M4DT Day 13th - Cloud Technologies for Metrology

INMETRO

Blockchains for monitoring Critical Infrastructures: learning from Data and Measurements

Wilson S. Melo Jr - PhD
wsjunior@inmetro.gov.br

April 27th, 2023

Who are we?

- **Laboratory of Metrology in Informatics (Lainf)**
  - Metrology for Information Technology
  - Measuring instruments reliability
  - Compliance with industrial IT products
  - Industry 4.0 and cybersecurity
  - Proficiency testing on software quality
  - Partnership within other public and private institutions

- **The Lainf in numbers**
  - PhD researchers: 6
  - Graduated and undergraduate students
    - 5 PhD students
    - 3 MSc students
    - 4 undergraduate students
  - Cooperation with the PTB and the University of Lisbon in projects regarding blockchains and Metrology, since 2019.

Main achievements on Blockchains + Metrology

2018	2019	2020	2021	2022
First ideas about blockchain-based applications in the Legal Metrology. - *Peters et al. (2018)* - *Melo et al. (2017)*	DMS using blockchains, blockchain-based PKI for smart meters, possible use of blockchains in the European Metrology Cloud Project. - *Melo et al. (2019)* - *Thiel and Wetzlich (2019)*	Privacy issues on blockchains and possible solutions exploring FE, PCP, and ZKP. - *Peters et al. (2020)* - *Yurchenko et al. (2020)*	The InterNMI blockchain network, field surveillance using blockchains. - *Moni et al. (2021)* - *Melo et al. (2021)*	Blockchains in the Metrology DT, measurements traceability, blockchain oracles and the Metroracle Project. - *Miličević et al. (2022)*

Main achievements on Blockchains + Metrology

What should be our next steps?

1) Need for more practical projects

2) Fill the gap between the “metrologists” and the “people” (e.g., meters manufacturers and users)

3) Use easy-understanding examples as case studies

Why Critical Infrastructures monitoring is suitable?

- **Cyber-physical CIs** are our target here!
  - Their monitoring demands sensing and **sensing demand measurements**
  - Wherever we have measurements, we will need Metrology
- The integrity of CIs is crucial for the economy, business, people's safety, environment, and even national sovereignty
  - This assurance depends on **reliable information**
  - … and blockchains are here to provide trustability on data

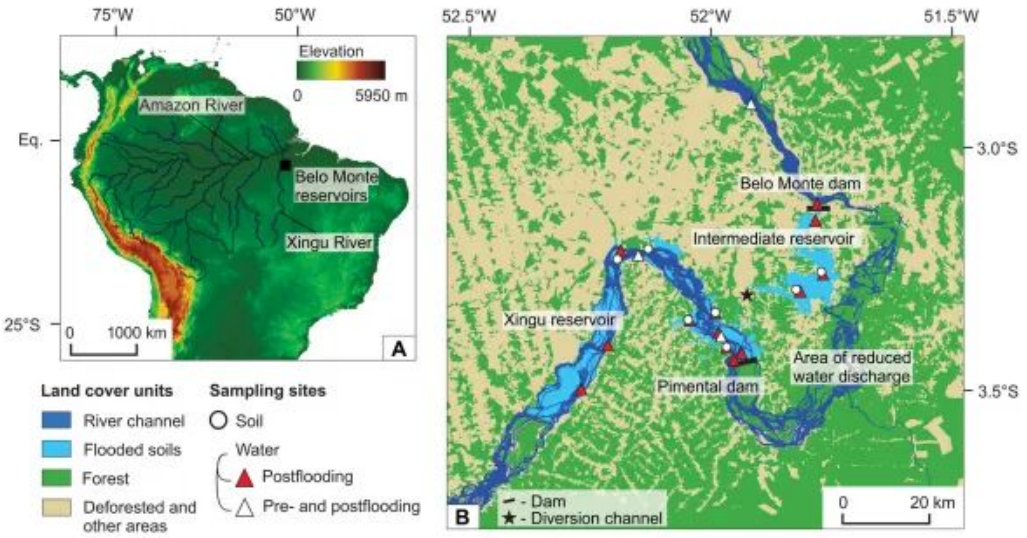
- So, how are we monitoring our CIs?
  - Are we collecting reliable information?
  - Are we storing all information properly?
  - Can we audit it any time we need?
  - Is this information protected against cyber attacks, including internal attacks such as data tampering and sabotage?

Our Case Study: smart monitoring of dam and slopes

- R&D project in a partnership - **Inmetro** and **NESA**
  - NESA built and operates **Belo Monte** hydroelectric plant
    - 18 energy generation units ⟶ 11.233,1 MW
    - Three million cubic meters of concrete
    - Discharge capacity of 62,000 m3/s.

Challenges on monitoring Belo Monte

- **Diversity of sensors**, including PZT, ultrasound, and others
- Sensing includes structural health (i.e., dam and slopes) but also **environmental monitoring** for compliance
- Monitoring can further include **images** and **soft sensors**
- **Points of measurement**: more than 3 thousand
- System must **collect**, **store**, and enable **data audit** reliably and transparently

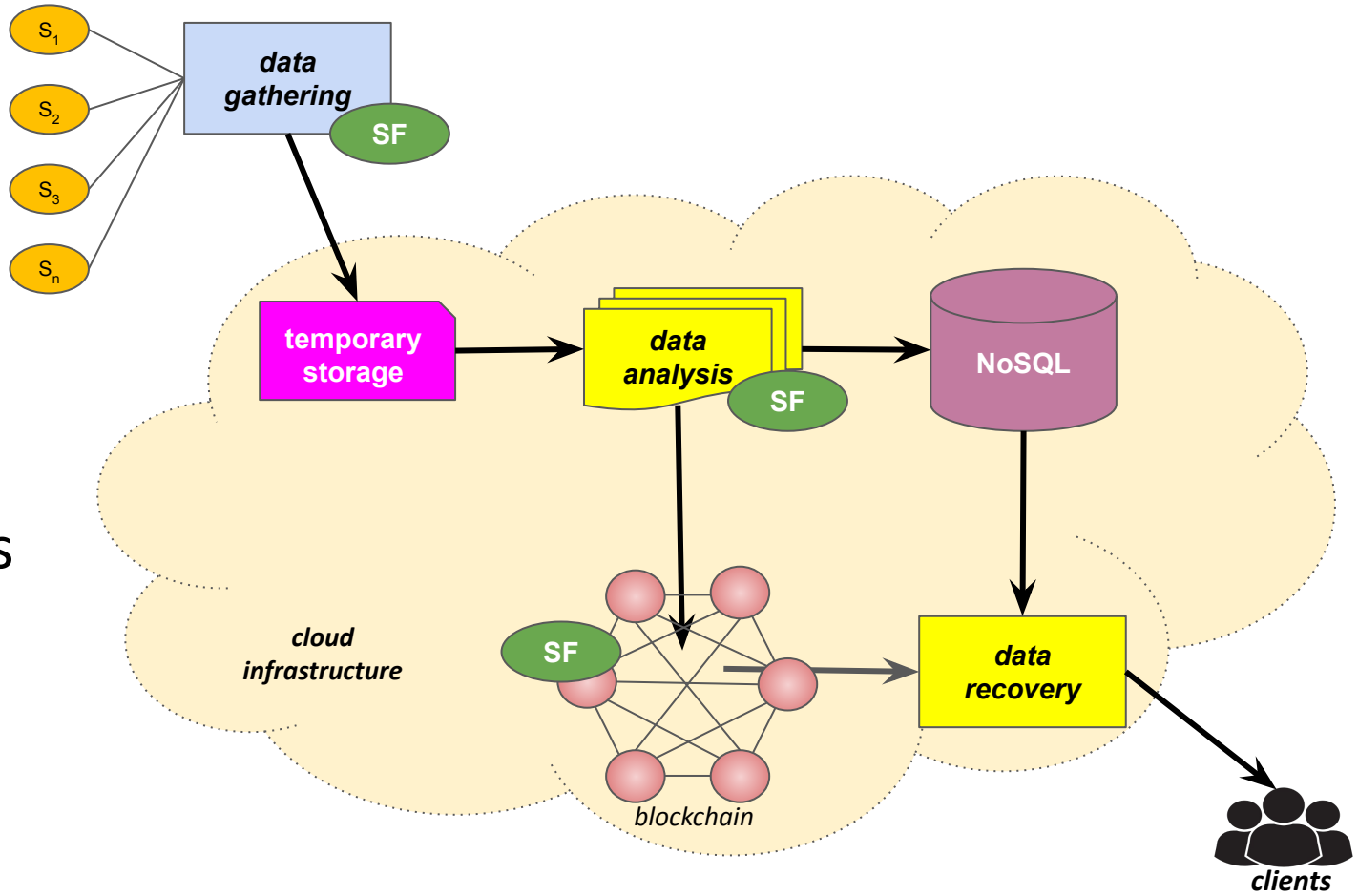


Evidently, we need attempt to

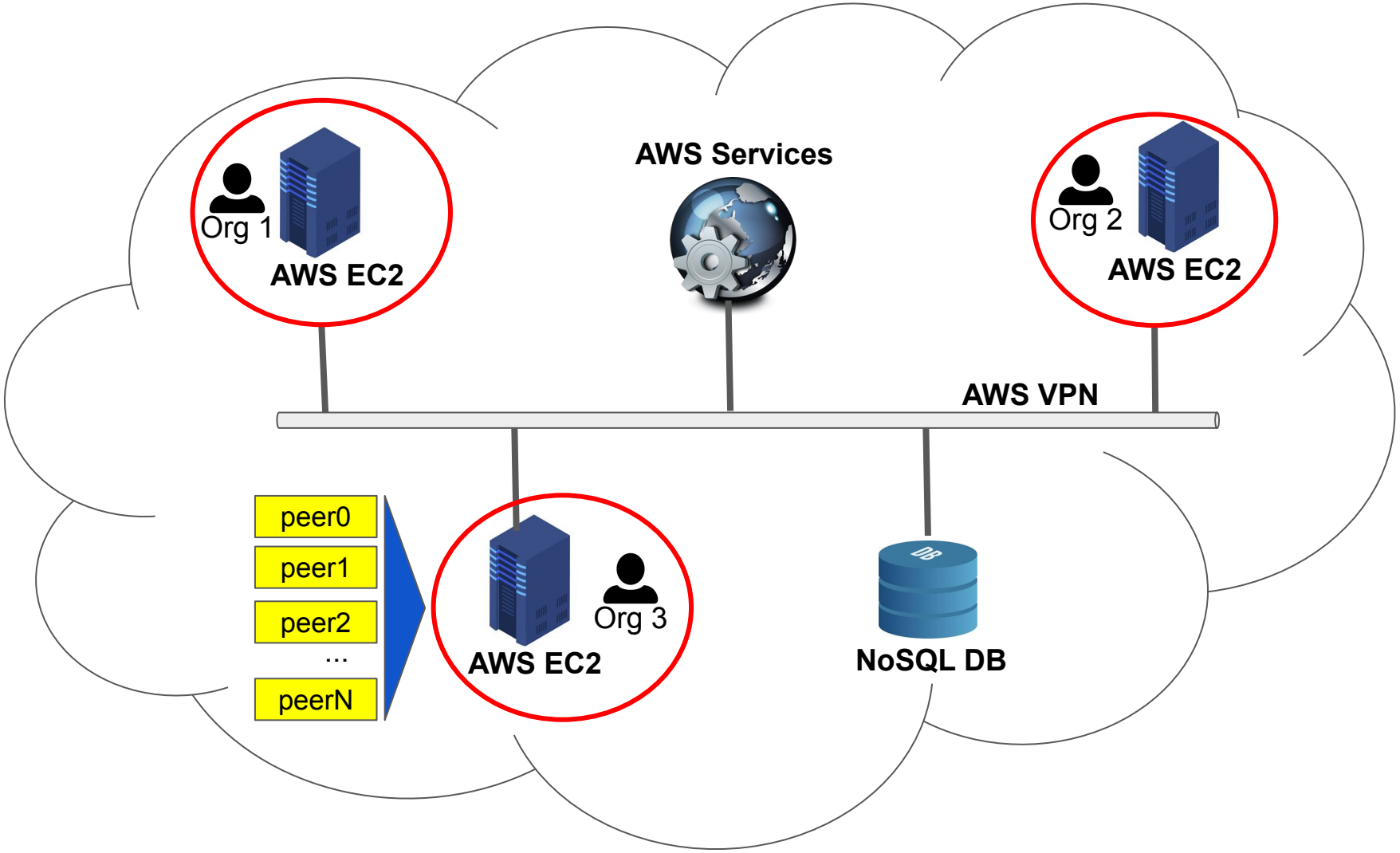
- the significant **amount of data** to store
- the need for **automated auditing process**
- this **process must be reliable** for any involved organization

Big data of Measurements into Blockchains

- **Blockchains do not scale throughput** as centralized systems
  - Big Data demand is a challenge for blockchains
- Our solution:
  - ***Off-chain* method**
  - Data replication in a NoSQL DB
  - Blockchains work as a **security mirror**
  - Data recovery audits data **by comparing both data sources**



The blockchain implementation roadmap

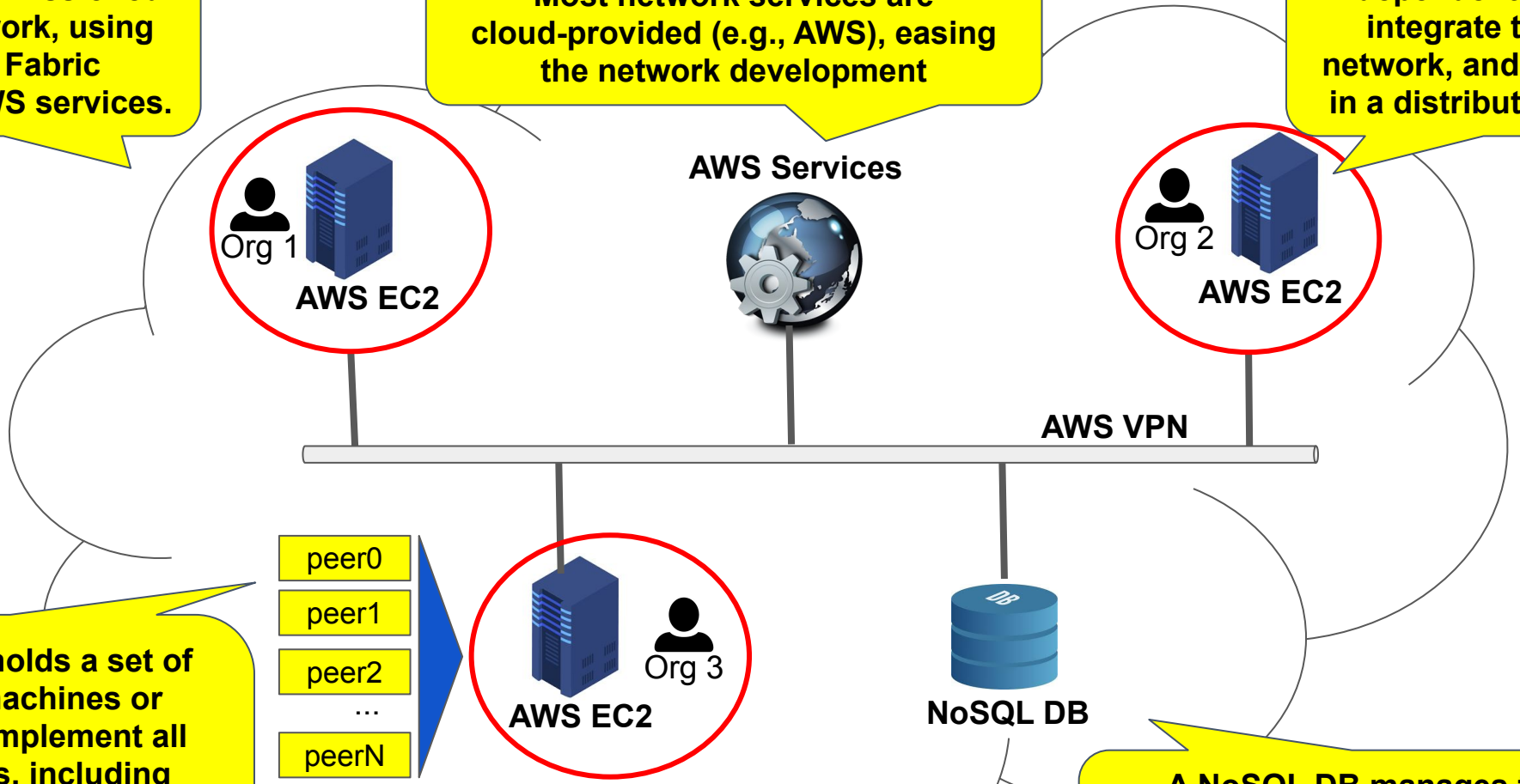


The blockchain implementation roadmap

Cloud-based permissioned blockchain network, using the Hyperledger Fabric platform and AWS services.

Most network services are cloud-provided (e.g., AWS), easing the network development

Independent organizations integrate the blockchain network, and also take part in a distributed consensus



Each organization holds a set of *peers* (i.e., virtual machines or containers) which implement all the blockchain roles, including smart contracts execution and validation (*endorsers*), replication (*committers*) and consensus (*orderers*).

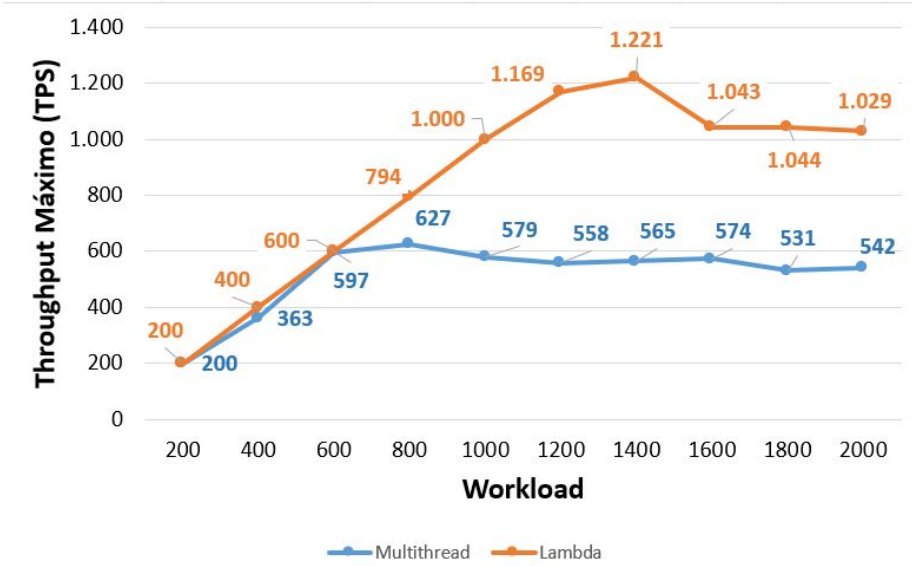
A NoSQL DB manages the *off-chain* data, ensuring performance and scalability whenever the data amount increases, as so fast querying

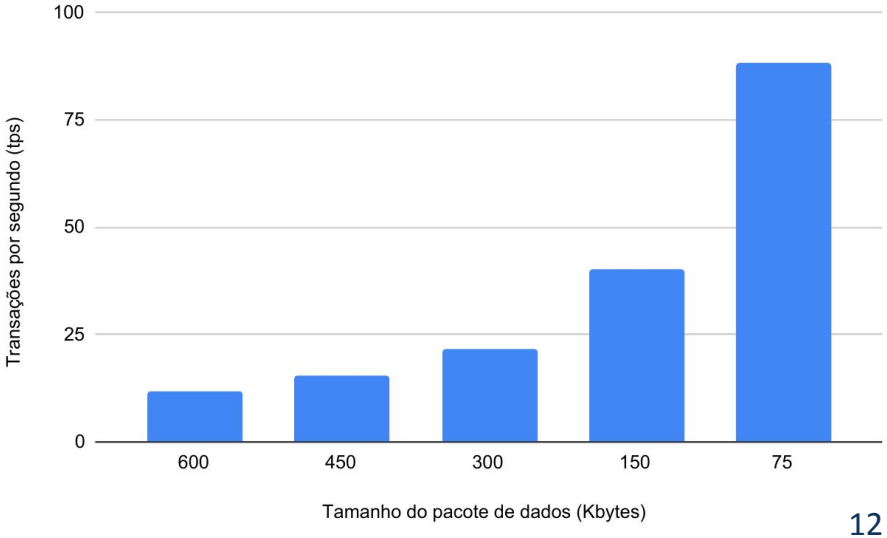
How does the data recovery audit information?

- The ***off-chain* approach** implies on comparison between the stored data and their cryptographic digests
  - Usually, digests are **cryptographic hashes**
  - One can include **similarity hashes (e.g., LSH)** and ***zero-knowledge proof* (ZKP)** protocols
- **Smart contracts** can perform data checking!
  - It is a valuable application for them since they verify measurements based on cryptographic properties
  - Moreover, **organizations can implement** their own smart contract verifier, enabling **independent auditing**
- On a deeper level, we can conceive this auditing by using autonomous **blockchain oracles** (centralized or distributed)

Performance issues

- Hyperledger Fabric **theoretically** treats until **2K tps (transactions per second)**
  - … but these practical scenarios are difficult to simulate
- By using **cloud services** (i.e., AWS Lambda), we got a **performance of 1,2K tps**
  - significantly higher than simulations using multi threaded clients or usual tools like Hyperledger Caliper
- The block size also impacts performance significantly
  - which means we can **optimize *off-chain*** data storing by aggregating data packages





Learned lessons and lessons we still want to learn

- CIs monitoring is a **fascinating**, **easy-for-understanding**, **challenging** study case involving Blockchains + Metrology
- A blockchain-based CI monitoring system also **enables data monetization** (e.g., eco credits or carbon credits)
  - … something **very attractive** and possibly **profitable** for companies who implement them
- The expressive measurement data amounts constitute a **Big Data** problem, demanding ideas to avoid blockchain performance issues
- **Data recovery is by itself a research topic** since it can include alternative checking mechanisms (e.g., LSH, ZKP)
  - and also open space for **third party off-chain oracles** and even new business models for meters manufacturers

Acknowledgment

- This research was partially sponsored by the **Norte Energia SA (NESA)**, grant P&D-S004/2021 - Project P&D ANEEL PD-07427-0421/2021.

- **Research team:**
  - Carlos Oliveira, Pablo Ortiz, Paulo Assumpção, Wilson Melo Jr e Luiz Fernando Rust
- **Papers related to this project:**
  - Assumpção, P., Oliveira, C., Ortiz, P., Melo, W., & Carmo, L. (2022, October). A Secure Cloud-based Architecture for monitoring Cyber-Physical Critical Infrastructures. In 2022 6th Cyber Security in Networking Conference (CSNet) (pp. 1-7). IEEE.
  - Oliveira, C. A., Assumpção, P., Ortiz, P., Melo, W., & Carmo, L. (2022, November). Auditoria de aplicações de Big Data usando Hashes de Similaridade e Blockchains. In Anais Estendidos do XII Simpósio Brasileiro de Engenharia de Sistemas Computacionais (pp. 32-39). SBC.
  - Assumpção, P., Oliveira, C., Melo, W., & Carmo, L. (2022, May). Sensors fingerprints using machine learning: a case study on dam monitoring systems. In 2022 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) (pp. 1-6). IEEE.

Ouvidoria: 0800 285 1818

inmetro.gov.br

linkedin.com/company/inmetro

instagram.com/inmetro_oficial

facebook.com/Inmetro

youtube.com/tvinmetro

twitter.com/Inmetro

slideshare.net/inmetro

flickr.com/inmetro

INMETRO

SECRETARIA ESPECIAL DE
PRODUTIVIDADE, EMPREGO E COMPETITIVIDADE

MINISTÉRIO DA
ECONOMIA

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL