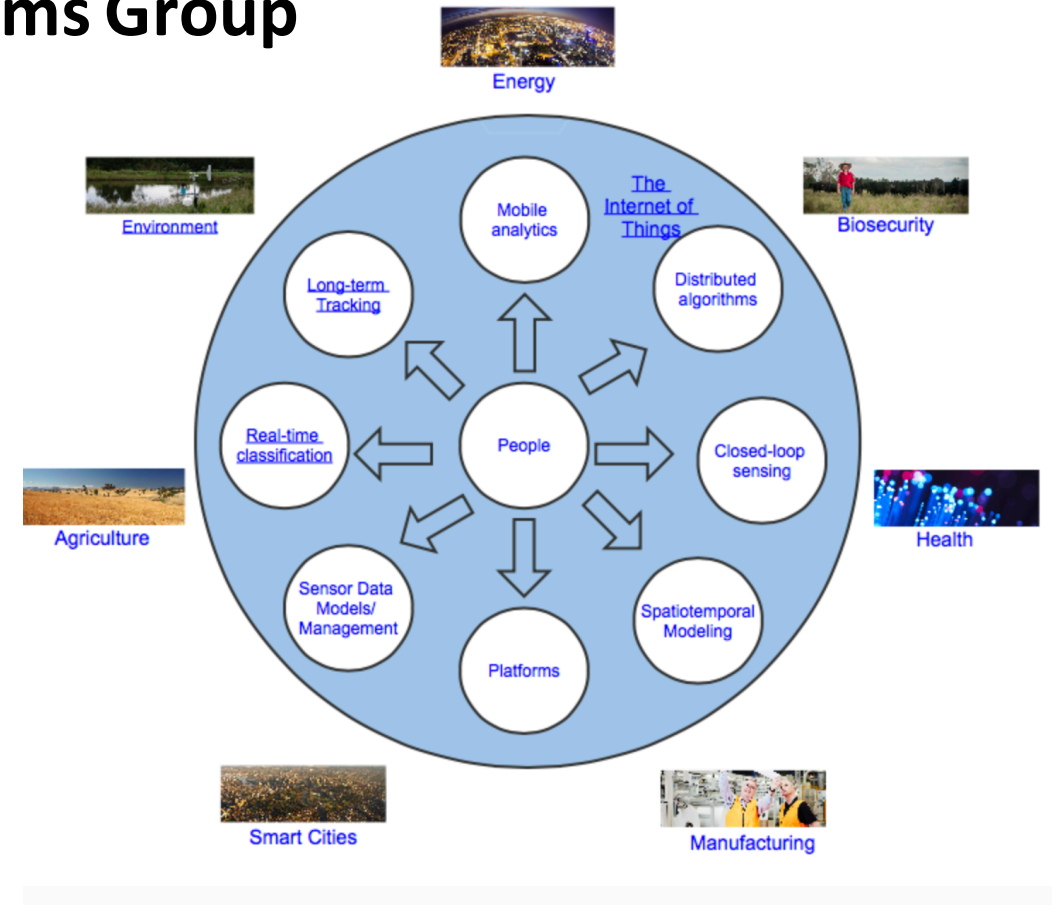
Blockchain for Internet of Things Security and Privacy

Prof Raja Jurdak
Senior Principal Research Scientist
Research Group Leader, Distributed Sensing Systems

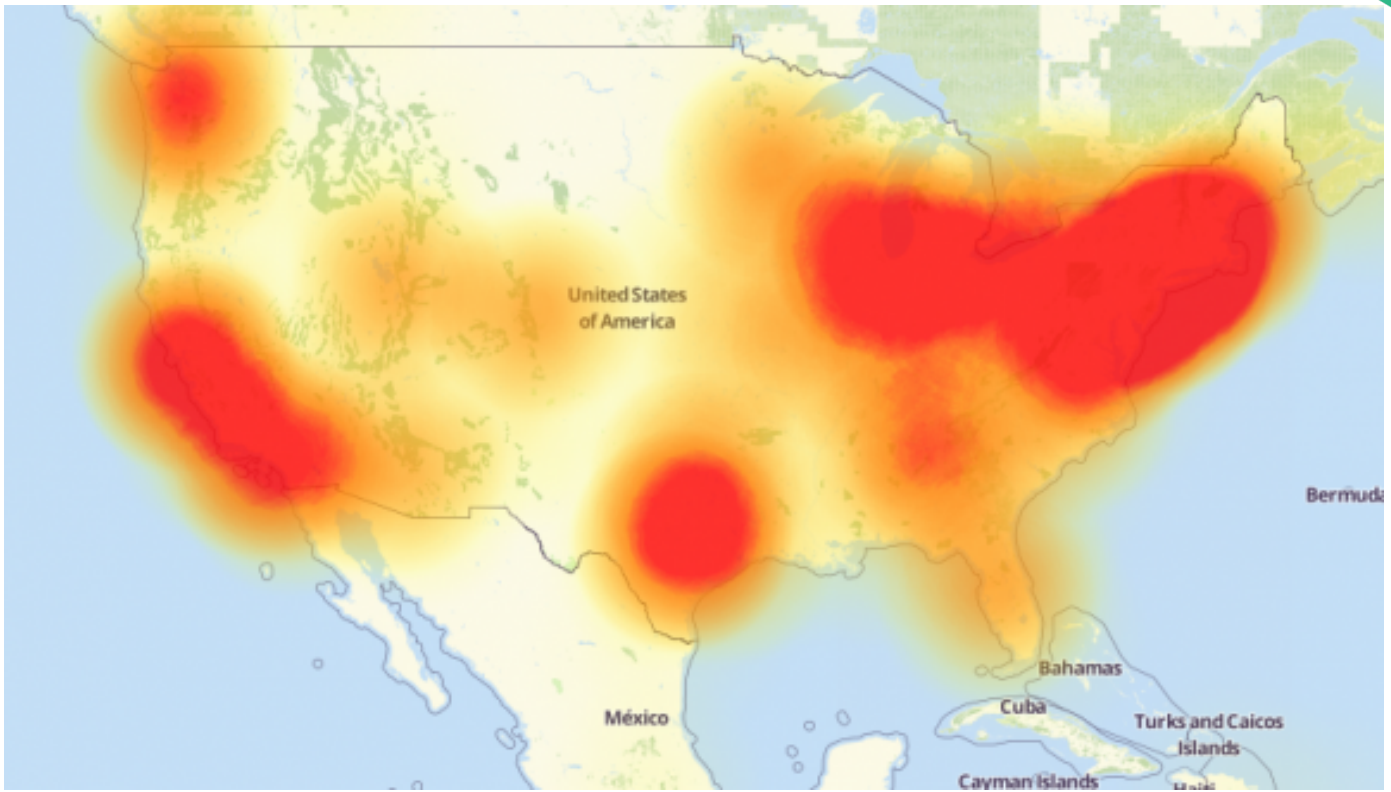
www.data61.csiro.au

Distributed Sensing Systems Group

- 45 researchers, postdocs, engineers, and students



IoT security and privacy is challenging



IoT Privacy and Security Challenges

- Heterogeneity in device resources
- Multiple attack surfaces
- Centralization
- Scale
- Context specific risks
- Poor implementation of security/privacy mechanisms in off-the-shelf products

IoT Privacy and Security Challenges

- Heterogeneity in device resources
- Multiple attack surfaces
- Centralization
- Scalability
- Application specific risks
- Poor implementation of security/privacy mechanisms in off-the-shelf products

BLOCKCHAIN

a possible solution

Blockchain Features

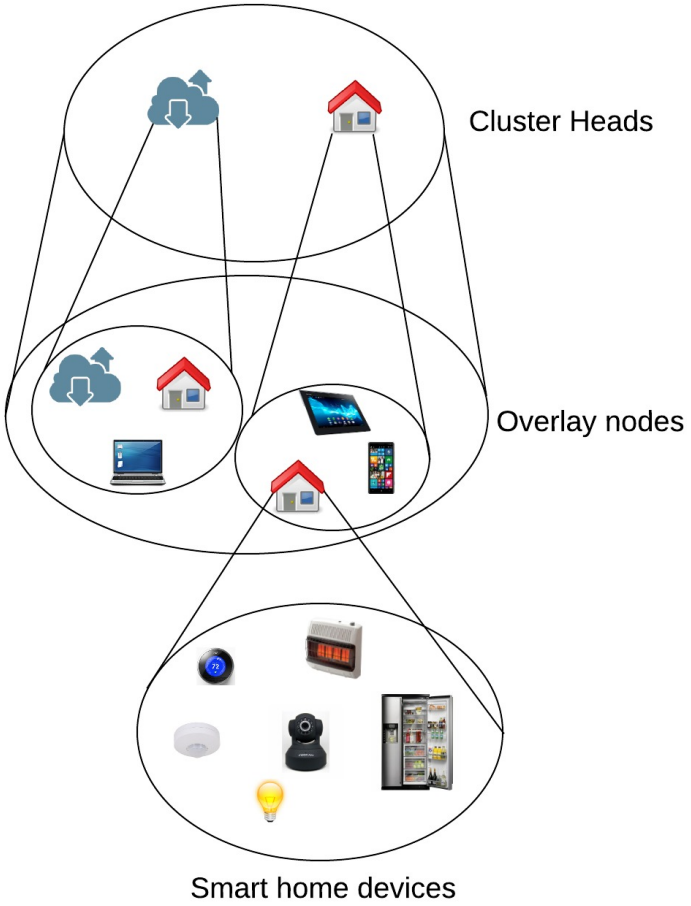
- A distributed immutable time-stamped ledger
- Creates a secure network over untrusted users
- Changeable PKs as users identity introduce high level privacy
- Demands for solving a puzzle to append blocks to the BlockChain (mining)

Blockchain challenges in IoT

BlockChain	IoT
Resource Consuming	Mostly devices are resource restricted
Block mining is time consuming	Demands low latency
BlockChain scale poorly with large networks	IoT is expected to contain a large number of nodes
BlockChain has high bandwidth consumption	IoT devices have limited bandwidth and resources

Blockchain for IoT

- **Hierarchical structure:** resource optimization, scalability
- **Limited nodes process BlockChain:** processing overhead



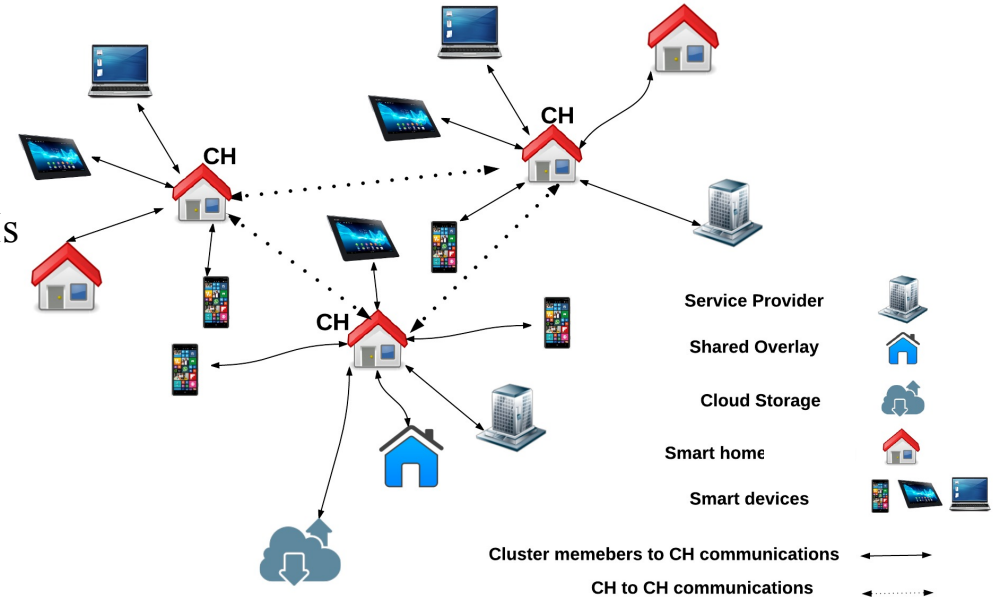
Dorri, Kanhere, Jurdak, IOTDI, 2017

Blockchain for IoT Features

Data and transactions flow separation: decrease delay, resource optimization

Reduce processing: Distributed trust between CHs

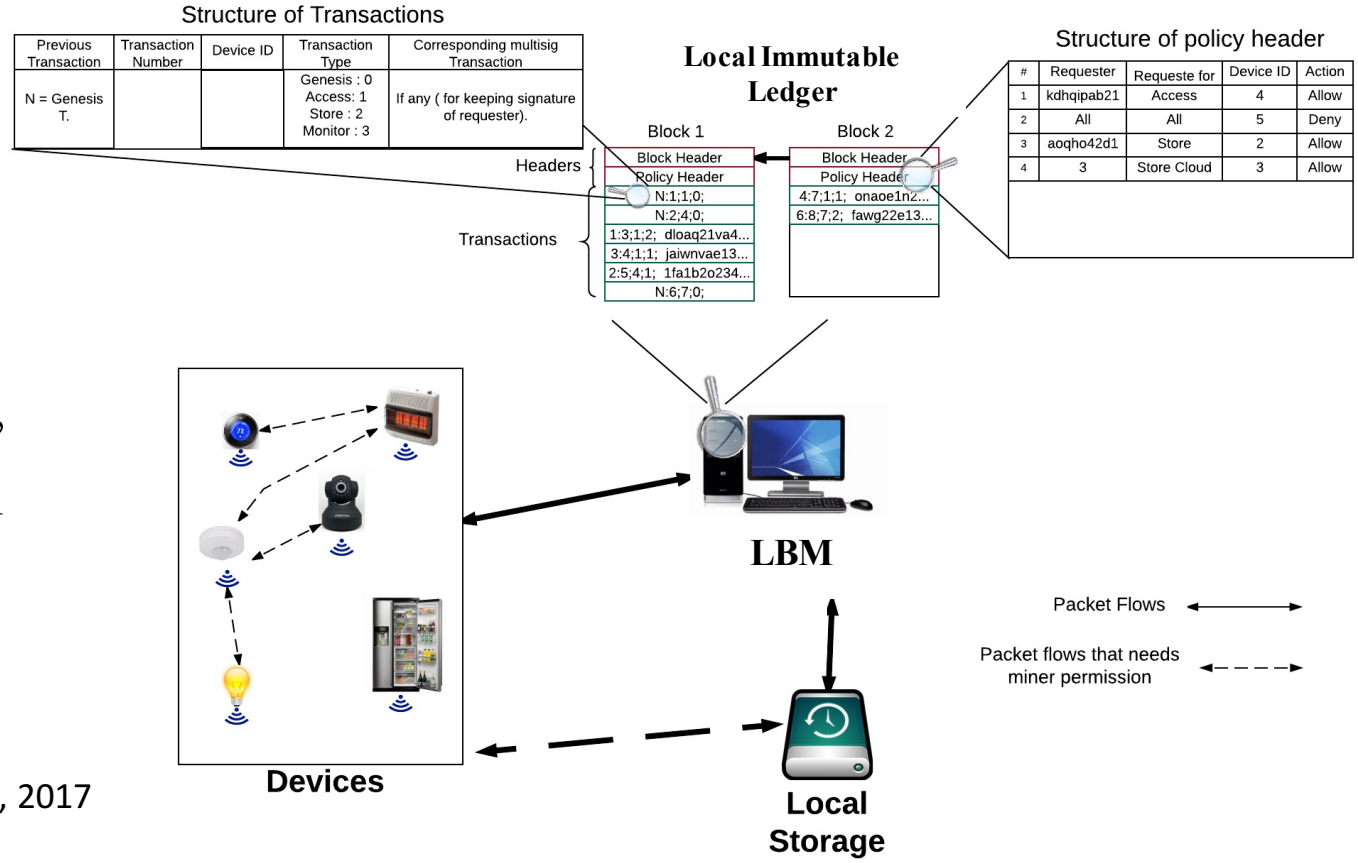
Two tiers of BlockChain: linked for further applications



Smart Home Transactions

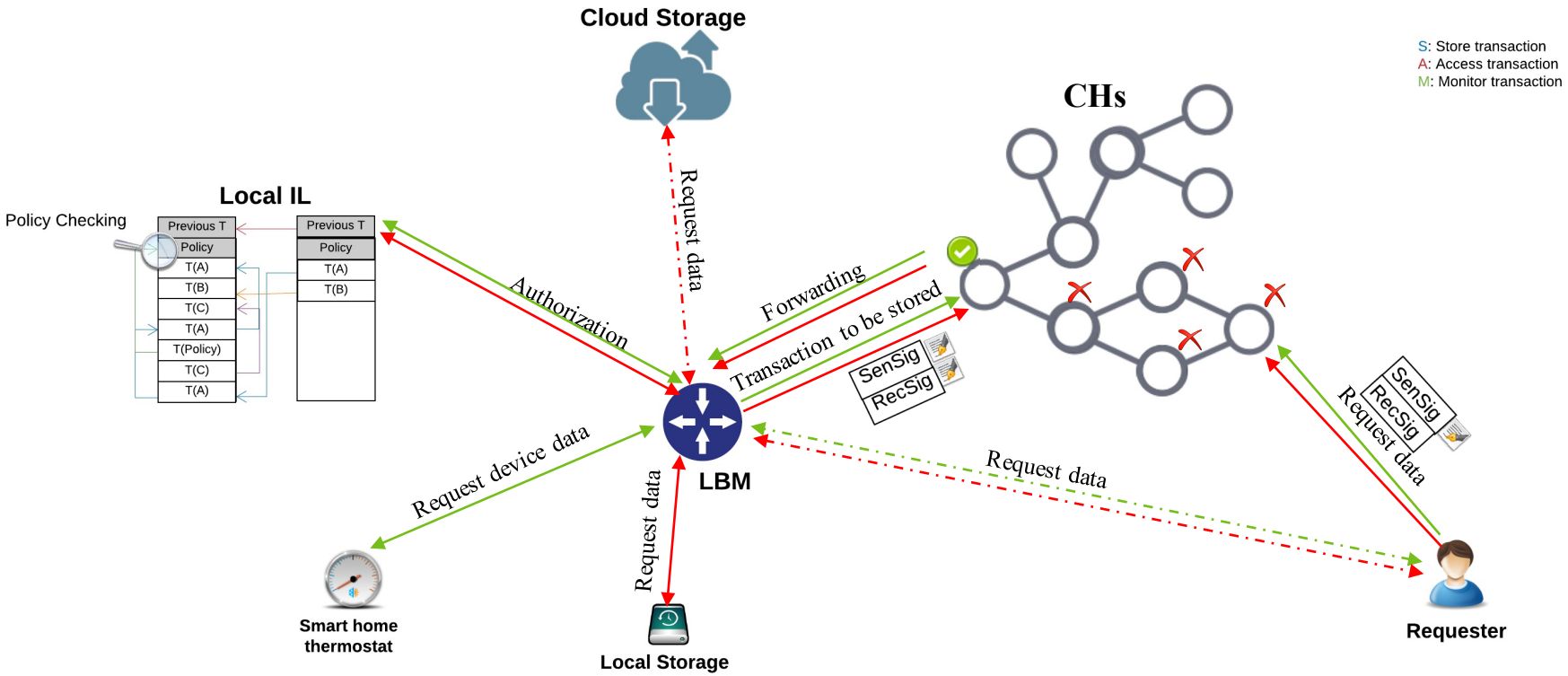
Indirectly accessible

IoT devices: security, resource optimization

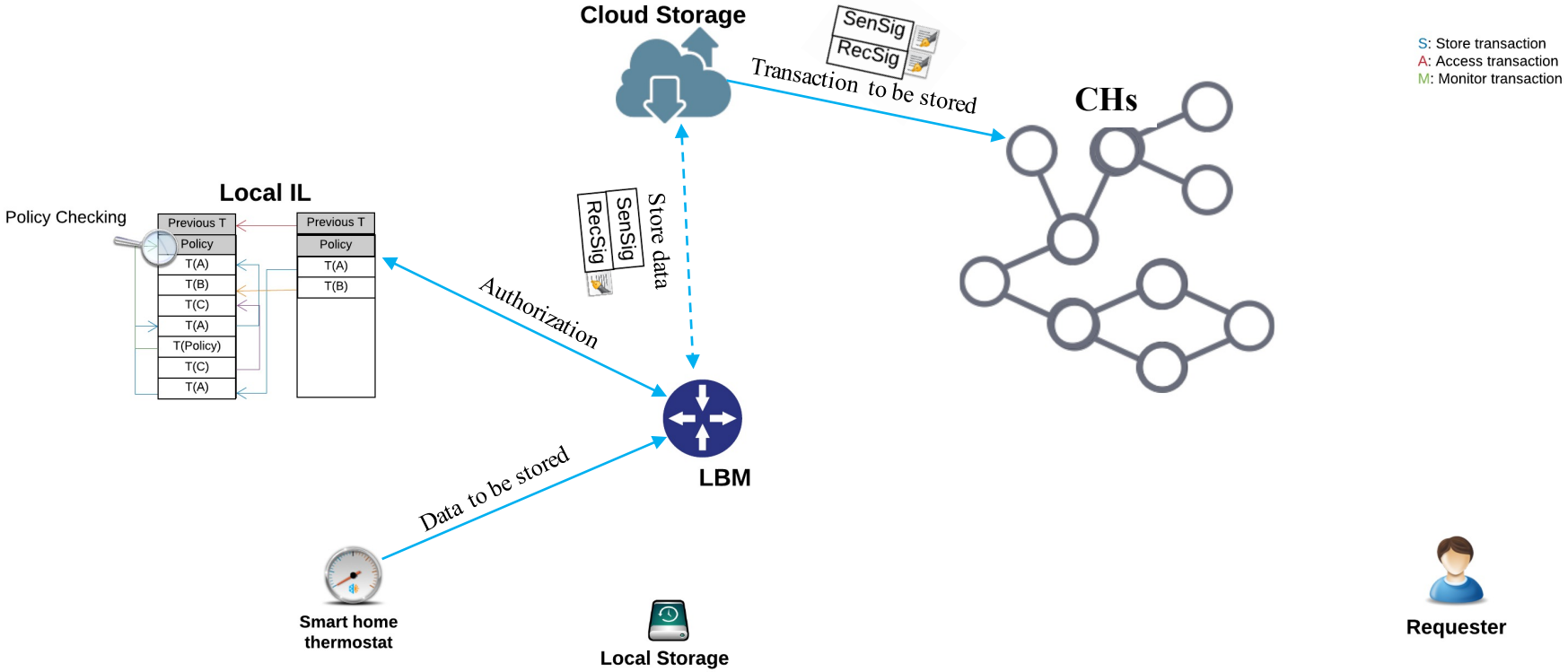


Dorri, Kanhere, Jurdak, Percom, 2017

Transactions handling



Transactions handling



Comparison with Classical Blockchain

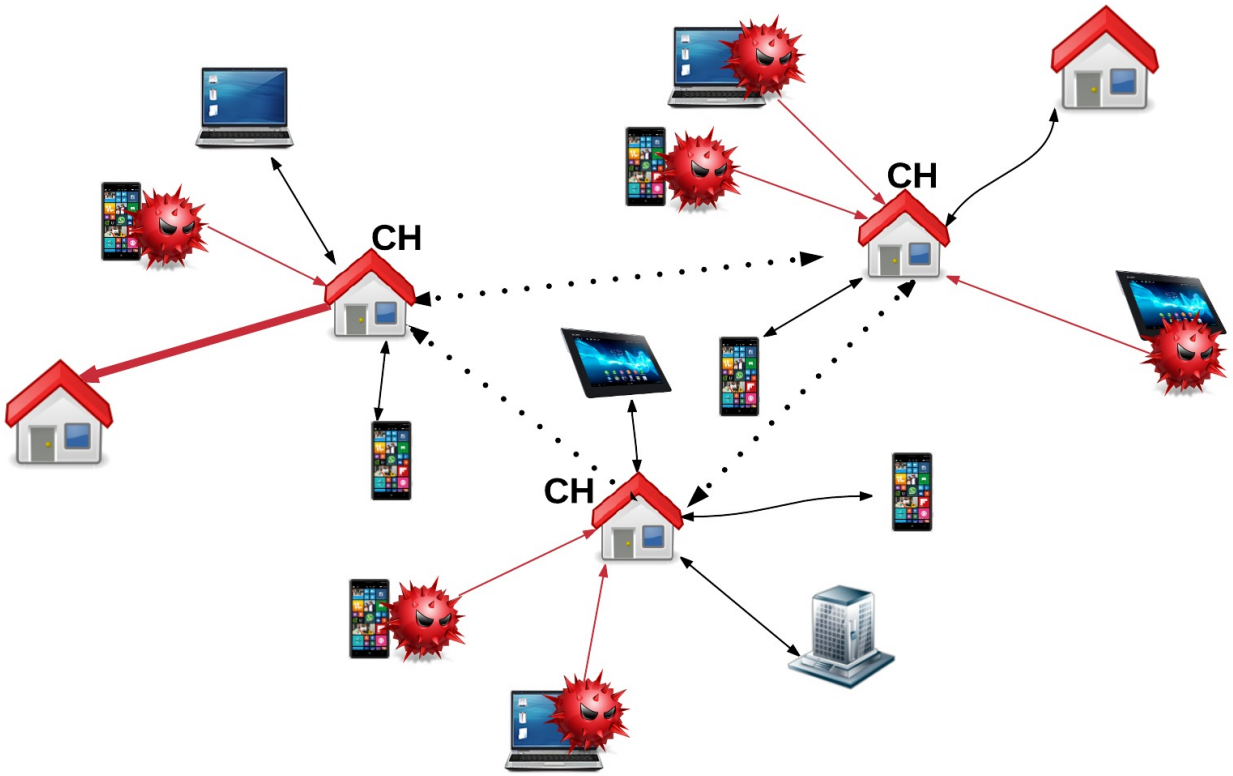
Our BlockChain Vs Bitcoin BlockChain

Feature	Bitcoin BlockChain	Immutable Ledger	Public BlockChain
Mining requirement	POW	None	None
Forking	Not allowed	Allowed	Allowed
Double spending	Not acceptable	Not applicable	Not applicable
Encryption	Asymmetric	Symmetric	Asymmetric
BlockChain visibility	Public	Private	Public
Transaction dissemination	Broadcast	Unicast	Unicast/Multicast

Security and privacy analysis

Accessibility threats

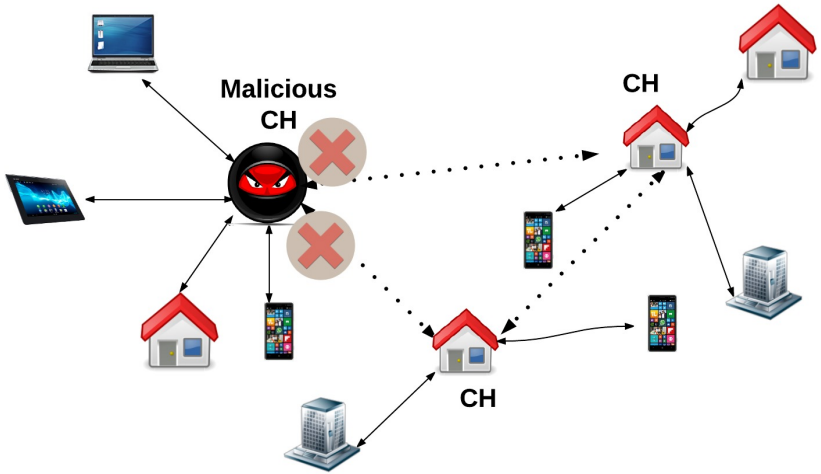
- DDOS attack
  - Devices are not directly accessible
  - Home manager controls all incoming and outgoing transactions
  - Keylists on CHs
  - Target threshold of received transactions



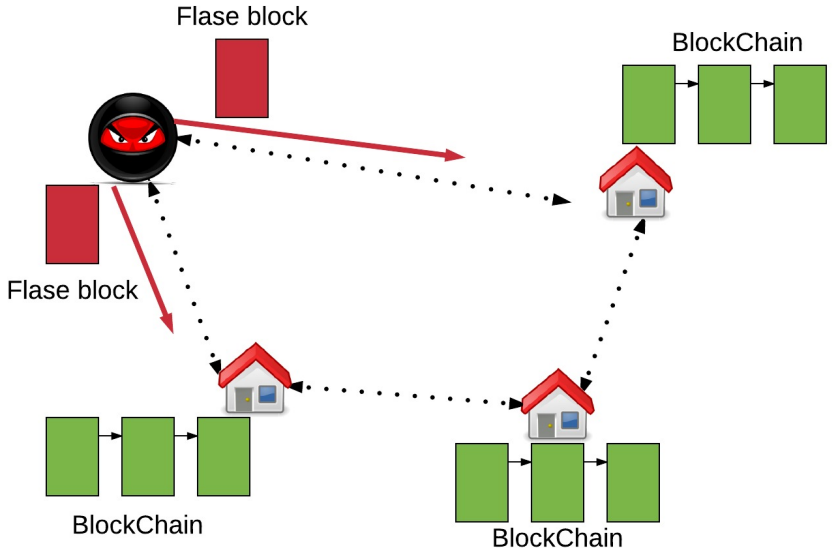
Security and privacy analysis

Accessibility threats

Dropping attack



Appending attack



Security and privacy analysis

Anonymity threats

- Linking attack

Video Intercome

PK=
ksnaiq1203ac

Smart phone
Location

PK=
ksnaiq1203ac

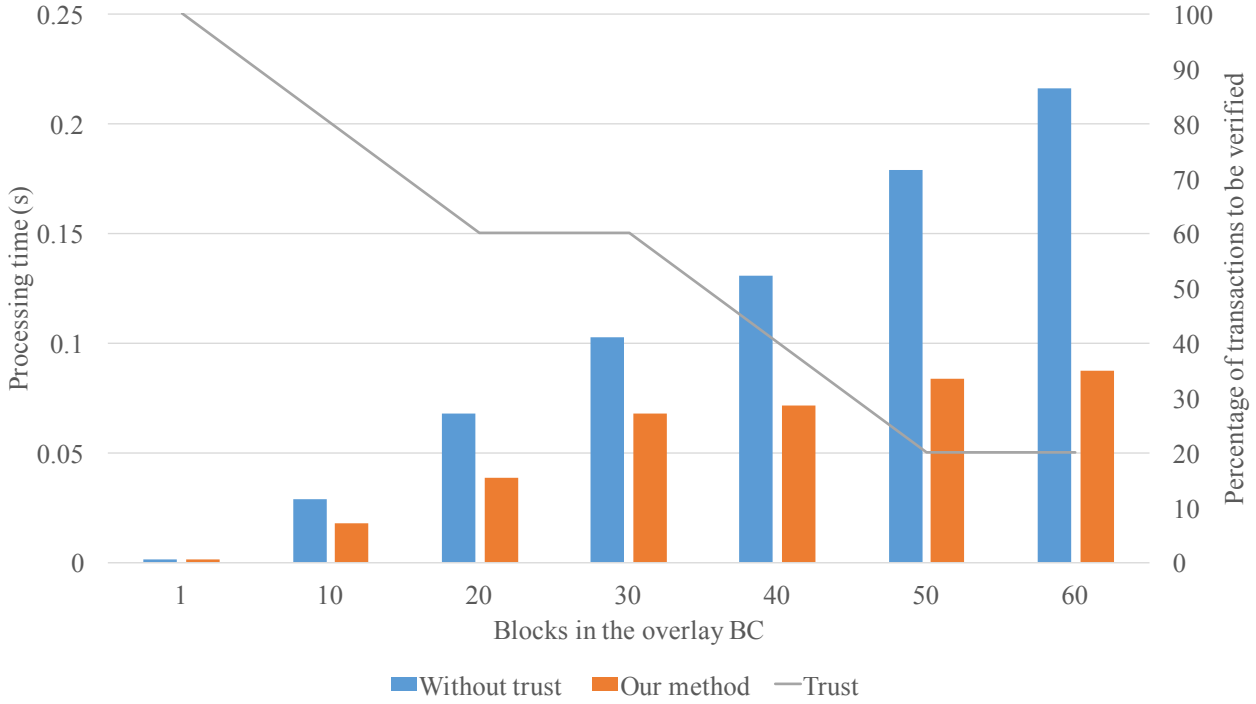
Social Media

"ksnaiq1203ac"
is Alice!!!

Performance evaluation

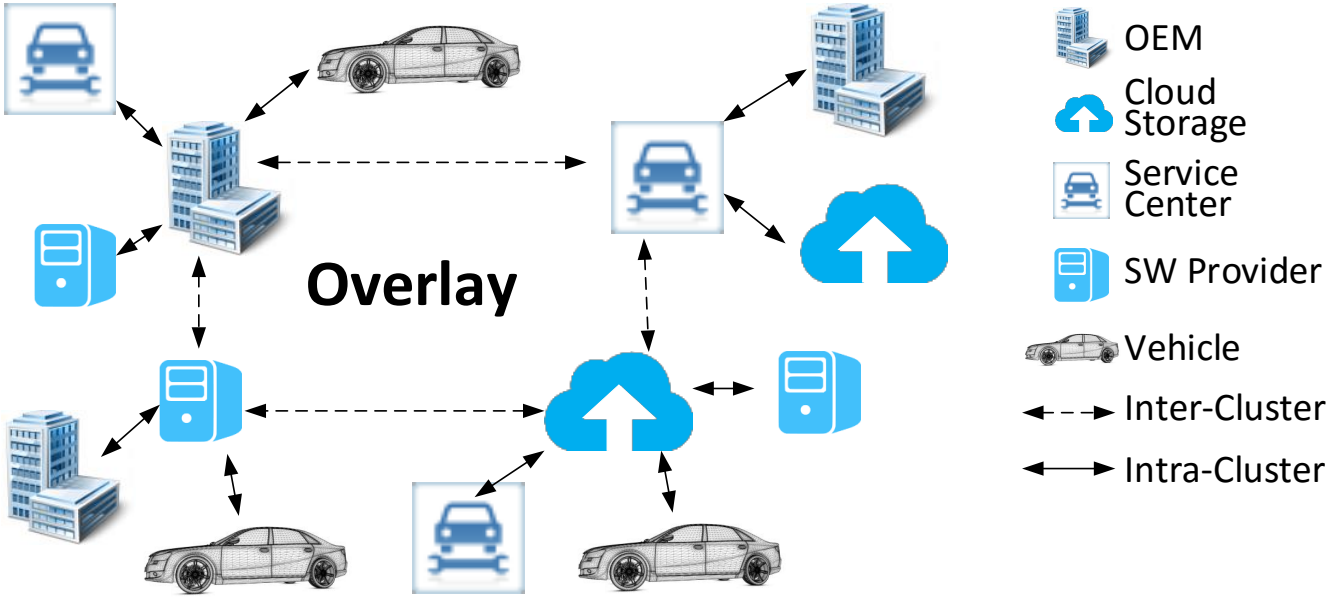
We conduct simulation using NS3 to study the trust method

50 nodes in which 13 are CHs



Other IoT Applications

- Future connected and autonomous vehicles
- Smart grids
- …



M. Steger, A. Dorri, S. Kanhere, K. Romer, R. Jurdak, and M. Karner, "BlockChains securing Wireless Automotive Software Updates – A proof of concept," To appear in Proceedings of the 21st International Forum on Advanced Microsystems for Automotive Applications (AMAA 2017), Berlin Germany, September 2017.

Summary

- Blockchain architecture for IoT security and privacy
- Maintains blockchain benefits with lightweight design
- Uses distributed trust to reduce block validation load
- Broadly applicable to other IoT applications

- Future work
  - Implement and evaluate architecture empirically
  - Methods for further scalability across network size and duration

DATA 61

Thank you

Raja Jurdak, PhD
Senior Principal Research Scientist
& Research Group Leader, Distributed Sensing Systems
Cyberphysical Systems Program
t +61 7 3327 4355
e raja.jurdak@csiro.au
w http://research.csiro.au/dss

www.data61.csiro.au

CSIRO

References

[1]: Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

[2]: Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum Project Yellow Paper 151 (2014).

[3]: Brambilla, Giacomo, Michele Amoretti, and Francesco Zanichelli. "Using Block Chain for Peer-to-Peer Proof-of-Location." arXiv preprint arXiv:1607.00174 (2016).

[4]: Hashemi, Sayed Hadi, et al. "World of Empowered IoT Users." 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, 2016.

Our other publications

[1]: Ali Dorri, Salil S. Kanhere, and Raja Jurdak. “Towards an Optimized BlockChain for IoT”, Second IEEE/ACM International Conference on Internet-of-Things Design and Implementation (IoTDI) 2017 (to be presented in April 2017)

[2]: Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home”, The 2nd IEEE Percom workshop on security privacy and trust in the Internet of things, 2017.

[3] Ali Dorri, Marco Steger, Salil S. Kanhere, and Raja Jurdak (2017). BlockChain: A distributed solution to automotive security and privacy. *arXiv preprint arXiv:1704.00073*.