Data privacy in Smart Grid

Blorin Project

Lorenzo Bracciale, PhD
Dipartimento di Ingegneria Elettronica

Data privacy team – University of Rome "Tor Vergata"

- Giuseppe Bianchi: full professor of cyber security

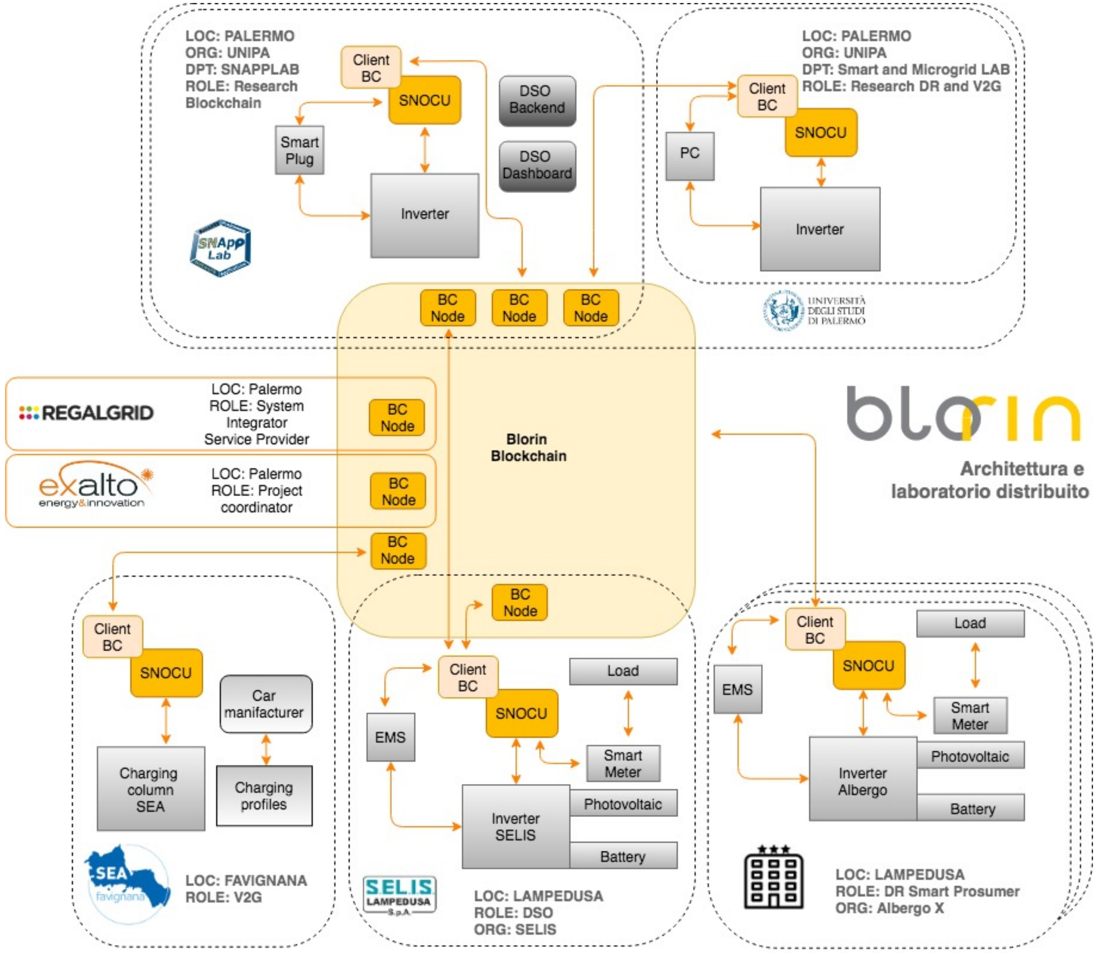
- Pierpaolo Loreti: assistant professor

- Lorenzo Bracciale: senior research

- Emanuele Raso: PhD student

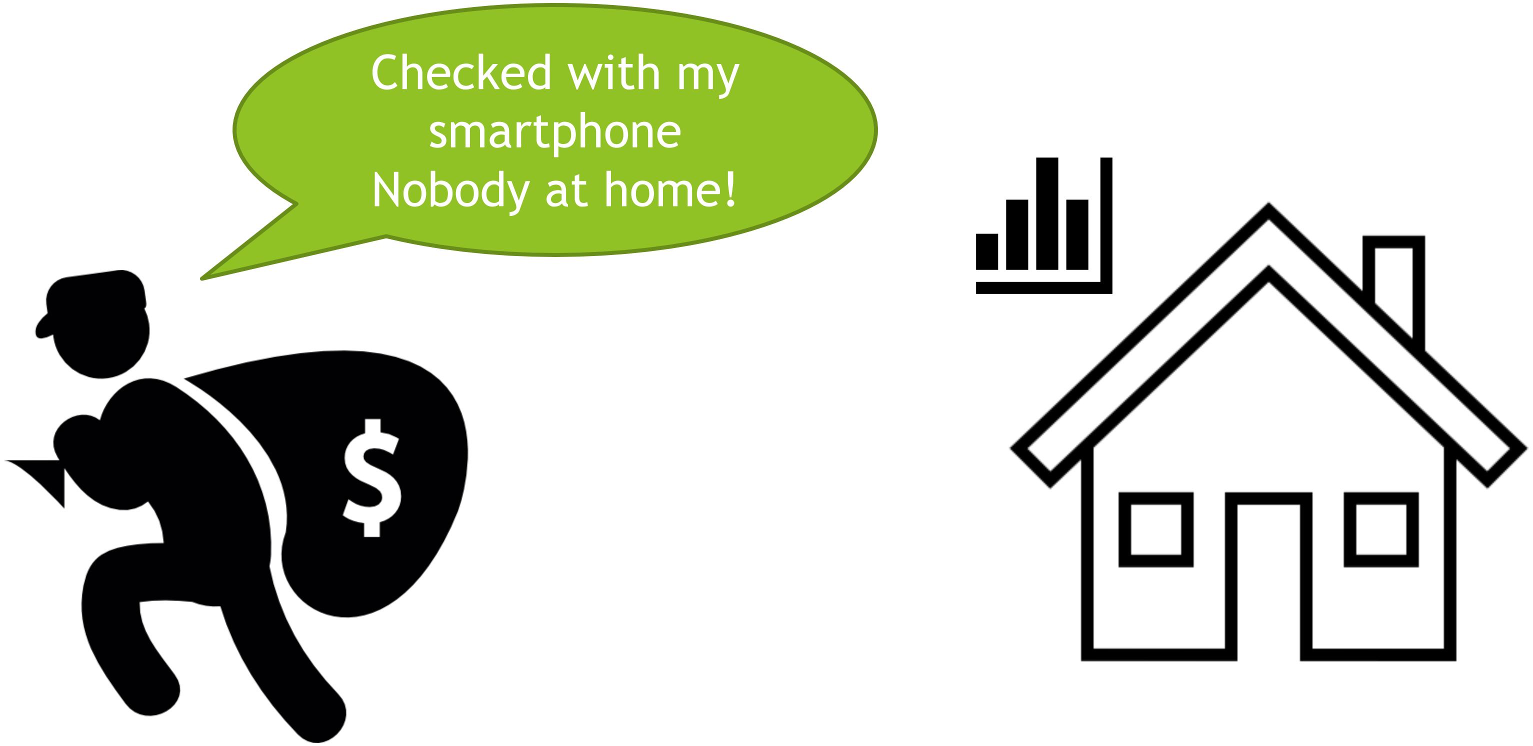
Il progetto Blorin – Demand & Response

- In the Demand&Response scenario, Blorin introduces blockchain for:
  - Trasparency/Accountability
  - Traceability
  - Trust
- Periodically publishing the power consumption on the blockchain, nodes can testify their adherence to the Demand request
  - And claim their reward!
- What about data privacy?



Is data privacy a concern? 1/2

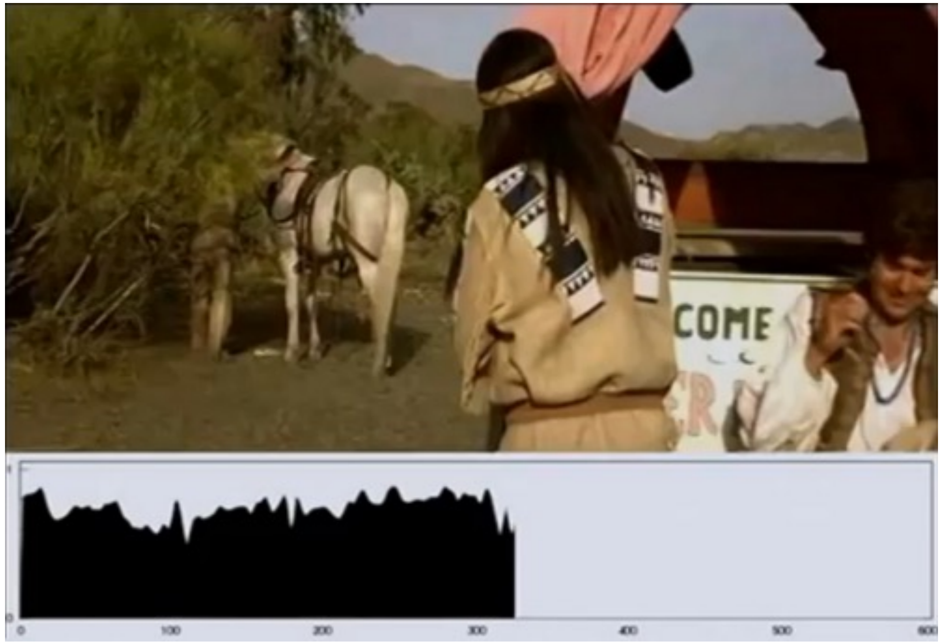
- Staightforward "application"



Is data privacy a concern? 2/2

- Energy fingerprint can disclose sensivive information

- In 2012 researchers proved they can disclose **which TV shows and movies** somebody watches using only the smart meter data*



Energy consumption of a plasma TV watching a movie

* https://nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/

Goals of the project (1/2)

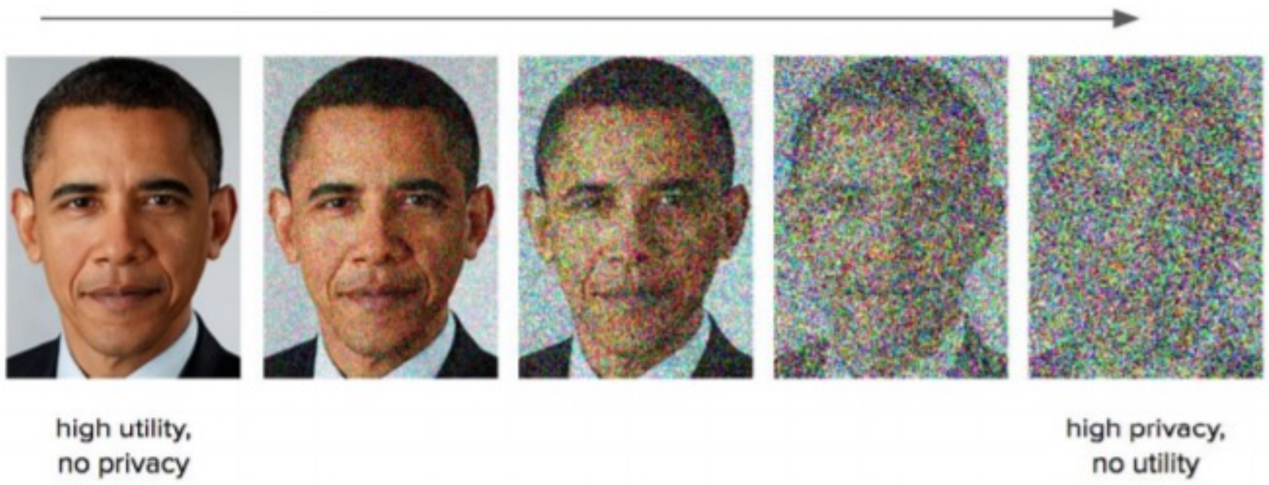
- Evaluate the application of **cryptographic mechanisms** such as SMC, ZKP, Homomorphic Encryption for handling transactions in a way that does not compromise user privacy;
- exploit devices such as TEE, TPM and SE integrated with smart meters and/or blockchain clients developed by DI in order to **avoid unwanted manipulation of raw data** acquired from the measuring devices or partially processed (e.g. time averages over appropriate windows not including demand response events);

Goals of the project(2/2)

- **preserving users' privacy** by assessing the difference between two load time profiles, the average one in the absence of DR events (baseline) and the current one during the DR event, without necessarily having to reveal the two profiles themselves;
- **Evaluate** battery usage profiles **without having to disclose** charge and discharge levels and vehicle mileage;
- defining algorithms with the best **compromise between transparency, security and privacy** through smart contracts. These will be run on specific Hyperledger Fabric channels, in order to ensure transparency in data validation and processing in distributed form;

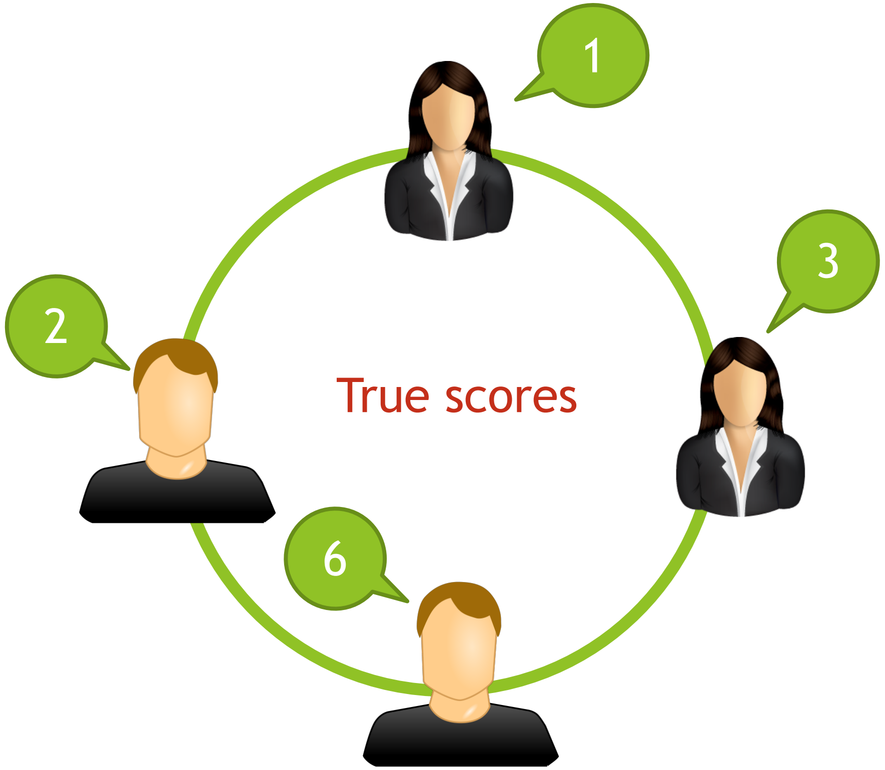
Privacy vs utility trade-off

- Sacrificing utility for privacy?
  - Other options?



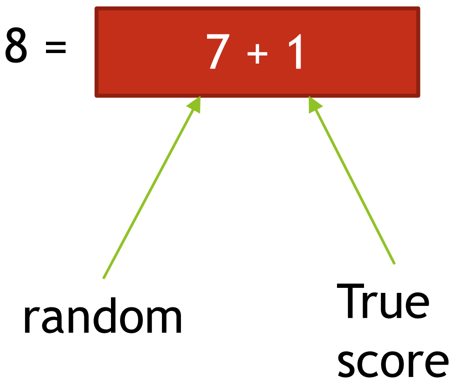
Example: privacy preserving aggregation

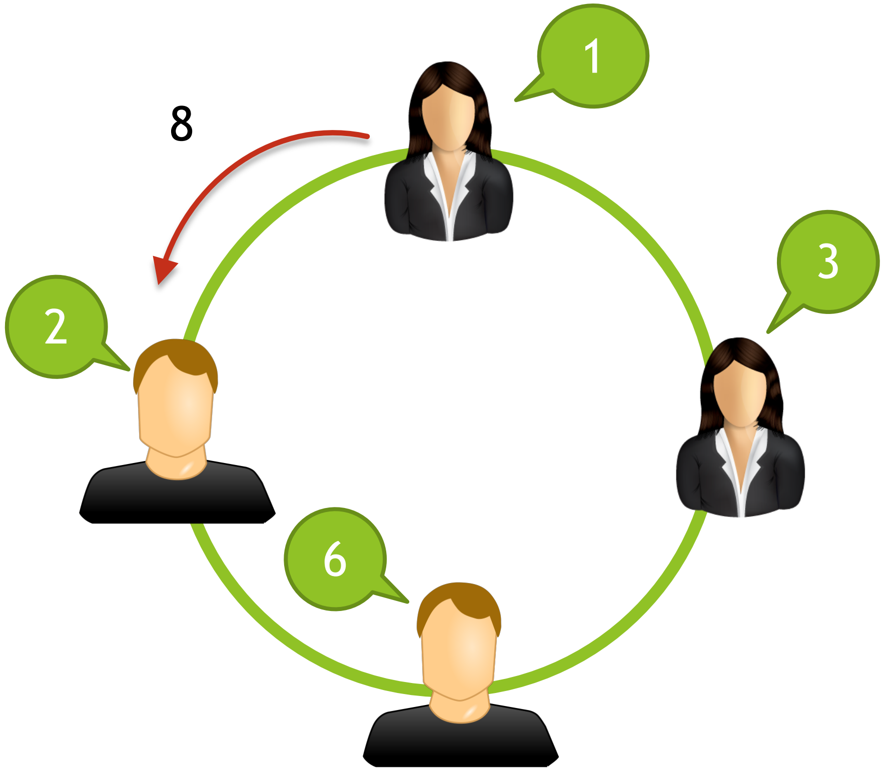
- Give a score to this talk (0-10) without revealing your vote to anybody (!) but disclosing only the average value
  - (simplified) secure multiparty computation example



Privacy preserving data aggregation

- User #1 takes a random number, e.g. 7
- Sum the number to her true score and pass the summation to user #2





Privacy preserving data aggregation

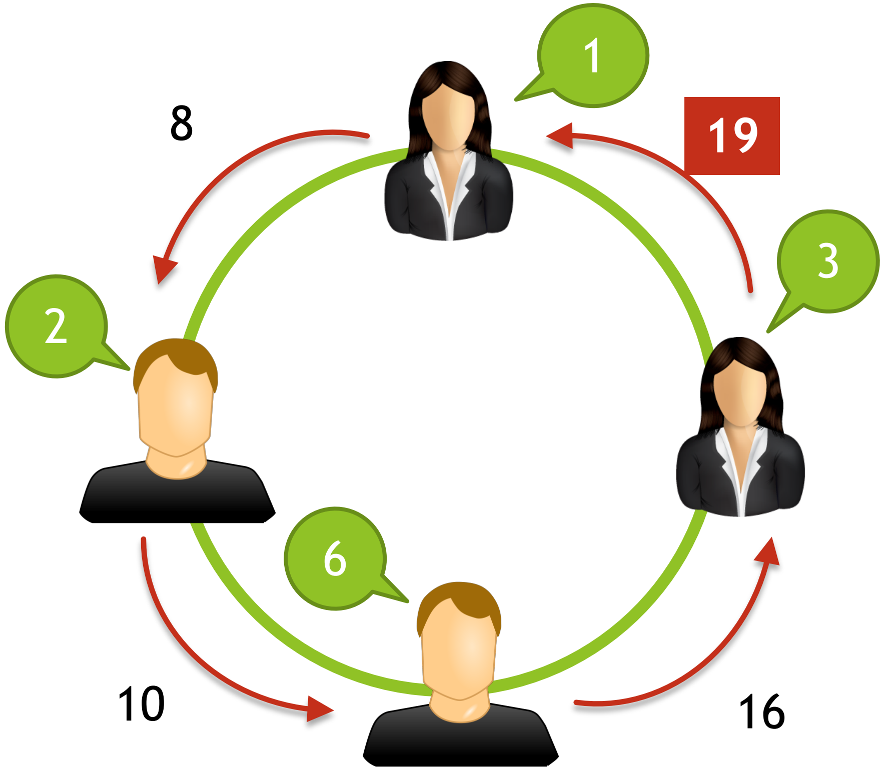
- Everybody sums her true score and pass the result to the next user
- Untill the result comes back to user #1

8 = 7 + 1

10 = 7 + 1 + 2

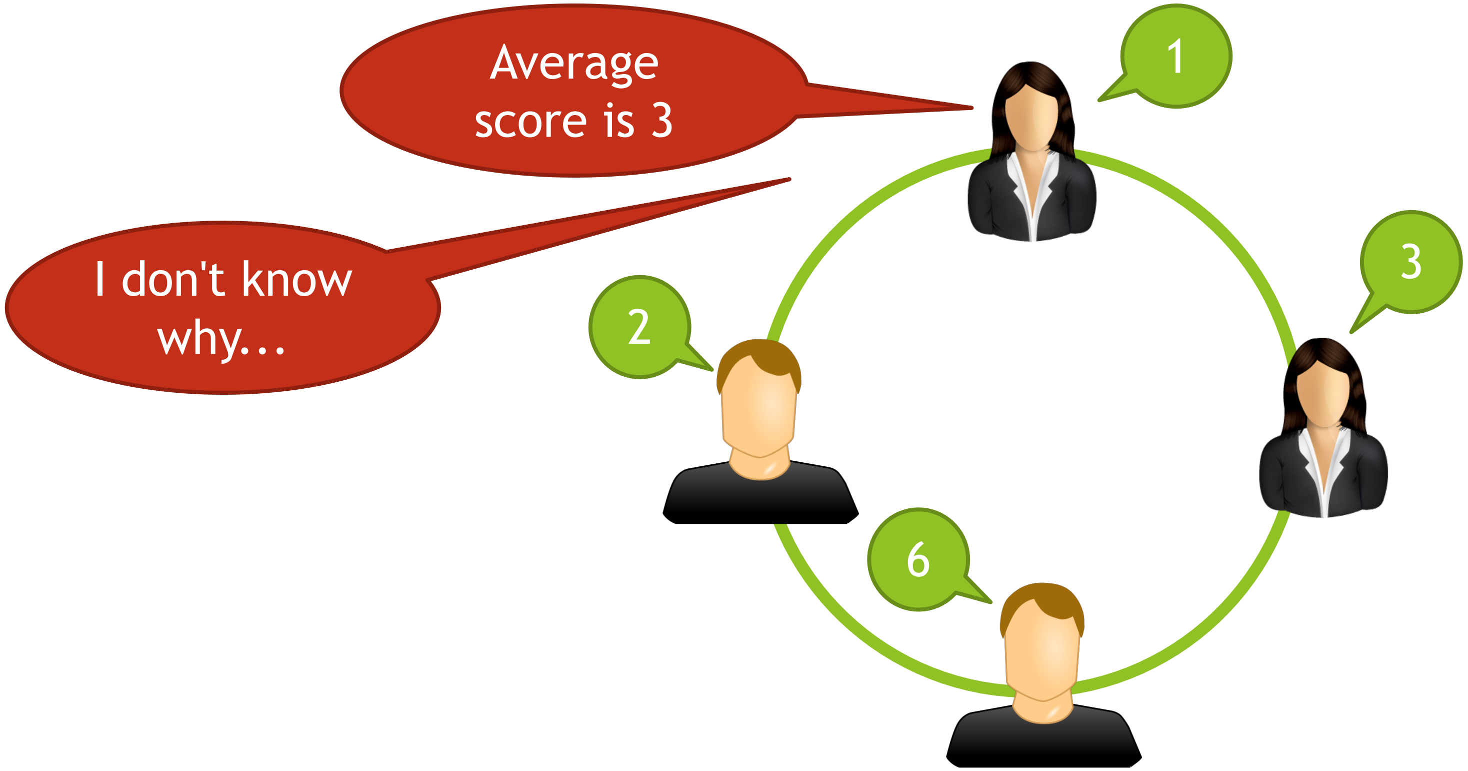
16 = 7 + 1 + 2 + 6

19 = 7 + 1 + 2 + 6 + 3



Privacy preserving data aggregation

- User #1 get back the result (19) and remove the random (7), obtaining the true sum (12)
- Dividing by the number of participants (12 / 4) she obtains the average score (3)



Thanks!