Security by Design for Sustainable Cyber-Physical Systems

ICCE Berlin 2020 Panel

10 Nov 2020 (Tue)

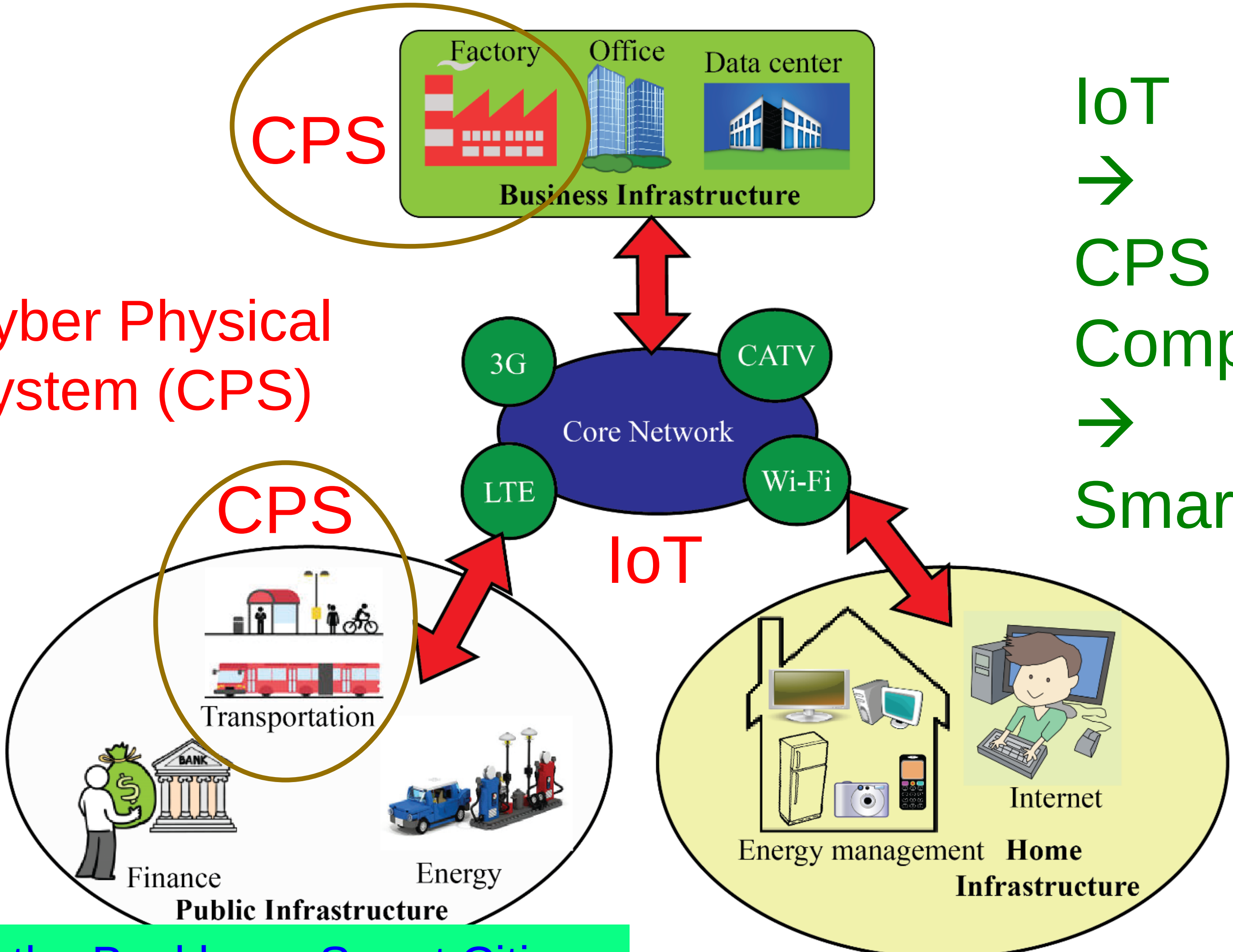
Saraju P. Mohanty

University of North Texas, USA.

Email: saraju.mohanty@unt.edu

More Info: http://www.smohanty.org

IoT → CPS → Smart Cities



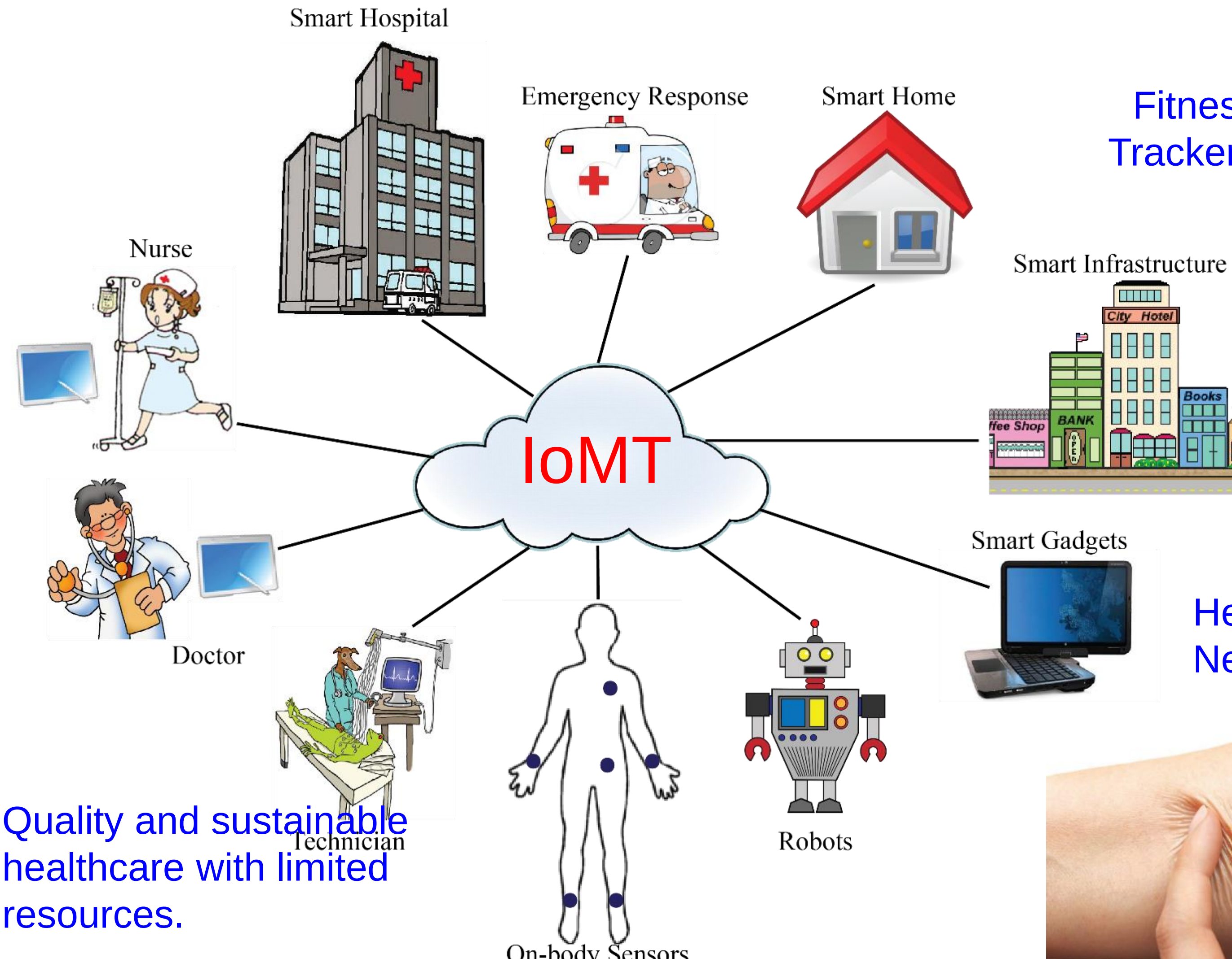
Cyber Physical System (CPS)

IoT → CPS (Smart Components) → Smart Cities

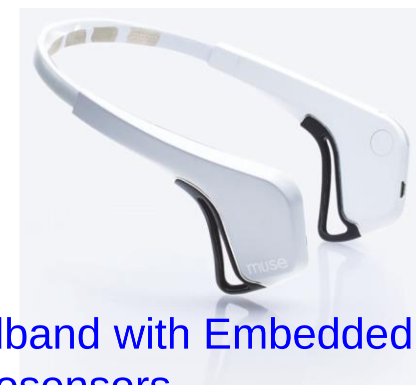
IoT is the Backbone Smart Cities.

Source: Mohanty CE Magazine July 2016

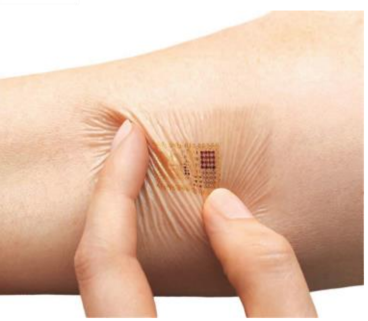
Healthcare Cyber-Physical System (H-CPS)



Fitness Trackers



Headband with Embedded Neurosensors

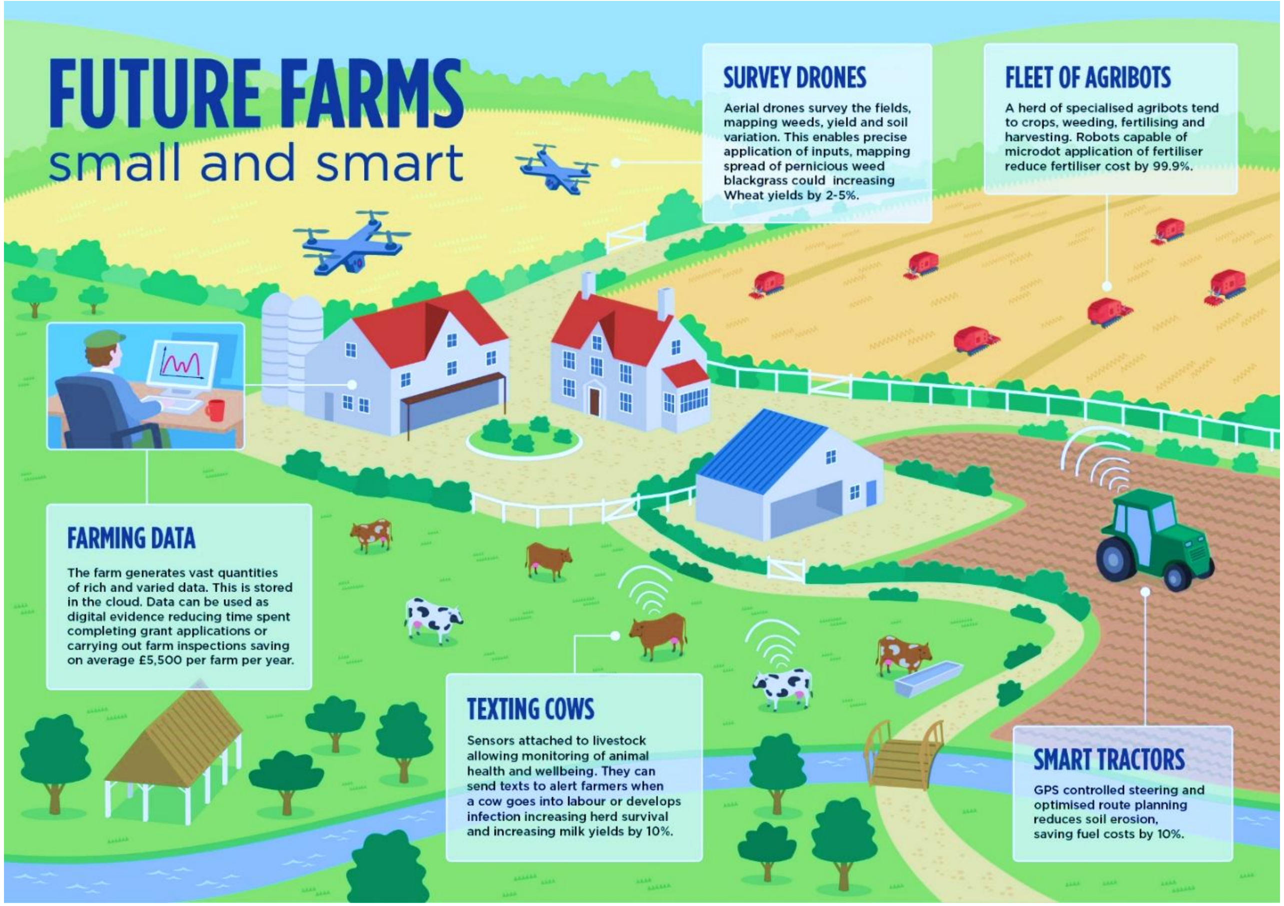


Embedded Skin Patches

Quality and sustainable healthcare with limited resources.

Source: Mohanty CE Magazine July 2016

Agriculture Cyber-Physical System (A-CPS)



Source: http://www.nesta.org.uk/blog/precision-agriculture-almost-20-increase-income-possible-smart-farming

Climate-Smart Agriculture Objectives:
- Increasing agricultural productivity
- Resilience to climate change
- Reducing greenhouse gas

http://www.fao.org

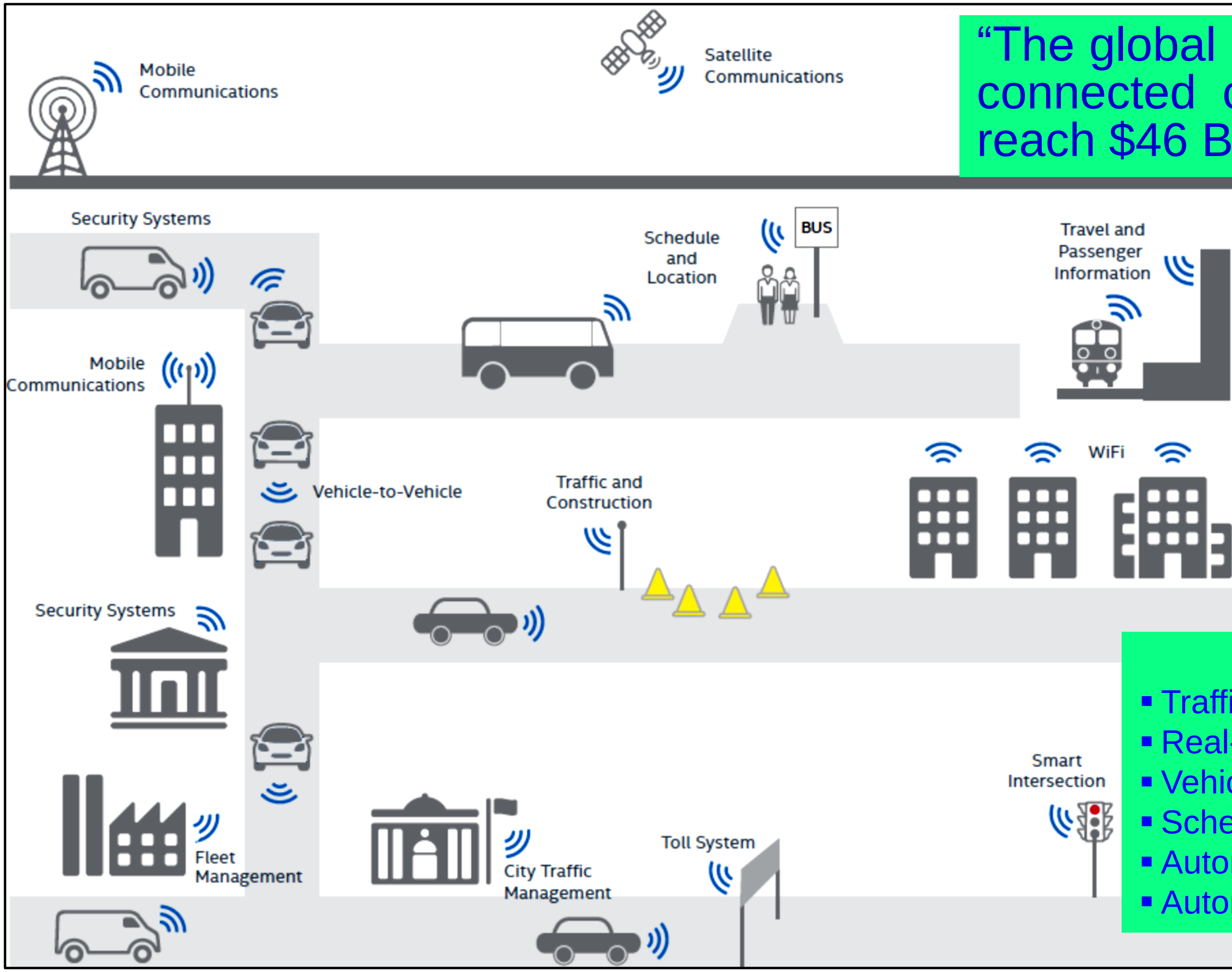
Automatic Irrigation System

Source: Maurya 2017, CE Magazine July 2017

Smart Agriculture/Farming Market Worth $18.21 Billion By 2025

Sources: http://www.grandviewresearch.com/press-release/global-smart-agriculture-farming-market

Transportation Cyber-Physical System (T-CPS)



"The global market of IoT based connected cars is expected to reach $46 Billion by 2020."

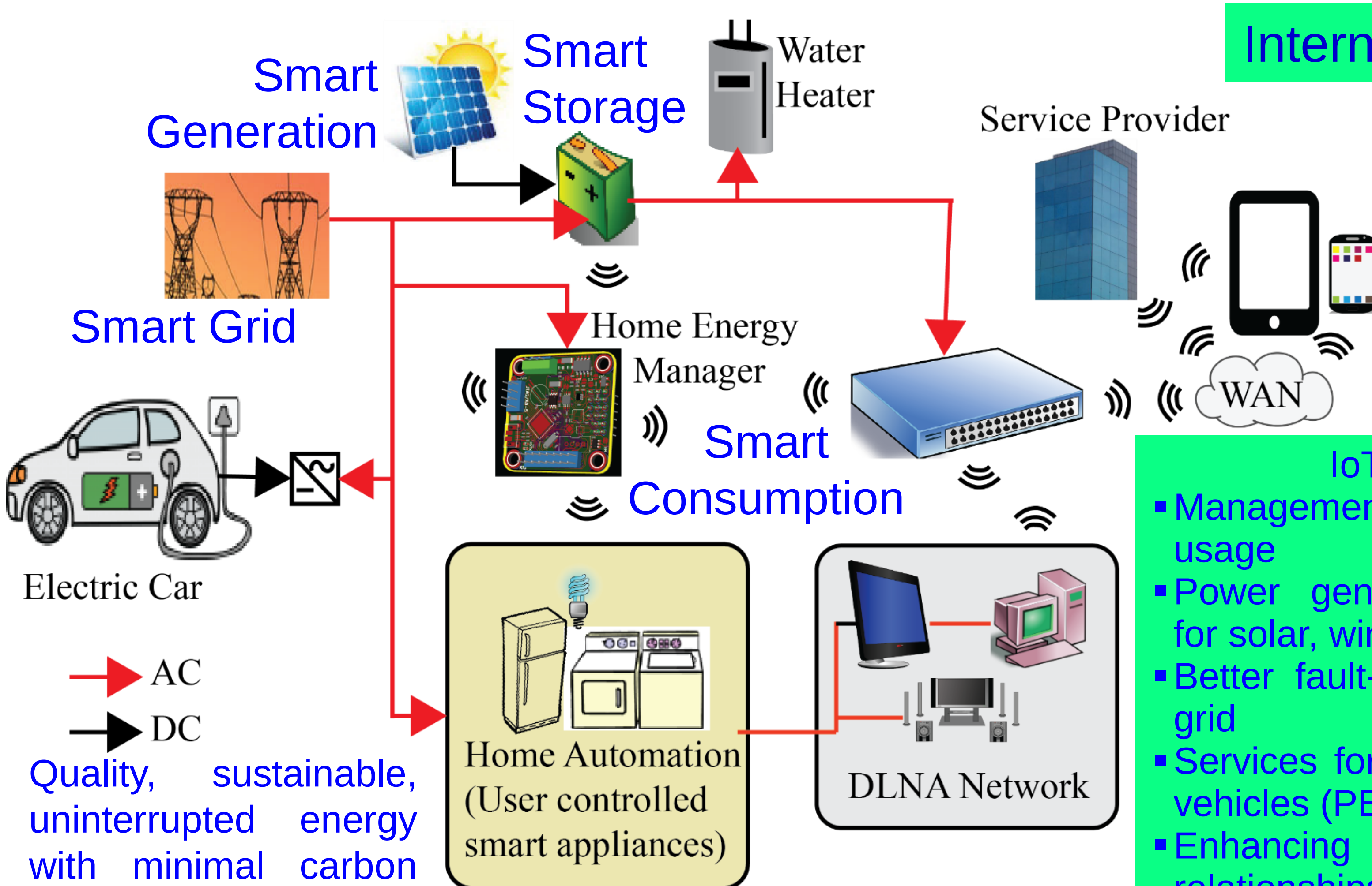
Source: Datta 2017, CE Magazine Oct 2017

IoT Role Includes:

- Traffic management
- Real-time vehicle tracking
- Vehicle-to-Vehicle communication
- Scheduling of train, aircraft
- Automatic payment/ticket system
- Automatic toll collection

Source: https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

Energy Cyber-Physical System (E-CPS)



Internet of Energy

Quality, sustainable, uninterrupted energy with minimal carbon footprint.

Source: Mohanty CE Magazine July 2016

IoT Role:

- Management of energy usage
- Power generation dispatch for solar, wind, etc.
- Better fault-tolerance of the grid
- Services for plug-in electric vehicles (PEV)
- Enhancing consumer relationships

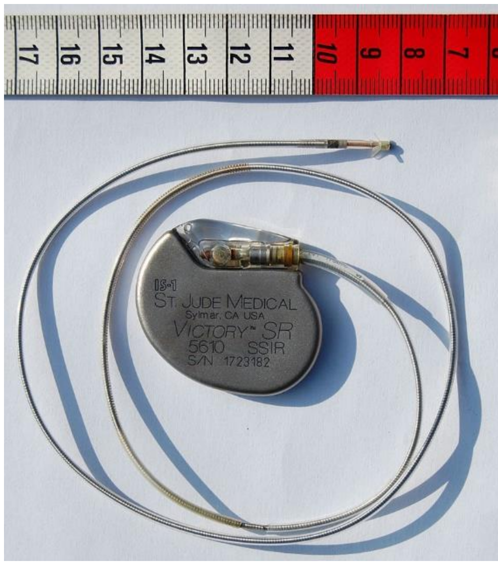
Smart Healthcare - Security and Privacy Issue

https://ctsoc.ieee.org

Selected Smart Healthcare Security/Privacy Challenges

- Data Eavesdropping
- Data Confidentiality
- Data Privacy
- Location Privacy
- Identity Threats
- Access Control
- Unique Identification
- Data Integrity
- Device Security

H-CPS Security Measures is Hard - Energy Constrained



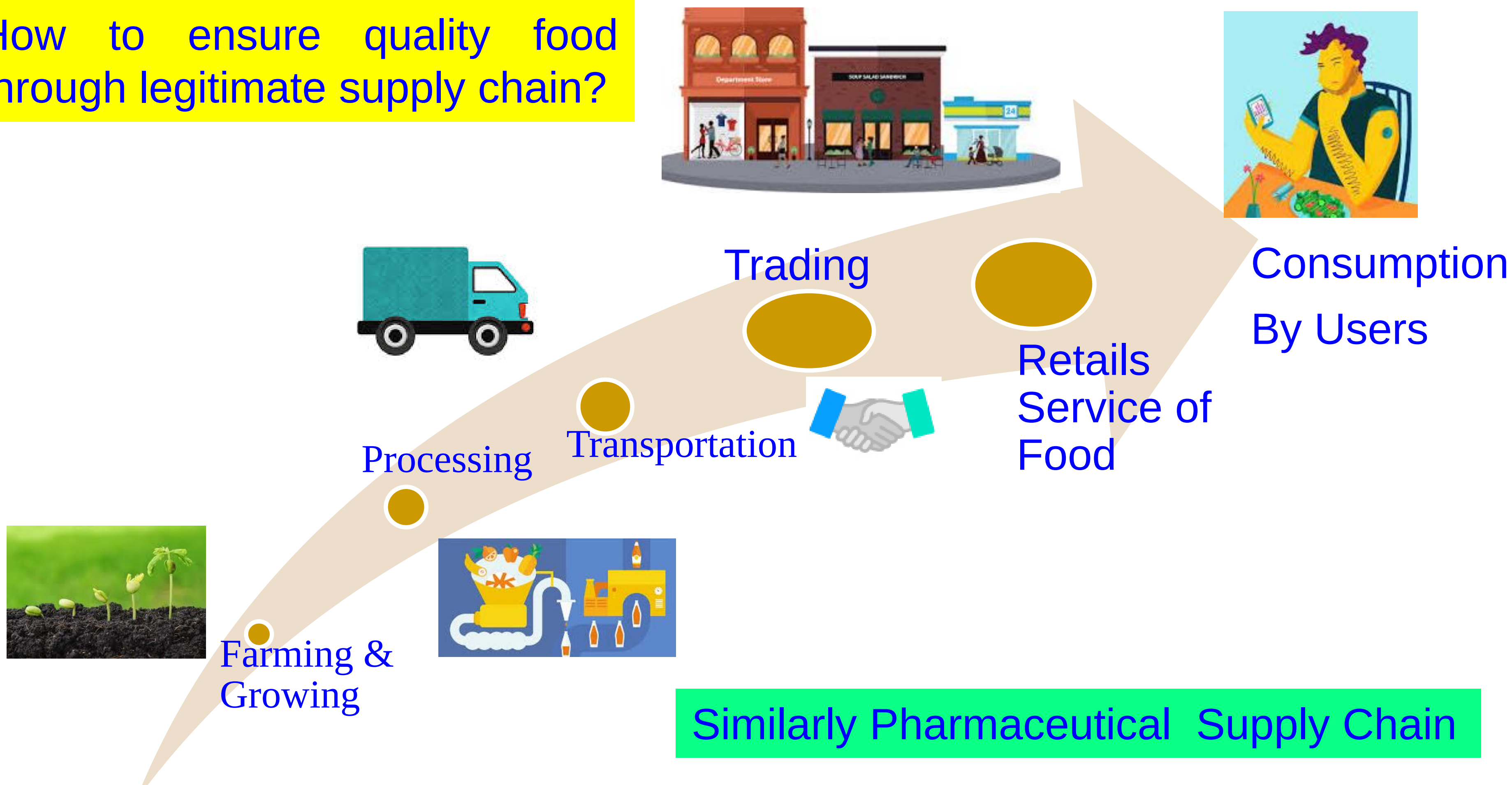
Pacemaker
Battery Life
- 10 years

Neurostimulator
Battery Life
- 8 years

- Implantable Medical Devices (IMDs) have integrated battery to provide energy to all their functions → Limited Battery Life depending on functions
- Higher battery/energy usage → Lower IMD lifetime
- Battery/IMD replacement → Needs surgical risky procedures

Food Supply Chain: Farm → Dinning

How to ensure quality food through legitimate supply chain?



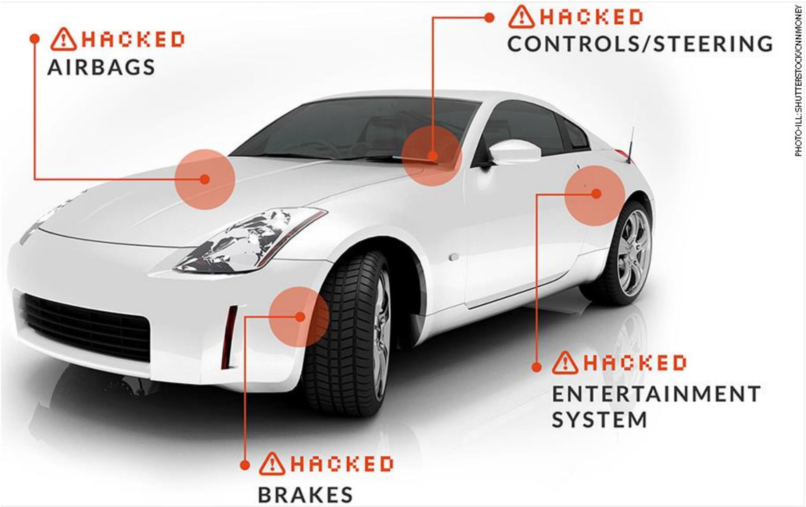
Similarly Pharmaceutical Supply Chain

Source: A. M. Joshi, U. P. Shukla, and **S. P. Mohanty**, “Smart Healthcare for Diabetes: A COVID-19 Perspective”, *arXiv Quantitative Biology*, arXiv:2008.11153, August 2020, 18-pages.

Security Challenge - System

Power Grid Attack

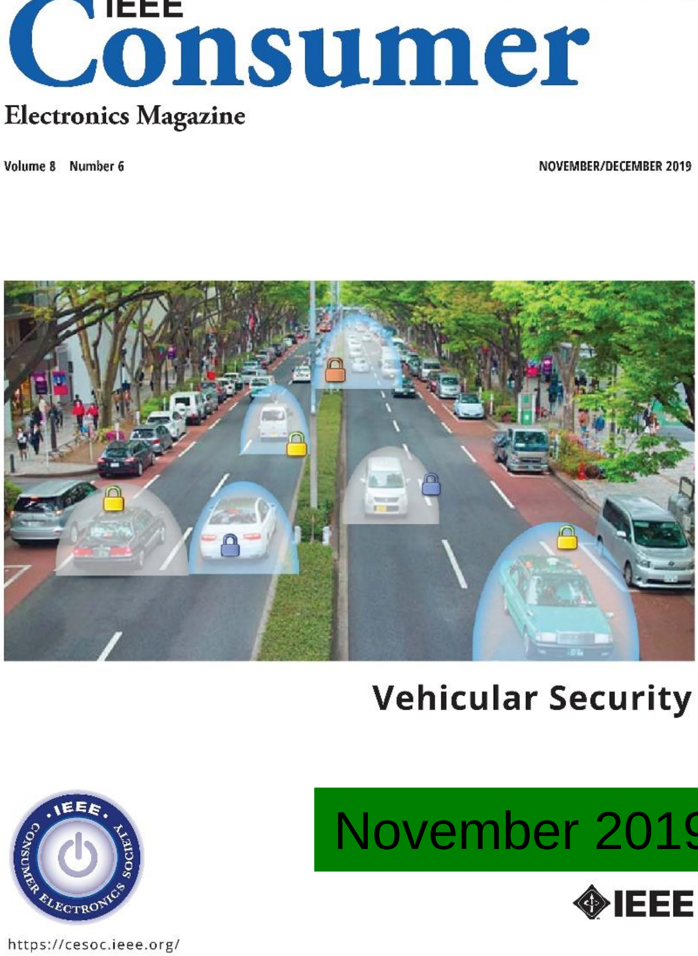
Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html



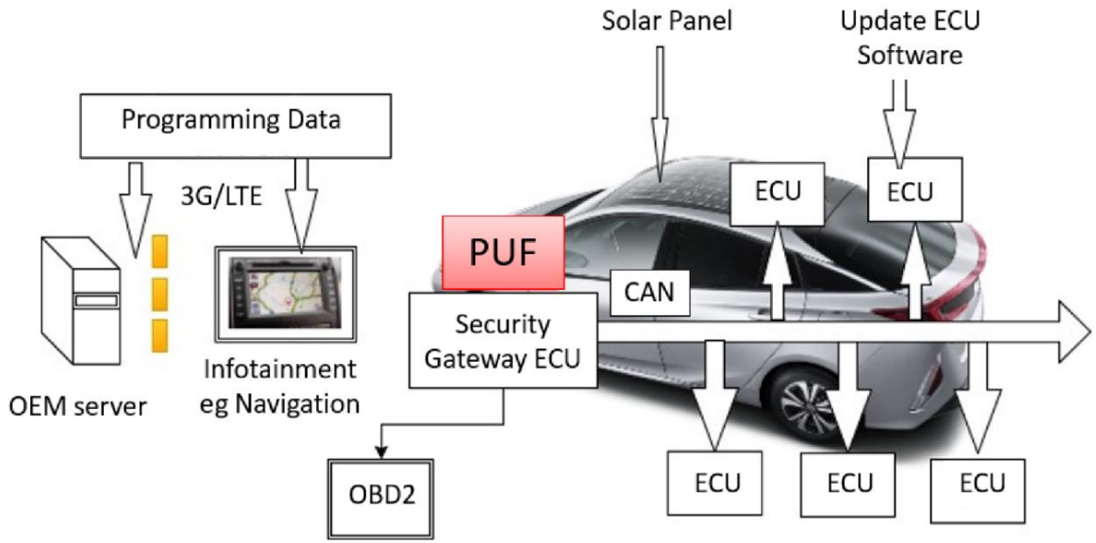
Source: http://money.cnn.com/2014/06/01/technology/security/car-hack/

Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

T-CPS Security is Hard – Time Constrained

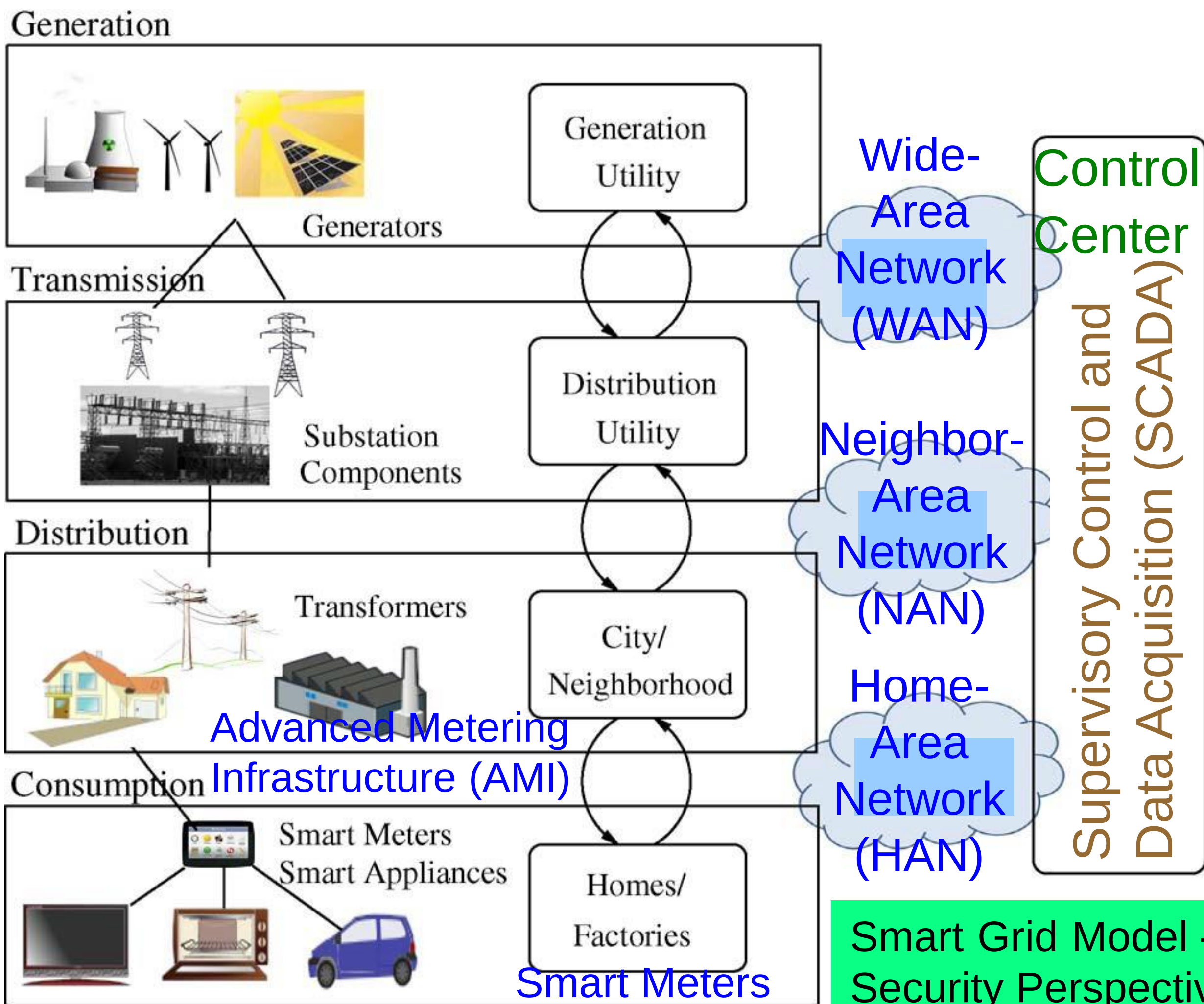


November 2019



Source: C. Labrado and H. Thapliyal, "Hardware Security Primitives for Vehicles," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 99-103, Nov. 2019.

Smart Grid - Vulnerability



Information and Communication Technology (ICT) components of smart grid is cyber vulnerable.

Data, Application/System Software, Firmware of Embedded System are the loop holes for security/privacy.

Network/Communication Components

Phasor Measurement Units (PMU)

Phasor Data Concentrators (PDC)

Energy Storage Systems (ESS)

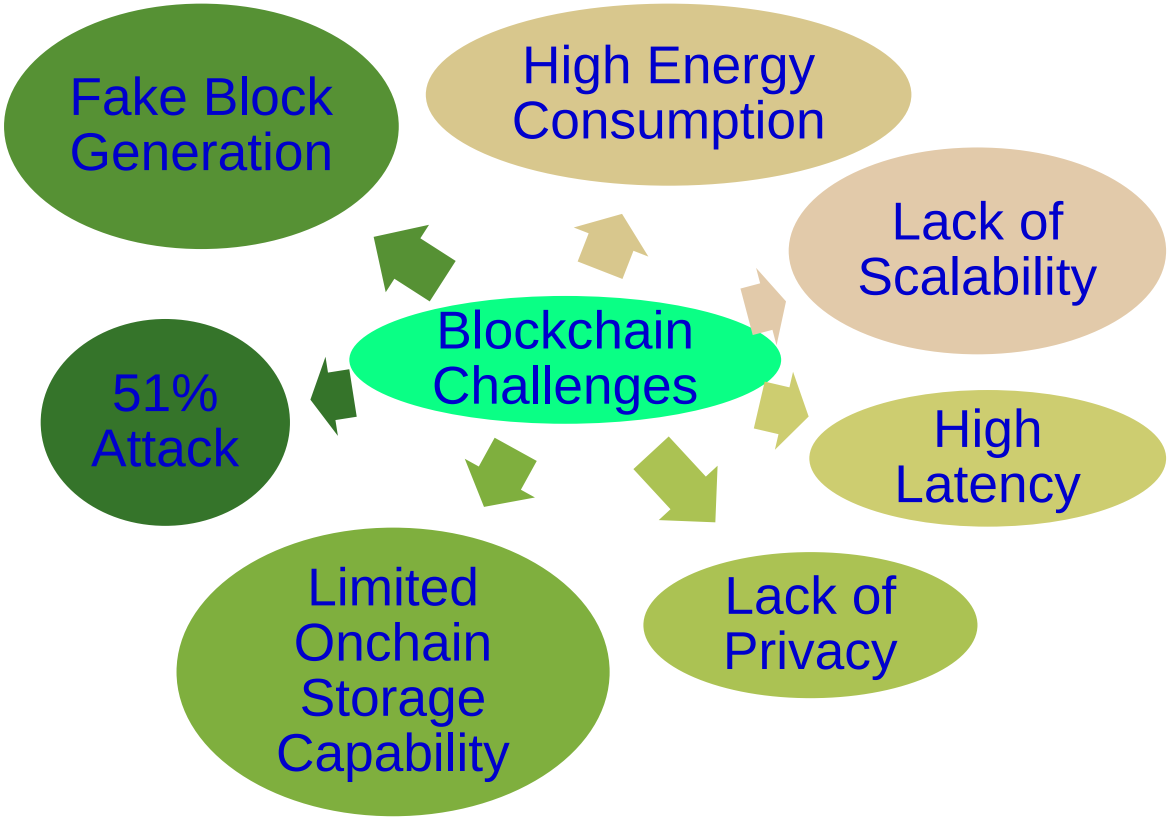
Programmable Logic Controllers (PLCs)

Smart Meters

Smart Grid Model – CPS Security Perspective

Source: Y. Mo *et al*., "Cyber–Physical Security of a Smart Grid Infrastructure“, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012.

Blockchain has Many Challenges



Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

Blockchain Energy Need is Huge

Energy for mining of 1 bitcoin

=

Energy consumption 2 years of a US household

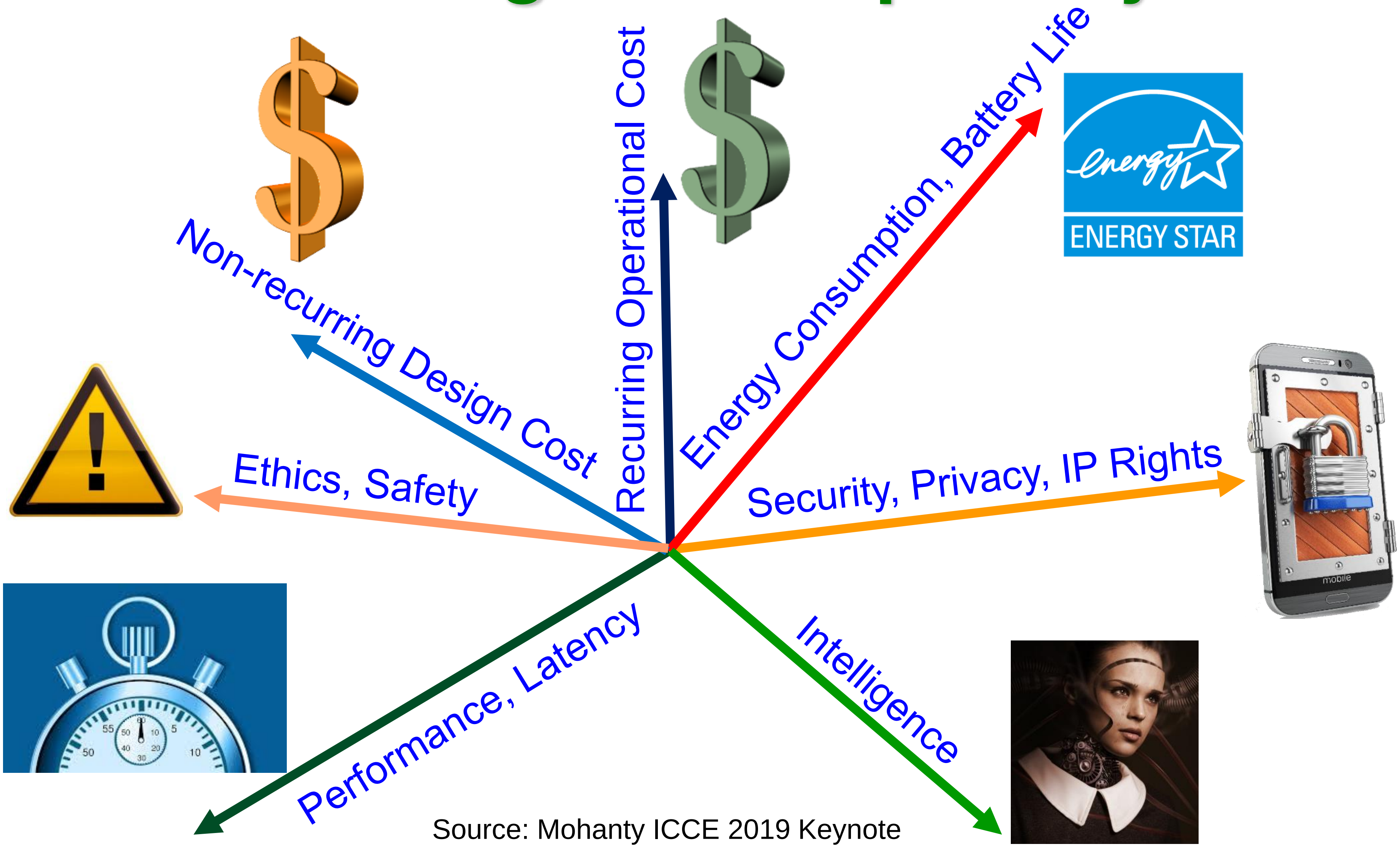
Energy consumption for each bitcoin transaction

=

80,000X

Energy consumption of a credit card processing

IoT/CPS Design – Multiple Objectives



Source: Mohanty ICCE 2019 Keynote

Security by Design (SbD) and/or Privacy by Design (PbD)

Embedding of security/privacy into the architecture (hardware+software) of various products, programs, or services.

Retrofitting: Difficult → Impossible!

Source: https://teachprivacy.com/tag/privacy-by-design/

Security by Design (SbD) and/or Privacy by Design (PbD)

7 Fundamental Principles

- Proactive not Reactive
- Security/Privacy as the Default
- Security/Privacy Embedded into Design
- Full Functionality - Positive-Sum, not Zero-Sum
- End-to-End Security/Privacy - Lifecycle Protection
- Visibility and Transparency
- Respect for Users

Source: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

Hardware-Assisted Security (HAS)

- Hardware-Assisted Security: Security provided by hardware for:

  (1) information being processed,

  (2) hardware itself,

  (3) overall system

Privacy by Design (PbD)

Security/Secure by Design (SbD)

- Additional hardware components used for security.
- Hardware design modification is performed.
- System design modification is performed.

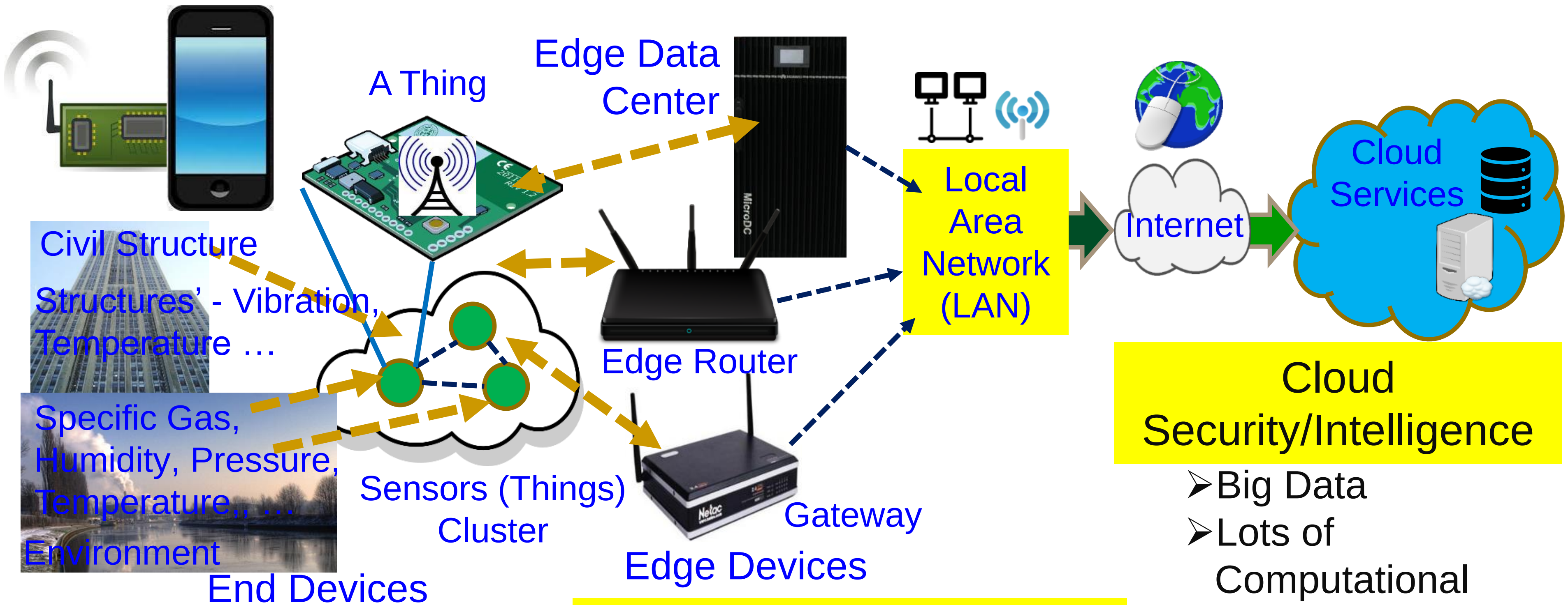
RF Hardware Security | Digital Hardware Security – Side Channel

Hardware Trojan Protection | Information Security, Privacy, Protection

IR Hardware Security | Memory Protection | Digital Core IP Protection

Source: Mohanty ICCE 2018 Panel

End, Edge Vs Cloud - Security, Intelligence



End Security/Intelligence

- Minimal Data
- Minimal Computational Resource
- Least Accurate Data Analytics
- Very Rapid Response

Edge Security/Intelligence

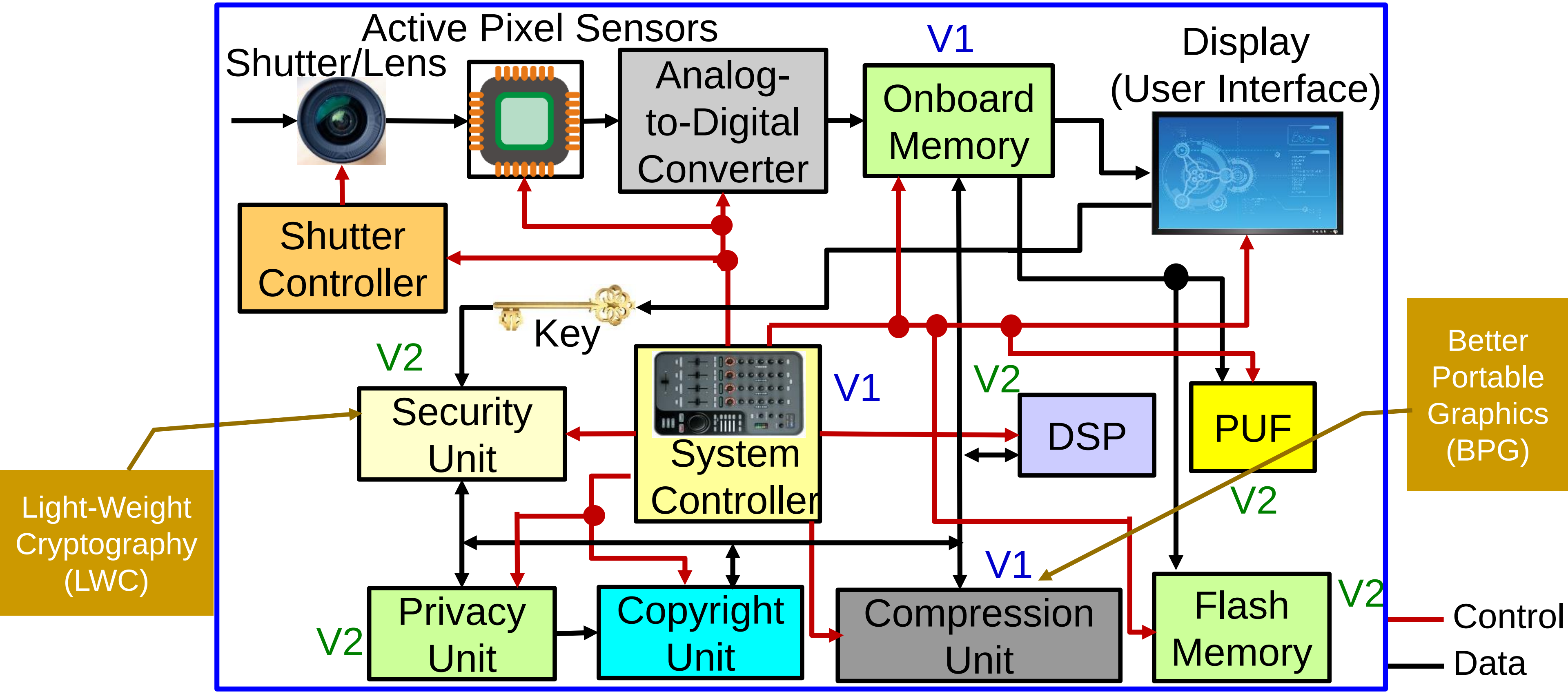
- Less Data
- Less Computational Resource
- Less Accurate Data Analytics
- Rapid Response

Cloud Security/Intelligence

- Big Data
- Lots of Computational Resource
- Accurate Data Analytics
- Latency in Network
- Energy overhead in Communications

Source: Mohanty iSES Keynote 2018 and ICCE 2019 Panel

Secure Digital Camera – My Invention

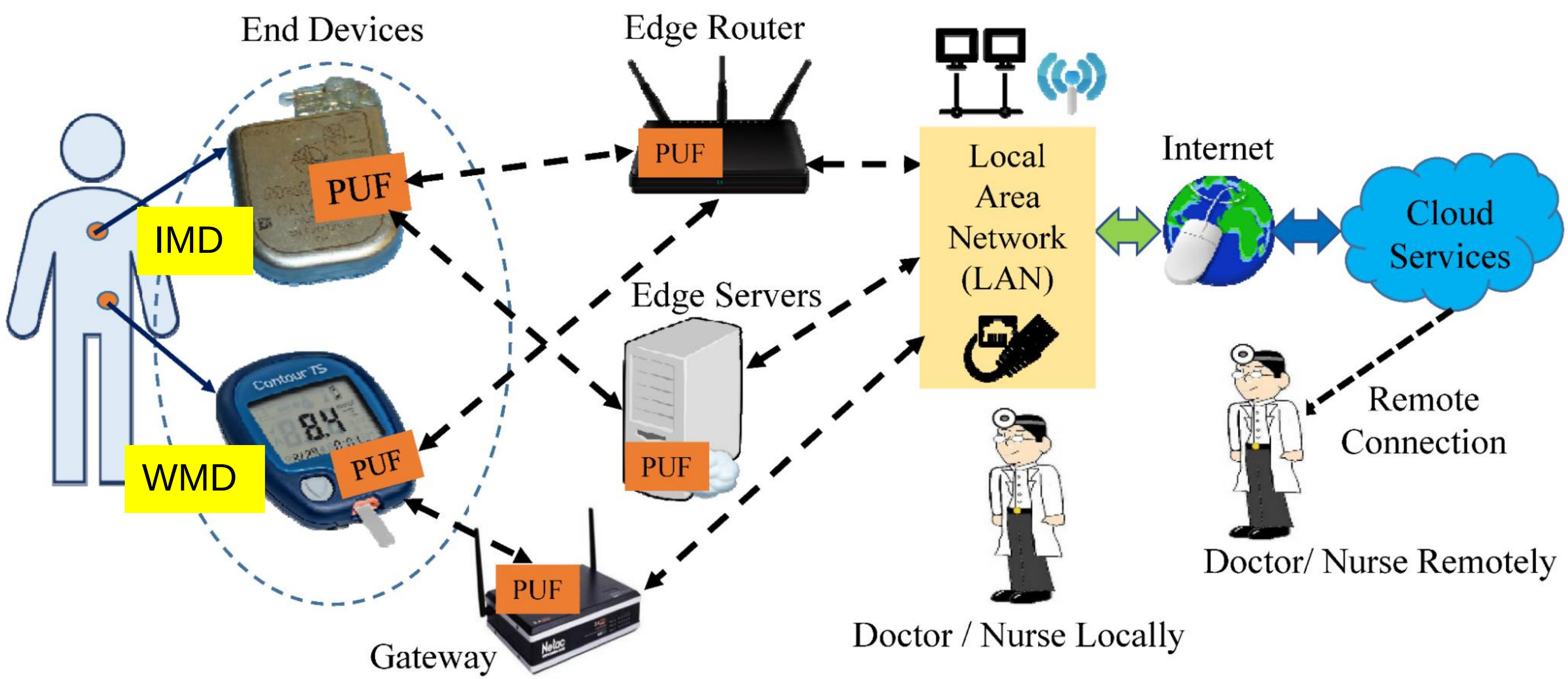


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

Security and/or Privacy by Design (SbD and/or PbD)

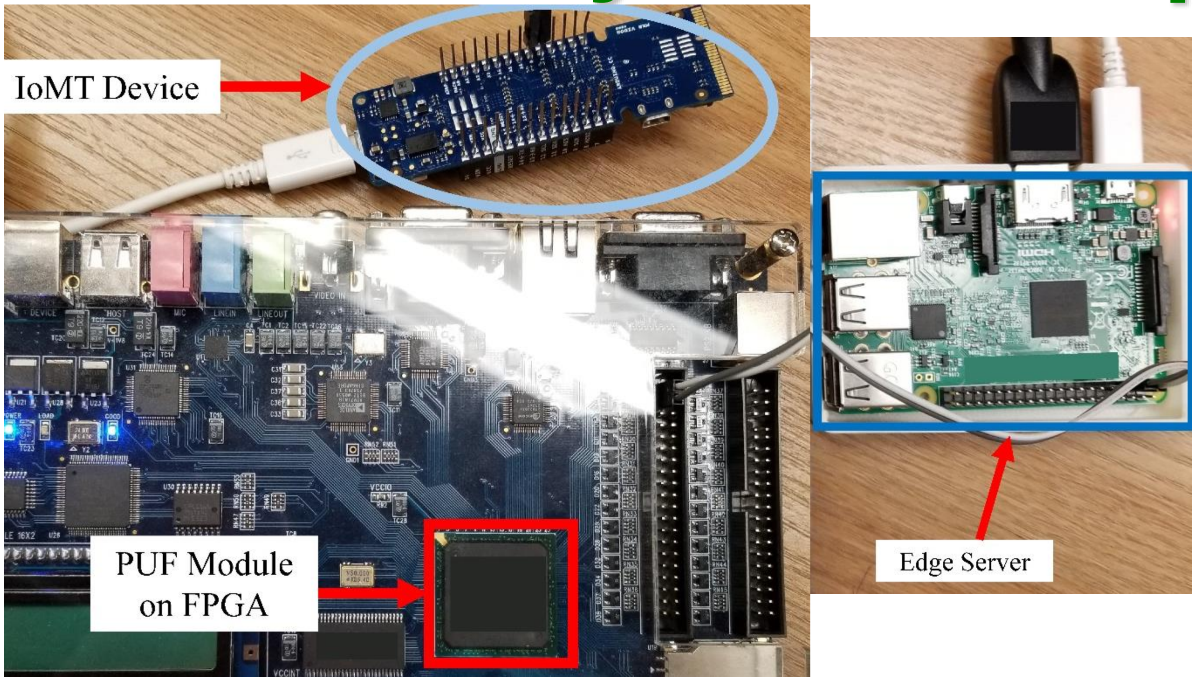
Source: S. P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management", Elsevier Journal of Systems Architecture (JSA), Volume 55, Issues 10-12, October-December 2009, pp. 468-480.

Our Secure by Design Approach for Robust Security in Healthcare CPS



Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security – Our Proposed PMsec



Average Power Overhead –
~ 200 μW

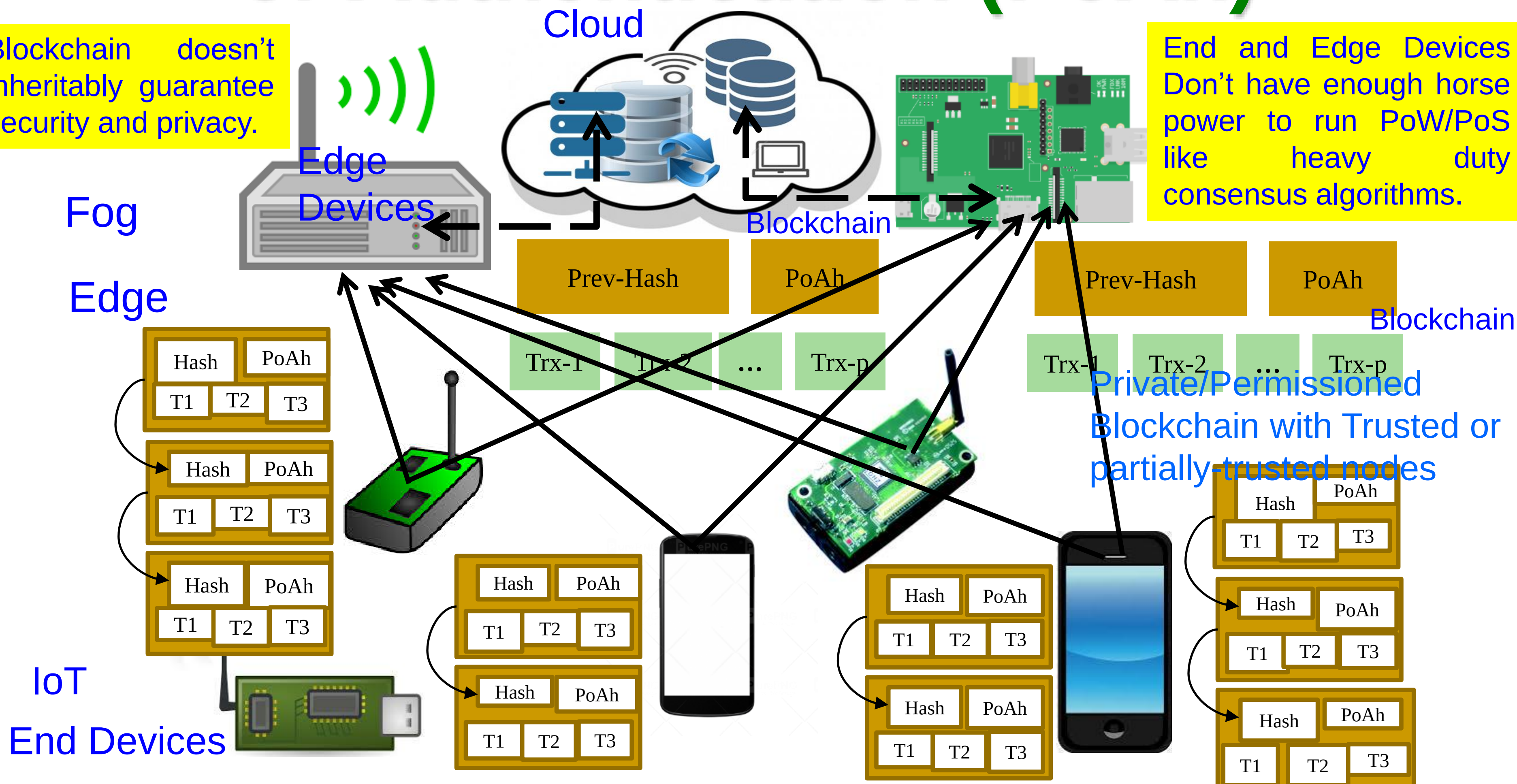
Proposed Approach Characteristics	Value (in a FPGA / Raspberry Pi platform)
Time to Generate the Key at Server	800 ms
Time to Generate the Key at IoMT Device	800 ms
Time to Authenticate the Device	1.2 sec - 1.5 sec

Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

IoT-Friendly Blockchain – Proof-of-Authentication (PoAh)

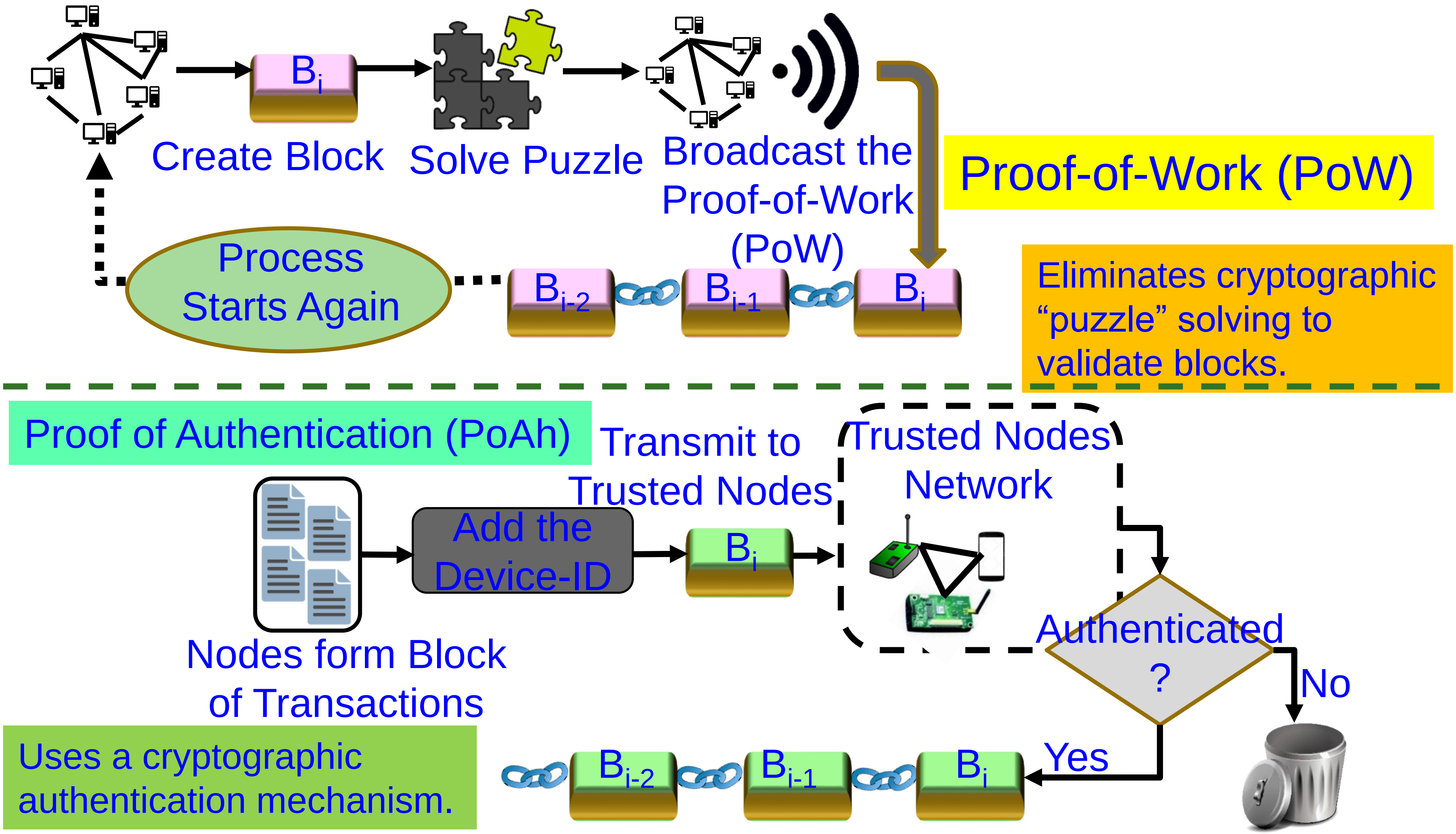
Blockchain doesn't inheritably guarantee security and privacy.

End and Edge Devices Don't have enough horse power to run PoW/PoS like heavy duty consensus algorithms.

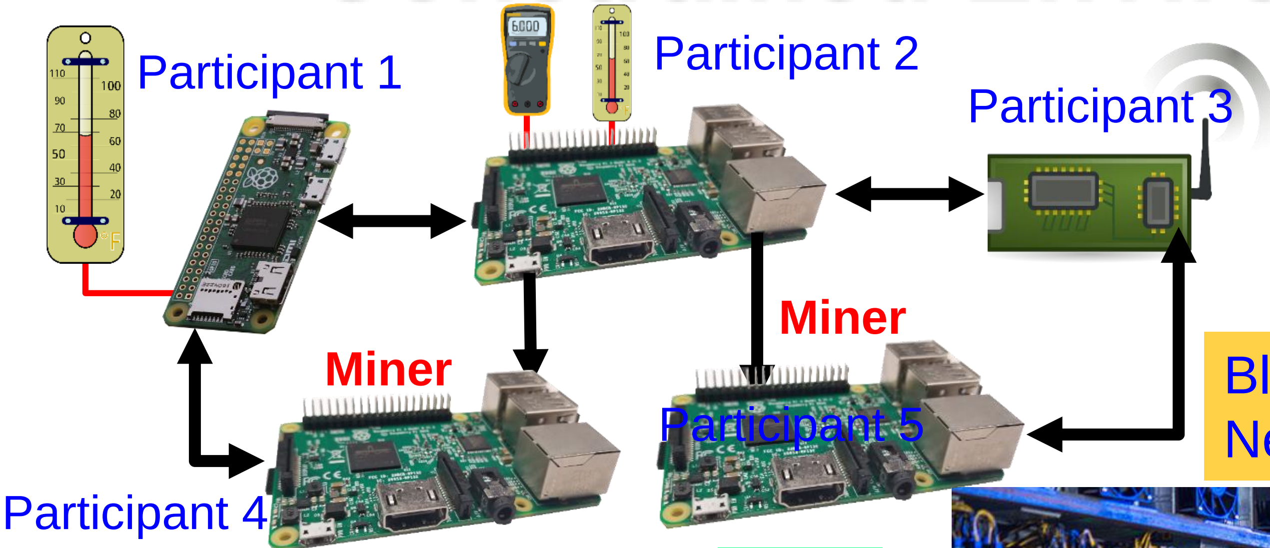


Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Vol. 38, No. 1, January 2019, pp. 26--29.

Our Proof-of-Authentication (PoAh)



Our PoAh-Chain Runs in Resource Constrained Environment



Blockchain using PoW Needs Significant Resource

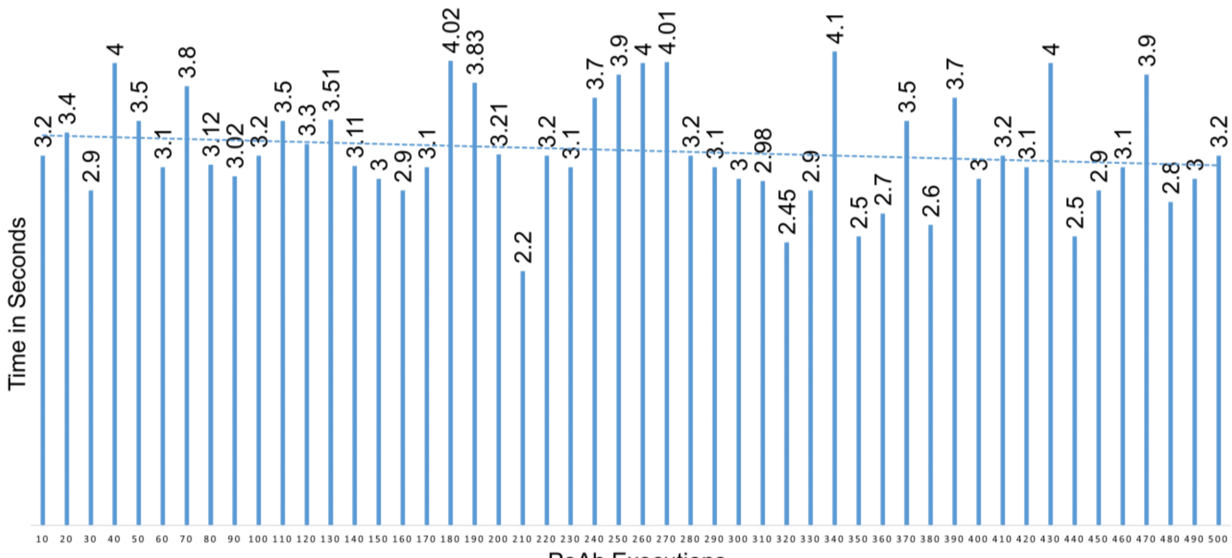
Our PoAh-Chain Runs here

5 W

500,0000 W

Our PoAh is 200X Faster than PoW While Consuming a Very Minimal Energy

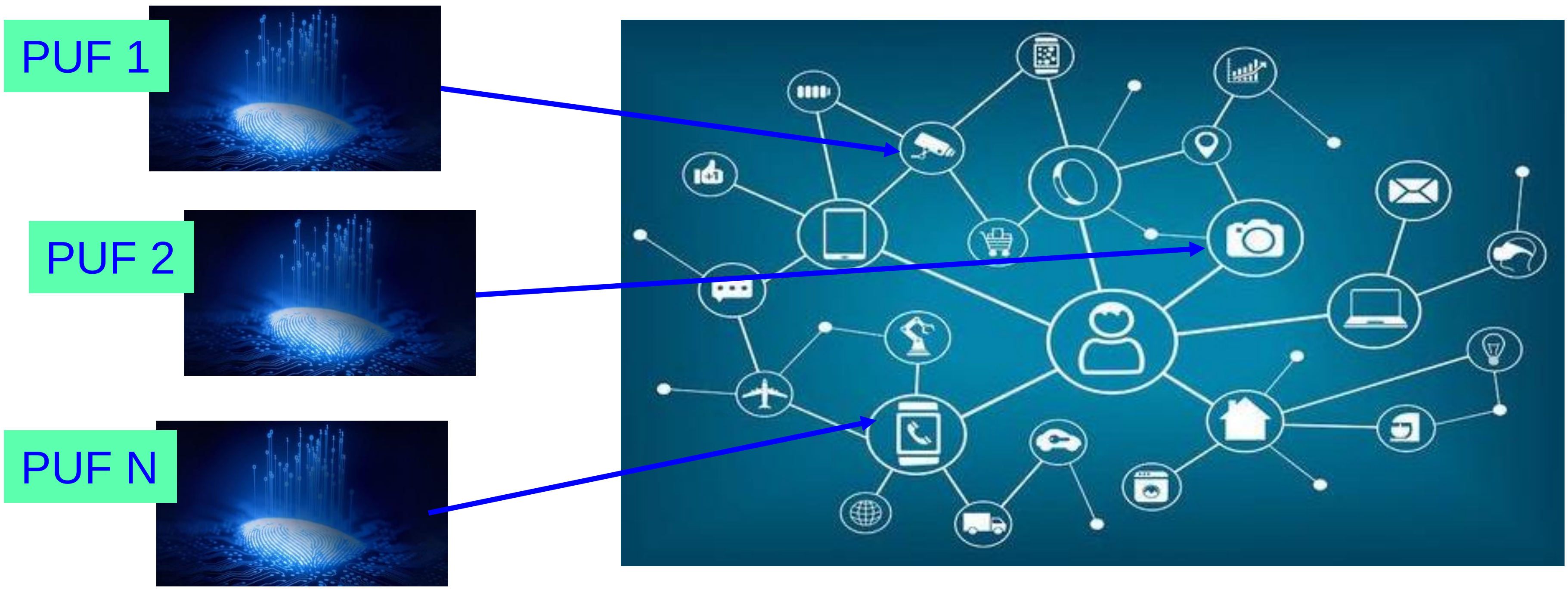
Consensus Algorithm	Blockchain Type	Prone To Attacks	Power Consumption	Time for Consensus
Proof-of-Work (PoW)	Public	Sybil, 51%	538 KWh	10 min
Proof-of-Stake (PoS)	Public	Sybil, Dos	5.5 KWh	
Proof-of-Authentication (PoAh)	Private	Not Known	3.5 W	3 sec



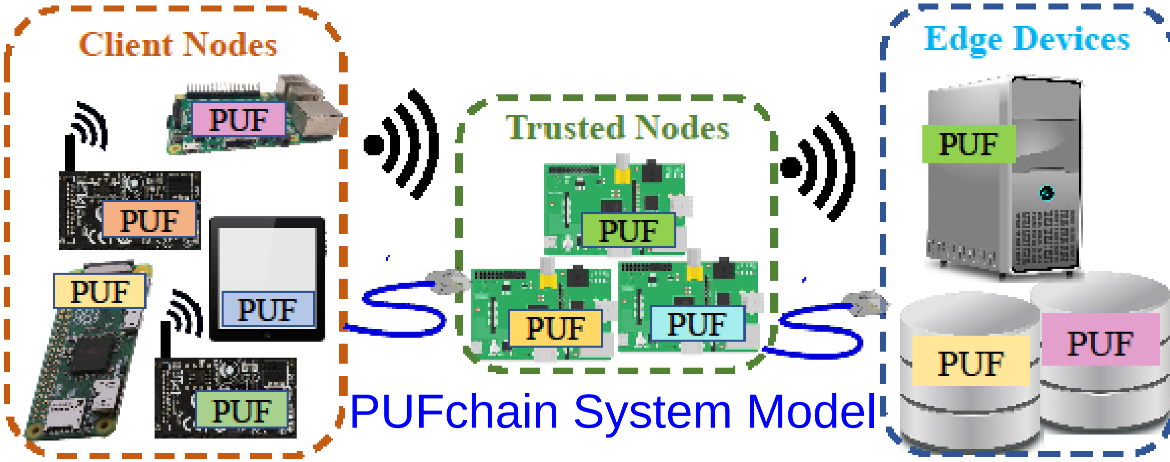
PoAh Execution for 100s of Nodes

Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", in *Proc. 37th IEEE International Conference on Consumer Electronics (ICCE)*, 2019.

We Proposed World's First Hardware-Integrated Blockchain (PUFchain) that is Scalable, Energy-Efficient, and Fast



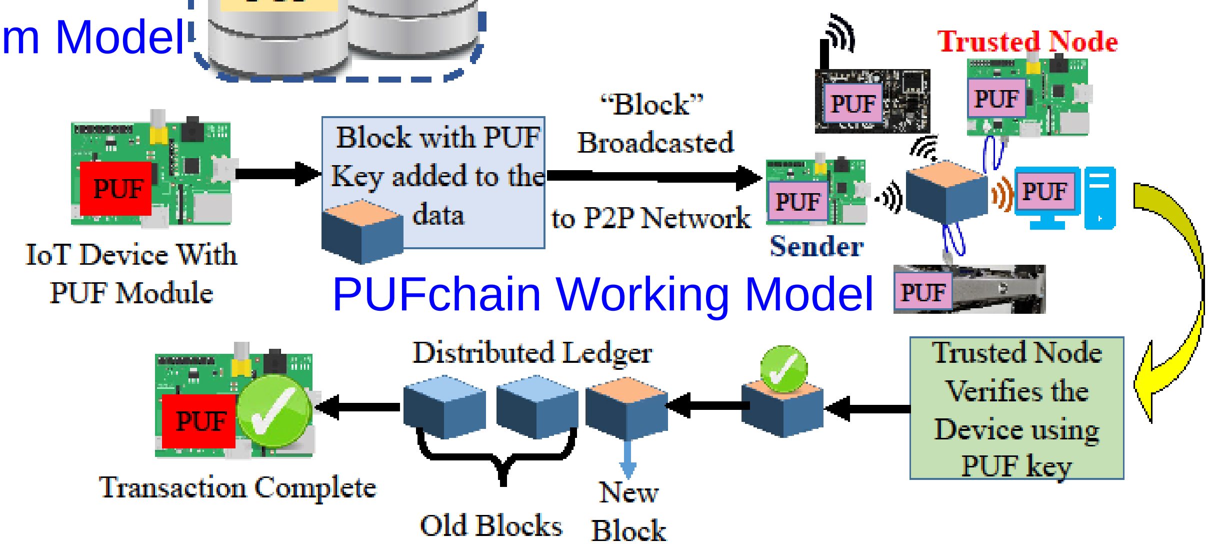
PUFchain: The Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System,
and Data Security

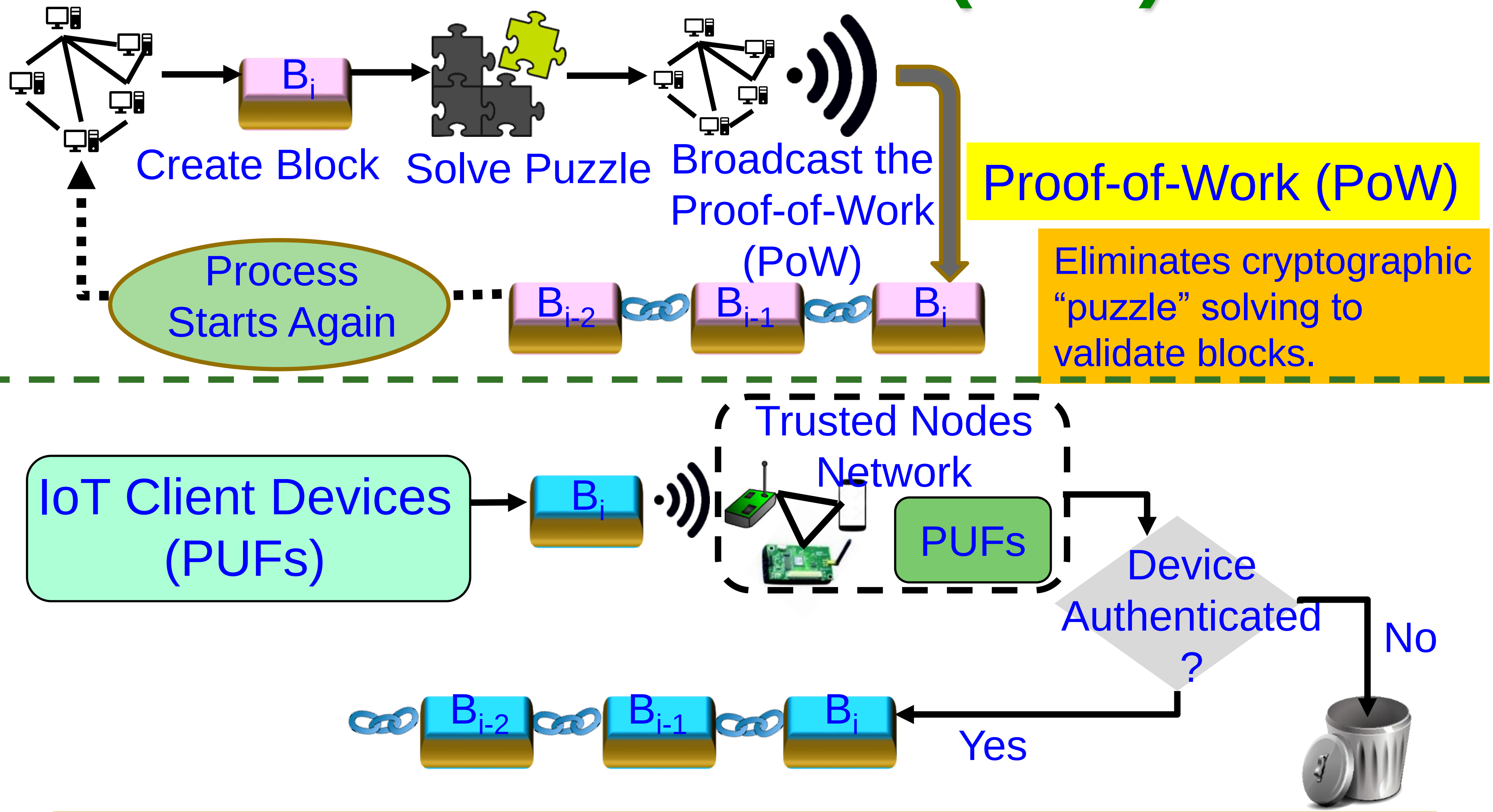
PUFChain 2 Modes:
(1) PUF Mode and
(2) PUFChain Mode



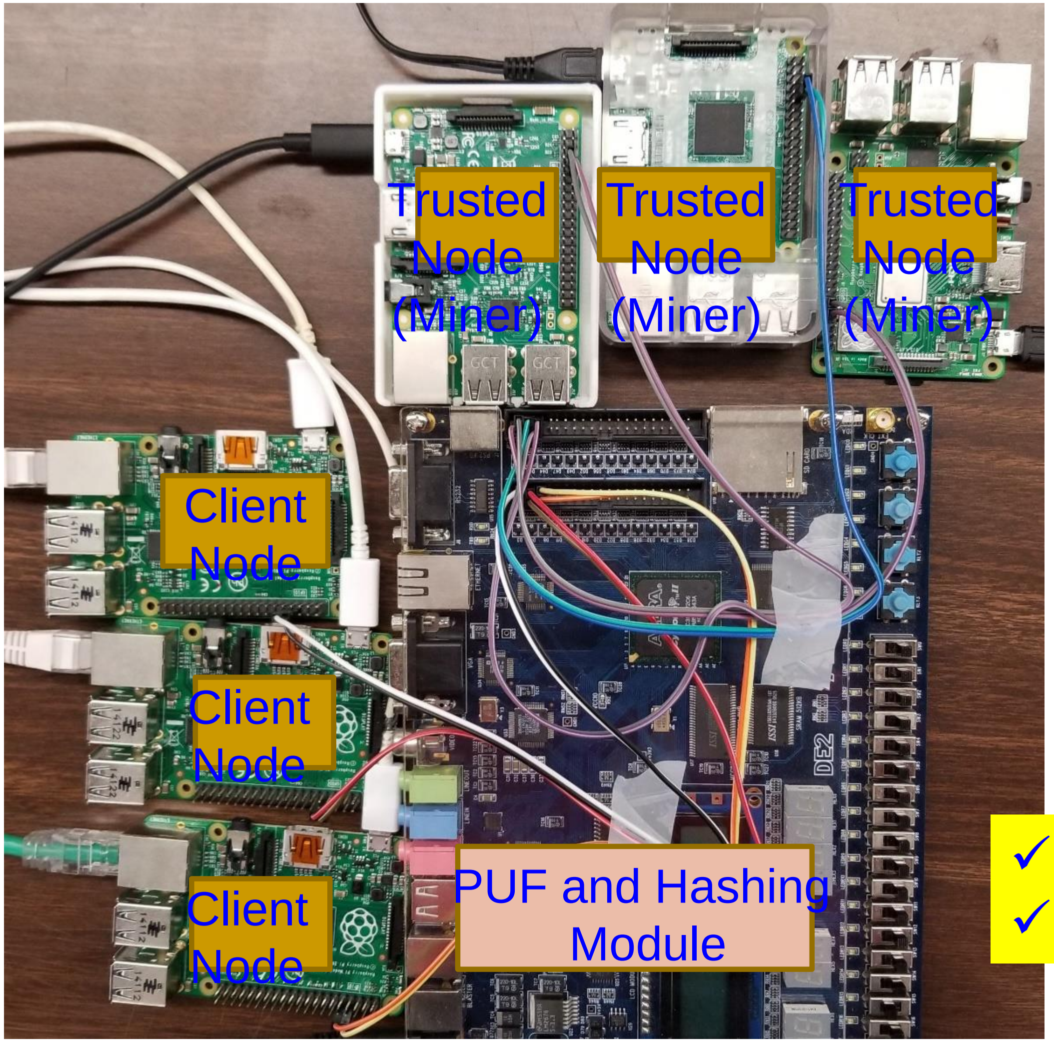
PUFchain Working Model

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

Our Proof-of-PUF-Enabled-Authentication (PoP)



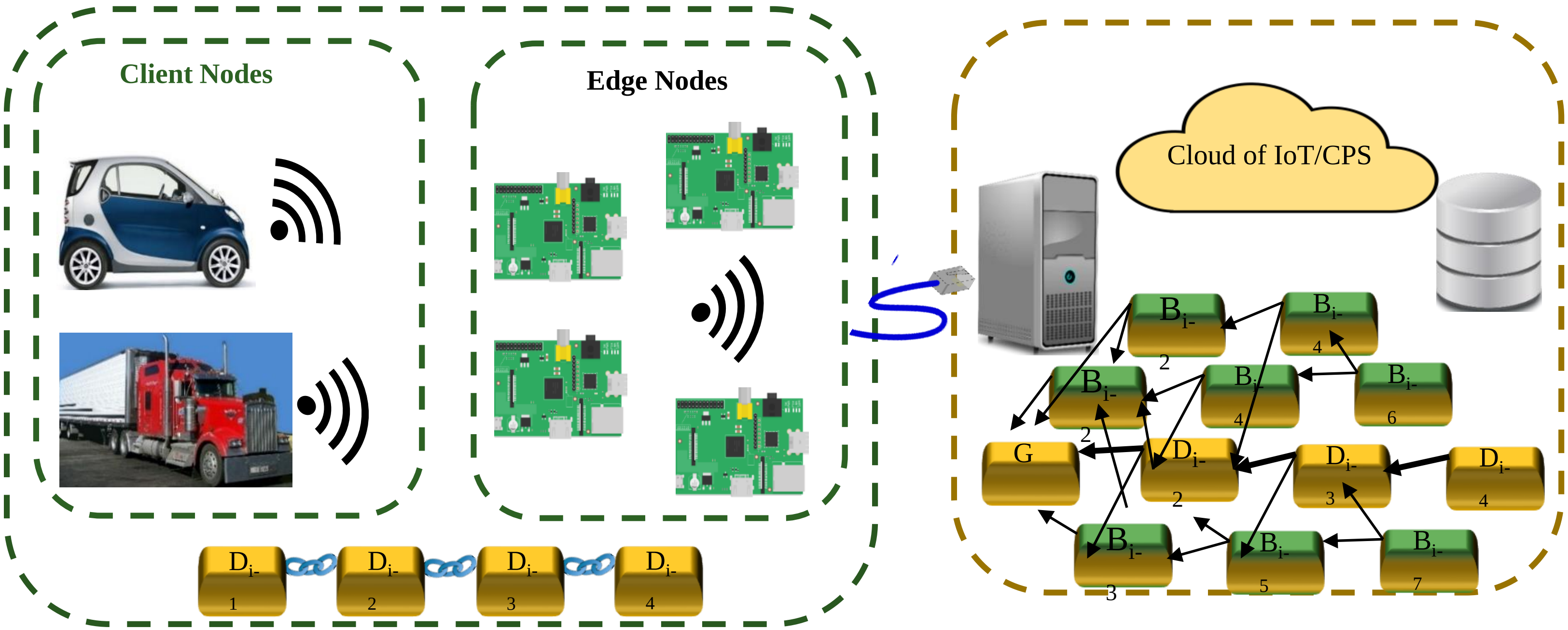
Our PoP is 1000X Faster than PoW



PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

- ✓ PoP is 1,000X faster than PoW
- ✓ PoP is 5X faster than PoAh

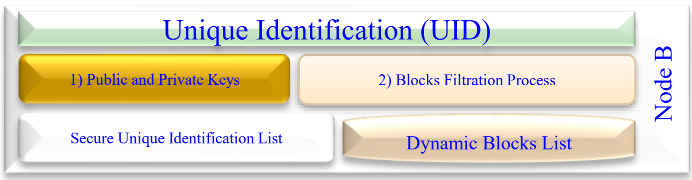
Our Multi-Chain Technology to Enhance Scalability

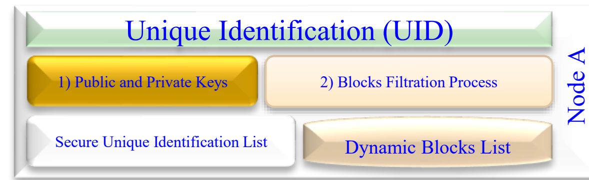


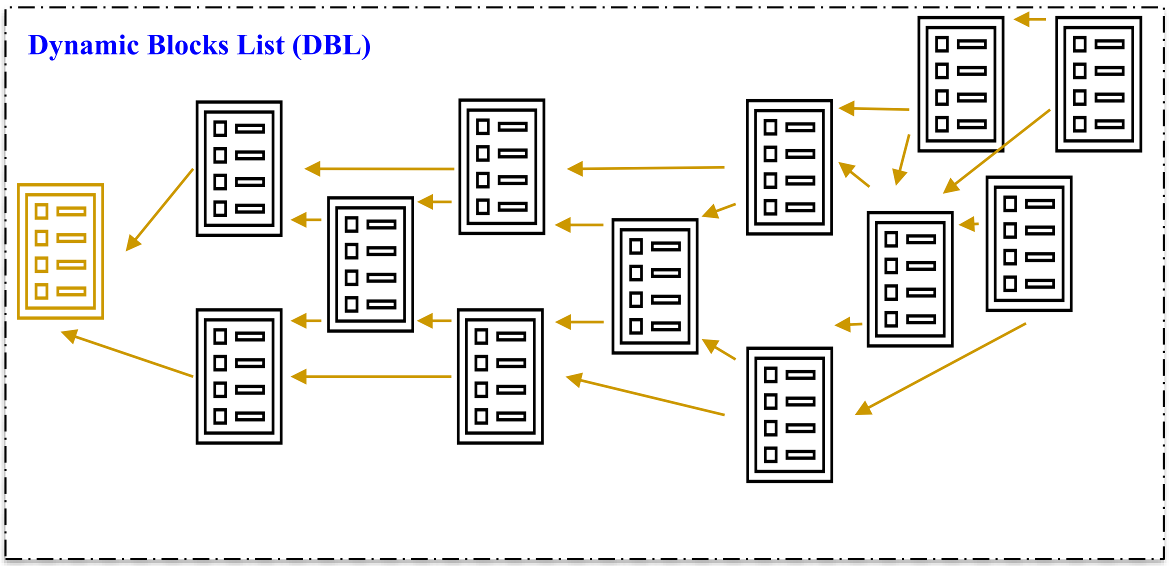
(a) Nodes-Chain (b) Multi-Blockchains

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446--451.

McPoRA -- Components







Secure Unique Identification List (SUIL)

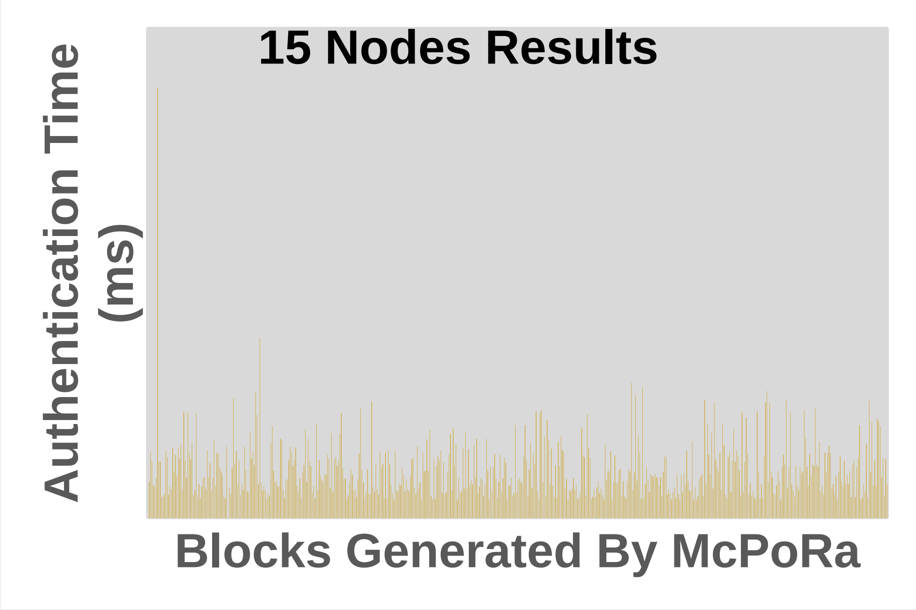
Secure IDs' file consists of all active Nodes joined the Private network.

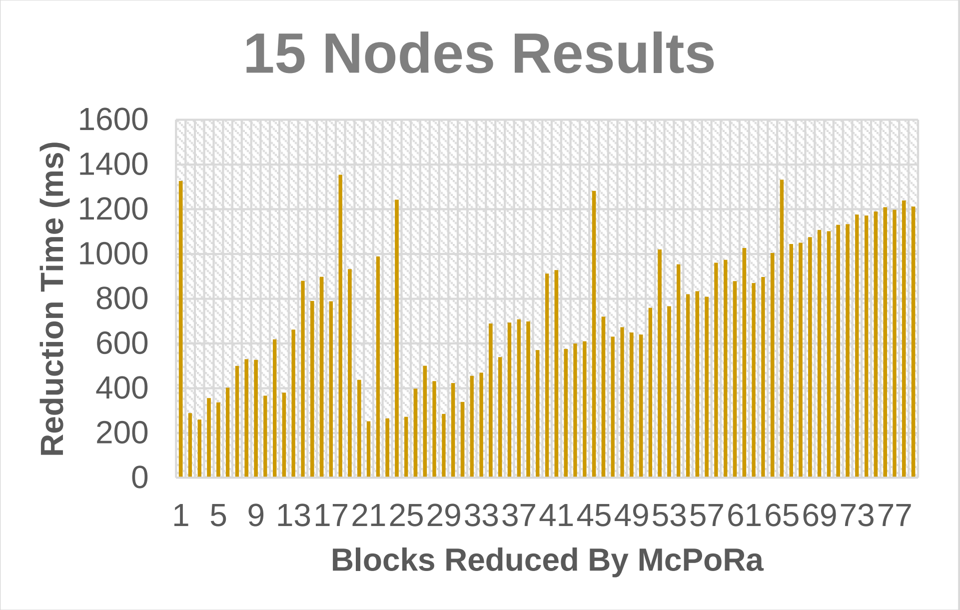
Hashed
Node A Unique Identification (UID)
Node B Unique Identification (UID)
Node C Unique Identification (UID)
Node D Unique Identification (UID)
Node E Unique Identification (UID)
Node F Unique Identification (UID)
Node G Unique Identification (UID)
Node H Unique Identification (UID)
Node I Unique Identification (UID)

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.

McPoRA – Experimental Results

Time (ms)	Authentication (ms)	Reduction (ms)
Minimum	1.51	252.6
Maximum	35.14	1354.6
Average	3.97	772.53





Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, “McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems”, *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.