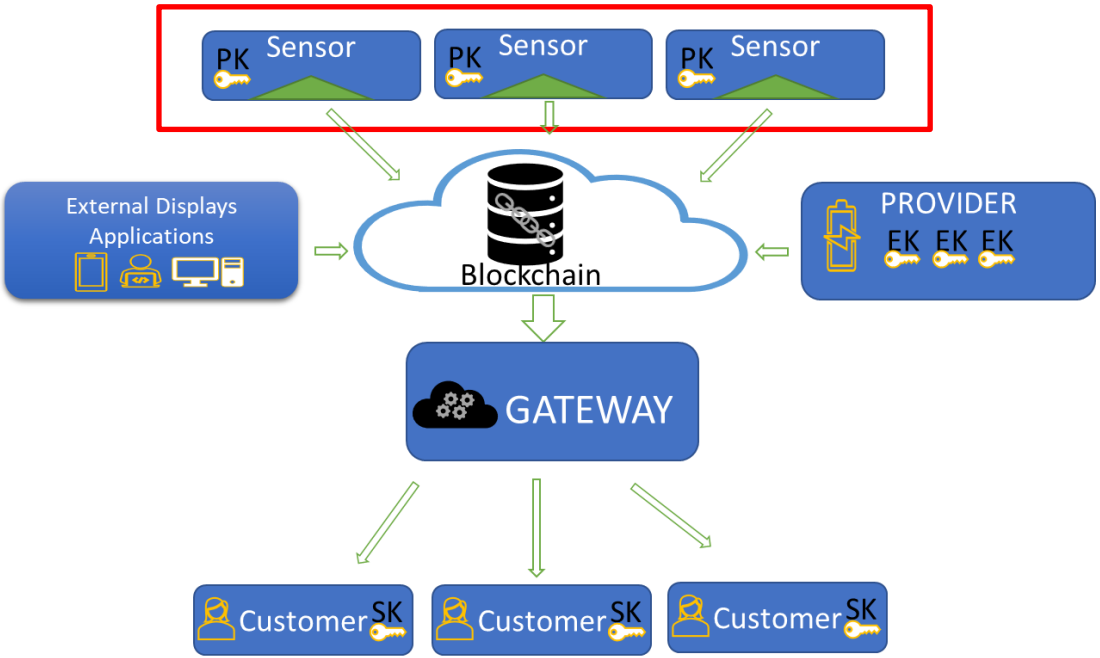
- Based on system integrity and hardware is physically sealed
- Software integrity is verified by calculating checksum over all relevant files and modules.
- Calculation of the checksum might be manipulated without breaking any seal.
- To prevent this, measurement instruments need to undergo regular updates
  - Requires recertification
  - Inconvenient for all stakeholders
- Desirable to have a verification method which does not verify the binary image itself, but the functionality contained therein.

Overview Of Security Primitives

Alternative model	Aim/Goal	Solution

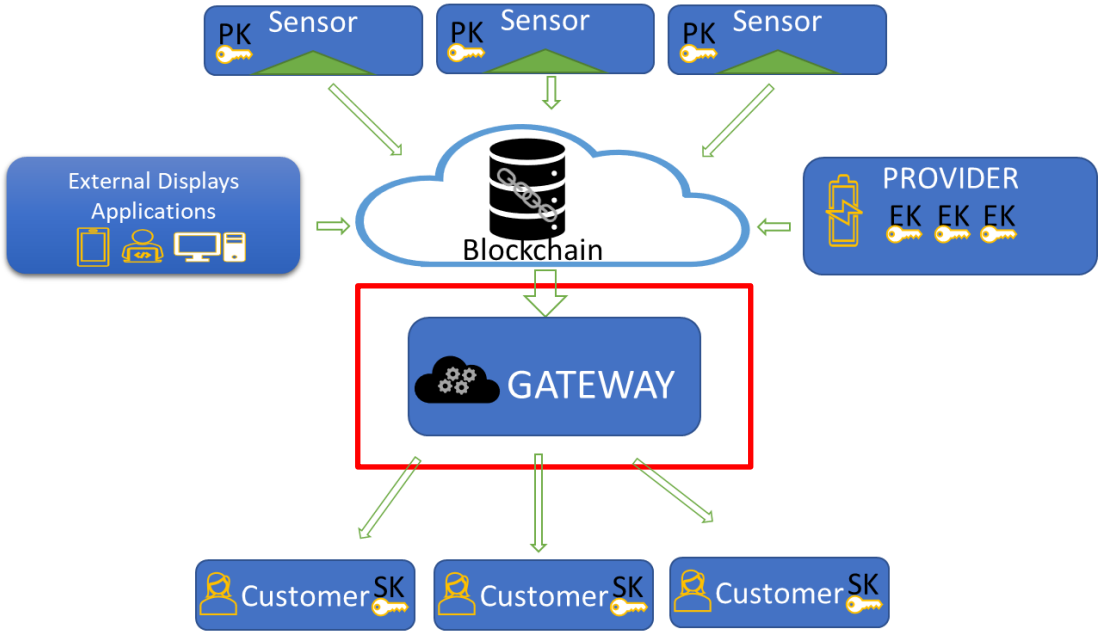
• Smart metering system based on
  • Functional Encryption
  • Blockchain Technology
	Reduce complexity of the system
	  • Achieve the required adequate level of metrological security
	  • Examine the limits and possibilities of blockchain and functional encryption on a simplified model of smart meter
		• Guarantee the data authenticity and privacy
		• Integrity of the algorithm establishing confidence in correctness of measurements

Proposed Concept (Sensor)



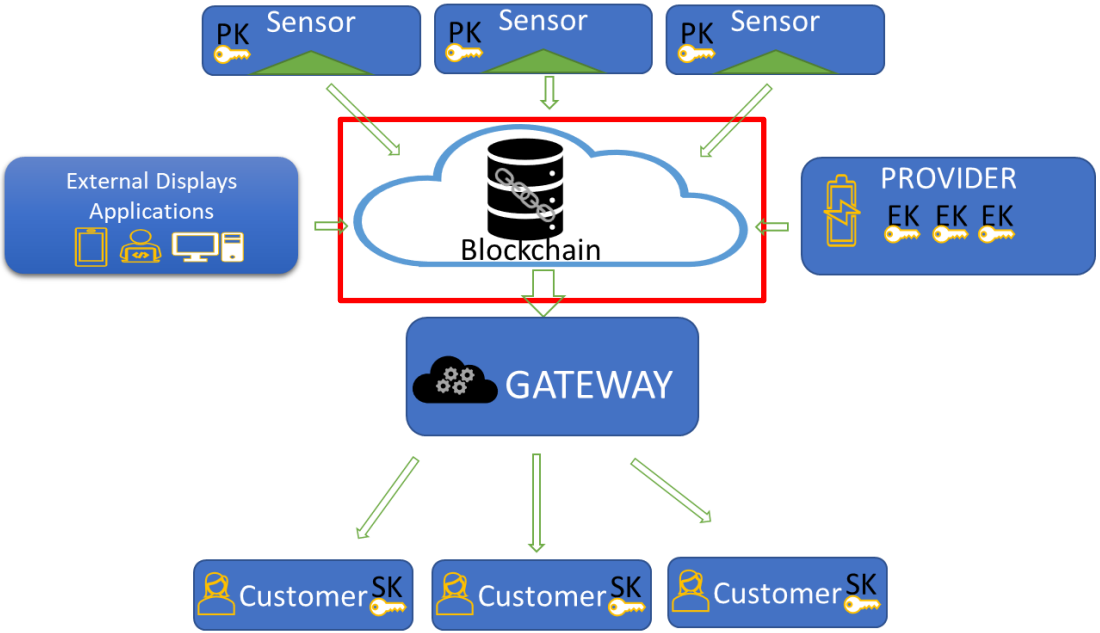
- Classic smart metering system consists of several sensors
- Produce measurement values in given time intervals.
- Here Sensors are classified as trustworthy
- Regularly checked for manipulation by market surveillance.
- Sensors are connected to a gateway

Proposed Concept (Gateway)



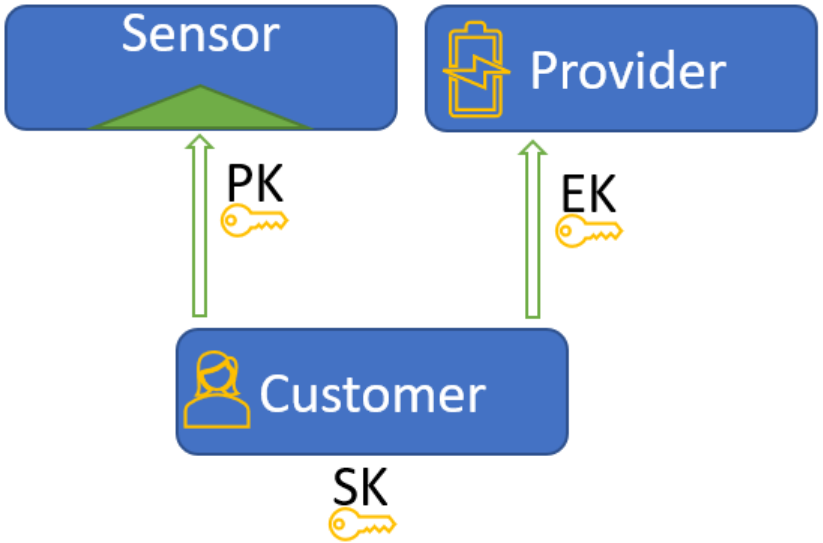
- Gateway represents the central unit, used for storing and further processing of measurement data.

Proposed Concept (Blockchain)



- Blockchain is an immutable and redundant storage for measurement data
- Privacy of measurement data is guaranteed by encryption

Functional Encryption



SK= generated randomly
PK= generated from SK using random algorithm
EK = Combination of function description and SK

- Functional encryption, similar to homomorphic encryption, allows calculations to be performed on encrypted data.
- However, the functional encryption provides a plaintext result of the calculation.
- Guarantees the integrity of the algorithm because the evaluation key is tied to the function.

Hyperledger Fabric

Hyperledger Fabric is a Blockchain Framework implementation And one of the Hyperledger Projects hosted by the Linux Foundation.

- Modular Architecture.
- Permission Based
- Membership Service Provider (MSP)
- Channel Feature
- Chaincode as Smart Contract
- Endorsement Policy

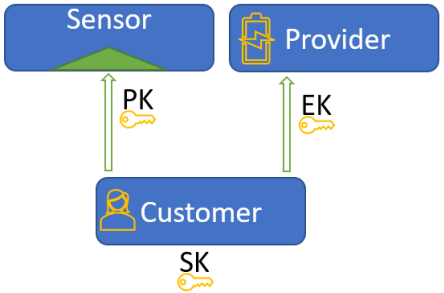
https://www.hyperledger.org/use/fabric

Implementation goals

- Find performance bottlenecks using minimal configuration of Hyperledger Fabric
- Determine Encryption overhead
- Check the practical feasibility considering given limitations

(e.g., reduced computing capacity of measurement device, timing constraints etc.)

Blockchain



Functional Encryption

Results

- Peer-container seems to reach the limit at 8 clients
- Encryption overhead depends on key size, but is significantly shorter than blockchain transaction time
- The presented solution is practicable even under minimal conditions.
- Assuming the higher computing capacity of the blockchain network, the solution could also be scaled in a larger context.

Use-Case #2:

When Measurements Meet Blockchain: On Behalf of an Inter-NMI Network

Moni, M.; Melo, W., Jr.; Peters, D.; Machado, R. When Measurements Meet Blockchain: On Behalf of an Inter-NMI Network. Sensors 2021, 21, 1564. https://doi.org/10.3390/s21051564

Public-Key Infrastructure (PKI)

- Requirement for digital certificates for smart meters
- Certification Authority (CA):
  - issues,
  - stores and
  - signs the digital certificates
- Register Authority (RA):
  - Verifies the identity and interface between the end user and the CA

Public-Key Infrastructure (PKI)

- Challenges and drawbacks on CA-based PKI
  - Depending on Trusted Third Parties (TTPs)
  - The management of digital certificates can be complex
  - PKI for smart meters can be very expensive

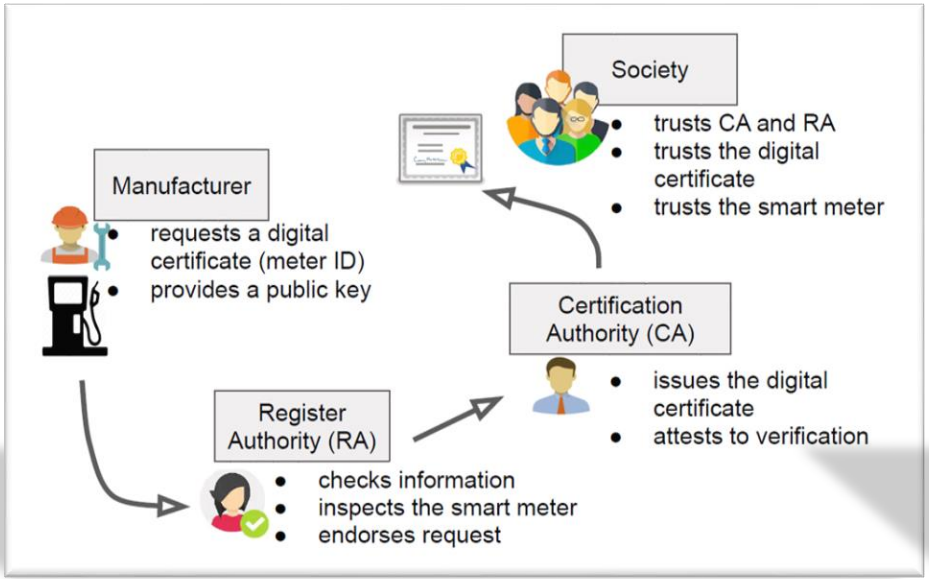
Melo, W., Jr.; Machado, R.C.S.; Peters, D.; Moni, M.
Public-Key Infrastructure for Smart Meters using Blockchains.
In Proceedings of the 2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT, Roma, Italy, 3–5 June 2020; p. 6.

PKI for Smart Meters

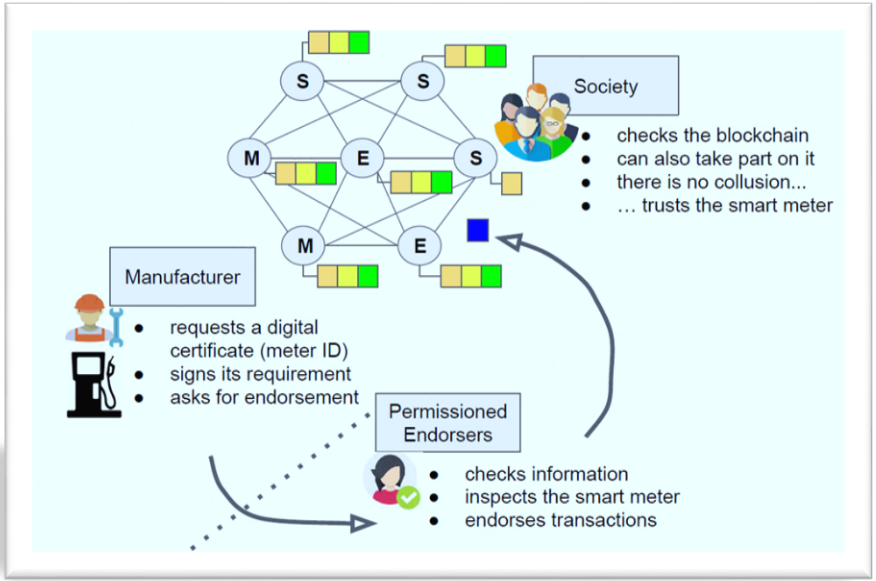
- Measurements and digital certificates
  - Assure integrity, authenticity and non-repudiation
  - Improve reliability
- Implications in Legal Metrology
  - Improve control activities related to software-controlled measuring instruments
  - Prevent frauds and tampering with measurements

Traditional CA vs Blockchain based PKI

Traditional CA-based



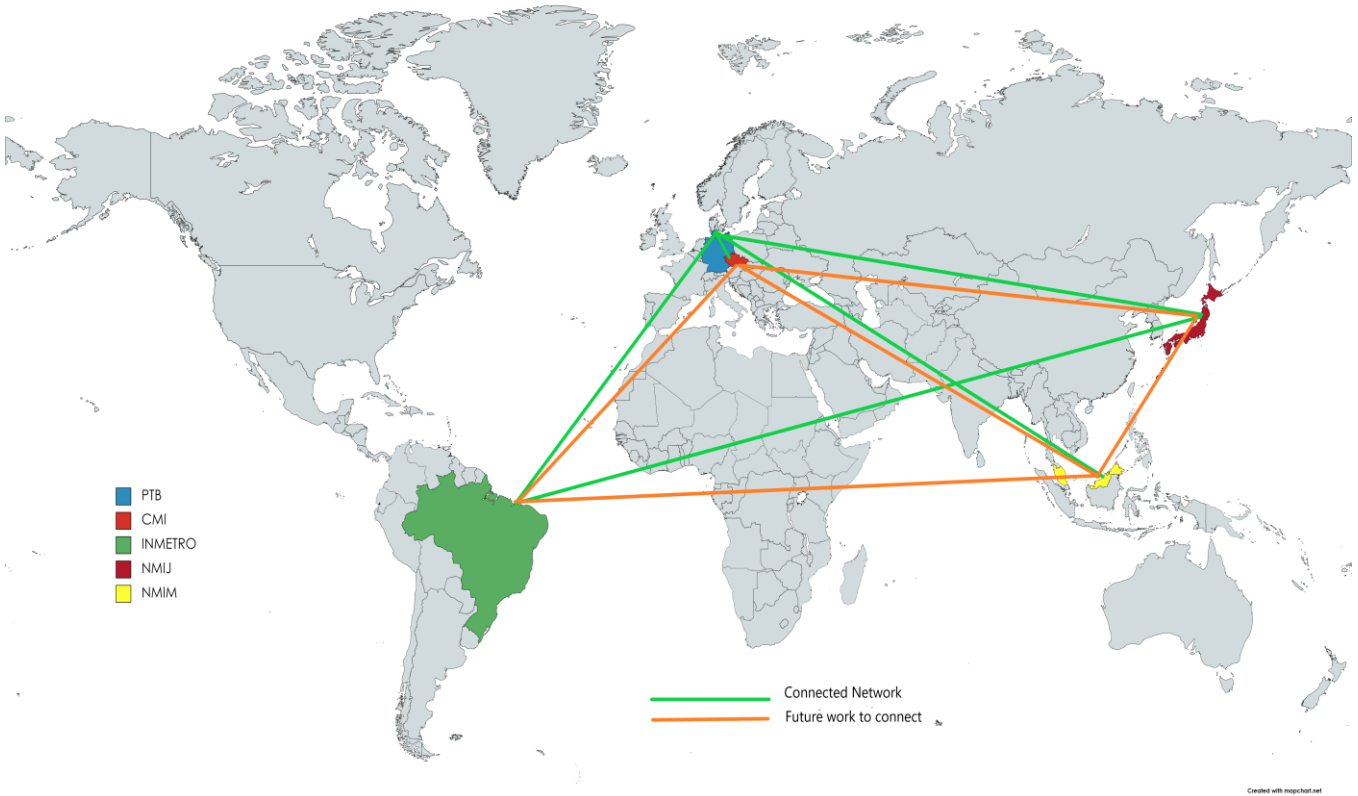
Blockchain-based



Proof-of-concept Implementation

- Blockchain network with 4 peers
- Generation of ECDSA (Elliptic Curve Digital Signature Algorithm)key pairs
- Experiment results
  - Registering the smart meters on the blockchain
  - Permissioned Endorsers insert the public keys
  - Smart contract verifies digital signatures, receiving the meter ID and the signature digest

Inter-NMI Network



Created with: https://www.mapchart.net/

5 nodes

(1) Physikalisch-Technische Bundesanstalt (PTB), Germany

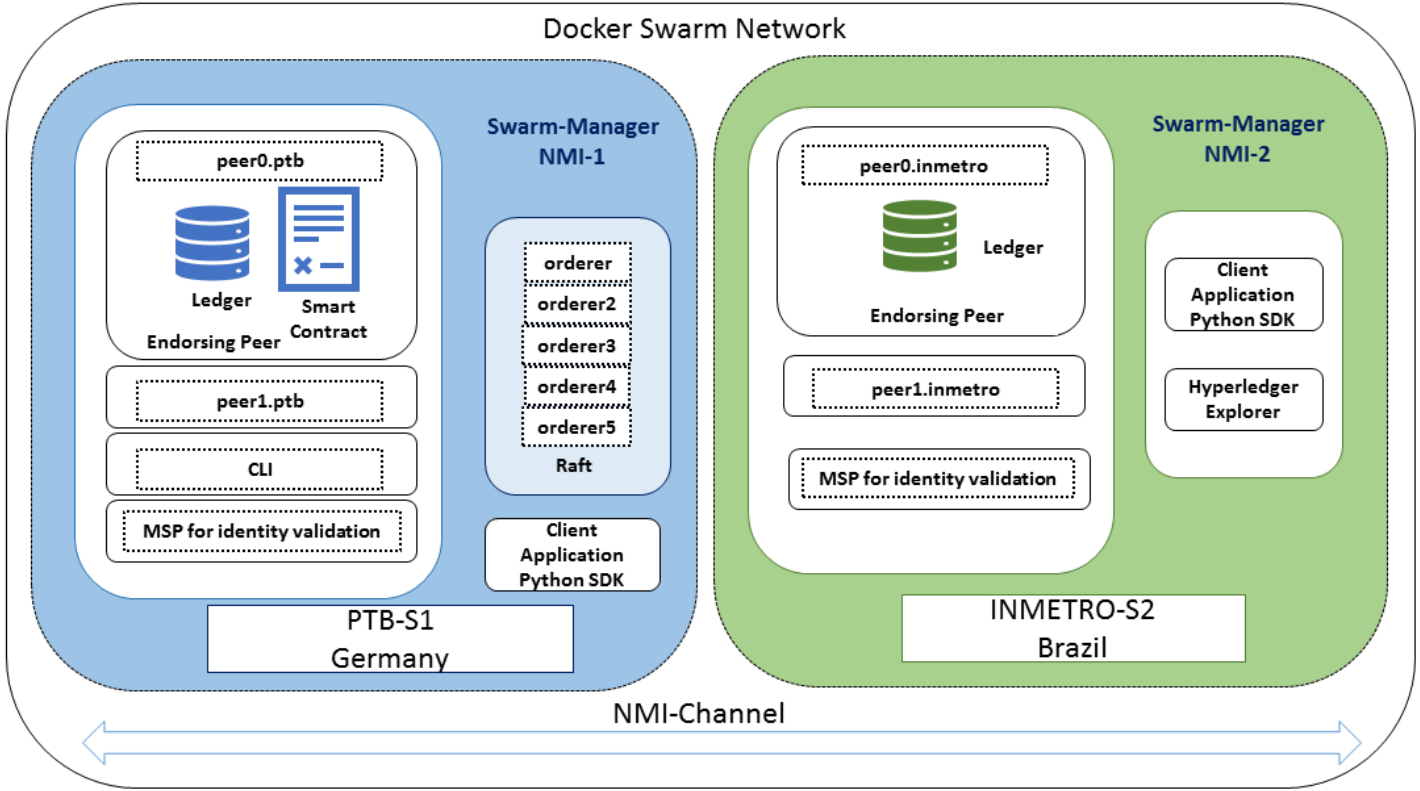
(2) Czech Metrology Institute (CMI), Czech Republic

(3) National Institute of Metrology, Standardization, and Industrial Quality (INMETRO), Brazil

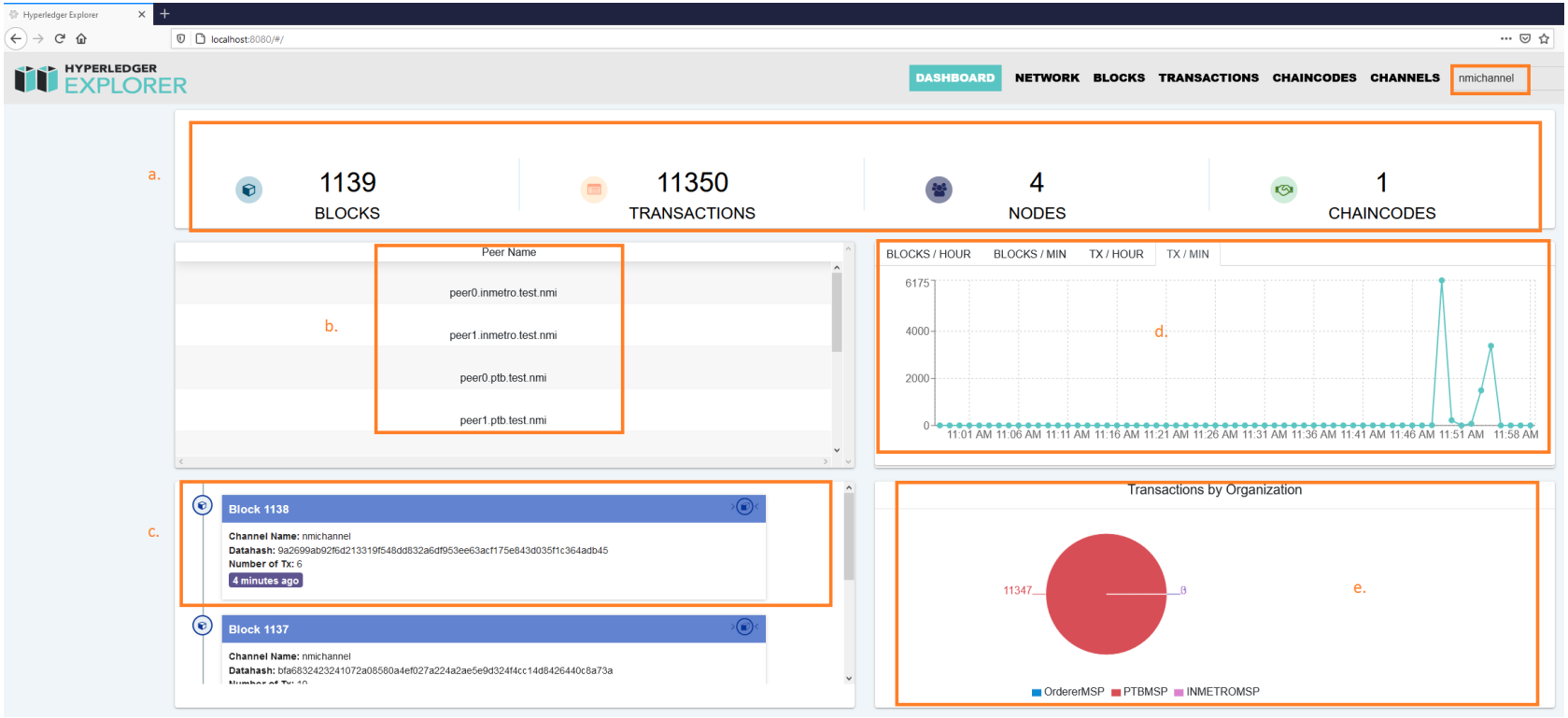
(4) National Metrology Institute of Japan (NMIJ), Japan

(5) National Metrology Institute of Malaysia (NMIM), Malaysia

International Network (Experimental)



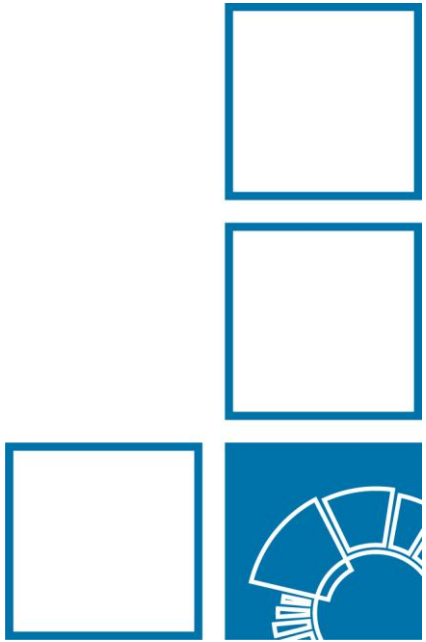
Performance Evaluation



Hyperledger Explorer https://github.com/hyperledger-labs/blockchain-explorer

Results

- Blockchain stores and attests public keys from smart meters;
- Meters sign their measurements using the respective private key
- No extra cost with digital certificates;
- Solution does not depend on a trust third party (TTP).
- Blockchain do not eliminate PKI rather interdependent technologies.



Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin
Abbestraße 2 - 12
10587 Berlin

Mahbuba Moni
E-Mail: mahbuba.moni@ptb.de
www.ptb.de