Côte d'Azur Blockchain Stampede

Industrial IoT blockchain: Evolution and performance

Luc Gerrits, Roland Kromes

University Cote d'Azur, LEAT / CNRS UMR 7248 (France)

Blockchain evolution and IoT optimization

Presented by Roland Kromes

IoT integration with Blockchain

- IoT hardware architectures/devices :
  - ***Constrained*** devices with ***limited*** frequency, ***limited*** battery lifetime, ***limited*** computational power, and ***limited*** memory for data storing.
- **Blockchain** technology needs a ***high*** computational power and its ***data*** increase ***infinitely*** (e.g Bitcoin uses now approximately 230 GB !)

Adaptability issues on IoT architectures. How to integrate IoT architectures and networks to the Blockchain technology ?

Introduction

- The thesis take part in the Smart IoT for Mobility project [1]

The infrastructure:

- Cars are connected on the blockchain.
- If an accident happens the car sends the measured data to the blockchain.

Vehicle equipments:

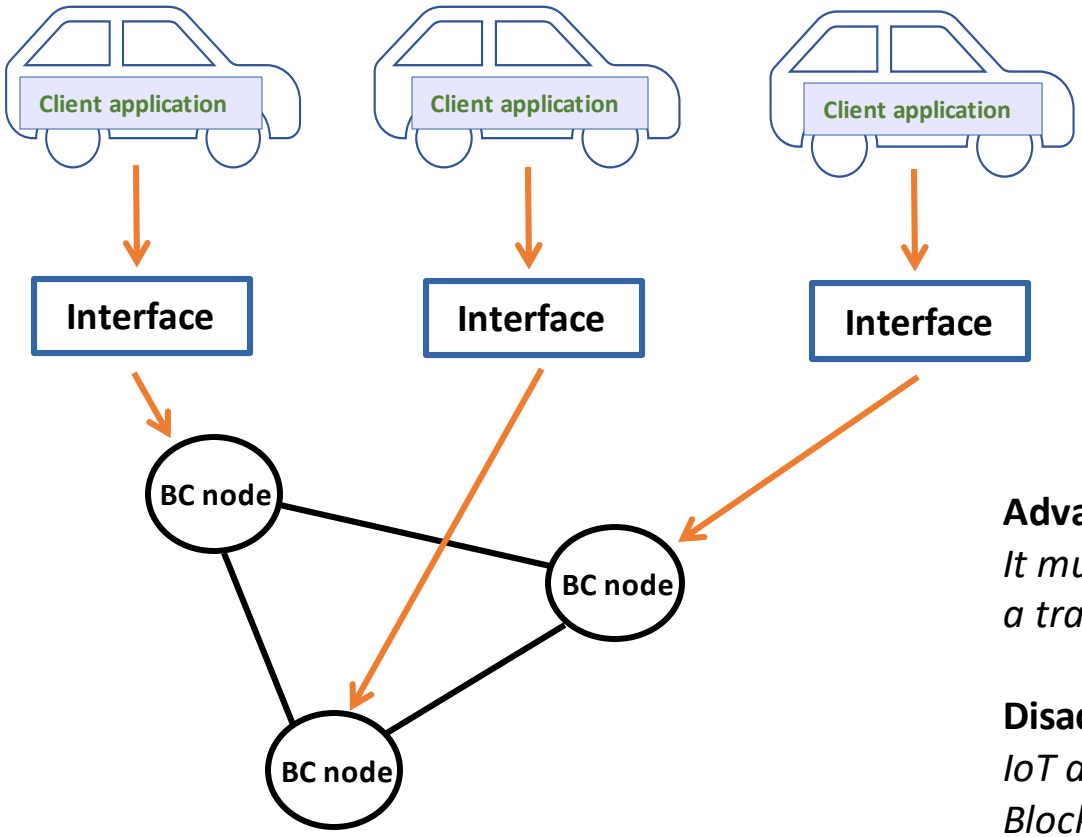
- Odometers (measure the mileage)
- Radars (detecting the safe-distance)
- 360° cameras
- Etc..

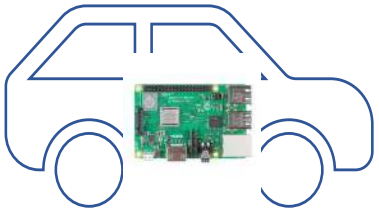
Idea:

- With Smart Contract we can provide a full traceability of the sent data in the accident case.
- Smart Contracts can make easier and faster the insurance and refound procedure.

[1] F.Verdier et al. Smart iot for mobility: Automating of mobility value chain through the adoption of smart contracts within IoT platforms. In17th Driving Simulation & VirtualReality Conference (DSC), 2018

Blockchain – IoT basic network structure





Car **equipped with an IoT device**, which communicates with a blockchain-based network.

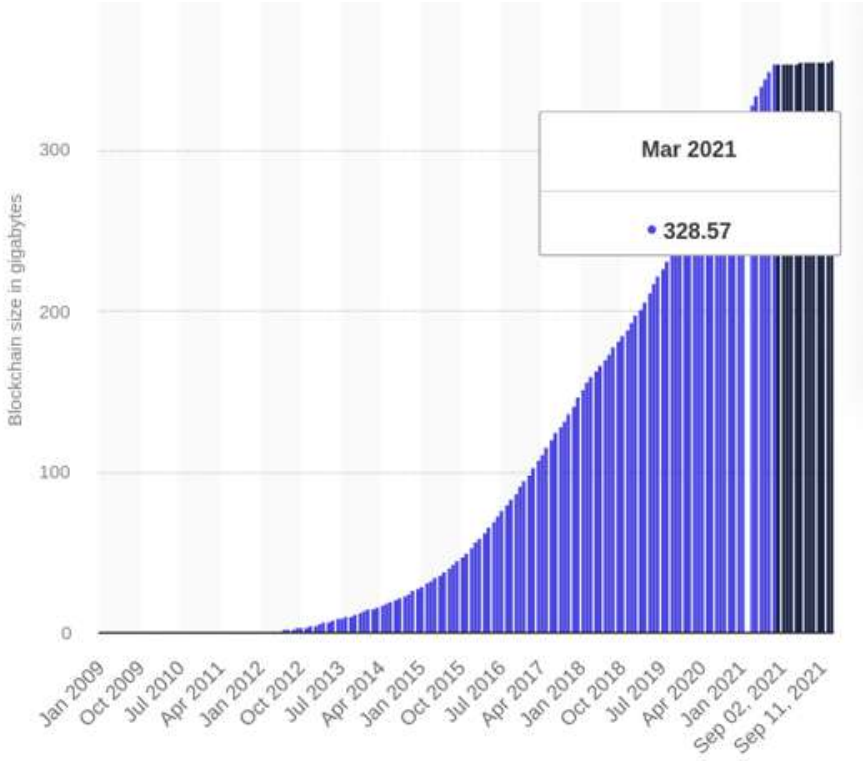
Advantage:
It must remain connected only for sending a transaction.

Disadvantage:
IoT does not take really/fully part in the Blockchain.

Client Application: Message creation and sending executed on IoT device embedded in the vehicle.

Blockchain – IoT improved network structure

- IoT device can send a large amount of data (vehicle sensors ~1MB to 1GB/Tx)
- Bitcoin 500Bytes/Tx

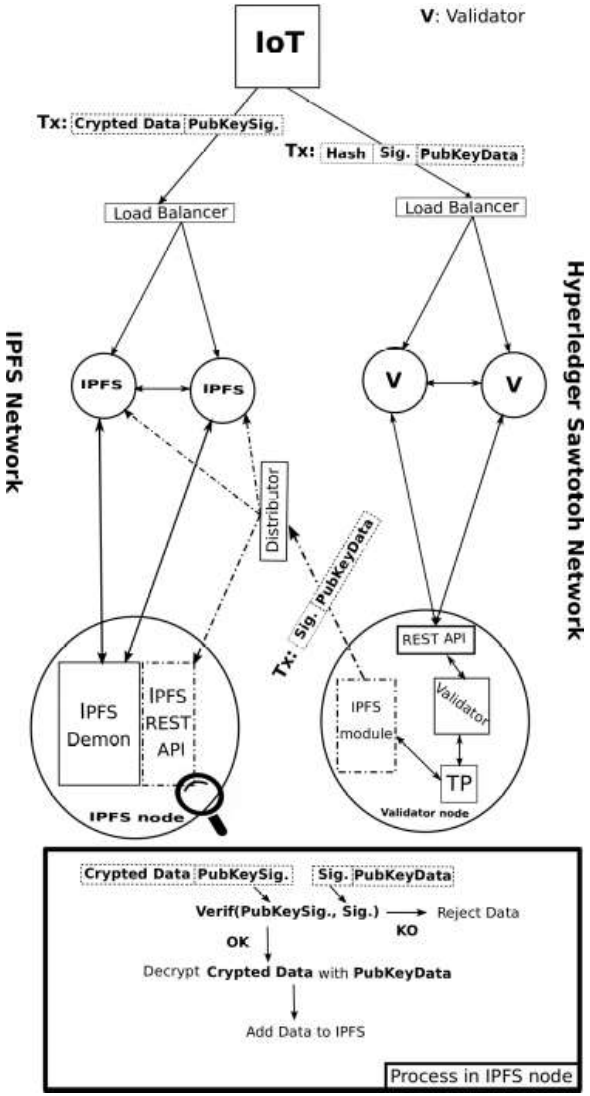


Increasing size of Bitcoin[2]

- Goal of the improved structure:
  - Optimize the increase of the blockchai's data size, but the structure remains decentralized

[2] https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

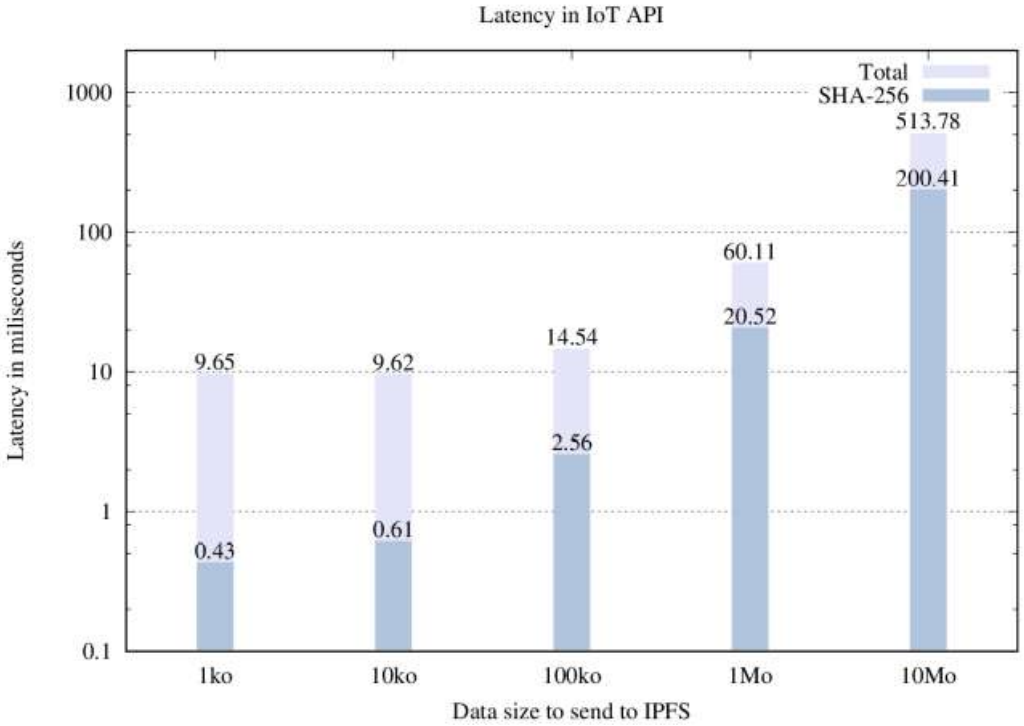
Blockchain – IoT improved network structure



- <u>Network components:</u>
  - Blockchain: **Hyperledger Sawtooth**
  - InerPlanetary Files System (**IPFS**) – Decentralized Storage system
  - **IoT** devices
- IoT device sends the ***hash*** of the data to the **Blockchain** and the raw data to **IPFS**
- ***Hash***: "fingerprint" of the data → pointer to the raw data in IPFS

Blockchain – IoT improved network structure

- ***Hash***: "fingerprint" of the data → pointer to the raw data in IPFS – (eg., ***SHA-256*** cryptographic hash function)



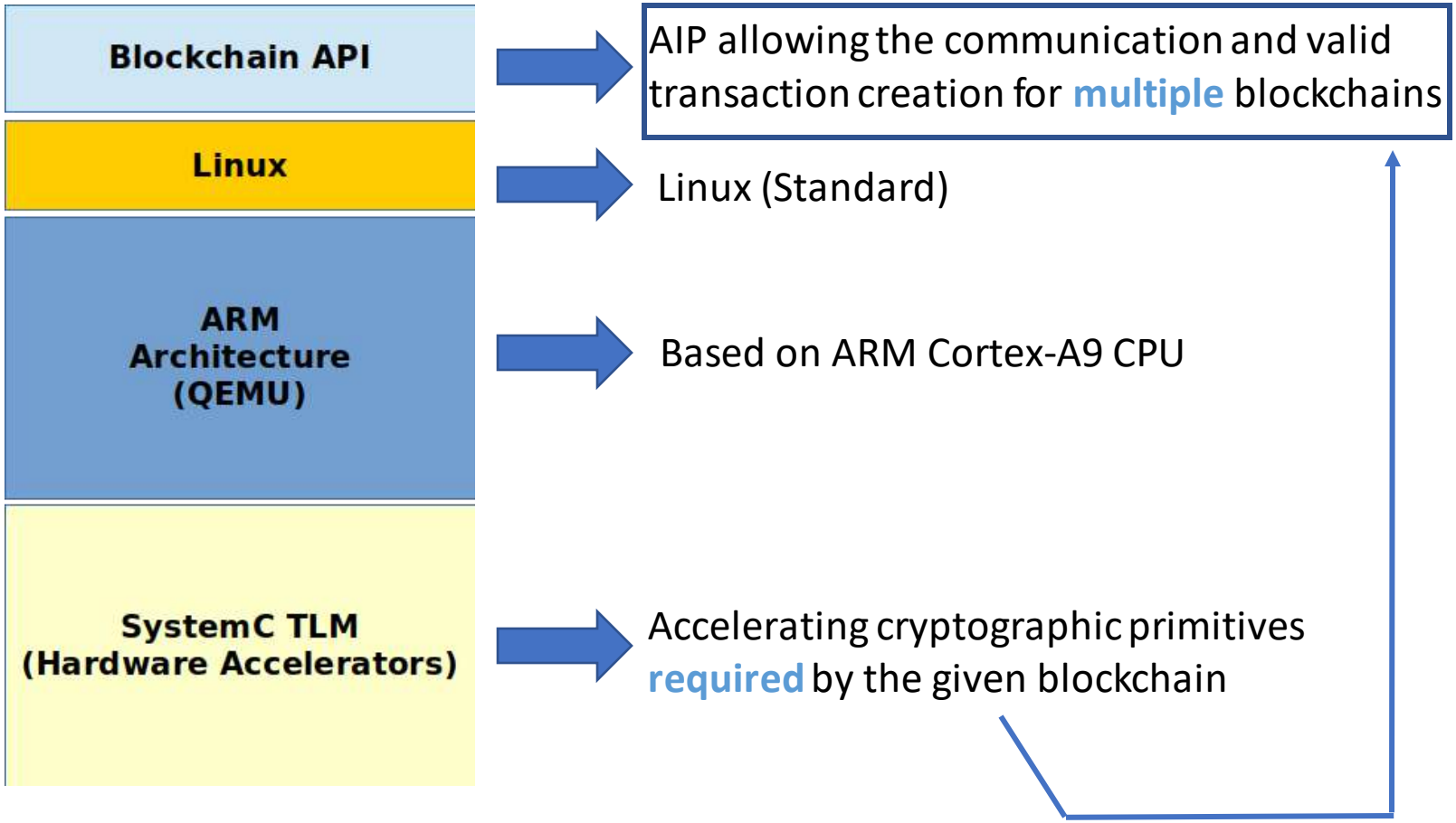
Influence of hash creation in the API executed on the IoT device [3]

When the data size is significant
→ the execution time increases
→ power consumption increases

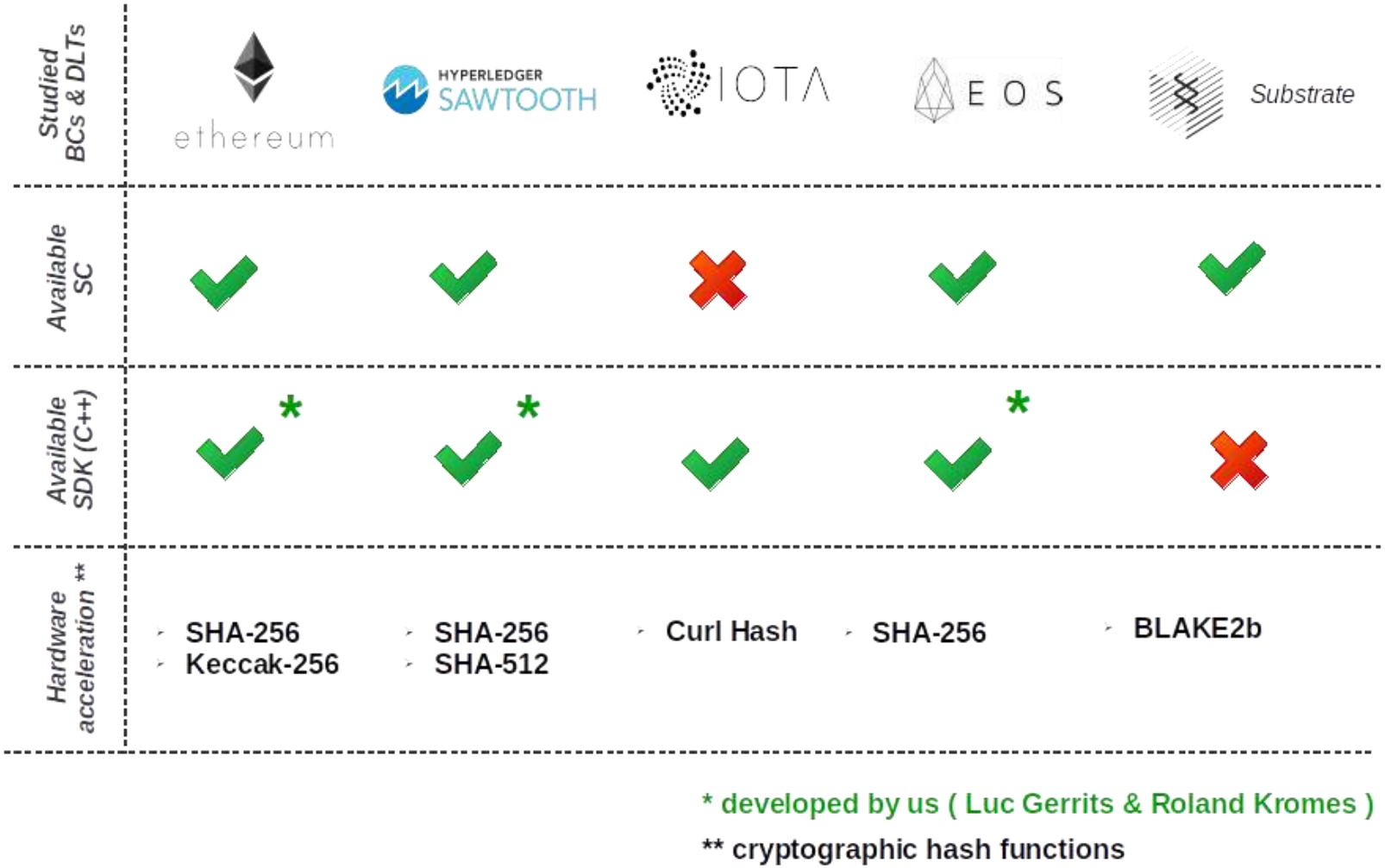
Designing a dedicated Low-Power consumption IoT architecture model

[3] L. Gerrits,R. Kromes, F. Verdier,A True Decentralized Implementation Based on IoT andBlockchain: a Vehicle Accident Use Case, COINS 2020 - IEEE International Conference onOmni-layer Intelligent Systems, Sep 2020, Madrid, Spain.

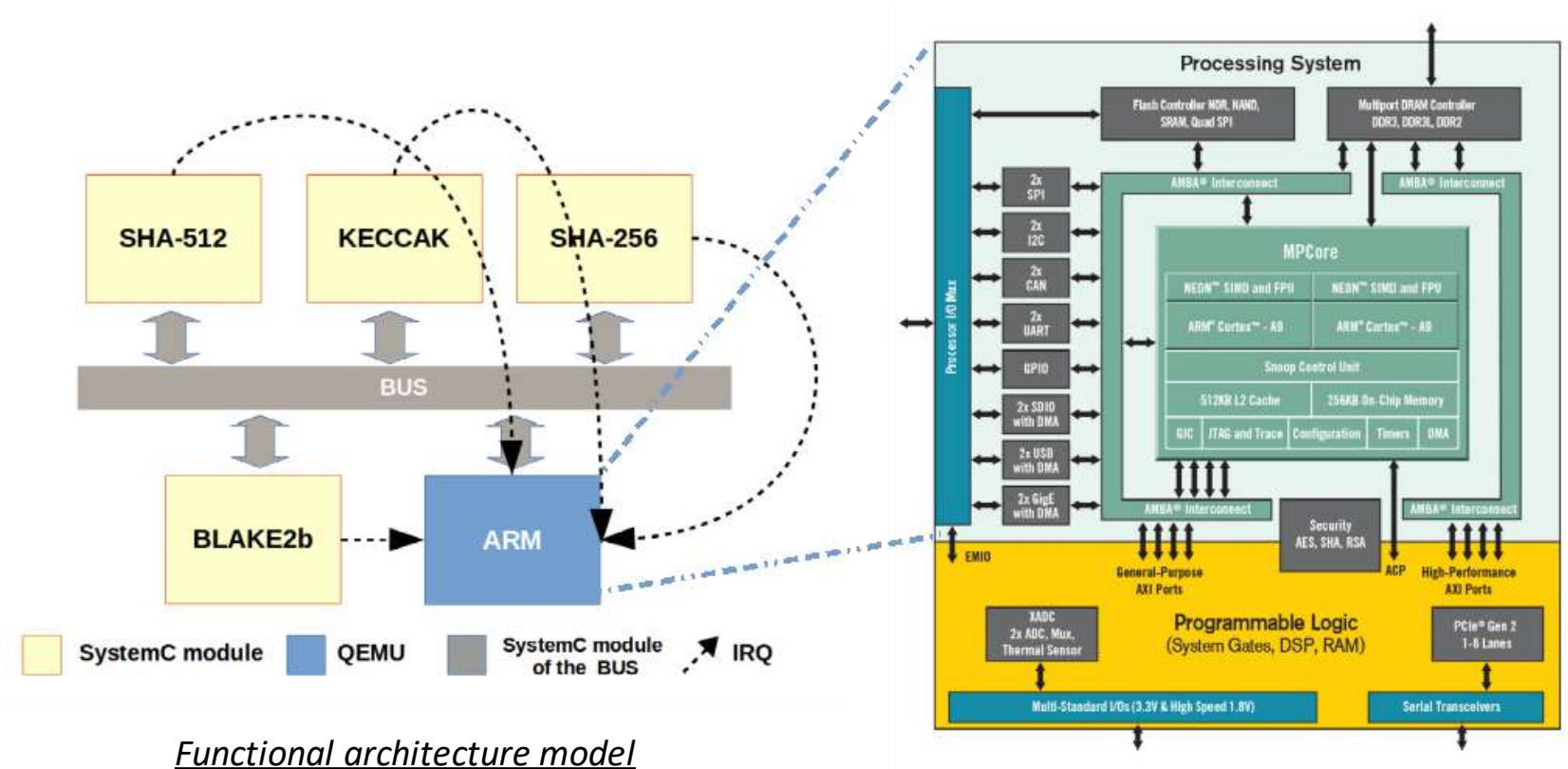
IoT Hardware Modelling and Requirements



Software development and Analysis



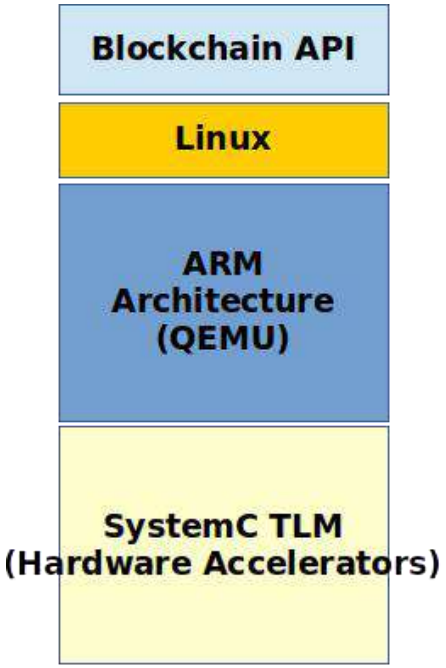
IoT Hardware Modelling and Requirements

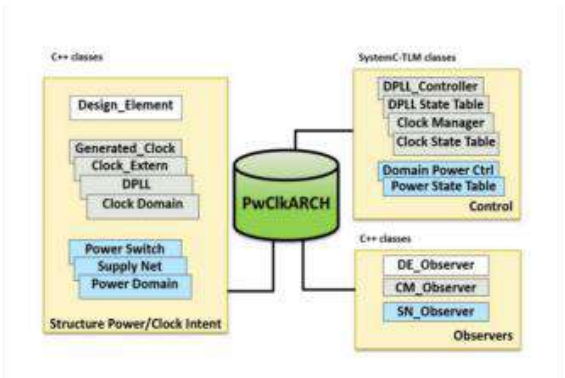


Functional architecture model

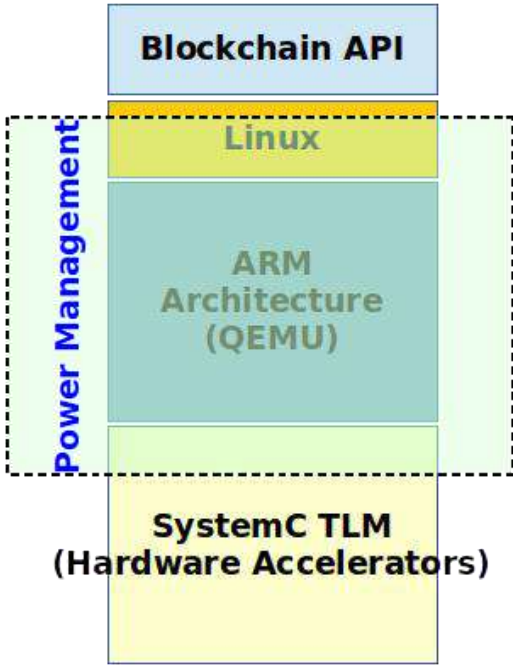
IoT Hardware Modelling and Requirements

Functional architecture model





Power Managed architecture model

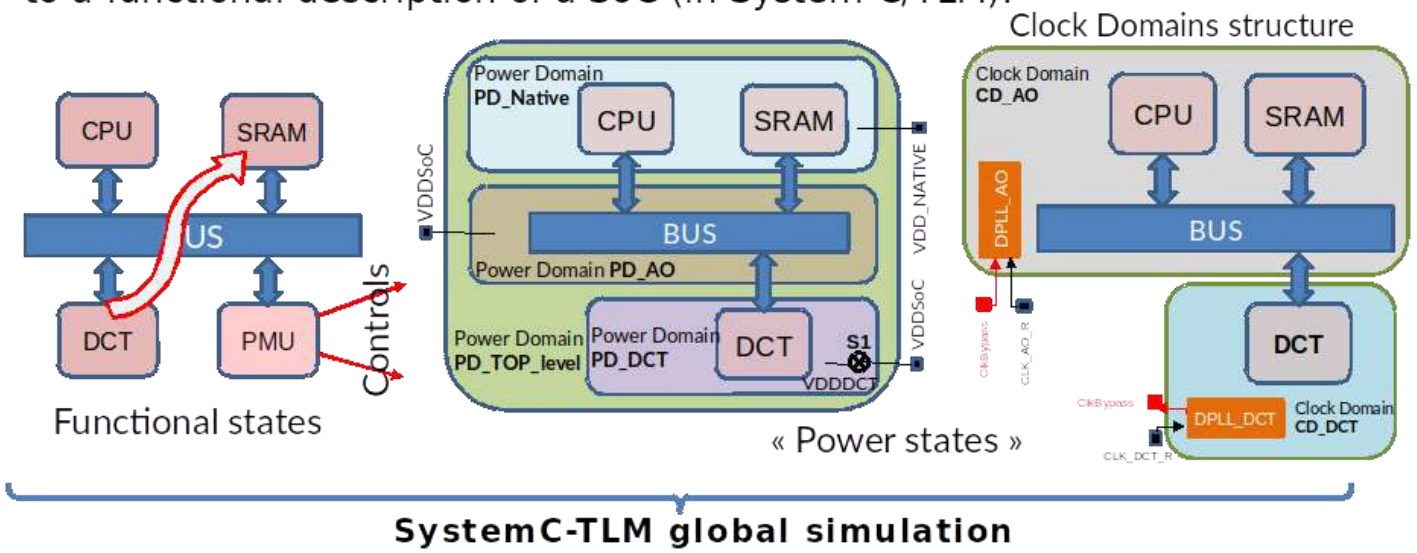


IoT Hardware Modelling and Requirements

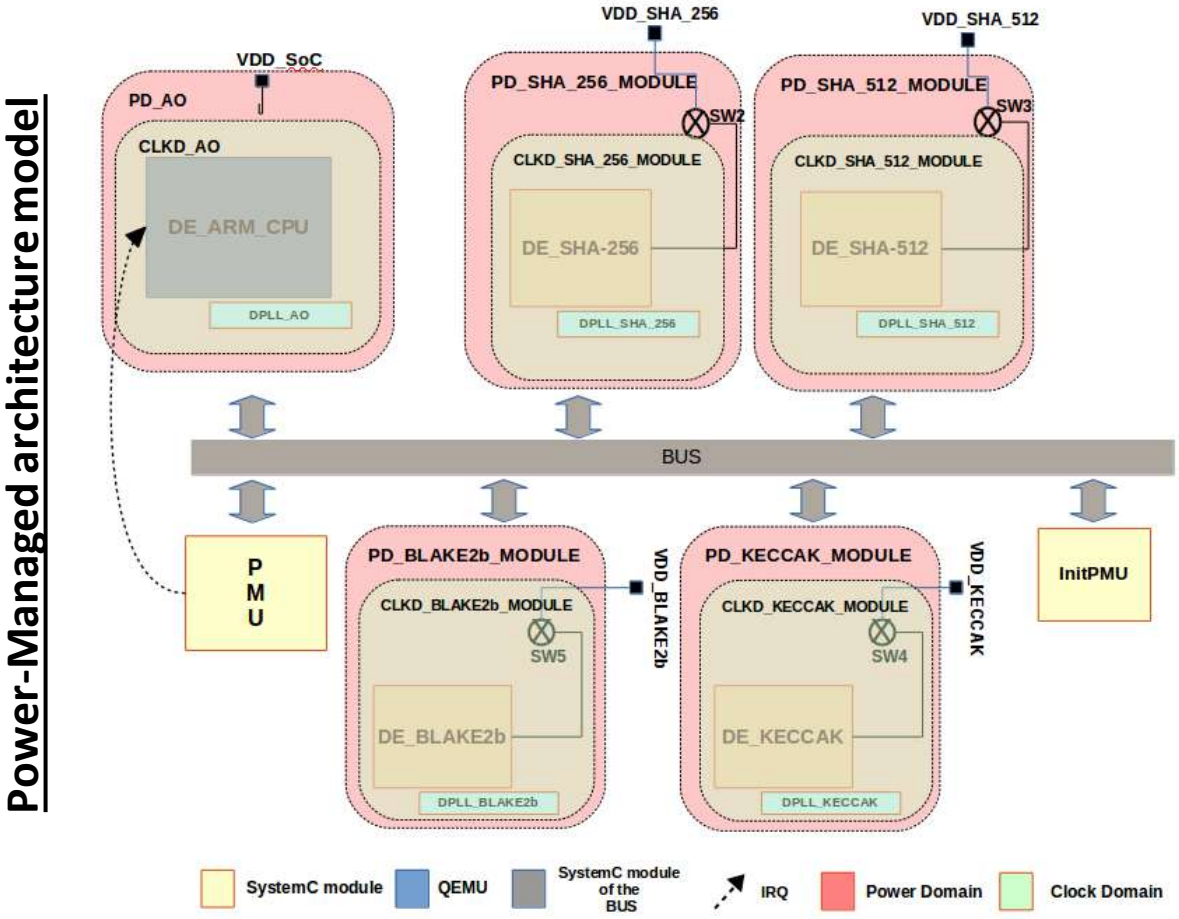
Power Management

PwClkARCH

Objective : Add **power/clock intent and its power management strategy** to a functional description of a SoC (in System-C/TLM).

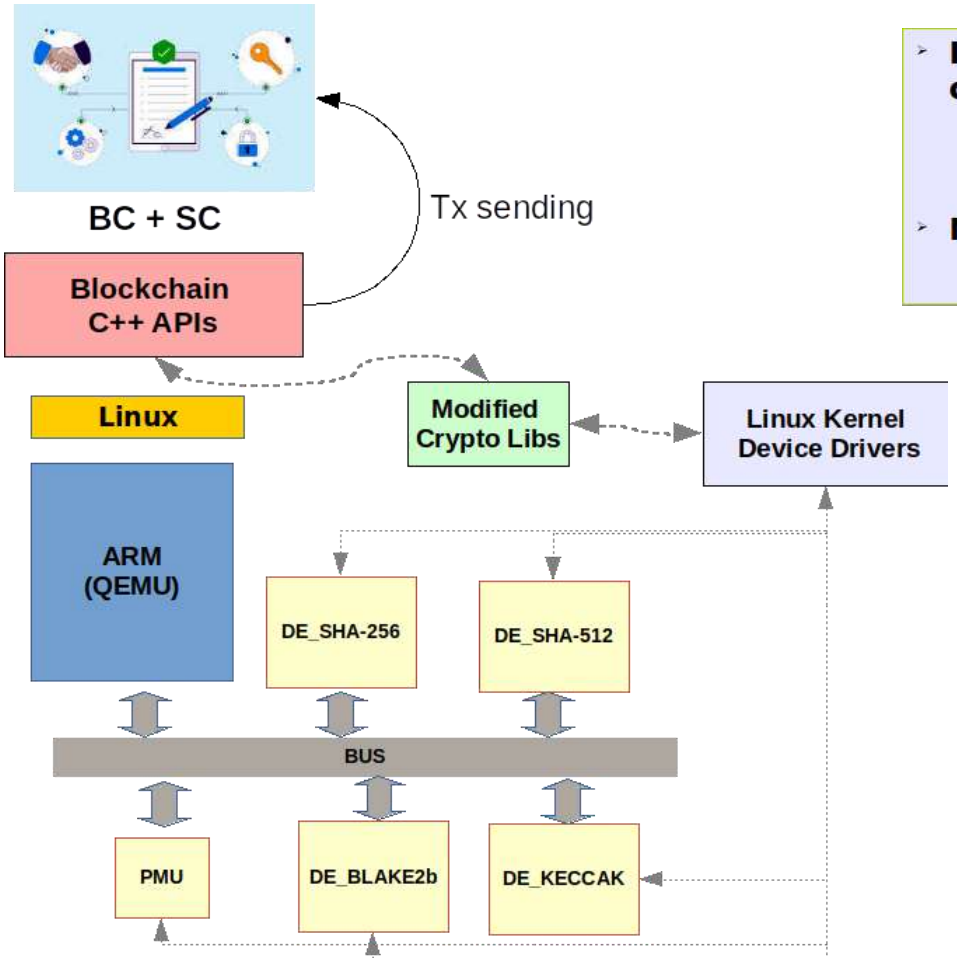


IoT Hardware Modelling and Requirements



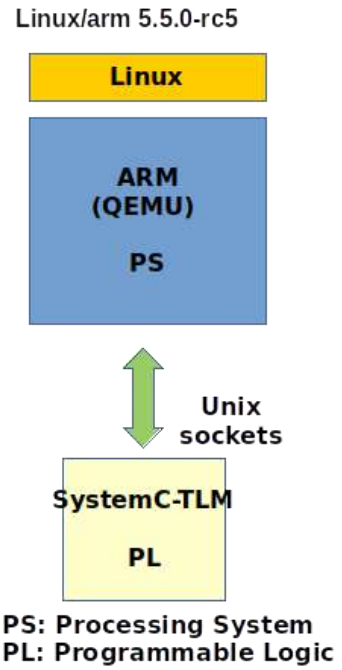
IoT Hardware Modelling and Requirements

Software development for hardware modeling



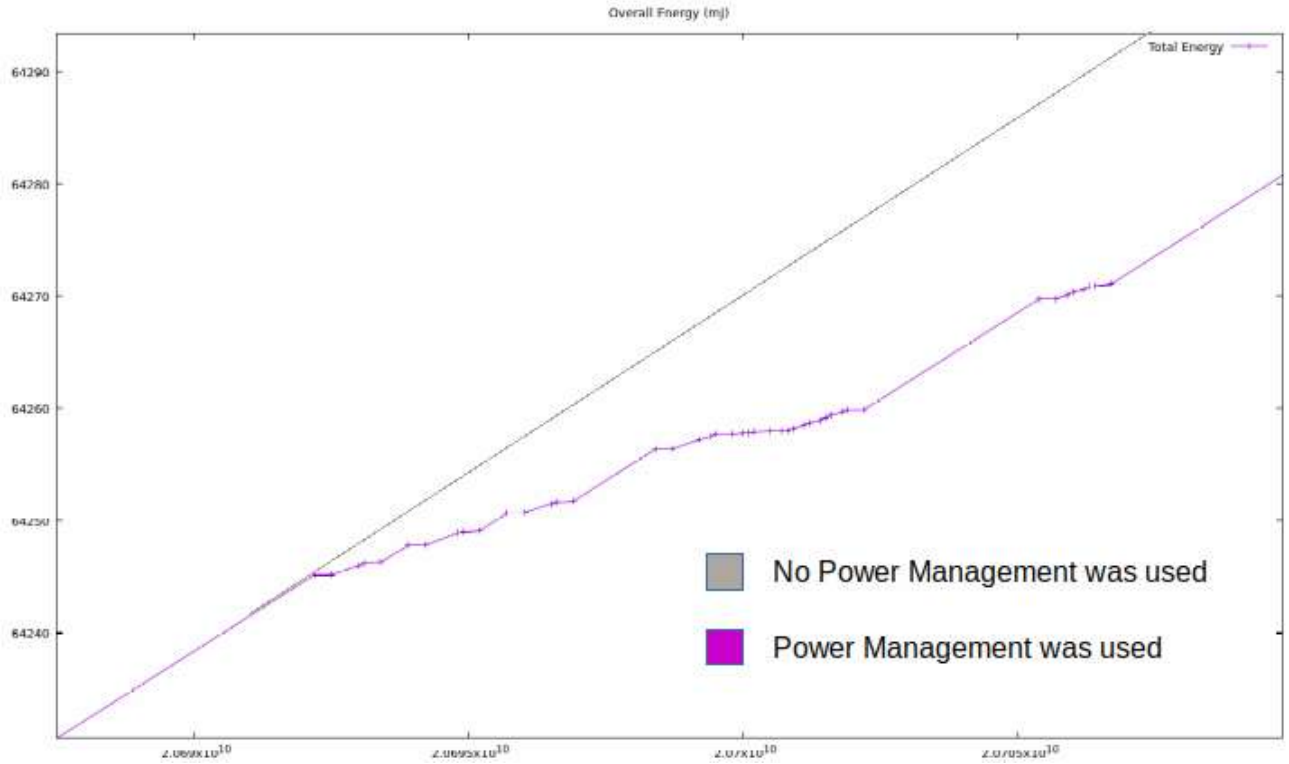
- **Implementation of Linux Kernel device drivers**
  - **Communication between Software and Hardware**
- **Modification of cryptographic libraries**

Early results



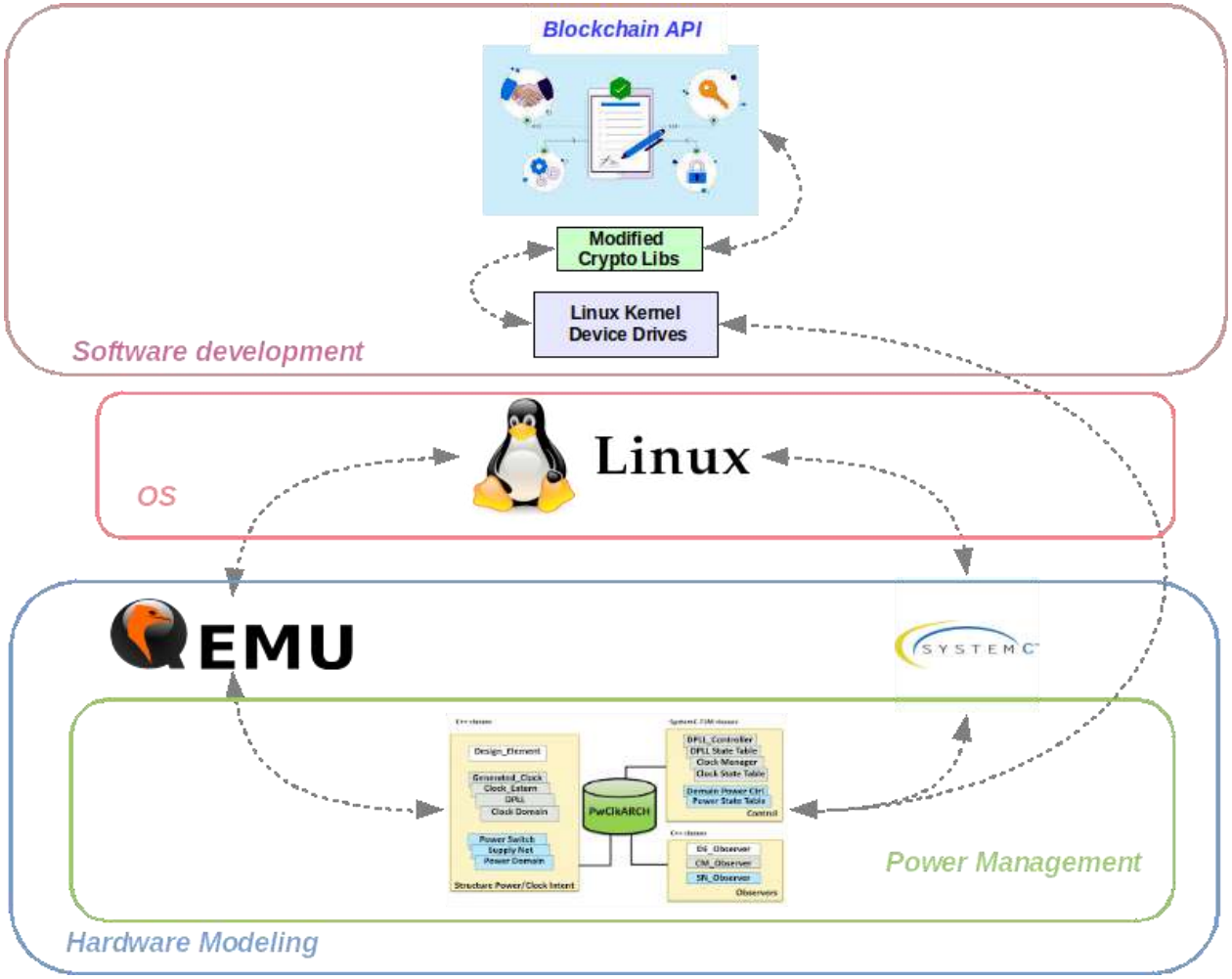
The proposed IoT hardware model with Power Management

- Running Hyperledger Sawtooth application:
  - Send a simply transaction



The total energy consumption (measured by PwClkARCH)

Overview of the Hardware and Software development



Use-case blockchain performances in a cloud

Presented by Luc Gerrits

What is “performance”?

Transaction speed/rate

- Throughput = Transaction per second sent to the blockchain
- Commits per second = finalized rate = Transaction added into the blockchain ledger permanently
- Transaction processing = transaction execution latency, can vary depending smart contract implementation

➢ In some cases Blockchain scalability can be a synonym of transaction speed

What can impact transaction speed?

Scalability

- **Limitation of the number of** participants
  →Typically related to blockchain consensus algorithm
- Peer-2Peer (P2P) networking efficacity = Optimization of new block distribution in the network
- **Forks in the chain**

Security

- Security **limitation** (cryptography,)
- **Expected resilience to evil actors**

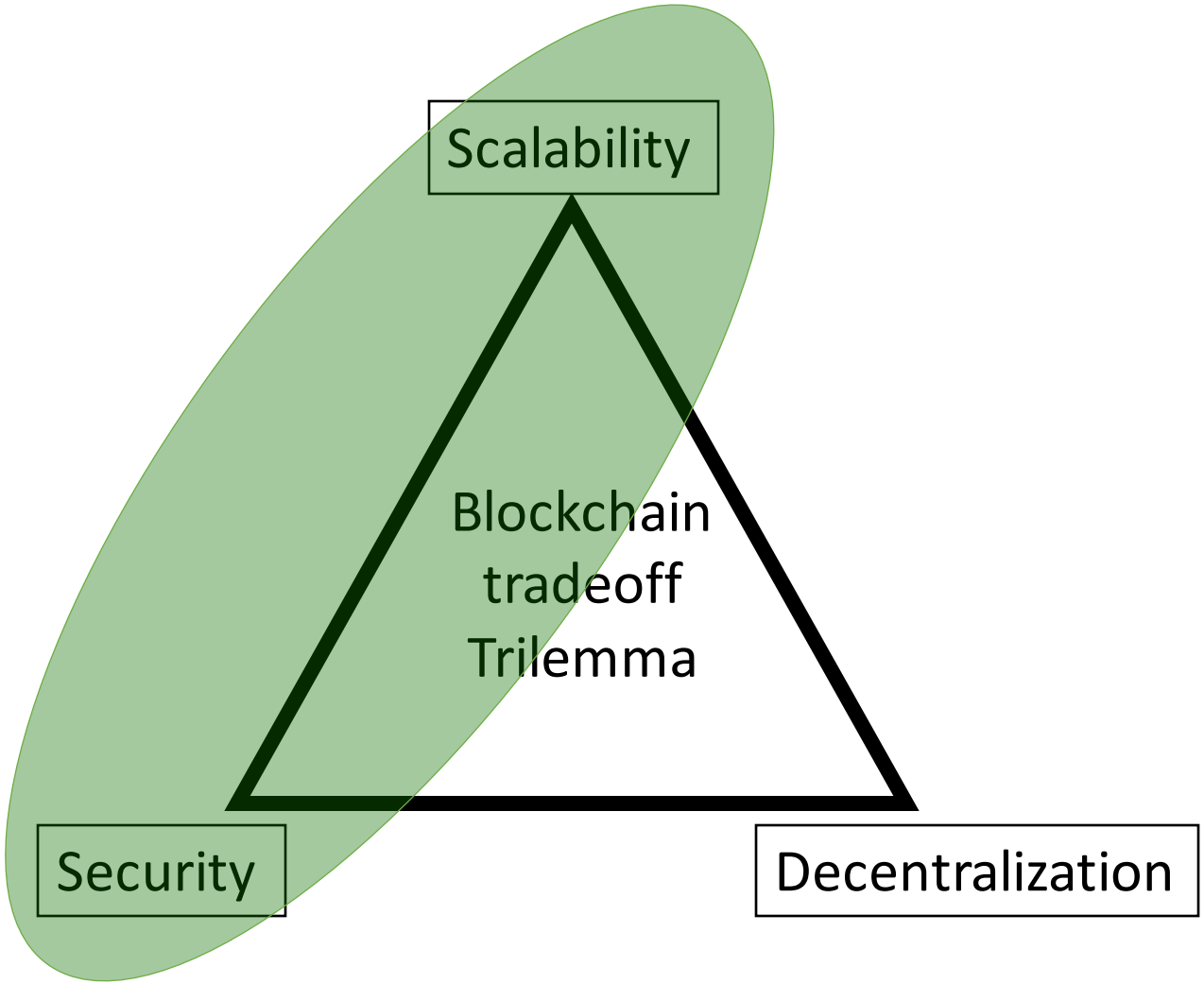
Decentralization

- Consensus algorithm
- Private/consortium/public blockchain

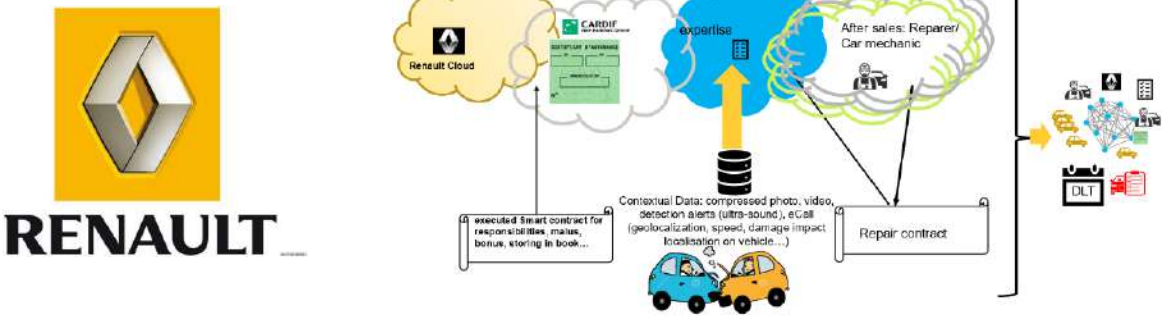
Consortium/private blockchain:

- Limited number of nodes participating in consensus
- Best suited for industrial projects
- Generally faster transaction speed than public blockchain

A Performances Trilemma



The use case requirements



Renault car fleet: ~10M in France

- Based on 2019 ONSIR accident report in France [4]:
  - The vehicular use case requires sending approximately 25 transactions per hour.

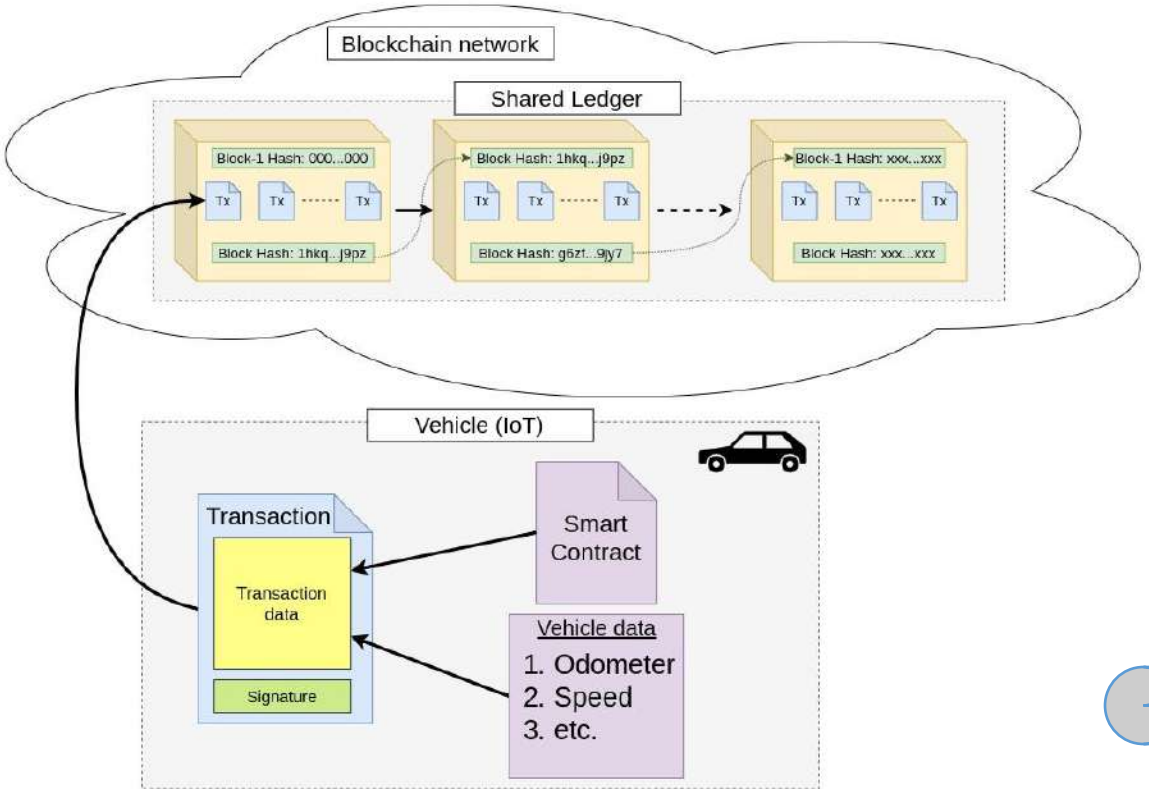
Cloud: why do we need you?

- Closer to real-world situation
- Simulation of a private/consortium blockchain network
- On-demand resources (CPU, RAM, …)
- Fully configurable (multiple nodes)

[4] ONISR. Bilan 2019 de la sécurité routière. [Online]. Available: https://www.onisr.securite-routiere.gouv.fr/

The use case requirements

Use case: Renault's cars are connected to blockchains deployed on several clouds and the cars IoTs can connect each time an accident occurs.



Use-case global architecture

Use case Smart contract

```
ACTION storeNewCar(car) {
        if(not authorized())
                return 0;
        car_array.push(car);
}

ACTION storeNewCrash(crash_data) {
        if(not authorized())
                return 0;
        crash_data_array.push(crash_data);
}
```

Implementations using Hyperledger Sawtooth

HYPERLEDGER SAWTOOTH + tas group an owl company

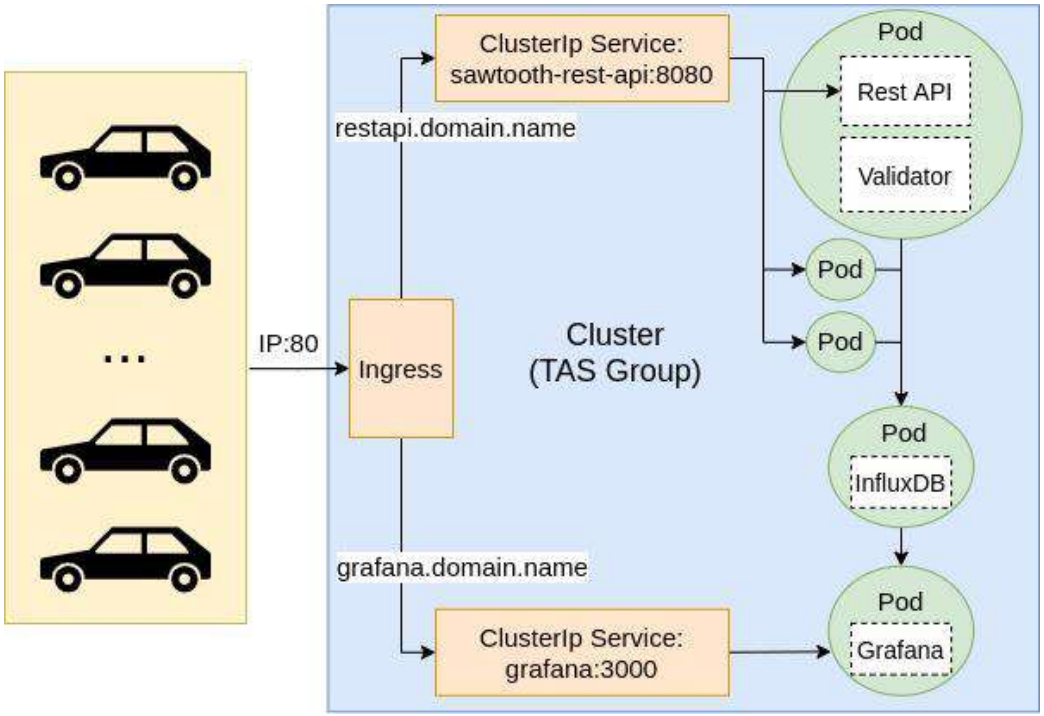
Modular, industrial focused blockchain [5]

Kubernetes cloud orchestration tool.
Totaling:
192 vCPU, 280GB RAM, 1.5 TB HDD Disk

[5] https://sawtooth.hyperledger.org/docs/core/releases/latest/

Implementations using Hyperledger Sawtooth

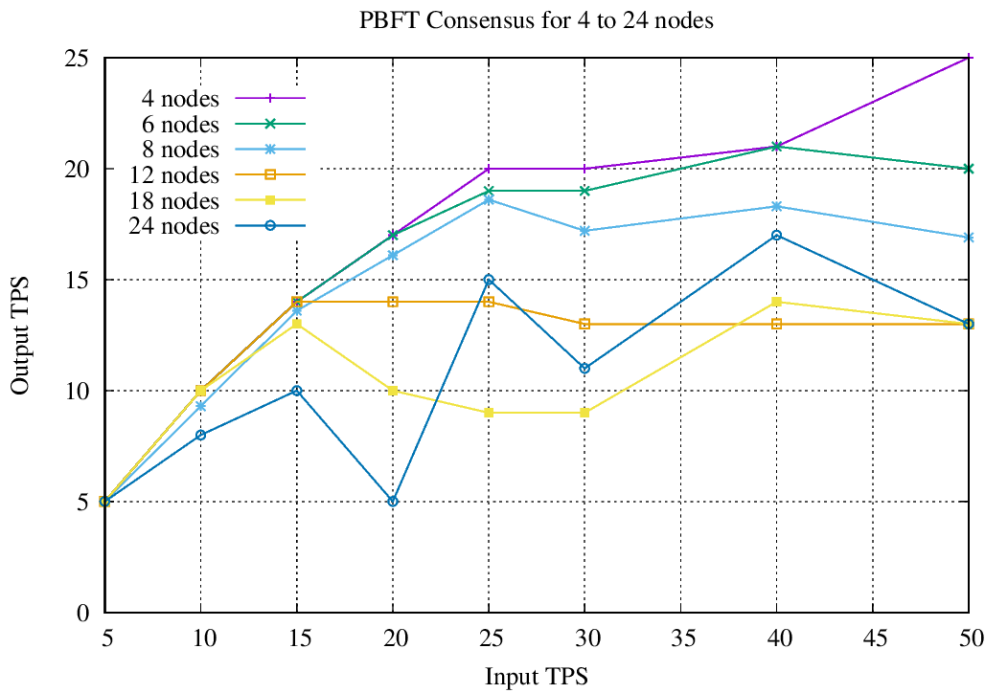
Benchmark: Total 120 measurements



Hyperledger Sawtooth network cloud deployment

Implementations using Hyperledger Sawtooth

Transaction rate measurements



Commit rate to be limited <25 tps

Hyperledger Sawtooth:

- Transaction threshold 25 commits per second, using the 4 nodes configuration.
- Based on 2019 accident report in France ONSIR report, this implementation meets the requirements

Ongoing study and perspectives

Ethereum results submitted to ACM Blocksys workshop

Test Substrate Blockchain Framework

Practical implementation on Renault vehicle

Continue, enhance IoT co-simulation using PwClkArch

Conclusion

- ✓ Successfully implemented industrial IoT use case
- ✓ Optimization of the IoT's overall energy consumption is possible
- ✓ Deployed Hyperledger Sawtooth blockchain (private network in cloud
- ✓ Better results than previous local implementation (Gerrits et al. COINS 2020)

Publications

- R. Kromes, F. Verdier. An IoT hardware modeling for using blockchain with Smart Contracts applications. 13ème Colloque National du GDR SOC2 Montpellier, Jun 2019, Montpellier, France.
- R. Kromes, L. Gerrits, F. Verdier. Adaptation of an embedded architecture to run Hyperledger Sawtooth Application, 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada.
- R. Kromes, F. Verdier. IoT devices hardware modeling for executing Blockchain and Smart Contracts applications. 16th ACS/IEEE International Conference on Computer Systems and Applications AICCSA 2019, ACS/IEEE, Nov 2019, Abu Dhabi, United Arab Emirates.
- L. Gerrits, R. Kromes, F. Verdier, A True Decentralized Implementation Based on IoT and Blockchain: a Vehicle Accident Use Case, COINS 2020 - IEEE International Conference on Omni-layer Intelligent Systems, Aug 2020, Barcelone, Spain. pp.6.
- L. Gerrits, T. Kilimou, R. Kromes, F. Verdier , A Blockchain cloud architecture deployment for an industrial IoT use case, COINS 2021 - IEEE International Conference on Omni-layer Intelligent Systems, Sep 2021, Madrid, Spain
- L. Gerrits,R. Kromes, T. Kilimou, F. Verdier,Hyperledger Sawtooth Blockchain for IoT-Blockchain Based Ecosystem, 15`eme Colloque National du GDR SOC2 Rennes, Jun 2021,Rennes, France.

Thank You ! Questions ?

Thesis director
Professor François Verdier

PhD candidate
Roland Kromes

PhD candidate
Luc Gerrits

Acknowledgement
This work has been supported by the French government, through the UCA and EUR DS4H Investments in the Future projects managed by the National Research Agency (ANR) with the reference number ANR-15-IDEX-0001 and ANR-17-EURE-0004.