Application of the OSGP protocol on the Ethereum platform.

Advisor: Dr. Valderi R. Q. Leithardt

Research Area: Distributed Systems.

Objectives

According to Farhangi, the current grid is unidirectional, converting only a third of the energy into electricity without recovering the losses. Almost 8% of the generated energy is lost along the transmission lines, while 20% of that generated energy is used only to meet peak demand. The next generation of electric power grids is known as the Smart Grid. These networks are expected to address the existing problems of the current power grid.

It should be mentioned that Smart Grid networks store a large amount of personal data. McDaniel and McLaughlin argue that Smart Grid systems are desirable to malicious hackers because any vulnerability can be easily monetized. Hackers who can compromise this technology can easily manipulate, for example, the energy costs of a home. The authors also say that in the United States, studies show that frauds in the consumption of non-automated electric energy caused a loss of six billion dollars.

The Open Smart Grid Protocol (OSGP) is present in several countries and is used in large scale for projects with smart meters. The OSGP Alliance developed it and published as a standard by the European Telecommunications Standards Institute (ETSI). It is one of the most widely used protocols for smart meters, and smart network applications and currently has more than 100 million devices supported. The OSGP follows a modern focus based on the OSI model using the layers of application, transport, and physics. Regarding security measures, OSGP uses methods that restrict access to data, encrypting data to prevent unauthorized access.

According to Zyskind et al., personal data and sensitive data should not be entrusted to third parties. Instead, users should have the power to control their

data without compromising security or limiting utility companies from providing personalized services based on the information collected. With a decentralized platform, making legal and regulated decisions about collecting, storing and sharing data should become a more straightforward task. One way to make this process reality is to use blockchains.

Therefore, based on the scenario mentioned in the previous paragraphs, students should implement the OSGP protocol in the blockchain of the Ethereum platform. In the end, the student should analyze the feasibility of using the OSGP protocol in the platform, identifying the best way to be applied.

Tasks and Chronology

T1 Study of the problem and state of the art;

T2 Study of the OSGP protocol;

T3 Study of the Etehreum platoform;

T4 Application development;

T5 Project report writing;

T6 Scientific article writing.

Schedule

	Feb	Feb	Mar	Mar	Apr	Apr	May	May	Jun	Jun
T1	X	X	X							
T2		X	X							
T3			X							
T4				X	X	X	X	X		
T5								X	X	
T6									X	X

Technical / Academic Requirements

Have good grades and knowledge in programming, distributed systems and computer networks.

Elements of Evaluation

The student must submit the following elements for evaluation:

- Printed report (see regulation on the number of copies);

- CD or DVD (or another element of mass memory) with implemented algorithms and copy of the report in PDF format;

- An article in digital format to include in the CD or DVD;

Expected Results

- Implementation of OSGP protocol in Ethereum platform;
- Survey of the state of the art and related works;
- Project report;
- Scientific article.

References

I. S. Ochôa, Valderi. R. Q. Leithardt, C. A. Zeferino and J. S. Silva, "**Data Transmission Performance Analysis with Smart Grid Protocol and Cryptography Algorithms**," 2018 13th IEEE International Conference on Industry Applications (INDUSCON), São Paulo, Brazil, 2018, pp. 482-486. doi: 10.1109/INDUSCON.2018.8627195

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8627195&isnumber=8627061

H. Faranghi. **“The path of the smart grid.”** IEEE Power and Energy Magazine. v. 8, n. 1, p. 18-28, 2010.

URL: https://ieeexplore.ieee.org/document/5357331

P. McDaniel, S McLaughlin. **“Security and Privacy Challenges in the Smart Grid”**. IEEE Security & Privacy. Los Alamitos, v. 7, n. 3, p. 75-77, 2009.

URL: https://ieeexplore.ieee.org/document/5054916

G. Zyskind. **“Decentralizing Privacy: Using Blockchain to Protect Personal Data.”** IEEE Security and Privacy Workshops. San Jose, 2015.

URL: https://ieeexplore.ieee.org/document/7163223

K. Christidis. **“Blockchains and Smart Contracts for the Internet of Things.”** IEEE Access**.** v. 4, n. 1, p. 2292-2303, 2016.

URL: https://ieeexplore.ieee.org/document/7467408/