WP3: Technology based Metrological Support Services

Daniel Peters, PTB
**WP 3: Technology based Metrological Support Services**

**Responsibility:** PTB, Daniel Peters

**Expected Deliverable:**

To develop new technology-driven *metrological support services* utilizing the digital representation.
WP3: Main Tasks

(1) Integration of Smart Contracts

(2) Support Services:

- Remote Verification
- Remote Software Maintenance
- Digital (e-)Verification Marking (COM2014/25)
- Digital Application for Verification
(1) **Integration of Smart Contracts**

(2) **Support Services:**

- Remote Verification
- Remote Software Maintenance
- Digital (e-)Verification Marking (COM2014/25)
- Digital Application for Verification
Majority of future measurement instruments will be connected to the internet, some of them will have a fully distributed character

Consequence:
Software bugs and novel threats make software updates indispensable, especially for network-connected devices

Current situation:
Even small changes on software could require a recertification process
Distributed Network by Design

Trustworthy Coordinating Platform

- Metrological Administration
- Digital Representation
- Shared Databases

Stakeholder Control

Stakeholder → Trusted-Node

Trusted-Node:
Trusted Metrological Architecture, e.g. provided by PTB, supervised by MA
Do we need a Blockchain?

- Is there a trusted third party?  
  - NO
  - Are there multiple users?  
    - NO
    - Are the users known?  
      - NO
      - Are the users trustworthy?  
        - NO
        - Consider a permissionless blockchain
        - YES
        - Consider a permissioned blockchain
      - YES
    - YES
    - You do not need a blockchain
  - YES

Wüst and Gervais, „Do you need a blockchain?“ In: Cryptology ePrint Archive, 2017/375
1. Clients send transactions.

2. Peers decide about new blocks.

3. Peers propagate and store the blocks in a chain.
Smart Contracts and DAOs

- Smart contracts are **computer programs** that can make decisions when certain conditions are met
- Concept was introduced by Szabo in 1996
- Blockchain offers a suitable medium for implementation
- A Decentralized Autonomous Organization (DAO): both humans and devices can cooperate with each other
- DAO actions are based on rules and processes dictated by smart contracts, as well as ownership relationships that are registered in a blockchain
Client Application
- Invoke and query the chaincodes
- Registry for events

Blockchain Network
- Create or join to a channel
- Install and upgrade chaincodes
- Instantiate chaincodes

Hyperledger Fabric

Chaincode Application
- Implement business rules
- Access the ledger (read/write)
- Emit events (notify)
• A complete **permissioned** blockchain platform
  - Hyperledger: a group of projects
  - Hosted by the Linux Foundation

• Modular platform
  - **Chaincode** = smart contracts
  - Consensus is an independent module (plugin)
  - Concepts of **endorsement** and **validation**
Our Currently Implemented Experiment

- **PTB**
  - Instantiate chaincode
  - Install chaincode
  - Invoke chaincode (encrypted)

- **endorser peers**

- **manufacturer**
  - Query chaincode (encrypted)

- **consumer**
  - Query chaincode (encrypted)

- **smart meters**
  - OPC-UA measurements (plain text)

- **gateway**
The Communication Procedure

1. Ask for endorsement (encrypted measurements)
2. Execute chaincode (homomorphic computing)
3. Return endorsement (encrypted result)
4. Prepare transaction
5. Encrypt measurements
6. Check endorsement
7. Broadcast transaction (encrypted result)
8. Order and validate transaction
9. Store encrypted measurements into the distributed ledger
Digitally transformed processes in Legal Metrology: (MC WP 3)
Infrastructure foundation for, e.g. Experimental Blockchain/Smart Contract applications.

If you like to join, please contact us!
Challenges ahead

- Implement FHE and PCP as chaincodes
- Create and maintain a inter-NMI blockchain network to research and experiments
  - PTB, Inmetro, NMIJ, …
Supporting Software Maintenance

Standard Procedure  § 40 (3) MessEV, (WELMEC Guide 7.2 Extension D)

1. Update available
2. Conformity of Update and Download Mechanism granted
3. Application/Update granted
4. Ensemble Test

Samples

Manufacturer

Verification Authorities

Notified Body

User

Instruments in use

Smart Contract

Conditions 1…n

Process

Result

16
Blockchain technology is **disruptive** and in its beta stage.

Very **promising**, because **legal metrology** directives and guides formulate many requirements, e.g., parameter integrity for the measuring instrument, durability of measurement result, and possibilities to identify transactions, which can all be fulfilled by a blockchain.

Examples are an update process and a decentralized audit trail.

**Challenges:**

- Embedded devices should handle the huge amount of data.
- Many approaches like **Proof-of-Work** and **Proof-of-Stake** algorithms, or even other technologies, e.g. **DAG-systems**, **Hashgraphs**.
(1) Integration of Smart Contracts

(2) Support Services:

- Remote Verification
- Remote Software Maintenance
- Digital (e-)Verification Marking (COM2014/25)
- Digital Application for Verification
(1) manufacturer calculates a cryptographically secured mathematical model (no source code needed) of the core measurement algorithm (called proof)

(2) Since the reconstruction of source code from proof by reverse engineering is not feasible, the signed proof could be saved by trusted entity and made publicly available
Current Security Architecture

- physical seal helps to recognize hardware-manipulation
- checksum as software integrity measure
- checksum is not flexible in case of updates
- checksum-routine could be manipulated to hide the changes on metrological software
- checksum is difficult to apply to distributed systems
Naive Approach

**rough idea:**
Only the raw sensor data and display value needed to verify each single measurement by reexecuting the core algorithm

**disadvantages:**
- the core algorithm is an intellectual property and should remain secret
- the raw sensor data and the display value are subject of privacy
- the manipulation of core algorithm could have a data-selective behaviour
Using Mathematical Proofs

**Verification process:**

1. Customer retrieves the proof from trusted entity by scanning a device-specific QR-code on device display.

2. Scanning another QR-Code with encrypted sensor data and display value.

3. The proof (1) and measurement data (2) get automatically combined. The result shows if the measurement was correct or not.

\[ \text{proof} + \text{QR} = \text{V or X} \]
Current advances in cryptography especially in the area of verifiable computing make novel methods for validation of algorithms possible, especially:

- Zero knowledge-proofs
- Probabalistic checkable proofs
- Homomorphic encryption and signatures
- Functional encryption
- Blockchain technology

A combination of these techniques allows us to provide a flexible verification solution to preserve algorithm privacy and data privacy at the same time.
Advantages at a Glance

- software updates possible as long as core algorithm is not changed
- improved security (compared to hashes (checksums))
- new software validation services provided to customers

- comfortable way to verify the measurement
- immediate result
- advanced data privacy compared to other methods

- simplification of software update process
- an alternative way for validation of distributed measurement instruments
- security improvement compared to checksums

- more comfortable verification process
- advanced complaint management possible
- possibility of remote software verification based on anonymous user data
Next steps:

Exemplary core algorithm implementation based on a simple measuring instrument

Cooperations are welcome!
Separating transaction endorsement from consensus

- Dedicated endorsers per chaincode
- Consensus service: Ordering for endorsed tx

Auditing at:
- System level, i.e., all system transactions
- User level, i.e., a user's transactions
- Contract level, i.e., contracts messages

https://www.biggerpockets.com/member-blogs/10586/70715-intro-to-the-hyperledger-project