UNIVERSITATEA TEHNICĂ DIN CLUJ-NAPOCA

Faculty of Automation and Computer Science

DSRL Distributed Systems Research Laboratory

Decentralized control of flexibility in DR programs using Blockchain and Zero-knowledge Proofs

Dr. Claudia Daniela Antal (Pop)

eDREAM enabling new Demand REsponse Advanced, Market oriented and secure technologies, solutions and business models

HORIZON 2020

PRO INVENT, Cluj-Napoca, ROMANIA,
18-20 November 2020

1

CERCETAREA SI TRANSFERUL TEHNOLOGIC LA UTCN

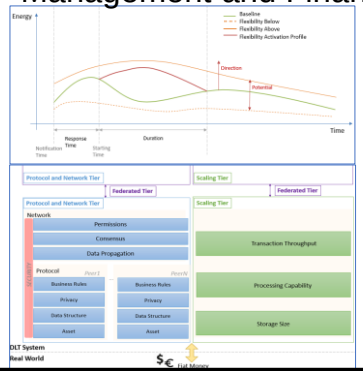
Presentation Outline

- Blockchain based Demand Response Management and Financial Settlement
- Blockchain and Zero-Knowledge Proofs- ZKP (ZK-Snarks)
- Demand Response using ZKP and Blockchain
  - DR registration
  - Systems interactions
  - DR monitoring
- Relevant Publications

2

CERCETAREA SI TRANSFERUL TEHNOLOGIC LA UTCN

Blockchain based Demand Response Management and Financial Settlement (1)



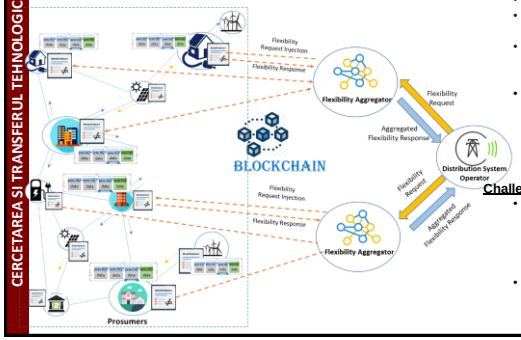
- The production and consumption forecasts are evaluated in order to detect any possible imbalances
- The DSO will ask the aggregators to address the imbalance by issuing a flexibility request
- The aggregators will use their resource/prosumer portfolio to answer to the Flexibility request

- Blockchain is the solution chosen for local flexibility markets management
- Prosumers can leverage on their flexible resources and aggregate with other peers to offer solutions to flexibility requests

3

CERCETAREA SI TRANSFERUL TEHNOLOGIC LA UTCN

Blockchain based Demand Response Management and Financial Settlement (2)



Opportunities

- Decentralized control
- Blockchain functioning as an escrow for the funds associated to DR Programs
- The flexibility response is evaluated through the smart contract and subject to consensus on chain
- Based on the delivered flexibility prosumers are evaluated and rewarded/penalized in near-real time

Challenges

- **Scalability**: the data received from the sensor can not be directly registered on chain => it would lead to high cost and a bottleneck due to the low transaction throughput
- **Privacy**: the consumption values should not be publicly revealed on chain

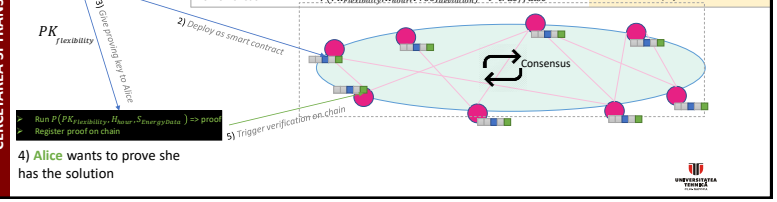
4

CERCETAREA SI TRANSFERUL TEHNOLOGIC LA UTCN

Blockchain and Zero-Knowledge Proofs - ZKP

> ZK-Snarks - as privacy solution

$G(F_{flexibility}) \Rightarrow (PK_{flexibility}, VK_{flexibility})$		
Generator Function G	Zokrates	
Program C	$F_{flexibility}$	field result = if flexibilityRequest[H_{hour}] > $S_{EnergyData}$ then flexibilityRequest[H_{hour}] − $S_{EnergyData}$ else $S_{EnergyData}$ - flexibilityRequest[H_{hour}] fi
Generated Keys	$PK_{flexibility}, VK_{flexibility}$	Generated by Zokrates based on $F_{flexibility}$
Prover function	$P(PK_{Flexibility}, H_{hour}, S_{EnergyData}) \Rightarrow proof$	Run by Zokrates locally
Verifier function	$V(VK_{Flexibility}, H_{hour}, Proof_{deviation}) \Rightarrow true/false$	Smart Contract deployed on chain



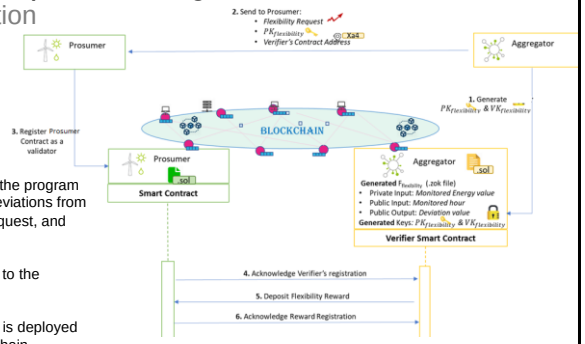
5

CERCETAREA SI TRANSFERUL TEHNOLOGIC LA UTCN

Demand Response using ZKP and Blockchain

> DR registration

- The aggregator defines the program $F_{flexibility}$, evaluating the deviations from the issues Flexibility Request, and generates the keys
- The proving key is sent to the prosumer
- The verification function is deployed as a smart contract on chain



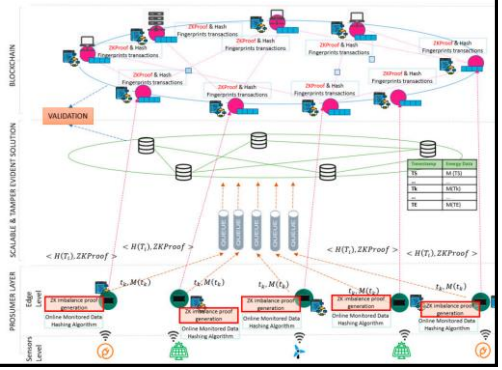
6

CERCETAREA SI TRANSFERUL TEHNOLOGIC LA UTCN

Demand Response using ZKP and Blockchain

> System Interaction

- Digital fingerprints are computed at edge level from the real time monitored values
- The energy value is computed and the imbalance proof generated
- The imbalance proof is registered on chain together with the digital fingerprint of the monitored values



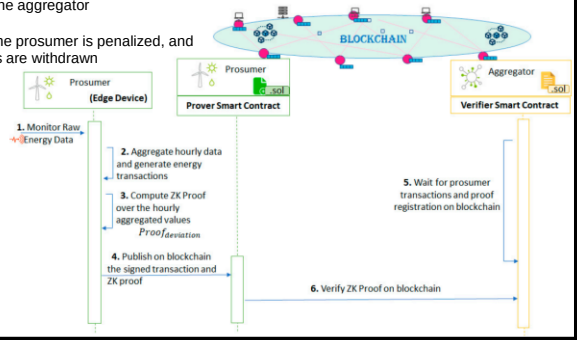
7

CERCETAREA SI TRANSFERUL TEHNOLOGIC LA UTCN

Demand Response using ZKP and Blockchain

> DR Monitoring

- The imbalance proof is validated by the verifier function deployed by the aggregator
- If the validation fails, the prosumer is penalized, and all the remaining funds are withdrawn



8

CERCETAREA SI TRANSFERUL TEHNOLOGIC LA UTCN

Relevant Publications

- Published Papers:
  - **Claudia Pop,** Tudor Cioara, Marcel Antal, Ionut Anghel, Ioan Salomie, and Massimo Bertoncini. "Blockchain based decentralized management of demand response programs in smart energy grids." Sensors 18, no. 1 (**2018**): 162. https://doi.org/10.3390/s18010162
  - **Claudia Pop**, Antal Marcel, Tudor Cioara, Ionut Anghel, David Sera, Ioan Salomie, ... & Bertoncini Massimo. "Blockchain-based scalable and tamper-evident solution for registering energy data. " Sensors, 19(14) (**2019**) : 3033, https://doi.org/10.3390/s19143033
  - **Claudia Pop**, Antal Marcel, Cioara Tudor, Anghel Ionut, Salomie Ioan, Bertoncini Massimo "A Fog Computing enabled Virtual Power Plant Model for Delivery of Frequency Restoration Reserve Services". *Sensors* **2019**, *19*, 4688. https://doi.org/10.3390/s19214688
  - **Claudia Pop**, Antal Marcel, Cioara Tudor, Anghel Ionut, Salomie Ioan, "Blockchain and Demand Response: Zero-Knowledge Proofs for Energy Transactions Privacy". *Sensors* **2020**, *20*, 5678.
- More info:
  - https://edream-h2020.eu/

9

CERCETAREA SI TRANSFERUL TEHNOLOGIC LA UTCN

Demo Movie

10