Uma Revisão Qualitativa do uso da Blockchain na Infraestrutura de Veículos Elétricos ⋆

Lucas Vargas Dias * **Tiago A. Rizzetti** ** **Wagner S. Brignol** ***
Luciane N. Canha *

* *Programa de Pós-Graduação em Engenharia Elétrica (PPGEE), Universidade Federal de Santa Maria (UFSM)*
** *Colégio Técnico Industrial de Santa Maria (CTISM), UFSM*
*** *Instituto Federal Sul-rio-grandense (IFSUL)*

Abstract: Due to the popularity of Blockchain technology, there have been many proposed applications of it in the Vehicle Electric Infrastructure (VEI). In this way, this work presents an overview of some proposals based on their Blockchain's utilization. Therefore, it provides a qualitative analysis of them and gives an overview of Blockchain technology and consensus algorithms. Finally, we indicate some future works and opportunities.

Resumo: Devido a popularidade da tecnologia Blockchain, uma grande quantidade de trabalhos tem explorado a sua utilização na Infraestrutura de Veículos Elétricos (VEI). Dessa forma, esse trabalho apresenta uma visão geral das propostas baseada no objetivo de uso da Blockchain. Adicionalmente, uma análise qualitativa das propostas é fornecida. Uma base teórica da Blockchain e de algoritmos de consenso são apresentadas, também. Por fim, oportunidades de trabalhos futuros são identificadas.

Keywords: Blockchain; Information security; Vehicle Electric Infrastructure; Vehicle Electric.

1. INTRODUÇÃO

Com a grande popularização de veículos elétricos (EVs) por volta de 2021, existe a necessidade de suprir a demanda de recarga deles. Para isso, diversos infraestruturas para recarga dos EVs (VEIs) existem. Essas podem ser de uso doméstico, domínio público ou privado (Bertineti et al., 2020).

Além disso, os EVs podem ter outras aplicações como a transação energética de veículo para veículo (V2V), veículo para rede (V2G), entre outros. Independente das aplicação, os dados trocados são considerados sensíveis e com isso, a comunicação deve ser confiável e segura (Kim et al., 2019). Na Internet, o *Transport Layer Security* (TLS) é amplamente utilizado. Para isso, pelo menos uma das partes comunicantes deve ter um certificado digital válido emitido por uma autoridade certificadora (CA) confiável por ambas as partes comunicantes. Contudo, isso cria ponto único de falha na CA como ocorre em (Dias et al., 2021) em que o controle dos nós em uma rede *Distributed Hash Table* (DHT) é por meio de certificados digitais.

Para contornar isso, é interessante o uso de tecnologias distribuídas. Uma tecnologia que tem sido alvo de estudo é a Blockchain. Essa, é uma rede *peer-to-peer* (P2P) que permite a interação confiável entre entidades que não confiam uma na outra. Isso se dá pelo uso de técnicas como assinatura digital, hash criptográfico e algoritmos de consenso (Shi et al., 2020). Sendo assim, este trabalho aborda uma visão geral da Blockchain e uma revisão de literatura do seu uso no contexto de VEI.

⋆ Os autores agradecem ao INCTGD, órgãos financiadores (CNPq processo n° 465640/2014-1, CAPES processo n° 23038.000776/2017-54 e FAPERGS n° 17/2551-0000517-1).

1.1 Estrutura do Trabalho

A Seção 2 apresenta uma visão geral da Infraestrutura para Veículos Elétricos (VEI). Em sequência, a tecnologia Blockchain é apresentada junto com algoritmos de consenso que podem ser utilizados na Seção 3. Após, algumas propostas de uso da Blockchain no contexto de Veículos Elétricos (EVs) são descritas e discutidas na Seção 4. Por fim, a Seção 5 conclui o trabalho e aponta possíveis trabalhos futuros.

2. INFRAESTRUTURA PARA VEÍCULOS ELÉTRICOS

Os veículos elétricos tem o objetivo de reduzir a poluição do ar e a dependência de derivados de petróleo no setor de transporte. A sua popularização aumenta, consequentemente, a quantidade de estações de recarga necessárias para dar suporte. A infraestrutura de recarga contempla em infraestrutura de energia e infraestrutura de controle e comunicação. A primeira fornece ao veículo elétrico um circuito ou sistema para fluxo de energia entre a rede elétrica e o veículo. Podendo ser classificada de acordo com o posicionamento do circuito de recarga, fluxo de energia ou requisitos de contatos físico. O circuito pode ser *on-board* ou *off-board*. O primeiro fica localizado junto ao veículo, enquanto que o segundo, junto a estação de recarga. Adicionalmente, a recarga pode ser cabeada ou sem-fio (Das et al., 2020).

A energia elétrica usada pode ser AC ou DC. Quando AC é usada, ela pode ter 3 níveis de funcionamento, sendo que os níveis 1 e 2 podem ser usados em residências, enquanto que o nível 3 requer permissão de concessionária e necessita de um transformador. O nível 1 e 2 trabalha, com tensão de 110V ou 220V em AC, com potência em torno de 2kW para recarga lenta. Além disso, o tempo de recarga fica na faixa de

2 até 6 horas. Por outro o lado, o nível 3 trabalha com uma potência média de 20kW e tensão de 380V e é comumente usado para recarga rápida. O nível 2 pode trabalhar dessa forma, também (Mohammed and Jung, 2021).

Por outro lado, o fluxo de energia entre o veículo e a rede de energia elétrica pode ser unidirecional ou bidirecional. No primeiro caso, existe apenas a recarga do veículo, enquanto que no segundo cago, o veículo pode estar em modo de carga ou descarga, onde é possível inserir energia elétrica na rede (Mohammed and Jung, 2021).

Adicionalmente, a infraestrutura de controle e comunicação de veículos elétricos é fundamental para monitoramento em tempo-real. Ela permite serviços como escalonamento para redução de consumo das estações de recarga em períodos de pico (Das et al., 2020). Vale ressaltar que os dados e aplicações usados em VEI são críticos pois podem afetar o Sistema Elétrico de Potência (SEP). Consequentemente, alguns requisitos relacionado a segurança da informação são necessários como a disponibilidade e integridade dos dados. Tais prerrogativas podem ser encontradas na tecnologia Blockchain, apresentada na Seção 3.

3. BLOCKCHAIN

A Blockchain é uma tecnologia que permite que entidades que não confiam uma no outra, se comuniquem de maneira confiável. Dessa forma, ela é chamada de uma rede sem confiança. Além disso, ela permite auditoria das comunicações e imutabilidade dessas (Miglani et al., 2020).

A Blockchain é um tipo de *Distributed Ledger Technology* (DLT). Ela tem esse nome porque cada bloco é interligado através do seu hash, formando uma cadeia de blocos em sequência. Por outro lado, existem DLTs em formato de grafo acíclico direcionado (DAG). Vale ressaltar que cada entidade, na Blockchain, possui um par de chaves assimétrica. A chave pública é aplicada em hash para endereçamento do nó, e a chave privada permite que ele assine digitalmente as transações (Shi et al., 2020).

Para isso, a rede utiliza uma arquitetura decentralizada com topologia de comunicação *peer-to-peer* (P2P). Para alocação de uma informação na rede, os nós precisam entrar em acordo sobre o novo bloco (Miglani et al., 2020).

As transações são armazenados em blocos. Cada bloco possui um carimbo de tempo, o hash do bloco anterior, uma árvore de *Merkle* das transações ou dados dentro do bloco, um *nonce* e o hash do respectivo bloco. A Figura 1 apresenta a estrutura de um bloco.

A interligação entre os blocos com o uso do hash do anterior cria uma cadeia. Essa cadeia torna difícil a modificação de um bloco já alocado. Para isso, todos os blocos posteriores teriam de ter seu hash recalculado, o que torna impraticável a modificação de dados já alocados. Adicionalmente, a referência para o bloco anterior indica que ele é confiável, com isso, os blocos há mais tempo na Blockchain vão aumentado seu nível de confiança (Miglani et al., 2020). A estrutura dos blocos forma uma lista encadeada, como visto na Figura 2. A Seção 3.1 apresenta alguns algoritmos de consenso para Blockchain.

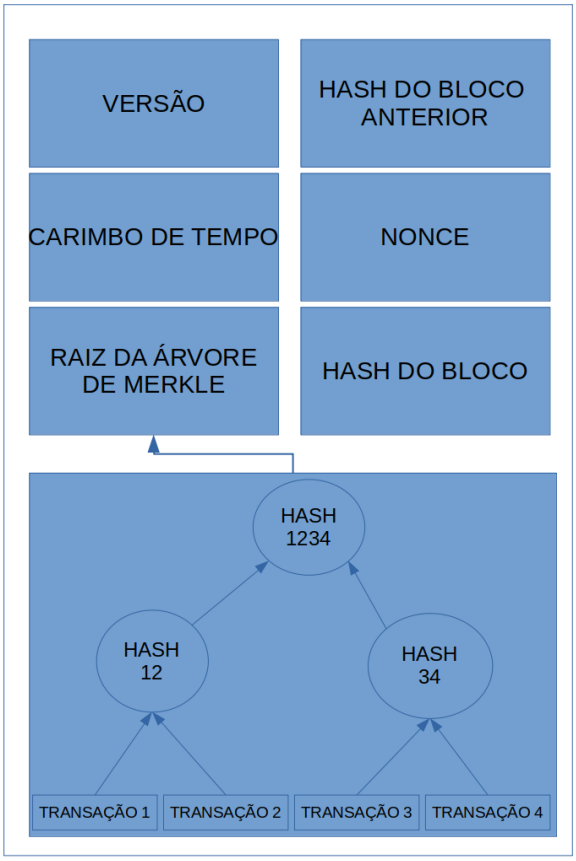

Figura 1. Estrutura de um bloco.

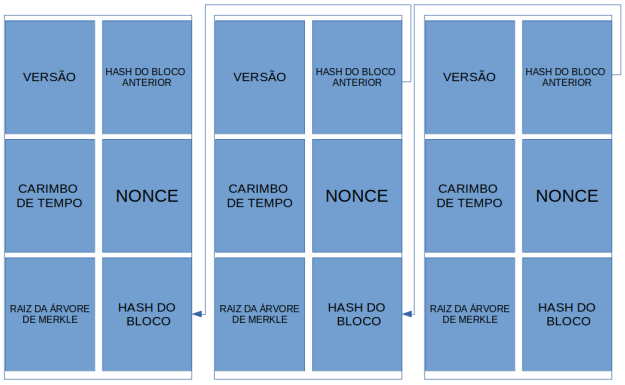

Figura 2. Estrutura básica da Blockchain.

3.1 Algoritmos de Consenso

A Blockchain possui uma arquitetura descentralizada. Mesmo em Blockchains privadas, os nós validadores são distribuídos. Dessa forma, eles necessitam entrar em consenso sobre as transações armazenadas na Blockchain. Existem uma diversidade de protocolos e mecanismos de consenso. Alguns deles são descritos a seguir.

Proof-of-Work O *Proof-of-Work* (PoW) é o mecanismo de consenso utilizado na rede do Bitcoin. Um novo é armazenado na Blockchain depois de um dos validadores encontrarem o PoW e enviar para todos verificarem. O PoW é baseado em funções de hash, que são funções inversíveis. Portanto, é fácil de computar um valor de entrada. Contudo, tendo o valor de saída, é difícil computacionalmente encontrar o valor de entrada.

O papel dos validadores no PoW é encontrar um *nonce* que satisfaça um hash baseado nas regras definidas na rede. Esse hash criptográfico possui um número de zeros definido nos bits iniciais de acordo com o grau de dificuldade. Quanto mais bits em zero, maior é a dificuldade de encontrar o *nonce*. Para encontrá-lo, os validadores fazem o cálculo por força-bruta. Com isso, no PoW os validadores são chamados mineradores (Miglani et al., 2020).

Uma vez que o *nonce* é encontrado e confirmado pelos validadores, o líder que encontrou o PoW recebe as transações e monta o novo bloco. Esse contém informações como o hash do bloco anterior, carimbo de tempo, versão, árvore de Merkle com as transações e o hash do novo bloco. Então, o bloco é enviado para os demais validadores. Após mais da metade dos nós validadores confirmarem o o bloco, ele é adicionado a Blockchain. Um dos principais aspectos de confiança e segurança do Bitcoin está na quantidade de nós para validação do bloco. Vale ressaltar que o primeiro bloco da Blockchain é denominado bloco *Genesis*. Ele consiste das mesmas informações que os demais, exceto o hash do bloco anterior (Bach et al., 2018).

Todavia, esse processo é lento. Isso faz com que o PoW não seja muito escalável devido a carga computacional necessária para resolvê-lo. Em média, um novo bloco demora cerca de dez (10) minutos para ser validado. Vale ressaltar que assinatura digital é aplicada nas transações contidas dentro do bloco (Shi et al., 2020). Isso garante autenticidade e integridade das transações.

Proof-of-Stake Essa Seção apresenta o mecanismo de consenso denominado *Proof-of-Stake* (PoS). Ele surge da necessidade de um mecanismo de consenso para Blockchain mais rápido que o PoW. Uma descrição do PoS é apresentada em sequência.

O PoS é um algoritmo de consenso que usa como base um *Stake*. Os nós que tiverem uma maior quantidade deles, tem a preferência para adicionar um novo bloco na Blockchain. Ele é composto da quatro (4) etapas:

- Validação do nó;
- Geração do Bloco;
- Validação do Bloco, e;
- Resolução.

Na primeira etapa, é verificado se o validador está apto a gerar o próximo bloco da Blockchain. Para isso, é analisado a informação da sua conta e de *Stake*s que ele possui. Uma vez que essas informações são verificadas, o validador gera um novo bloco e é gerada uma PoS.

A geração do bloco consiste em adicionar as transações a árvore de Merkle, o hash do bloco anterior e demais informações juntamente com o PoS. Isso é enviado aos validadores da Blockchain para verificação. Caso, esteja tudo adequado e as informações estejam corretas. O bloco é passado para a fase de resolução (Li et al., 2017).

Nessa fase, os *fork*s da Blockchain são verificados. Ou seja, é checado se não existe concorrência de adição de novos blocos a Blockchain. Se isso for detectado, o novo bloco é descartado e o validador deve repetir todo o processo novamente.

Um dos principais obstáculos para a utilização do PoS é a falta de clareza da definição de *Stake*s e a desvantagem que ele pode criar. Por exemplo, se o *Stake* for criptomoeda, a tendência é que os nós que os sejam mais ricos monopolizem o uso da Blockchain. Contudo, ainda assim, por volta de 2021, ele é usado na criptomoeda Ethereum (Li et al., 2017).

Proof-of-Authority Essa Seção apresenta o mecanismo de consenso denominado *Proof-of-Authority* (PoA). Os mecanismos PoS e PoW são utilizados em Blockchains públicas, caracterizadas pela flexibilidade de entrada de novos nós na rede, sem controle de acesso sofisticado. Contudo, algumas aplicações requerem um controle de acesso mais rígido. Dessa forma, o PoA é uma alternativa de consenso para isso.

Os algoritmos PoS e PoW se resumem a geração do bloco e a verificação de alguma informação adicional, *nonce* e *Stake*, respectivamente. Após, os nós votam se aceitam o novo bloco e requerem confirmação de mais de 50% dos validadores.

Em contrapartida, o PoA é diferente na primeira etapa. Ele oferece maior desempenho e menor troca de mensagens comparado ao PoS e PoW. Um conjunto de nós são definidos como nós de confiança nos quais são denominados autoridades.

Cada autoridade possuí um identificador único e a maioria delas são pressupostas honestas, especificamente $50\% + 1$ das autoridades. Para fazer uma nova validação de bloco na Blockchain, os clientes dela geram uma transação e enviam a uma das autoridades. Essa autoridade é definida em um esquema de rotação. Nesse esquema, um *slot* de tempo é definido para cada autoridade. Vale ressaltar que a definição e cálculo de *slot* é definido em cada aplicação de PoA (De Angelis et al., 2018).

Delegated Proof-of-Stake A respectiva Seção descreve o mecanismos de consenso denominado *Delegated Proof-of-Stake* (DPoS). O algoritmo busca resolver o possível problema de controle por parte dos nós com maior quantidade de *Stake*s no PoS.

No DPoS, vários nós geralmente votam para escolher a delegação. Essa é conhecida como produtores de bloco, e o seu papel na Blockchain é sugerido pelo próprio nome. A seleção da delegação é arbitrária bem como a implementação dela. Por exemplo, uma implementação poderia usar a criptomoeda como voto.Além disso, o DPoS fornece um processamento de transações mais rápido que o PoS e PoW. Contudo, devido a necessidade de eleição, o DPoS pode apresentar falhas (Hu et al., 2020).

Por exemplo, ele pode se tornar mais centralizado. Uma entidade pode colocar uma grande quantidade de nós na rede que pudessem ter um grande impacto na eleição e escolher um validador de seu controle. Isso, em larga escala, pode caracterizar ataques *Sybil*, em que um entidade insere uma grande quantidade de nós em uma rede P2P para controlar

o que pode ser compartilhado entre os nós (Saad and Radzi, 2020; Dias et al., 2021).

Para realizar uma transação, o cliente escolhe um dos validadores e envia sua transação para ele. Após, com critérios estabelecidos de acordo com a aplicação, a transação é armazenada na Blockchain. Vale ressaltar que o DPoS é voltado a Blockchains privadas ou em consórcio. Dessa forma, muitos aspectos da rede são subjetivos ao contexto da aplicação.

Practical Byzantine Fault Tolerance Essa Seção apresenta o mecanismo de consenso denominado *Practical Byzantine Fault Tolerance* (PBTF). O algoritmo é anterior aos sistemas de Blockchain. Ele é voltado para tolerância a falhas. O mecanismo busca mascarar falhas de software e até mesmo ataques maliciosos (De Angelis et al., 2018). Ele é um algoritmo composto pelas fases *pre-prepare*, *prepare* e *commit*.

Na primeira fase, o nó líder envia uma mensagem *broadcast* para os demais requisitando o valor que os nós querem fazer o *commit*. Em sequência, na fase de *prepare*, os nós respondem uma mensagem com o valor requisitado. Por fim, na fase de *commit*, o líder confirma se a requisição foi respondida por mais de 33% da rede (Miglani et al., 2020). O PBTF pode ser visto com maior detalhes em (Castro et al., 1999).

3.2 Contratos Inteligentes

Essa Seção aborda os contratos inteligentes que, segundo (Szabo, 1997), formalizam e garantem as interações de computadores usando protocolos e interfaces bem definidas. Por exemplo, uma máquina de venda automática de alimentos recebe como entrada o valor de R$5,00 e o cliente escolhe um produto de R$2,00, então, a máquina devolve o troco e o produto para o cliente.

No contexto de Blockchain, os contratos inteligentes também são um programa de computador com lógica bem definida. Ele fornece execução automática e facilita transações na Blockchain. Adicionalmente, eles permitem a transferência de bens na Blockchain. A plataforma Ethereum foi uma das primeiras Blockchains a suportarem contratos inteligentes (Namasudra et al., 2020).

Para a execução de um contrato inteligente, são necessárias duas coisas, (i) um quantidade do criptoativo fornecida aos validadores para execução, e (ii) a função a ser executada. Para isso, a assinatura da função é aplicada a um hash e os parâmetros da função são convertidos para Hexadecimal (Hu et al., 2021).

4. APLICAÇÃO DE BLOCKCHAIN NO CONTEXTO DE VEI

Essa Seção apresenta uma visão geral de algumas propostas relacionados ao uso de Blockchain no contexto de VEI. Elas recaem em aplicações que visam a contabilidade de dados ou gerenciamento do sistema de energia elétrica.

A Subseção 4.1 apresenta as aplicações que usam da Blockchian como meio para armazenamento de dados como a quantidade de energia recarregada ou inserida na rede elétrica ou até mesmo transações monetárias. Por outro lado, a Subseção 4.2 trata do uso de Blockchain para uma melhor configuração do SEP considerando VEI. Por fim, uma análise qualitativa é feita sobre os trabalhos visando alguns requisitos como preservação de privacidade e ponto-único de falha na Subseção 4.3.

4.1 Contabilidade

O trabalho proposto por (Huang et al., 2019) utiliza Blockchain como forma de pagamento. O objetivo é otimizar o escalonamento de recarga de VEIs e reduzir os custos. Adicionalmente, (Huang et al., 2019) utiliza variáveis como o nível de potência disponível dos EVs, a distância entre as estações de recarga e os VEIs, entre outras informações. A proposta (Huang et al., 2019) indica o uso da tecnologia para a preservação de privacidade dos proprietários dos VEs. Contudo, os autores não detalham como essa questão é abordada.

Por outro lado, (He et al., 2018) utilizam uma Blockchain em consórcio para incentivar a utilização das estações de recarga. No modelo tradicional, cada empresa tem sua infraestrutura. Dessa forma, cada uma tem seu aplicativo, formas de pagamento e outras coisas. Portanto, os consumidores necessitam instalar diversas aplicações, por exemplo. A tecnologia Blockchain é genérica e o consórcio faz seu uso como meio de incentivo através do fornecimento de crédito aos clientes.

Além disso, (He et al., 2018) empregam um consenso baseado na falha dos generais bizantinos. Então, 2/3 dos validadores necessitam entrar em acordo sobre o novo bloco. Por fim, (He et al., 2018) definem a quantidade de nós que cada empresa controla e usam escalonamento para a validação dos blocos.

Em contrapartida, a proposta de (Guo et al., 2020) utiliza a Blockchain para escalonar os consumidores e as estações de recarga. A arquitetura é formada por eles e por um gerenciador central. Os consumidores enviam uma requisição de recarga ao gerenciador central. Então, ele verifica a disponibilidade das estações de recarga e responde uma lista com as disponíveis aos consumidores. Por sua vez, o consumidor seleciona a estação de recarga na qual tem seu estado armazenado na Blockchain e ela faz uma atualização reservando para o consumidor. A ideia da Blockchain é de uma rede distribuída sem ponto-único de falha. Todavia, o uso do gerenciador central viola isso, além de diminuir a escalabilidade da proposta.

A proposta de (Wei and Ma, 2021) possuem o mesmo problema de ponto-único de falha. Todavia, o sistema é composto por EVs, Agregador Local (LAG), Agregador Central (CAG) e uma Autoridade Confiável (TA). A trabalho (Wei and Ma, 2021) busca preservar a privacidade dos EVs com a Blockchain e assinatura digital baseada em atributos. Inicialmente, a TA gera o par de chaves assimétricas e os atributos da CAG e LAG. Por outro lado, cada EV cria seus par de chaves e solicita os atributos à TA. Em sequência, a TA calcula os atributos e os envia ao EV.

Após isso, o EV pode requisitar uma recarga. Primeiramente, ela gera uma mensagem com diversos dados como carimbo de tempo, quantidade de energia solicitada e outras. Então, cada EV faz assinatura digital da mensagem e envia ao CAG. Por sua vez, ele faz a verificação e envia uma lista de LAGs ao EV. Então, ele é escolhe um da lista, solicita uma recarga de energia e envia seu endereço na Blockchain. Após isso, o LAG responde o seu endereço na Blockchain. Por fim, a recarga inicia e o EV paga o LAG através da Blockchain (Wei and Ma, 2021).

Em alternativa, (Gao et al., 2018) utiliza a Blockchain para a preservação de privacidade do consumidor no pagamento. O usuário entra em contato com a Autoridade de Registro (RA) para ingressar na rede Blockchain. RA assina a chave pública do usuário para gerar o endereço dele. Além disso, a proposta diz que um usuário pode solicitar um endereço dez (10) vezes. Dessa forma, um agente malicioso terá maior dificuldade em inferir a identidade de um usuário da Blockchain. Todavia, a proposta de (Gao et al., 2018) têm ponto-único de falha na RA e a Blockchain é a Hyperledger. Vale ressaltar que a Blockchain é privada, então apenas nós previamente definidos podem fazer a validação de blocos.

Para realizar uma recarga, o consumidor requisita ela a estação de recarga. Ela responde com o preço da recarga. Após isso, o consumidor cria uma transação na Blockchain e envia o identificador dela para a estação de recarga. Por fim, a estação verifica a transação na Blockchain e inicia a transferência de energia elétrica (Gao et al., 2018).

A Blockchain Hyperledger também é utilizada no trabalho de (Kim et al., 2019). A arquitetura é composta por operador, agregadores de energia (EAG) e EVs. O operador tem o papel de autorizar os EVs a realizaram a recarga de energia. Por outro lado, os EVs geram seu par de chaves assimétricas e enviam elas e seus identificadores ao operador. Ele, por sua vez, registra os EVs na configuração da rede.

Adicionalmente, EAG e EV fazem autenticação mútua quando o EV quer fazer uma recarga. Eles entram em acordo sobre um segredo compartilhado. Após isso, o EV envia o horário para a recarga, quantidade de energia e de valor financeiro ao EAG. Além disso, o EV envia o hash do segredo compartilhado para o EAG verificá-lo. Em sequência, EAG geram e validam blocos na Blockchain (Kim et al., 2019).

O protocolo proposto em (Kim et al., 2019) é resistente a ataques MITM. Porém, possui ponto-único de falha no operador. Portanto, um ataque de negação de serviço pode negar o acesso de novos EVs na recarga. Além disso, a fase de autenticação entre EAG e EV não usa assinatura digital, apenas funções de Hash, possibilitando ataques de personificação. Por fim, a informação da requisição de recarga está em texto plano. Sendo assim, um agente malicioso tem a possibilidade de inferir os dados e o usuário, quebrando a privacidade dos usuários na proposta de (Kim et al., 2019).

Por outra via, (Sun et al., 2020) deseja fazer a transação de energia entre PHEVs. A Blockchain é usada como forma de pagamento. Eles informam que fornecerão energia elétrica, enquanto outros requisitam recarga a *Energy Fog Node* (EFN). Essa entidade faz o escalonamento de descarga e recarga dos PHEVs. Após isso, é iniciado a transação energética. As duas partes (fornecedor e consumidor de energia elétrica) assinam uma transação que será armazenada na Blockchain. O algoritmo de consenso usado é o DPoS e cada EFN fica localizado em uma determinada região geográfica. Ele também recebe a requisição de *Wallet* dos PHEVs (Sun et al., 2020). Dessa forma, caso subvertido, o EFN pode personificar os participantes da transação energética. Também, um agente malicioso pode gerar uma transação falsa.

Em contrapartida, (Duan et al., 2020) não especificam a geração do par de chaves assimétricas. Eles empregam a Blockchain para contabilidade da transação energética em uma Cidade Inteligente. As informações de consumo/produção de energia elétrica das unidades de geração distribuída, EVs, concessionária e outros são armazenadas na Blockchain. O status energético será usado para escalonamento e gerenciamento otimizado da consumo de energia elétrica da Cidade Inteligente. Todavia, a preservação de privacidade na proposta de (Duan et al., 2020) não é abordada.

De outro modo, a Blockchain é aplicada na proposta de (Wang et al., 2019) para a preservação de privacidade. O endereço dos nós são aleatórios. Contudo, o trabalho neglicencia em ponto-único de falha. Isso se dá pelo fato do uso de uma Autoridade Certificadora (CA). Os nós recebem o certificado dela para entrar na Blockchain, tendo em vista que ela é privada.

Além disso, (Wang et al., 2019) usam *Proof-of-Reputation* como mecanismos de consenso. Ele é baseado no PoW. Entretanto, os nós com melhor reputação terão menor esforço para encontrar o *nonce*.

Ademais, a Blockchain é usada para transação energética para VEs no modelo V2V. Vale ressaltar que o endereço é mantido junto ao conjunto de energia disponível dos VEs para a verificação na recarga de energia V2V (Wang et al., 2019).

Outrossim, o trabalho proposto por (Li and Hu, 2020) apresenta a mesmo problema com uso da CA. A Blockchain é em consórcio e os participantes da rede necessitam ter certificado digital para ingressar na rede. Aditivamente, a Blockchain é baseada em Hyperledger e o mecanismo de consenso usado é o Kafka. Esse é mais escalável quando comparado ao consenso PoW (Li and Hu, 2020).

O objetivo de (Li and Hu, 2020) é fazer o escalonamento de recarga e descarga de EVs. Para isso, um algoritmo heurístico é usado. A preservação de privacidade também é abordada na proposta. Devido o controle de acesso dos participantes na Blockchain, agente maliciosos externos não podem acessar o serviço e dados dos participantes (Li and Hu, 2020). Contudo, um agente malicioso interno pode inferir o conjunto de energia transferida entre EVs, bem como o identificador do EV. Uma forma de contornar isso é cada EV possuir um grande conjunto de certificados digitais.

Em (Lin et al., 2020), a Blockchain é em consórcio, também. A arquitetura proposta é composta por *Mobile Edge Computing* (MEC), EVs inteligentes e TA. Outrossim, o algoritmo de consenso utilizado é uma mescla entre PoW e PBFT. A TA gera o par de chaves e certificado digital das entidades participantes (Lin et al., 2020). Segundo os autores, a abordagem fornece escalabilidade e um nível adequado de segurança. Todavia, o uso da TA apresenta ponto-único de falha.

Aditivamente, a Blockchain aplicada em (Zhou et al., 2019a) é em consórcio. Contudo, o consenso utilizado é o PoW. Sendo assim, a proposta possui uma taxa de transações menor que em (Lin et al., 2020). A arquiteura é formada por EVs, EAGs e *Edge computing Service Provider* (ESP). Uma autoridade confiável gera o par de chaves pública e privada dos EVs, além do seus certificados digitais. Eles ligam uma identidade real a uma chave pública. Portanto, a preservação de privacidade em (Zhou et al., 2019a) é fraca. Além disso, (Zhou et al., 2019a) incentivam os EVs a fazerem a transação energética baseada na sua carga.

Em (Zhou et al., 2019b), o modelo de sistema usado é similar a arquitetura de (Zhou et al., 2019a). Blockchain é em consórcio e o algoritmo de consenso usado é o PoW. Todavia, (Zhou et al., 2019b) utilizam um algoritmo de escalonamento para a transação energética em um modo V2G. Os EVs com maior nível de energia disponível tem a preferência para injetar energia elétrica na rede. Além disso, em (Zhou et al., 2019b), contratos inteligentes são aplicados com os EVs. Ele armazena a capacidade de energia do EV e a recompensa. Porém, assim como (Zhou et al., 2019a), o sistema é dependente de uma TA. Dessa forma, acarretando em ponto-único de falha.

Por outra via, a proposta de (Hu et al., 2019) utiliza um algoritmo de consenso baseado em PBFT. A proposta tem por objetivo minimizar o custa de geração e a variação de carga diária a nível de transmissão, distribuição e de troca de bateria. O gerador de energia armazena o resultado da otimização de cada nível na Blockchain. Todavia, (Hu et al., 2019) não especificam a configuração da Blockchain. Sendo assim, um agente malicioso pode inferir os dados dos EVs e geração de energia caso a Blockchain seja pública.

Em contrapartida, a arquitetura proposta em (Chen and Zhang, 2019) faz a preservação de privacidade dos EVs. Um Centro de Serviço de Veículo (VSC) registra os EVs na Blockchain e gera de maneira aleatória pseudônimos. Além disso, o sistema permite a verificação da assinatura digital de mensagens em lote e a Blockchain armazena a transação energética. (Chen and Zhang, 2019) aplicam uma moeda digital como mecanismo de incentivo para uso do sistema. Contudo, a arquitetura tem ponto-único de falha no VSC. Por fim, o algoritmo de consenso usado é o PBFT.

Por outra via, o trabalho de (Li and Hu, 2019) não possui ponto-único de falha e preservam a privacidade dos usuários. Todavia, o sistema de energia elétrica não é gerenciado. (Li and Hu, 2019) propuseram uma esquema de otimização para recarga e os pares que farão a transação. Os EVs informam que desejam ser fornecedores de energia elétrica e outros informam que desejam fazer a recarga do EV.

Por fim, o trabalho de (Hassija et al., 2020) usam uma DLT diferente da Blockchain usada nos demais trabalhos. A estrutura é denominada *tangle* e é baseada em Grafos acíclicos dirigidos (DAG). Uma novo bloco deve referenciar outros dois já existentes na estrutura. Em especial, a plataforma IOTA é usada. Na proposta, o suporte de transação energética é V2G e G2V. Os EVs informam na IOTA que possuem energia em excesso. Quando a demanda do SEP está alta, ele pode escolher os EVs para suprirem a demanda. Dessa forma, a proposta é escalável. Todavia, a proposta tangencia a preservação de privacidade na divulgação do estados dos EVs e do SEP na plataforma. Algoritmos baseados na teoria dos jogos são usados para criar uma concorrência entre os EVs em busca do menor preço e para encontrar o melhor equilíbrio no fornecimento/consumo de energia elétrica (Hassija et al., 2020) .

4.2 Gerenciamento do Sistema de Energia Elétrica

A proposta de (Guo et al., 2019) aplica Contratos Inteligentes na Blockchain voltados a tecnologia V2G. Mais especificamente, três (3) Contratos Inteligentes são implantados (Guo et al., 2019). Um deles é usado para indicar o nível de consumo de energia elétrica. Baseado nisso, o EV requisita seu funcionamento como produtor ou consumidor da energia elétrica. Para cada uma das operações, o Contrato Inteligente executa e fornece compensação no modo produtor.

Por outro lado, (Liu et al., 2018) busca minimizar a flutuação do nível de energia elétrica e o custo geral de recarga para os usuários de EVs. A proposta aplica a Blockchain para escalonar a Recarga/Descarga de EVs. Baseada na demanda, os EVs podem inserir energia elétrica na rede ou fazer uma recarga. O escalonamento utiliza o perfil de consumo do EV que é calculado diariamente. Aditivamente, a proposta de (Liu et al., 2018) utiliza a Blockchain Ethereum.

Outra abordagem que faz uso dessa Blockchain é a proposta de (Wang et al., 2020). Todavia, o mecanismo de validação é o PoW. Sendo assim, a proposta não se torna tão escalável e possui uma taxa de transação por segundo menor. (Wang et al., 2020) busca distribuir a *Virtual Power Plant* (VPP) através da Blockchain. Aditivamente, VPP fornece a previsão do consumo de energia elétrica. Dessa forma, EVs podem fornecer energia elétrica se a previsão resulta em cargas de pico. Além disso, a proposta de (Wang et al., 2020) usa Swarm para armazenar as informações.

Cada bloco de transação armazena o endereço Swarm. Sendo assim, a proposta de (Wang et al., 2020) possui ponto-único de falha no cluster Swarm. Além disso, a proposta não preserva a privacidade dos EVs porque cada cliente tem seu endereço armazenado no Swarm.

Em outra via, o trabalho apresentado em (Yang et al., 2019) aplica Contratos Inteligentes para automatizar mecanismos de resposta à demanda. Os nós calculam seu consumo e verificar os sistemas de armazenamento de energia elétrica (ESS). Cada entidade atualizar seu estado periodicamente e isso faz possível o ajuste de consumo de energia elétrica.

A teoria dos jogos é usada para escalonamento de transação de pares de compradores/vendedor de energia. As partes estabelecem um contrato inteligente e inicia a transação de energia (Yang et al., 2019). Com isso, a preservação de privacidade não é abordada porque os nós sempre compartilham seu estado de energia elétrica. Por fim, (Yang et al., 2019) não especificam a configuração da Blockchain e nem a autenticação das entidades na transação energética.

4.3 Discussão

Essa Seção apresenta uma discussão sobre as propostas de uso da tecnologia Blockchain voltadas para EVs. As métricas verificadas são a finalidade de utilização da Blockchain como contabilidade e sistema de gerenciamento. Além disso, outros aspectos são verificados como a preservação de privacidade dos consumidores. Dependendo a forma de aplicação, um agente malicioso pode inferir onde um EV fez a recarga ou ainda prever hábitos de utilização. Por fim, é verificado se os trabalhos apresentem ponto-único de falha. Essa métrica foi escolhida pelo fato de que a Blockchain é uma tecnologia distribuída. Contudo, a aplicação equivocada dela pode apresentar problemas na aplicação.

A Tabela 1 apresenta as métricas atingidas ou não por cada trabalho. Uma grande parte dos trabalhos apresenta ponto-único de falha. Isso é devido o uso de uma Blockchain privada que requer uma permissão explícita dos nós da rede. Além

Tabela 1. Comparação de Características.

Trabalho	Contabilidade	Sistema de Gerenciamento	Preservação de Privacidade	Ponto único de falha
(Huang et al., 2019)	V	X	X	V
(He et al., 2018)	V	X	X	V
(Guo et al., 2020)	V	X	X	X
(Wei and Ma, 2021)	V	X	V	X
(Gao et al., 2018)	V	X	V	X
(Kim et al., 2019)	V	X	X	X
(Sun et al., 2020)	V	V	V	X
(Duan et al., 2020)	V	V	X	V
(Wang et al., 2019)	V	X	V	X
(Li and Hu, 2020)	V	X	V	X
(Lin et al., 2020)	V	V	V	X
(Zhou et al., 2019a)	V	V	X	X
(Zhou et al., 2019b)	V	V	X	X
(Hu et al., 2019)	V	V	X	X
(Chen and Zhang, 2019)	V	X	V	X
(Li and Hu, 2019)	V	X	V	V
(Hassija et al., 2020)	V	X	X	V
(Guo et al., 2019)	X	V	V	V
(Liu et al., 2018)	V	V	X	V
(Wang et al., 2020)	V	V	X	X
(Yang et al., 2019)	V	V	X	V

disso, uma parte considerável não aborda a preservação de privacidade. Como a maior parte dos trabalhos usam uma Blockchain privada, é possível que os nós infiram a identidade um dos outros e consequentemente os dados armazenados na Blockchain.

5. CONCLUSÃO

A tecnologia Blockchain aparece como um conceito amplamente difundido e utilizado na literatura. Algumas de suas características como a disponibilidade e integridade dos dados torna interessante o seu uso no contexto de VEI (Fu et al., 2021). Contudo, a tecnologia utilizada de maneira equivocada pode trazer alguns desafios.

Muitas propostas na literatura usam a tecnologia para a contabilidade de dados ou gerenciamento do sistema através da aplicação de contratatos inteligente. Entretanto, muito destes acabam por tangenciar a preservação de privacidade ou ainda criar pontos únicos de falhas.

Por fim, as principais contribuições deste trabalho consistem na revisão de literatura sobre mecanismos de consenso para Blockchain e apresentação de propostas de VEI em conjunto com a tecnologia. Alguns dos trabalhos futuros ficam uma análise detalhada dos protocolos abordados, uma proposta de uso da Blockchain para VEI com preservação de privacidade e sem ponto único de falha.

AGRADECIMENTOS

Os autores agradecem ao INCTGD, órgãos financiadores (CNPq processo n° 465640/2014-1, CAPES processo n° 23038.000776/2017-54 e FAPERGS n° 17/2551-0000517-1).

REFERÊNCIAS

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)*, 1545–1550. IEEE.

Bertineti, D.P., Canha, L.N., Brignol, W., Medeiros, A.P., de Azevedo, R.M., and Nadal, Z.L. (2020). Flexible energy management strategy for electric vehicles charging stations. In *2020 55th International Universities Power Engineering Conference (UPEC)*, 1–6. IEEE.

Castro, M., Liskov, B., et al. (1999). Practical byzantine fault tolerance. In *OSDI*, volume 99, 173–186.

Chen, X. and Zhang, X. (2019). Secure electricity trading and incentive contract model for electric vehicle based on energy blockchain. *IEEE Access*, 7, 178763–178778.

Das, H., Rahman, M., Li, S., and Tan, C. (2020). Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review. *Renewable and Sustainable Energy Reviews*, 120, 109618.

De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., and Sassone, V. (2018). Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain.

Dias, L.V., Rizzetti, T.A., Brignol, W.S., and Canha, L.N. (2021). Inserção de infraestrutura de chave pública no projeto opendht. In *Anais do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, 379–384. SBC.

Duan, Q., Quynh, N.V., Abdullah, H.M., Almalaq, A., Do, T.D., Abdelkader, S.M., and Mohamed, M.A. (2020). Optimal scheduling and management of a smart city within the safe framework. *IEEE Access*, 8, 161847–161861.

Fu, Z., Dong, P., Li, S., Ju, Y., and Liu, H. (2021). How blockchain renovate the electric vehicle charging services

in the urban area? a case study of shanghai, china. *Journal of Cleaner Production*, 315, 128172.

Gao, F., Zhu, L., Shen, M., Sharif, K., Wan, Z., and Ren, K. (2018). A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE network*, 32(6), 184–192.

Guo, C., Huang, X., Zhu, C., Wang, X., and Cao, X. (2019). Distributed electric vehicle control model based on blockchain. In *IOP Conference Series: Materials Science and Engineering*, volume 486, 012046. IOP Publishing.

Guo, J., Ding, X., and Wu, W. (2020). A double auction for charging scheduling among vehicles using dag-blockchains. *arXiv preprint arXiv:2010.01436*.

Hassija, V., Chamola, V., Garg, S., Krishna, D.N.G., Kaddoum, G., and Jayakody, D.N.K. (2020). A blockchain-based framework for lightweight data sharing and energy trading in v2g network. *IEEE Transactions on Vehicular Technology*, 69(6), 5799–5812.

He, Q., Xu, Y., Yan, Y., Wang, J., Han, Q., and Li, L. (2018). A consensus and incentive program for charging piles based on consortium blockchain. *CSEE Journal of Power and Energy Systems*, 4(4), 452–458.

Hu, T., Liu, X., Chen, T., Zhang, X., Huang, X., Niu, W., Lu, J., Zhou, K., and Liu, Y. (2021). Transaction-based classification and detection approach for ethereum smart contract. *Information Processing & Management*, 58(2), 102462.

Hu, W., Yao, W., Hu, Y., and Li, H. (2019). Collaborative optimization of distributed scheduling based on blockchain consensus mechanism considering battery-swap stations of electric vehicles. *IEEE Access*, 7, 137959–137967.

Hu, Z., Du, Y., Rao, C., and Goh, M. (2020). Delegated proof of reputation consensus mechanism for blockchain-enabled distributed carbon emission trading system. *IEEE Access*, 8, 214932–214944.

Huang, X., Zhang, Y., Li, D., and Han, L. (2019). An optimal scheduling algorithm for hybrid ev charging scenario using consortium blockchains. *Future Generation Computer Systems*, 91, 555–562.

Kim, M., Park, K., Yu, S., Lee, J., Park, Y., Lee, S.W., and Chung, B. (2019). A secure charging system for electric vehicles based on blockchain. *Sensors*, 19(13), 3028.

Li, W., Andreina, S., Bohli, J.M., and Karame, G. (2017). Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, 297–315. Springer.

Li, Y. and Hu, B. (2019). An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain. *IEEE Transactions on Smart Grid*, 11(3), 2627–2637.

Li, Y. and Hu, B. (2020). A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles. *IEEE Transactions on Industrial Informatics*, 17(3), 1968–1977.

Lin, X., Wu, J., Mumtaz, S., Garg, S., Li, J., and Guizani, M. (2020). Blockchain-based on-demand computing resource trading in iov-assisted smart city. *IEEE Transactions on Emerging Topics in Computing*.

Liu, C., Chai, K.K., Zhang, X., Lau, E.T., and Chen, Y. (2018). Adaptive blockchain-based electric vehicle participation scheme in smart grid platform. *IEEE Access*, 6, 25657–25665.

Miglani, A., Kumar, N., Chamola, V., and Zeadally, S. (2020). Blockchain for internet of energy management: Review, solutions, and challenges. *Computer Communications*, 151, 395–418.

Mohammed, S.A.Q. and Jung, J.W. (2021). A comprehensive state-of-the-art review of wired/wireless charging technologies for battery electric vehicles: Classification/common topologies/future research issues. *IEEE Access*.

Namasudra, S., Deka, G.C., Johri, P., Hosseinpour, M., and Gandomi, A.H. (2020). The revolution of blockchain: State-of-the-art and research challenges. *Archives of Computational Methods in Engineering*, 1–19.

Saad, S.M.S. and Radzi, R.Z.R.M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, 10(2).

Shi, S., He, D., Li, L., Kumar, N., Khan, M.K., and Choo, K.K.R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, 101966.

Sun, G., Dai, M., Zhang, F., Yu, H., Du, X., and Guizani, M. (2020). Blockchain-enhanced high-confidence energy sharing in internet of electric vehicles. *IEEE Internet of Things Journal*, 7(9), 7868–7882.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First monday*.

Wang, Y., Su, Z., and Zhang, N. (2019). Bsis: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network. *IEEE Transactions on Industrial Informatics*, 15(6), 3620–3631.

Wang, Z., Ogbodo, M., Huang, H., Qiu, C., Hisada, M., and Abdallah, A.B. (2020). Aebis: Ai-enabled blockchain-based electric vehicle integration system for power management in smart grid platform. *IEEE Access*.

Wei, G. and Ma, Y. (2021). Privacy protection strategy of vehicle-to-grid network based on consortium blockchain and attribute-based signature. In *IOP Conference Series: Earth and Environmental Science*, volume 661, 012027. IOP Publishing.

Yang, X., Wang, G., He, H., Lu, J., and Zhang, Y. (2019). Automated demand response framework in elns: Decentralized scheduling and smart contract. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1), 58–72.

Zhou, Z., Wang, B., Dong, M., and Ota, K. (2019a). Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1), 43–57.

Zhou, Z., Wang, B., Guo, Y., and Zhang, Y. (2019b). Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 3(3), 205–216.