Towards Better Availability and Accountability for IoT Updates by means of a Blockchain

Aymen Boudguiga, Nabil Bouzerna, Louis Granboulan, Alexis Olivereau, Flavien Quesnel, Anthony Roger, Renaud Sirdey

Accélérateur de la transformation numérique

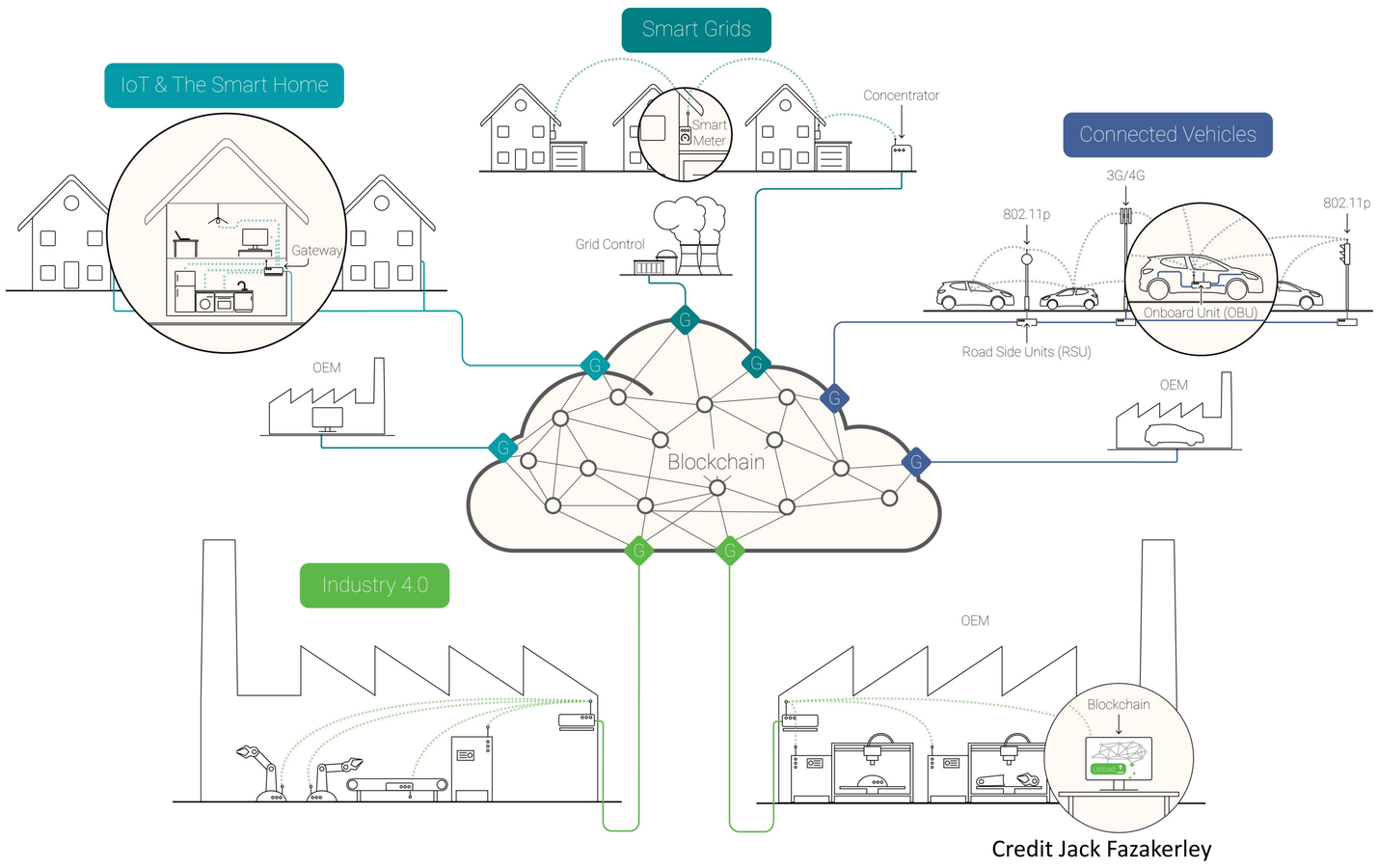
IEEE Security & privacy on the Blockchain 2017 (IEEE S&B 2017) - 29 April 2017

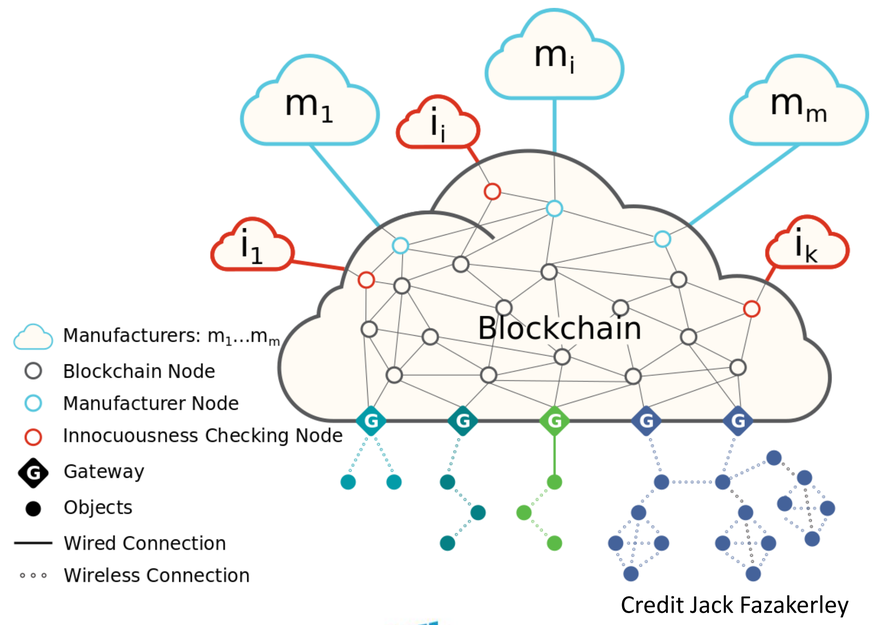
Towards Better Availability and Accountability for IoT Updates by means of a Blockchain

Aymen Boudguiga, Nabil Bouzerna, Louis Granboulan, Alexis Olivereau,
Flavien Quesnel, Anthony Roger and Renaud Sirdey

Context: Internet of Things

- Huge number of devices with full or limited connectivity to the Internet
- By 2030, around 30 billions of devices will exchange hundred of zettabytes of data
- Massive deployment ➔ more vulnerabilities ➔ need for a universal software update infrastructure





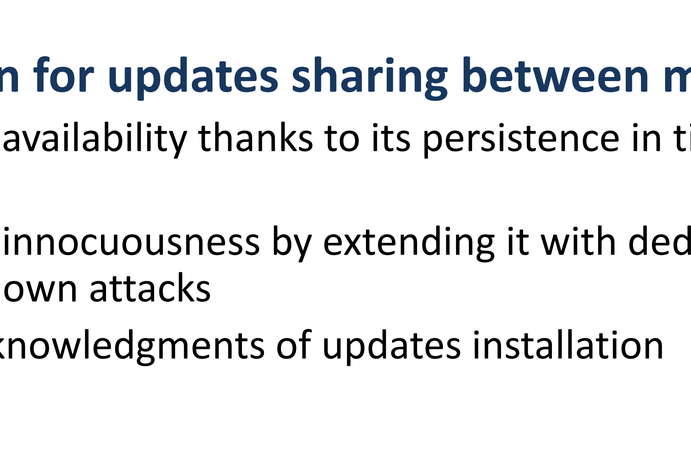
BLOCKCHAIN

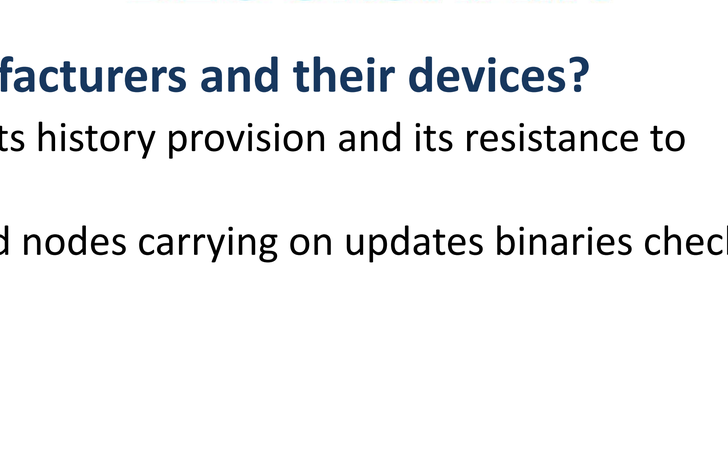
Idea: why not use a blockchain for updates sharing between manufacturers and their devices?

- Blockchain provides updates availability thanks to its persistence in time, its history provision and its resistance to Denial of Services attacks
- Blockchain provides updates innocuousness by extending it with dedicated nodes carrying on updates binaries checking against vulnerabilities and known attacks
- Blockchain stores devices acknowledgments of updates installation

IRT SystemX Prototype:

- Use of Multichain, a permissioned blockchain
- Use of Bitcoin blockchain for Multichain bootstrap
- Blockchain update infrastructure deployed on VMs
- Devices implemented physically (tens of raspberry pi) or virtually (up to 800 VMs per server)
- PGP keys usage for updates encryption and signature





Publication at:

- IEEE Security & privacy on the Blockchain 2017 (IEEE S&B 2017) - 29 April 2017

Contact : nabil.bouzerna@irt-systemx.fr