

# Proposta de Arquitetura para o Uso de Blockchain em Redes Smart Grid

Iago S. Ochoa<sup>1,2</sup>, Bruno A. da Silva<sup>1</sup>, Valderi R. Q. Leithardt<sup>1</sup>

<sup>1</sup>LEDS – Universidade do Vale do Itajaí (UNIVALI)  
Rua Uruguai, 458 – Caixa Postal 360 – 88302-901 – Itajaí– SC – Brazil

<sup>2</sup>Serviço Nacional de Aprendizagem Industrial (SENAI)  
Brusque – SC – Brazil

{iago.ochoa, silvabruno}@edu.univali.br, valderi@univali.br

**Resumo.** *Este artigo descreve uma arquitetura para aplicações smart grid que utilizam blockchains. Para o desenvolvimento da arquitetura foi utilizado uma taxonomia de blockchain já existente. Os índices de atendimento aos requisitos, de um sistema smart grid, foram definidos baseando-se nos tópicos apresentados na taxonomia existente. Ao fim da análise, a arquitetura do sistema smart grid que utiliza de blockchain é proposta.*

## 1. Introdução

Os sistemas de geração, transmissão e distribuição de energia elétrica estão passando por uma grande transformação. A incorporação de novas tecnologias na rede elétrica está tornando o sistema mais inteligente e eficiente, essa transformação é chamada de smart grid. Segundo [Heirman 2012] um sistema smart grid aumenta a eficiência e rentabilidade do sistema elétrico, melhorando a confiabilidade, resiliência e qualidade da rede.

As principais dificuldades existentes para a implementação das redes smart grid são a segurança e a privacidade dos usuários. Segundo [McDaniel and McLaughlin 2009], uma falha de segurança pode gerar prejuízos bilionários. No que se refere a privacidade, é possível saber se um usuário da rede está em casa com base em seu padrão de consumo de energia elétrica. Para obter sucesso na implementação das smart grids, os problemas mencionados devem ser corrigidos de maneira holística.

Em 2008, o conceito de blockchain foi apresentado através da criptomoeda bitcoin. Proposto por [Nakamoto 2008], através do bitcoin, a blockchain se mostrou uma tecnologia revolucionária devido a garantia de integridade em transações ponto a ponto sem a necessidade da auditoria de terceiros. Além disso, a blockchain também garante segurança e privacidade nas transações realizadas.

Em [Abdella and Shuaib 2018] é feita uma análise de diversas soluções já existentes que utilizam de blockchain no cenário smart grid. Diferentes arquiteturas são utilizadas para atingir o mesmo objetivo. Com base nisso, é proposto neste artigo, uma arquitetura voltada para o uso de blockchain em cenários smart grid. O objetivo principal é definir quais as tecnologias mais viáveis a serem utilizadas em redes smart grid que utilizem de blockchain.

Este artigo está estruturado da seguinte maneira: Na seção 2 é feita a análise de uma taxonomia existente para blockchains. Na seção 3 é desenvolvida uma arquitetura

com base na taxonomia apresentada na seção 2 para sistemas smart grid que utilizam de blockchain. Na seção 4 são apresentadas as considerações e trabalhos futuros.

## 2. Taxonomia para blockchain

Segundo [Hlava 2014], taxonomia é a utilização de tópicos para definição de um objeto. As taxonomias estabelecem uma maneira de descrever conteúdos de forma conceitual. As mesmas se tornam vantajosas para um grande volume de informações de um determinado assunto.

Será utilizada como referência para o desenvolvimento da arquitetura proposta a taxonomia apresentada por [Xu et al. 2017]. Os autores definem uma taxonomia desenvolvida para sistemas que utilizam blockchain com referência em diversas literaturas. São abordados tópicos referentes ao tipo de blockchain (centralizada ou privada), tipo de armazenagem de dados (on-chain ou off-chain), algoritmos de consenso (PoW, PoS e PoC), entre outras características. Para desenvolvimento da arquitetura, também foram utilizados os resultados de [Ochoa et al. 2018]

## 3. Modelo Proposto

Nesta seção é apresentada a arquitetura proposta com base na taxonomia estudada. Primeiramente são elencados os principais tópicos utilizados no desenvolvimento do modelo. Por fim, é apresentada a arquitetura desenvolvida com base nas informações descritas.

**Tipo:** remete a distribuição da blockchain. Blockchains centralizadas costumam ser armazenadas em um único servidor, onde os usuários possuem permissões restritas que são definidas pelo host da rede. Blockchains parcialmente descentralizadas são acessíveis para todos, porém apenas os nós mineradores armazenam e realizam operações de escrita na blockchain, nós normais possuem permissão apenas de leitura, não possuindo a blockchain armazenada. Por fim, nas blockchains descentralizadas qualquer usuário pode realizar operações de escrita e leitura na rede, geralmente esse tipo de blockchain é pública, permitindo o acesso a qualquer pessoa.

**Atividade:** refere-se ao armazenamento dos dados e realização das atividades na blockchain. Em plataformas onchain, os dados e atividades são armazenados e feitos na própria blockchain. Em sistemas offchain os dados e atividades são feitos fora da blockchain (e.g. transações da lightning network do bitcoin não são feitas na blockchain principal).

**Consenso:** forma de validar as informações na blockchain. O algoritmo PoW (Proof-of-work) garante o consenso na rede através da resolução de um problema criptográfico. O algoritmo PoS (Proof-of-stake) seleciona os mineradores dos blocos com base na quantidade de criptomoeda que o usuário possui, quanto maior a quantidade de criptomoeda, maior a chance do usuário ser escolhido para minerar o bloco.

**Nova blockchain:** remete ao desenvolvimento de blockchains para aplicações específicas. Uma sidechain consiste em uma blockchain conectada a outra blockchain realizando a troca de informações, essa técnica permite que o mercado existente não se fragmente com o desenvolvimento de novas aplicações. A técnica de mineração unida utiliza um mesmo algoritmo para a mineração em duas ou mais blockchains diferentes, permitindo ao usuário obter diferentes criptomoedas utilizando um mesmo algoritmo de mineração.

Com base nas características apresentadas por [Xu et al. 2017], a Tabela 1 foi desenvolvida para apresentar as características e requisitos necessários de uma blockchain voltada para o cenário smart grid. Os itens S, E e P da tabela se referem respectivamente a segurança, eficiência e performance. Os itens serão elencados de forma que "✓" representa que o atributo é pouco satisfeito, "✓✓" representa que o atributo é parcialmente satisfeito e "✓✓✓" representa que o atributo é completamente atendido.

Tabela 1. Classificação de eficiência dos atributos selecionados.

Tópico	Item	Descrição	S	E	P
Tipo	Centralizada	Armazenada em um servidor com permissões restritas, geralmente privada	✓	✓✓	✓✓✓
	Parcialmente Descentralizada	Segregação em nós mineradores (escrita) e nós normais (leitura)	✓✓	✓✓	✓✓
	Descentralizada	Sem permissão, geralmente acessível a todos (pública)	✓✓✓	✓✓	✓
Atividades	Onchain	Dados armazenados em transações na própria blockchain	✓✓✓	✓✓	✓✓
	Offchain	Dados armazenados em servidores externos (P2P, cloud)	✓	✓	✓✓
Consenso	PoW	Poder computacional elevado	✓✓✓	✓✓	✓
	PoS	Poder computacional de baixo nível	✓✓✓	✓✓✓	✓✓✓
Nova blockchain	Sidechain	Criação de blockchain paralela, "conectada" com a blockchain principal	✓✓✓	✓✓✓	✓✓✓
	Mineração unida	Mineração em paralelo de duas blockchains com um algoritmo de mineração.	✓✓	✓	✓

Observando os atributos descritos na Tabela 1, definimos que uma blockchain voltada para o cenário smart grid deve ser parcialmente descentralizada. Os nós mineradores devem ser escolhidos com base em informações de escalabilidade obtidas da blockchain e devem ser atualizados sempre que possível. As atividades devem ser feitas de forma onchain, todas as informações devem ser registradas na blockchain para garantir a privacidade e segurança do usuário. O algoritmo de consenso utilizado deve ser o PoS, a escolha deste algoritmo foi feita devido a sua eficiência e performance comparada ao algoritmo PoW [Bach et al. 2018]. Por fim, devem ser utilizadas aplicações em sidechain para garantir escalabilidade da rede e a não fragmentação das blockchains existentes.

#### 4. Considerações e Trabalhos Futuros

Com o desenvolvimento deste trabalho, foi possível identificar critérios importantes para a definição de uma arquitetura padrão para o uso de blockchain em redes smart grid. A arquitetura proposta neste artigo visa obter segurança, eficiência e performance em nível máximo para sistemas smart grid que utilizam de blockchain.

Para trabalhos futuros pretende-se desenvolver testes e implementações em cada camada do framework apresentado. Já foram desenvolvidos testes de escalabilidade em sidechains e de custo monetário para aplicações reais. Os resultados obtidos nestes testes serão utilizados em implementações futuras da arquitetura proposta.

Por fim, conclui-se que este trabalho apresenta contribuição científica na área de sistemas distribuídos pois apresenta uma arquitetura de rede que pode obter desempenho elevado nos requisitos necessários para implementação de redes smart grid que utilizam blockchains.

## 5. Agradecimentos

Este trabalho foi financiado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) - Código Financeiro 001.

## Referências

- Abdella, J. and Shuaib, K. (2018). Peer to peer distributed energy trading in smart grids: A survey. *Energies*, 11(6).
- Bach, L. M., Mihaljevic, B., and Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1545–1550.
- Heirman, D. (2012). What makes smart grid — smart — and who is in the “game”? *IEEE Electromagnetic Compatibility Magazine*, 1(2):95–99.
- Hlava, M. (2014). *The Taxobook: Principles and Practices of Taxonomy Construction (Part 2 of a 3-Part Series): Principles and Practices of Building Taxonomies, Part 2 of a 3-Part Series*. Morgan Claypool.
- McDaniel, P. and McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security Privacy*, 7(3):75–77.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Ochoa, I. S., Leithardt, V. R. Q., Zeferino, C. A., and Silva, J. S. (2018). Data transmission performance analysis with smart grid protocol and cryptography algorithms. In *2018 13th IEEE/IAS International Conference on Industry Applications (INDUSCON)*.
- Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., and Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE International Conference on Software Architecture (ICSA)*, pages 243–252.