Flash Memory Summit

Firewall of Things, Firewall of Memory Chips

Hiroshi Watanabe

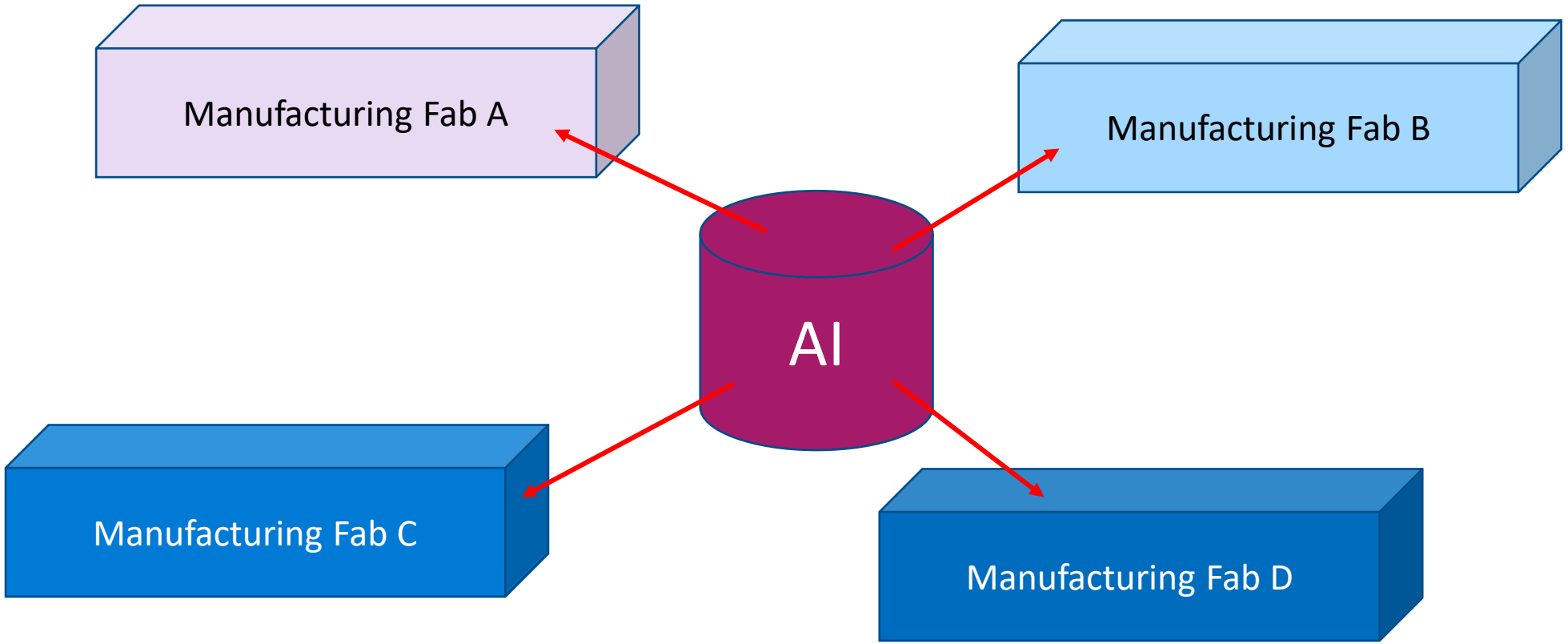
National Yang Ming Chiao Tung University

35 YEARS OF NAND FLASH MEMORY INNOVATION

Global manufacturing systems

Flash Memory Summit

To more efficiently use AI in the global manufacturing, the remote-control shall become indispensable undoubtedly.



35 YEARS OF NAND FLASH MEMORY INNOVATION

A rough estimation using moderate scale semiconductor manufacturing

Flash Memory Summit

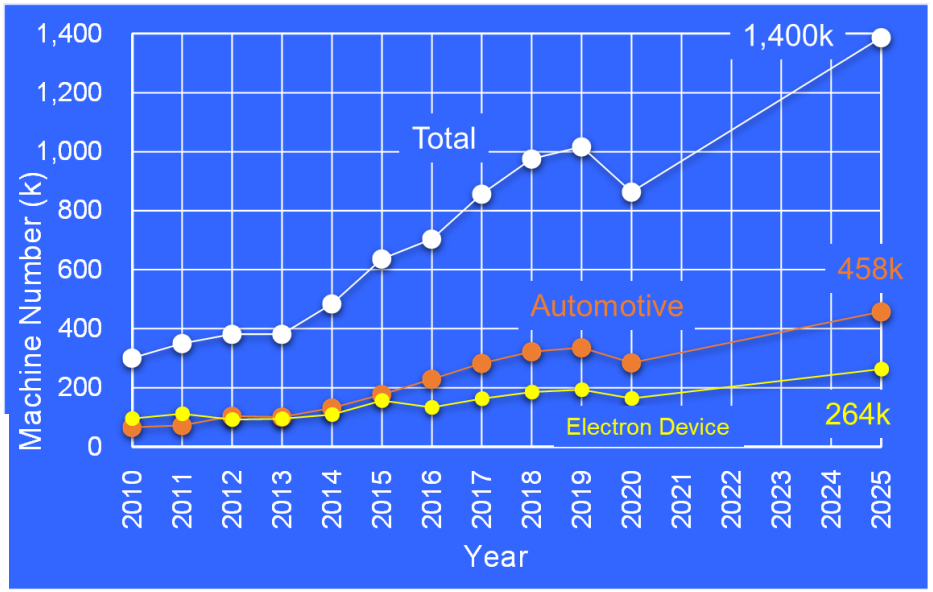
Semiconductor fabs

Fab Capacity	Estimated units
40 ~ 45k	2 ~ 3k
> 100k	5 ~ 7k

(wafer/month)

Researched by

Widevil© Technology Research



- Market is increasing.
- Any types of industries, in any countries/regions, all of manufacturing is an attacking target.

Company names (countries/regions)	Summary
BlueScope Steel Limited (Australia) Steal	In May 2020, the production line ceased running; which affects the Business.
ASCO Industries (Belgian) Aerospace	Belgian aircraft parts maker. In June 2019, the factories in EU and NA stopped production.
Norsk Hydro ASA (Norway) Aluminum	A big enterprise of Aluminum. In March 2019, the factories stopped production all over the world. The amount of loss is more than 70-MUSD.
HOYA (Japan) Optical lens	In Feb. 2019, the virus infection was found in Thailand. The production of lens had ceased running for 3-months.
TSMC (Taiwan)	In August 2019, the factory stopped production. The amount of loss is about 240 M-USD.
Merck (USA) Life-Bio Science	In June 2017, the production line ceased running. The amount of loss is about 870 M-USD
Honda (Japan) Motorization	All N. American auto assembly plants were suspended for six days (Mar. 23, 2020)
Colonial Pipeline Pipeline system	In May 2021, the largest pipeline system for refined oil products in US stopped.

35 YEARS OF NAND FLASH MEMORY INNOVATION

AI is demanded but is an attacking target.

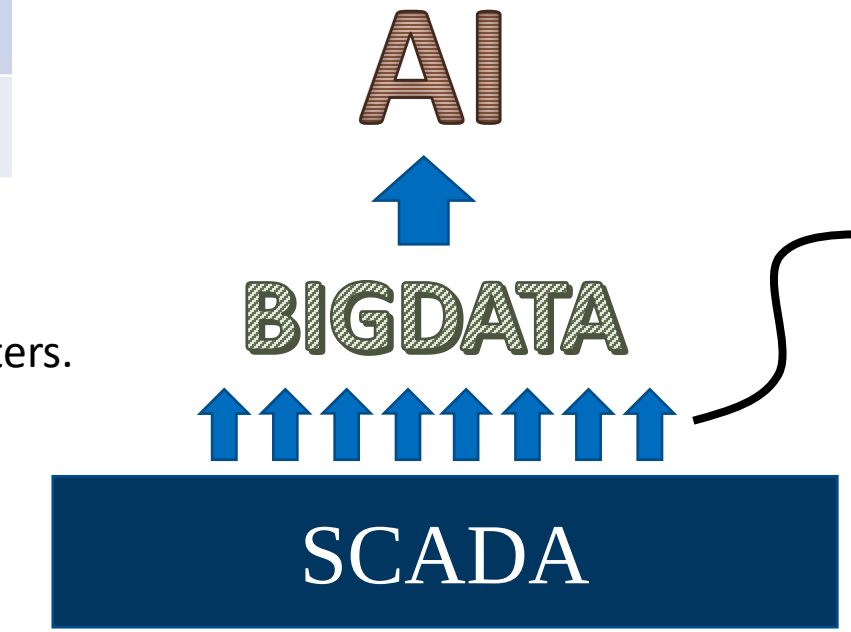
Semiconductor fabs

Fab Capacity	Estimated units	No. parameters
40 ~ 45k	2 ~ 3k	200 ~ 300k
> 100k	5 ~ 7k	500 ~ 700k

(wafer/month)

SCADA/IoT sensors collect parameters.

It malfunctions with manipulated data being input.



Trustworthy?

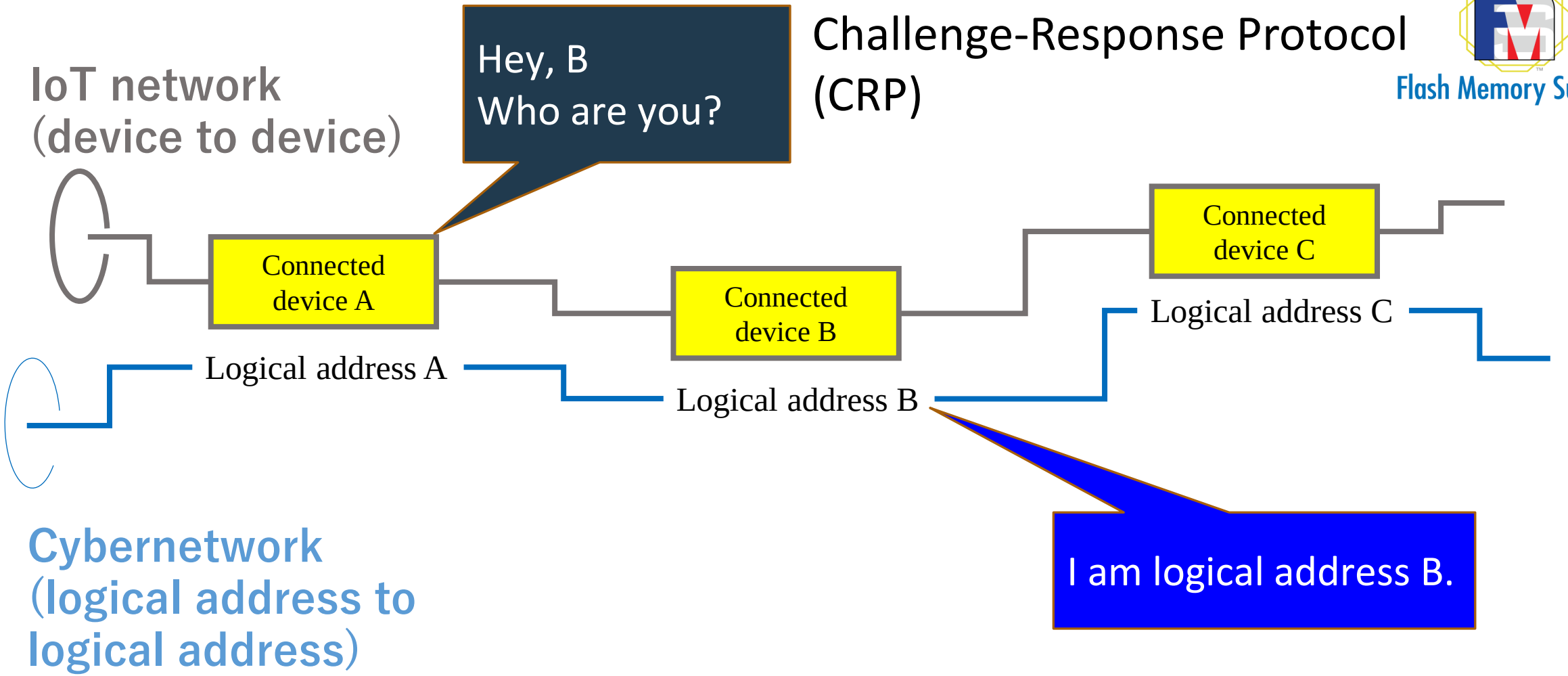
Otherwise

Oracle Problem

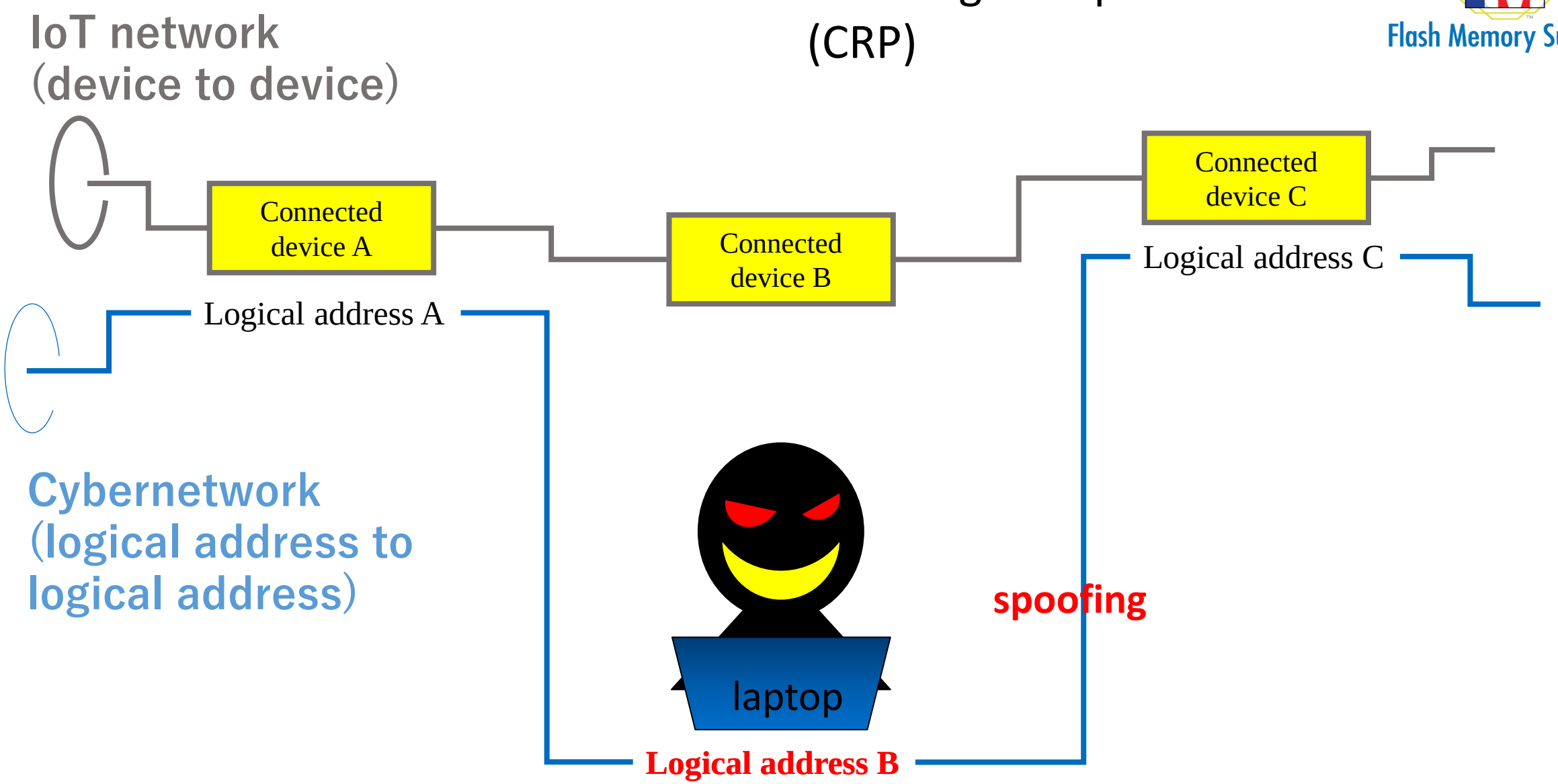
SCADA = Supervisory control and data acquisition

National Taiwan University, National Yang-Ming Chiao-Tung University, Asia University, SEMI/E187

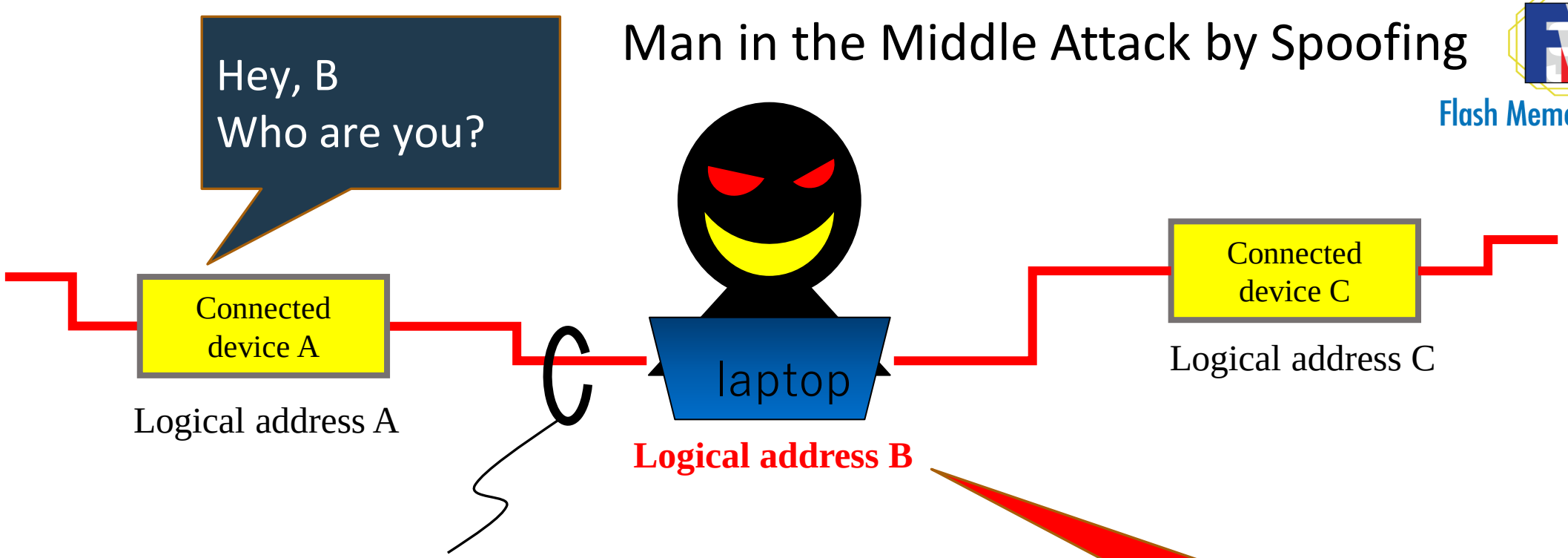
Challenge-Response Protocol (CRP)



Challenge-Response Protocol (CRP)



Man in the Middle Attack by Spoofing

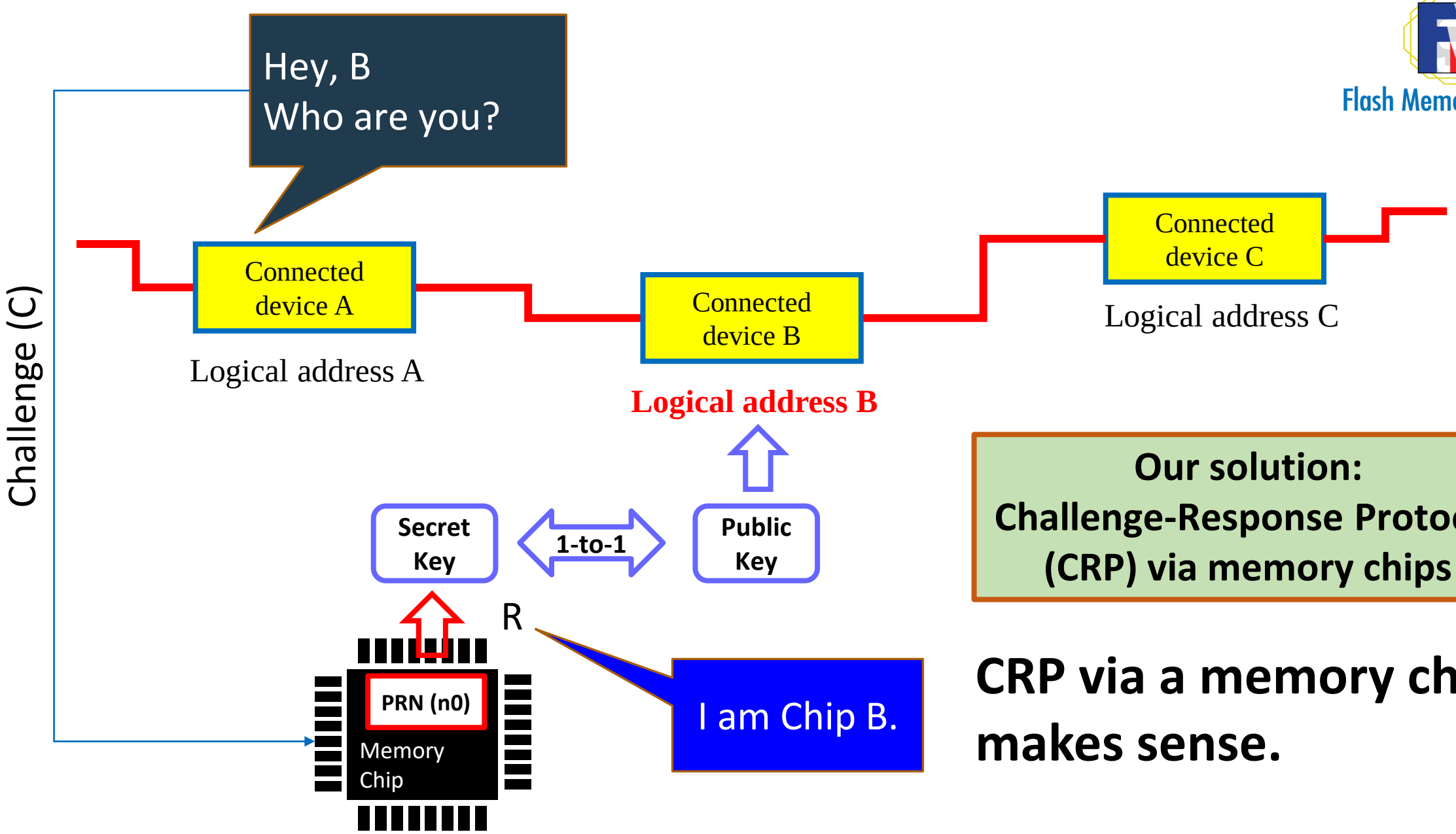


Protected by Blockchain (BC)

Difficult to **find if spoofed or not.**

Root of Trust

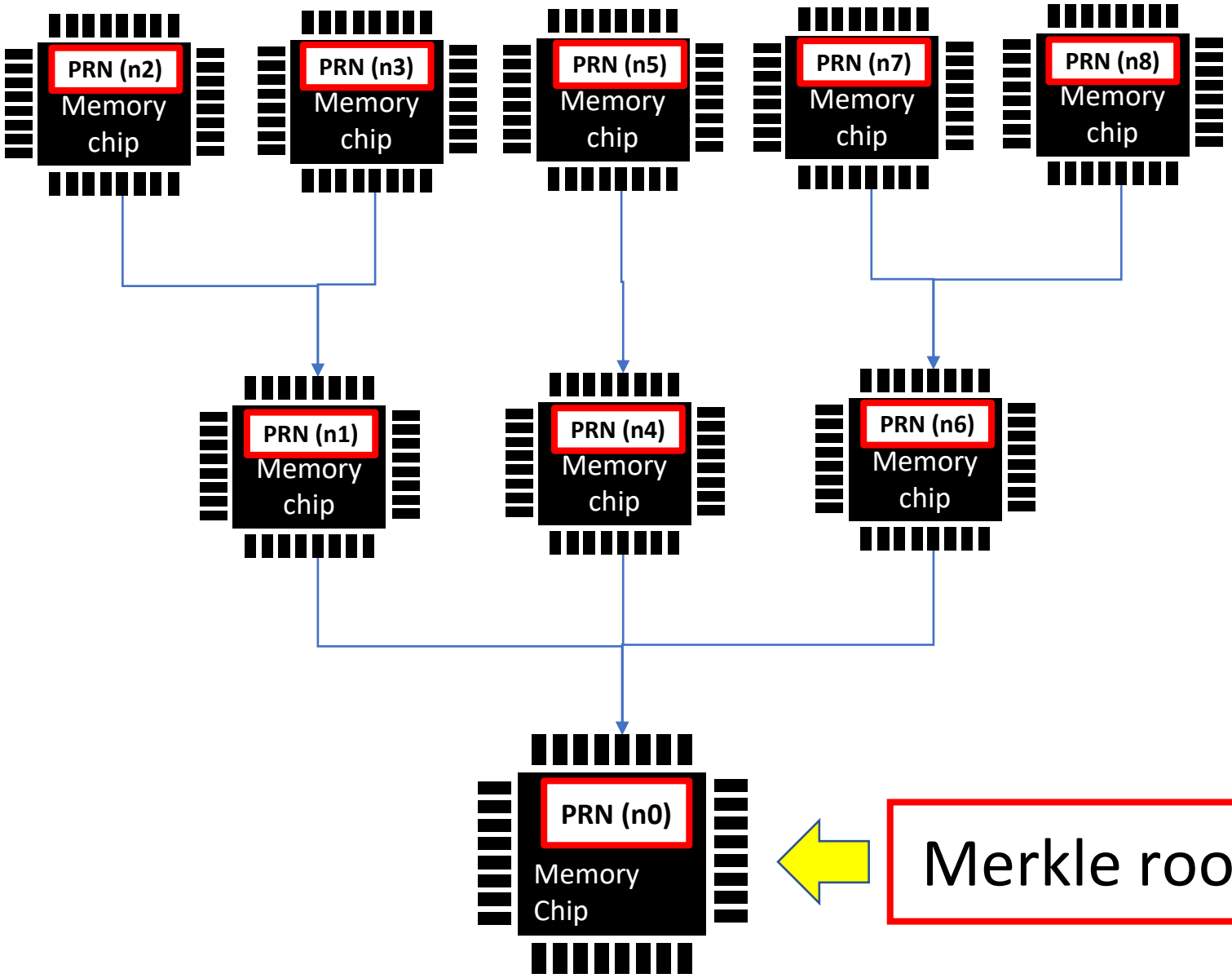
CRP does not make sense.



Our solution: Challenge-Response Protocol (CRP) via memory chips

CRP via a memory chip makes sense.

PRN = Physical Random Number

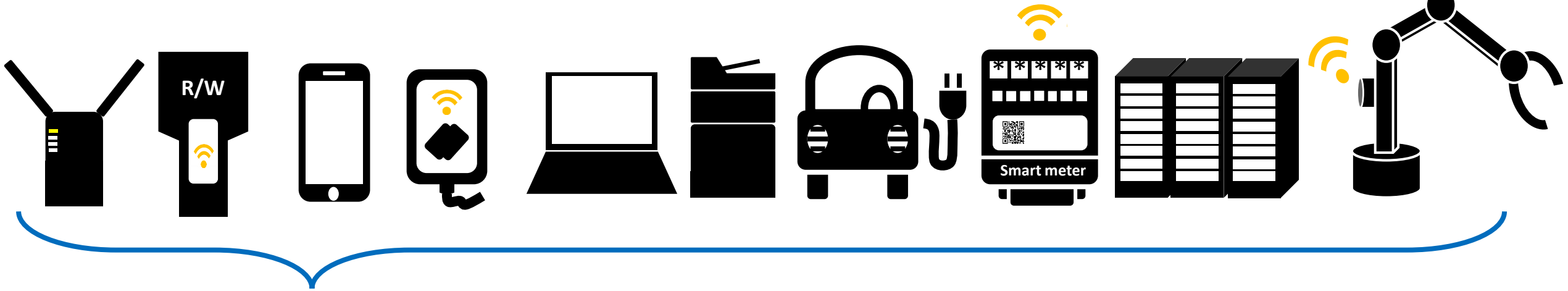


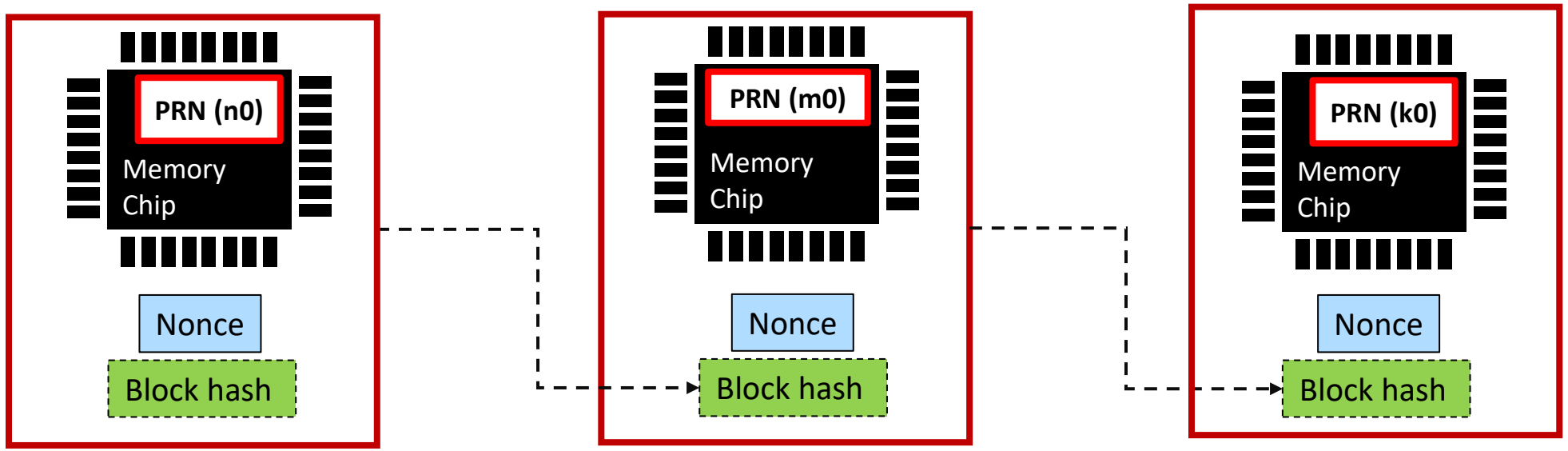
Merkle tree of memory chips

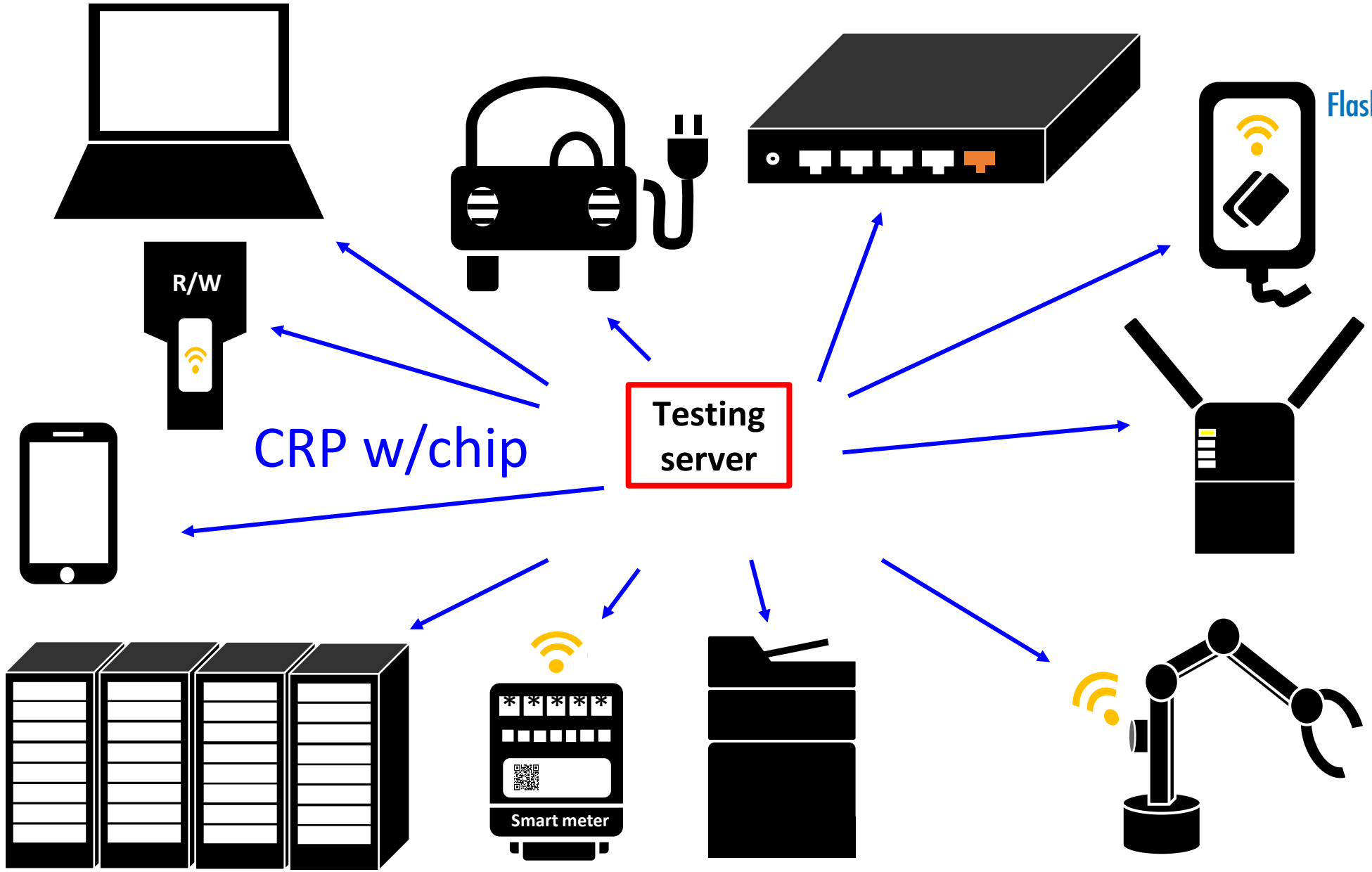
Our solution: Challenge-Response Protocol (CRP) via memory chips

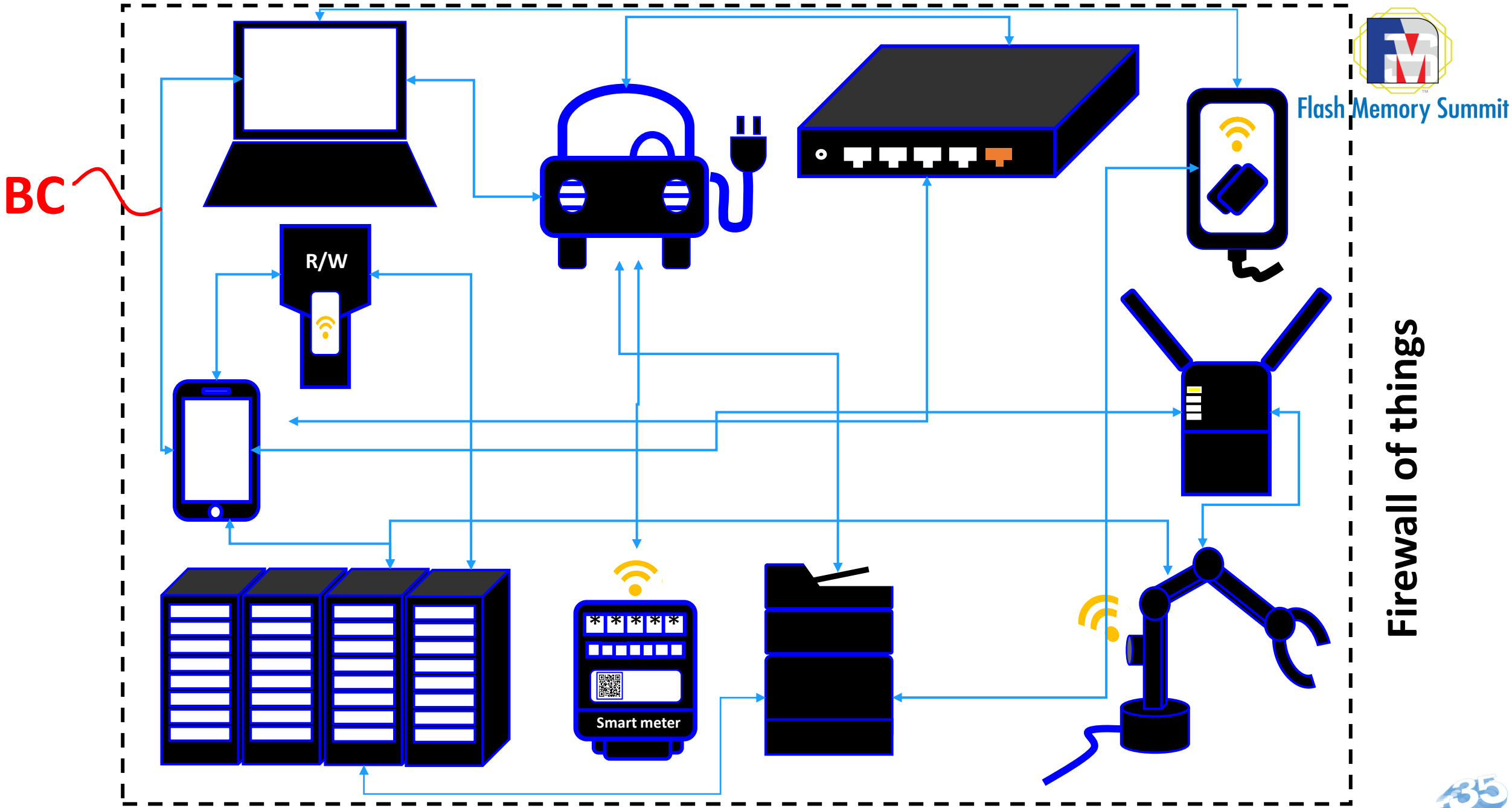
Merkle root (n0)

BC of memory chips (Blockchain of Things)









Two experimental demonstrations

Flash Memory Summit

Firewall of IoT sensors

- **SCADA:** IoT sensors collects data of equipment
- Remote-control of semiconductor manufacturing (Taiwan)
  - National Taiwan University,
  - National Yang-Ming Chiao-Tung University, Asia University,
  - SEMI/E187
- Supported by the ministry of science and technology of Taiwan (MOST)

SCADA = Supervisory control and data acquisition

Firewall of R/Ws

- **R/W** collects data from RFID tags.
- Distribution of perishable foods in a major supermarket chain (Japan)
  - beyond-blockchain, Inc.,
  - Monokoto Design Inc., Waseda University
- Supported by Tokyo Metropolitan Industrial Technology Research Institute (TIRI)

MonoKoto .inc BeyondBlockchain

https://beyondbc.co.jp/en/

https://monokotodesign.co.jp/

35 YEARS OF NAND FLASH MEMORY INNOVATION

Rollup

Firewall of memory chips

- CRP via memory chip
- PRN specific to chip (n)
  - $R_n(C) = f\big(C, PRN(n)\big)$
  - $SK_n(C) = g\big(R_n(C)\big)$
  - $PK_n(C) = \bar{g}\big(R_n(C)\big)$
- Authentication to entry with proof of no spoofing

Firewall of things

- Merkle tree of memory chips
- Compatible to existing BC
- BC of things with root-of-trust while things have a memory chip

Acknowledgement:
K. Saito, J. Liang, K. Taniguchi, S. Torisawa, T. Kato, KY. Tsai, J. Chen, L. Chang, Y. Hirota, A. Kinoshita, T. Okada, S. Miyazaki, H. Fukuyama, H. Nakayama

