



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

► To cite this version:

Aymen Boudguiga, Nabil Bouzerna, Louis Granboulan, Alexis Olivereau, Flavien Quesnel, et al.. Towards Better Availability and Accountability for IoT Updates by means of a Blockchain. IEEE EUROCRYPT Security & privacy on the Blockchain 2017 (IEEE S&B 2017), Apr 2017, Paris, France. , 2017. hal-01536096

HAL Id: hal-01536096

<https://hal.science/hal-01536096>

Submitted on 10 Jun 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

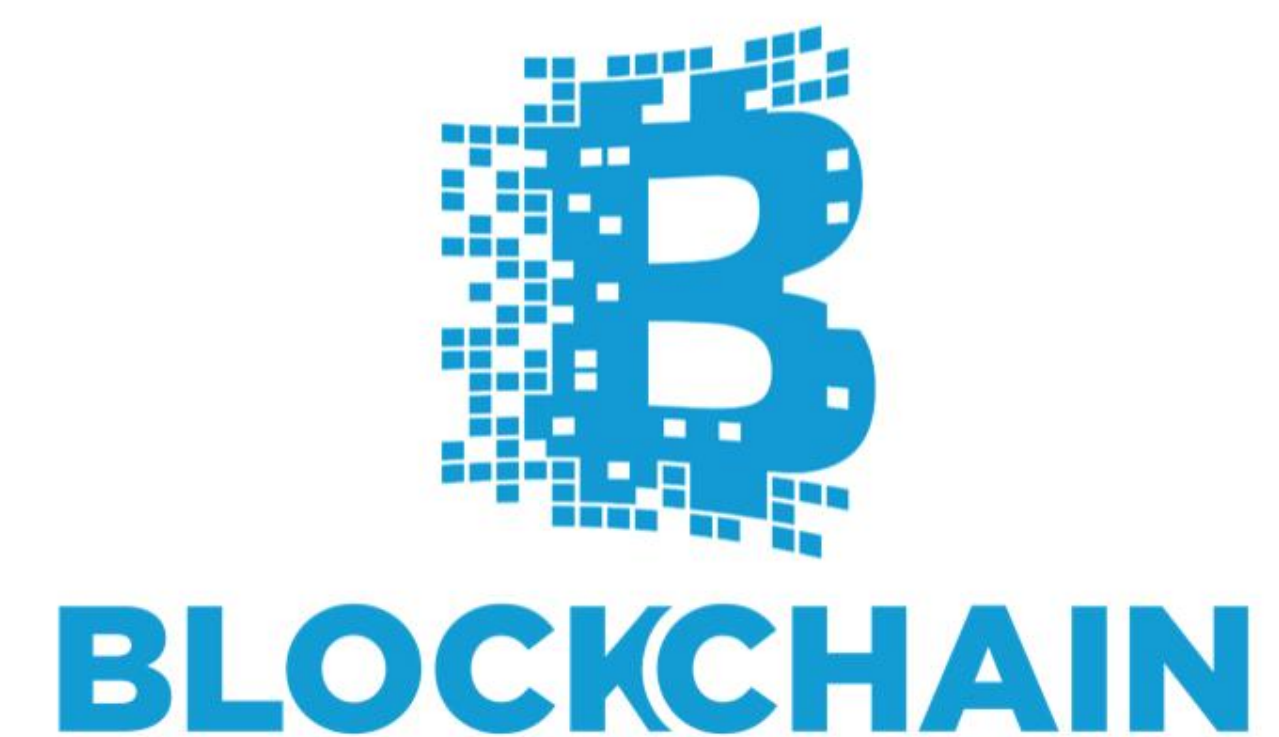
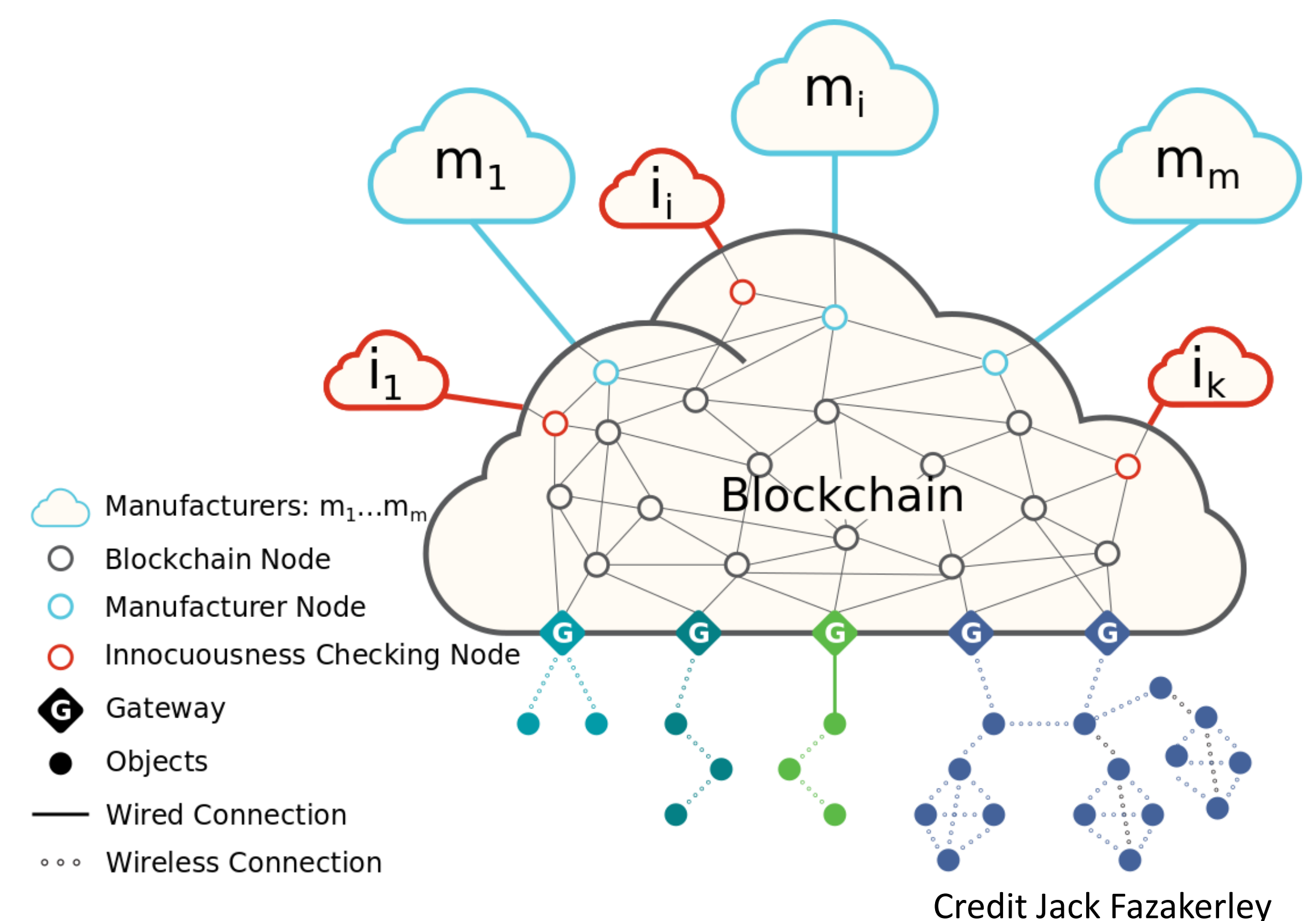
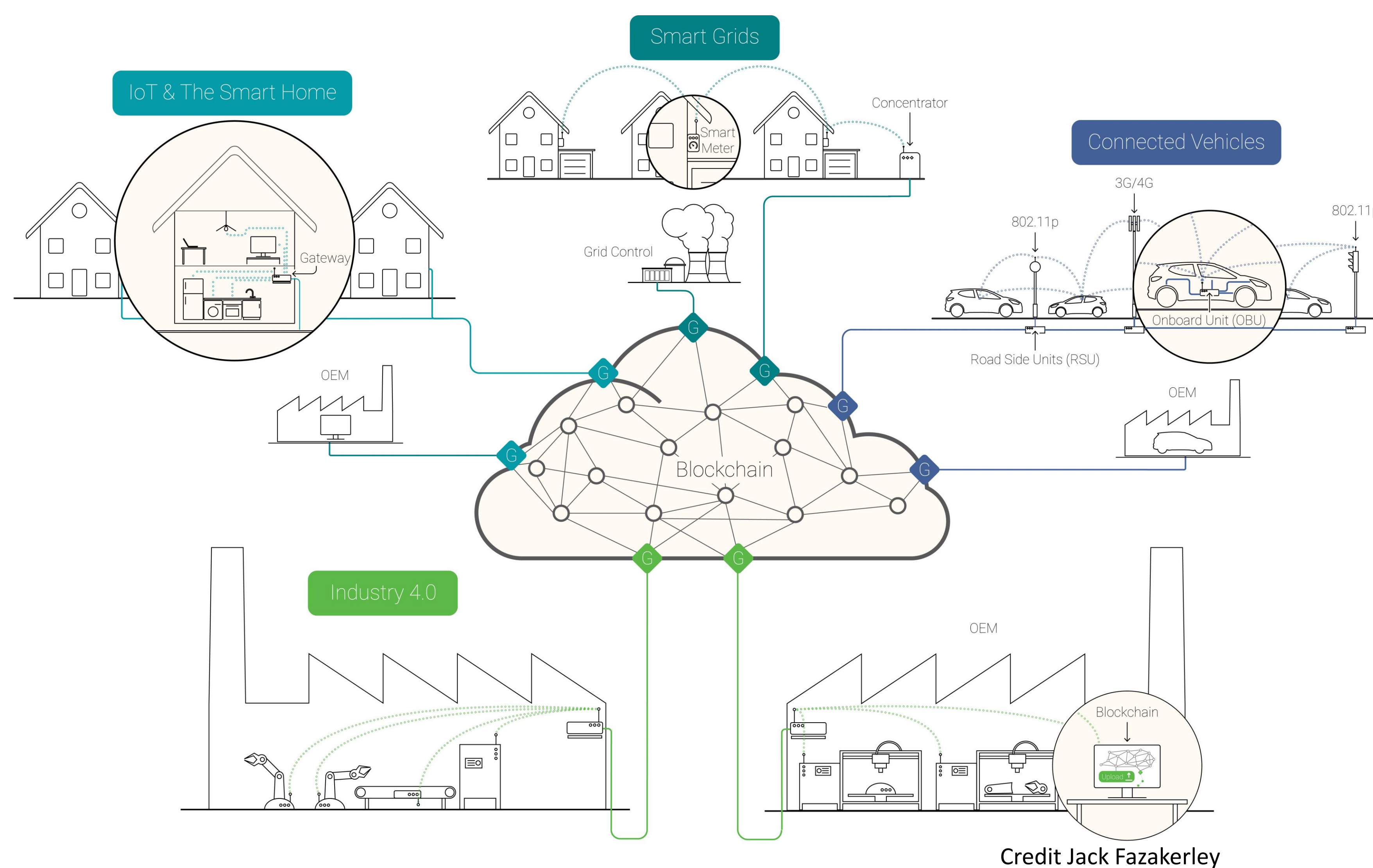
Copyright

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

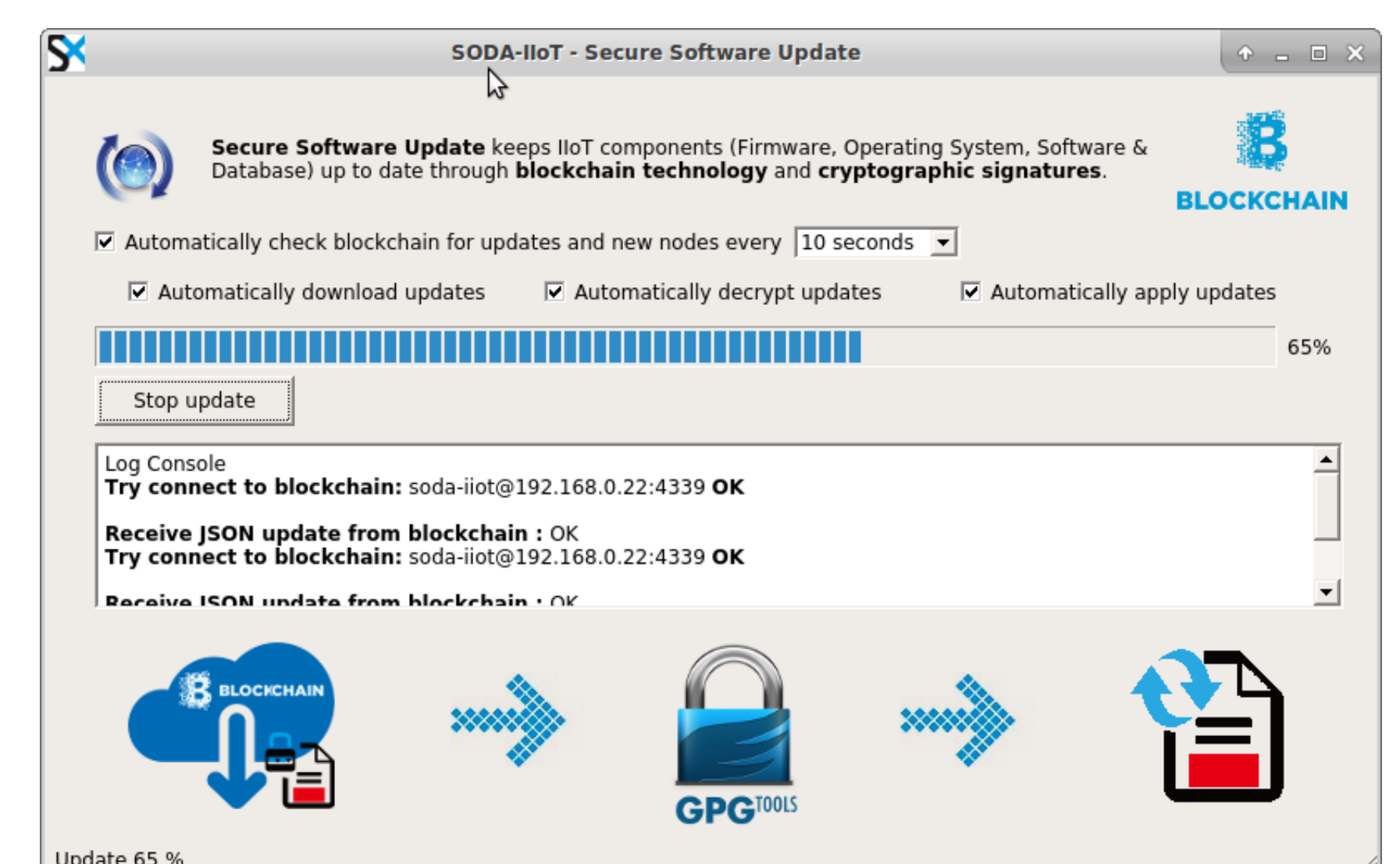
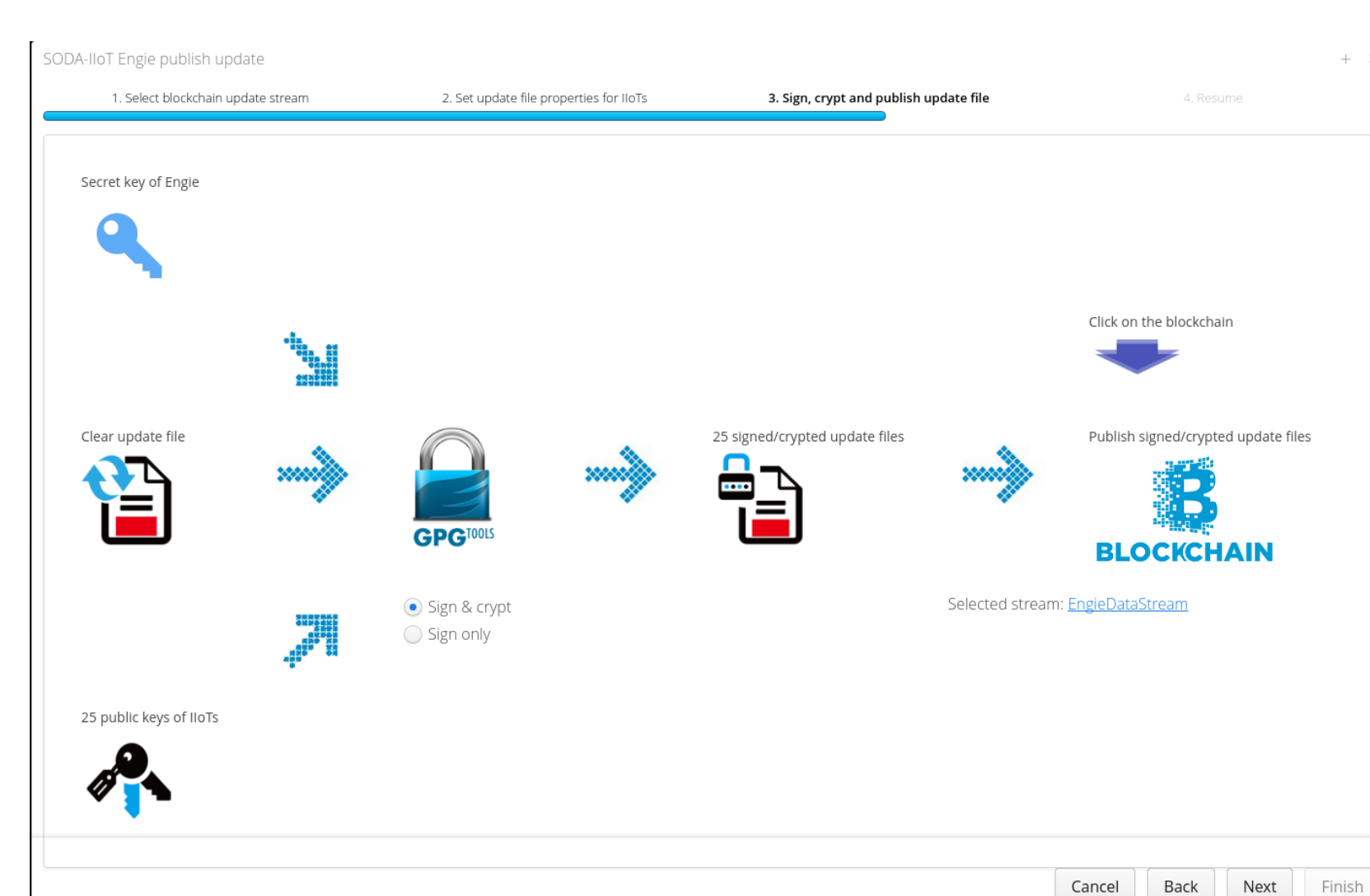
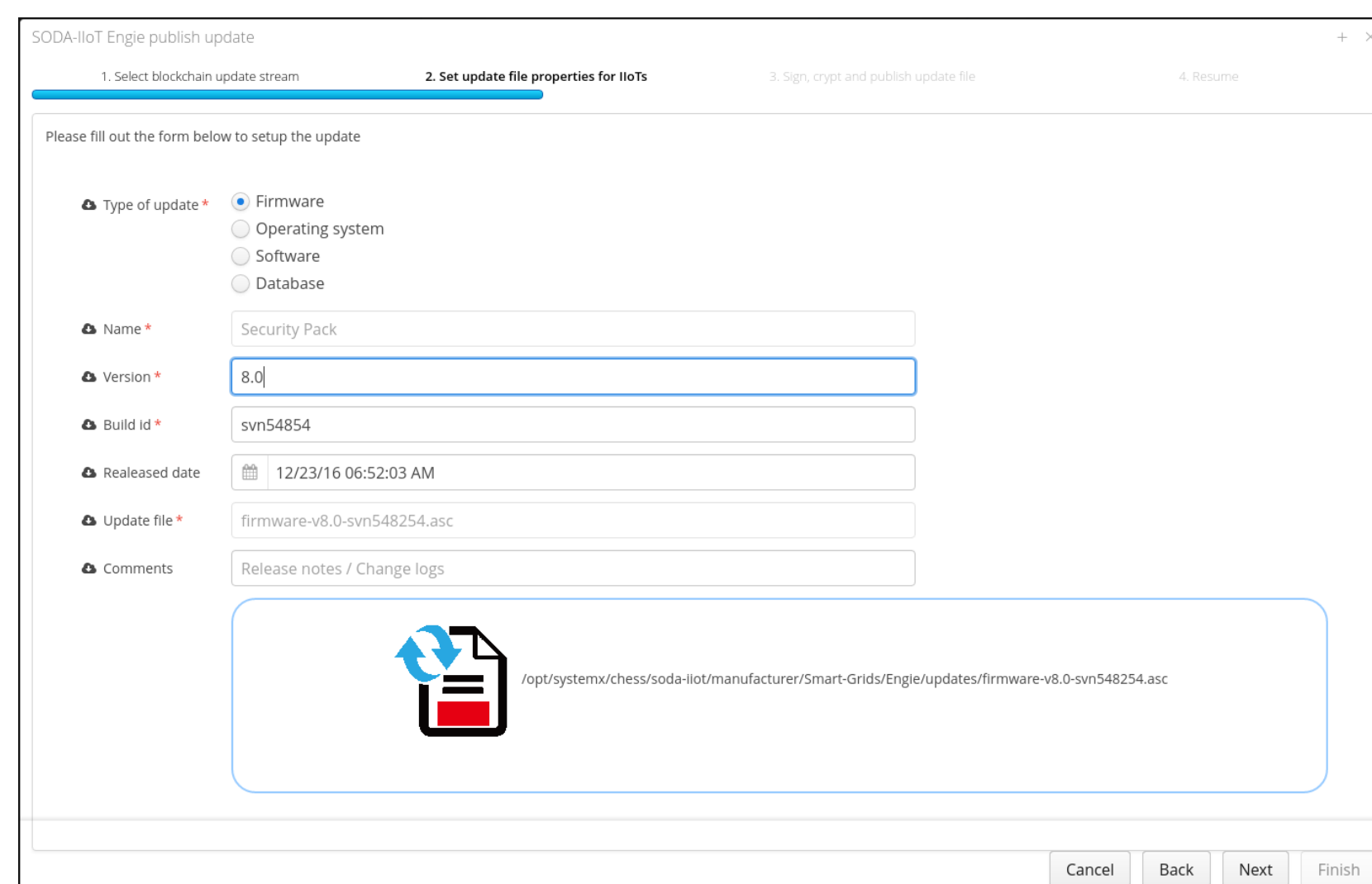


Idea: why not use a blockchain for updates sharing between manufacturers and their devices?

- 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