Capítulo 4

Blockchain para Segurança em Redes Elétricas Inteligentes: Aplicações, Tendências e Desafios

Diogo M. F. Mattos (UFF), Dianne S. V. Medeiros (UFF), Natalia C. Fernandes (UFF), Marcela T. de Oliveira (UFF), Gabriel R. Carrara (UFF), Arthur A. Z. Soares (UFF), Luiz Claudio S. Magalhães (UFF), Diego Passos (UFF), Ricardo C. Carrano (UFF), Igor M. Moraes (UFF), Célio V. N. Albuquerque (UFF), Débora C. Muchaluat-Saade (UFF)

Abstract

The electric power grid is the world's largest engineering system, and its secure and reliable operation is vital to human activities. The introduction of intelligence in the electrical power grid imposes challenges that require new techniques and approaches to provide cybersecurity. In this chapter, we discuss the use of blockchain to provide security and reliability to smart grids. Blockchain allows, in a distributed peer-to-peer network, untrusted nodes to correctly and verifiably interact with each other, without any reliable intermediary. We explore smart contracts, codes resident in blockchain that automate multi-step processes as a way to automatically trade electric energy. We present the Hyperledger Fabric, Multichain, Parity and Corda platforms for the development of blockchain applications. We also discuss initiatives, challenges and research opportunities of blockchain technology in the electrical sector.

Resumo

A rede elétrica é o maior sistema de engenharia do mundo e o seu funcionamento seguro e confiável é vital para as atividades humanas. A introdução de inteligência nas redes elétricas impõe desafios que requerem novas técnicas e abordagens de segurança cibernética. Este capítulo discute o uso da tecnologia blockchain para prover segurança e confiabilidade às redes elétricas inteligentes. A tecnologia blockchain permite que, em uma rede par-a-par distribuída, nós não confiáveis interajam entre si, sem haver qualquer intermediário confiável, de maneira correta e verificável. O capítulo discute como os contratos inteligentes, códigos residentes na blockchain que automatizam processos de múltiplas etapas, podem ser usados na comercialização automática de energia. São apresentadas as plataformas Hyperledger Fabric, Multichain, Parity e Corda para o desenvolvimento de aplicações sobre blockchain. O capítulo apresenta ainda iniciativas, desafios e oportunidades de pesquisa da tecnologia blockchain no setor elétrico.

4.1. Introdução

A rede elétrica é o maior e mais bem-sucedido sistema de engenharia do mundo [Mo et al., 2012]. A confiabilidade alcançada pelas redes elétricas é muitas vezes superior à alcançada em sistemas de comunicação [Dütsch e Steinecke, 2017]. Contudo, nas últimas décadas, o desenvolvimento das redes elétricas não tem acompanhando os avanços industriais e sociais que aumentam as demandas de suprimento de energia [Wang e Lu, 2013]. Nesse sentido, para atender às demandas crescentes por energia, é necessário agregar novas fontes à rede elétrica e gerenciar de maneira eficiente as fontes tradicionais, como hidroelétrica e termoelétrica, como também as fontes renováveis e variáveis, como energia eólica e solar. Para tanto, o *National Institute of Standard and Technology* (NIST) reuniu esforços para definir a próxima geração das redes elétricas, referenciada como *Smart Grids* ou Redes Elétricas Inteligentes [Greer et al., 2014].

As redes elétricas inteligentes integram tecnologias de comunicação bidirecional nas redes elétricas [Mo et al., 2012, Guimarães et al., 2013] e, assim, os diversos equipamentos que fazem parte das redes elétricas passam a formar uma infraestrutura dinâmica e interativa, com a capacidade de gerenciar o consumo de energia, como através da infraestrutura avançada de medição (*Advanced Metering Infrastructure* – AMI) [Sui et al., 2009] e das aplicações de resposta à demanda [Gunter et al., 2008]. No entanto, o cenário das redes elétricas é composto por uma variedade de sistemas, com numerosos proprietários e sujeitos a diversos mecanismos e agências de regulação. A variedade de atores e sistemas se comunicando no mercado de energia elétrica suscitam um grande número de vulnerabilidades [Mo et al., 2012]. As novas vulnerabilidades relacionam-se com a agregação de fontes distribuídas de geração de energia à rede e com o fato de os novos atores, nós da rede, não confiarem totalmente nos demais, já que os nós podem pertencer a organizações distintas e não ter sua identidade e comportamento atestados. Dessa forma, o cenário de redes elétricas inteligentes é propício para a aplicações que se baseiam na tecnologia *Blockchain*, referenciada neste capítulo como Cadeia de Blocos [Christidis e Devetsikiotis, 2016, Mengelkamp et al., 2018b]. A cadeia de blocos tem o potencial de simplificar os processos de negociação no mercado de energia elétrica, que são impactados pela introdução de novas fontes de geração de energia elétrica renováveis e distribuídas, e de garantir a verificabilidade das ações na rede de comunicação [Dütsch e Steinecke, 2017].

Segurança e Privacidade em Redes Elétricas Inteligentes

As redes elétricas inteligentes agregam tecnologias de comunicação de dados às redes de geração, transmissão e distribuição de energia elétrica para permitir maior controle e monitoramento em tempo real da carga gerada e consumida na rede. Ademais, as redes elétricas inteligentes permitem o desenvolvimento de novas aplicações e agregam novas formas de geração à rede, muitas vezes de pequena escala e distribuídas [Lopes et al., 2016, Mengelkamp et al., 2018b]. A geração distribuída implica a necessidade de controle fino da rede elétrica e, em especial, a adoção de mecanismos automatizados para negociação de energia elétrica pelos consumidores finais, que passam a ser produtores e consumidores de energia, chamados de "prossumidores" (*prosumers*).

A Figura 4.1 mostra os quatro componentes principais em uma rede elétrica: a geração, a transmissão, a distribuição e o consumo. Vale ressaltar que paralelamente à

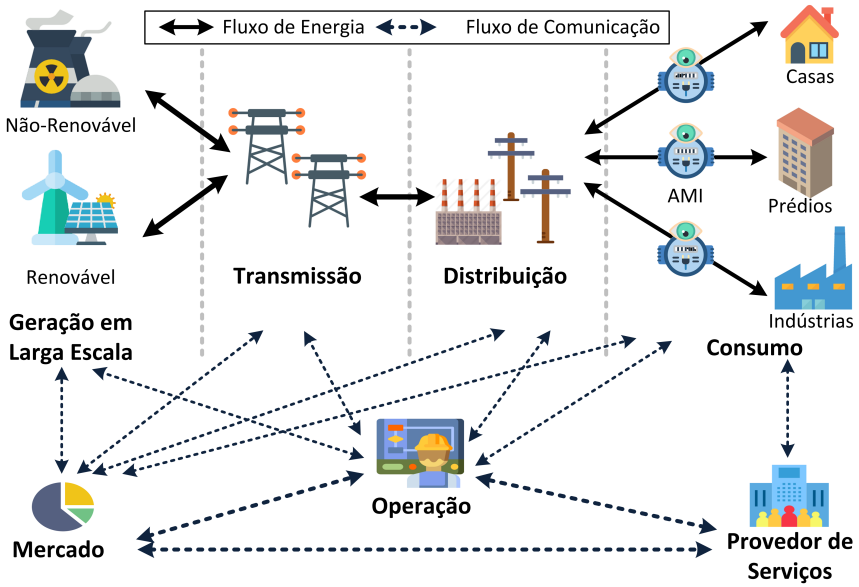


Figura 4.1. Fluxos de comunicação e os quatro principais componentes das redes elétricas. A Geração produz energia de diferentes maneiras. A Transmissão move a energia elétrica em altas voltagens através da infraestrutura. A Distribuição transforma a energia elétrica para média e baixa voltagem e distribui para o consumo. Os consumidores usam a energia elétrica.

infraestrutura dedicada para o fornecimento de energia, desde a geração até o consumo, há uma variedade de sistemas com diversos proprietários distintos que negociam, operam e fornecem a energia elétrica aos consumidores [Mo et al., 2012]. A ação dos sistemas paralelos à infraestrutura elétrica é muitas das vezes regulada por mecanismos governamentais para garantir o correto funcionamento da rede elétrica. Nas redes elétricas inteligentes, a rede de comunicação é subjacente à rede elétrica e tem por finalidade amparar a comercialização, a medição e o monitoramento da geração, transmissão, distribuição e consumo de energia elétrica. A rede de comunicação movimenta os dados de transações e monitoramento entre os diversos atores envolvidos no sistema, como os mercados de negociação de energia, os centros de controle e operação e os provedores de serviços aos consumidores finais.

Com a introdução das tecnologias de comunicação na rede elétrica, novos vetores de ataques aparecem. Destacam-se três vetores de ataque à segurança e à privacidade das redes elétricas inteligentes [Chen et al., 2012, Li et al., 2012]:

- **ataque de vulnerabilidade** causado pelo mau funcionamento de um dispositivo ou canal de comunicação ou simplesmente pela falta de sincronização entre informações de controle. As informações de controle podem ser comprometidas pela maneira como são fornecidas ou pelas condições de canal não confiáveis, levando a um processo de controle incorreto. As vulnerabilidades são provocadas principalmente pela confiabilidade intrínseca na rede de comunicação. A ausência de mecanismos para a realização de diagnósticos e a gravação de registros de ações dificultam a localização das vulnerabilidades. Vale ressaltar a existência de vulnerabilidades provocadas pela infiltração de dispositivos infectados no perímetro de segurança, como memórias USB [Langner, 2011];

- **ataque de injeção de dados** visa alterar as medidas de alguns medidores, a fim de manipular as operações da rede elétrica inteligente. O impacto desse ataque é principalmente a perda de receita. No entanto, dependendo do número de sensores controlados pelo atacante, é possível que o atacante force determinadas ações de controle sobre a rede elétrica, podendo levar a impactos catastróficos como a ocorrência de apagões em grandes áreas urbanas [Guimarães et al., 2013, Noce et al., 2017];

- **ataque intencional** é quando o atacante é capaz de ter total compreensão da topologia da rede e, portanto, pode utilizar totalmente a estrutura da rede para interromper as operações, paralisando alguma fração dos nós. O ataque intencional pode ser implementado por meio de ataque coordenado de negação de serviço (*Denial of Service* - DoS) e contribui para a interrupção da rede devido a desconexões de nós da rede de comunicação subjacente.

No novo cenário das redes elétricas inteligentes, torna-se imperativa a adoção de novas tecnologias capazes de assegurar a confiabilidade da rede elétrica, mesmo quando não há confiança entre os pares, de permitir o controle e a manutenção dos dados de produção e de consumo de energia de forma distribuída, de permitir a auditoria do histórico de transações de compra e venda de energia elétrica de maneira irrefutável e, por fim, de garantir que contratos de compra e venda de energia elétrica sejam executados corretamente, independentemente da cooperação dos participantes. Portanto, a tecnologia de cadeia de blocos é uma das viabilizadoras de aplicações seguras em redes elétricas inteligentes [Jesus et al., 2018].

Cadeia de Blocos para a Segurança entre Nós Não Confiáveis

A tecnologia de cadeia de blocos permite o desenvolvimento de aplicações sobre uma rede par-a-par, em que os membros não confiáveis interagem entre si, sem um intermediário confiável, mas de maneira verificável. A cadeia de blocos consiste em um histórico imutável de transações em uma estrutura de dados distribuída, em que cada nó da rede contém uma réplica de todos os blocos. Cada nó participante do sistema executa protocolos de consenso que validam as transações e as agrupam em blocos, que são encadeados usando uma referência ao bloco antecessor. A referência é um resumo criptográfico (*hash*), obtido através de algoritmos criptográficos unidirecionais. Essa propriedade torna improvável a recuperação dos dados originais a partir do resumo criptográfico gerado, garantindo a integridade do conteúdo e a segurança da cadeia. A cadeia de blocos é uma tecnologia capaz de atender às necessidades do sistema de coleta de dados, dando mais transparência e agilidade à comercialização de energia, na medida em que permite que as medições de fluxo de energia, assim que geradas, sejam disponibilizadas em um repositório distribuído e auditável. Paralelamente, um contrato inteligente (*smart contract*) [Bartoletti e Pompianu, 2017], uma evolução da cadeia de blocos para execução de códigos distribuídos, é essencial para a negociação segura de energia elétrica entre geradores, consumidores e "prossumidores", ao passo que assegura a execução dos contratos pela rede par-a-par subjacente à cadeia.

Contratos inteligentes (*smart contracts*) são definidos como a execução dos termos de um contrato através de um protocolo de transações computacionais [Wood, 2014,

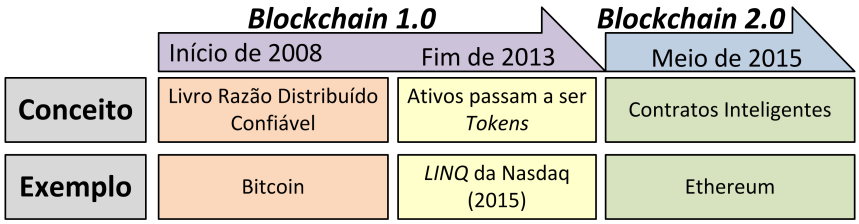


Figura 4.2. Gerações no desenvolvimento da tecnologia de cadeia de blocos. O conceito surge com o livro-razão confiável e distribuído implantado pela Bitcoin, evolui para a transação de ativos na forma de *tokens* e se concretiza como uma segunda geração após a introdução de contratos inteligentes na estrutura de dados da cadeia. Adaptado de [Dütsch e Steinecke, 2017].

Christidis e Devetsikiotis, 2016]. Assim, um contrato inteligente traduz as cláusulas de um contrato real para código que é executado em um ambiente capaz de forçar o seu correto funcionamento [Szabo, 1997]. Ao se considerar a execução dos contratos inteligentes como uma aplicação de cadeia de blocos, os contratos inteligentes são códigos armazenados na própria cadeia de blocos. Dessa forma, um contrato inteligente é uma aplicação armazenada na cadeia de blocos, acessível através de um endereço conhecido. Um contrato inteligente é ativado quando uma transação é disparada para o seu endereço, em que podem ser implementados diversos tipos de ação sobre diferentes ativos. No contexto de redes elétricas inteligentes, os contratos inteligentes são apontados como uma solução viável para realizar a negociação segura e descentralizada de energia [Aitzhan e Svetinovic, 2018].

As aplicações em cadeia de blocos ainda estão em fase inicial de industrialização. No desenvolvimento da tecnologia de cadeia de blocos, é possível diferenciar três momentos principais e definir duas gerações, mostrados na Figura 4.2. A *blockchain 1.0* refere-se à tecnologia de armazenamento de transações na cadeia, de forma distribuída e através da criação de ativos na forma de *tokens*. A primeira aplicação a ganhar notoriedade no uso de cadeia de blocos foi a criptomoeda Bitcoin [Nakamoto, 2008], introduzida em 2009. A ideia central é criar um livro-razão distribuído em uma rede par-a-par seguro e confiável. Um marco na evolução da tecnologia foi o uso da cadeia de blocos para gerir de forma segura a transferência de ativos sob a forma de *tokens*, a partir de 2013. Em 2015, essa tecnologia passou a ser usada pelo sistema LINQ da Nasdaq para armazenar transações privadas seguras[1]. A segunda geração da tecnologia, referenciada como *blockchain 2.0* [Greve et al., 2018], consiste na introdução dos contratos inteligentes. A plataforma Ethereum [Wood, 2014] foi a primeira a suportar os contratos inteligentes ao permitir o armazenamento de código de execução automática na cadeia. A principal evolução entre a primeira e a segunda gerações foi que, a exemplo da Bitcoin, a linguagem de programação das cadeias de blocos da primeira geração eram "orientadas a pilha" e não permitiam laços (*loops*) no código executável, a fim de evitar ciclos mortos (*deadlocks*) no sistema. Já em sistemas de segunda geração, como a Ethereum, são permitidas as execuções de laços nos código, que consomem créditos, no caso da Ethereum quantificados em *Ether*, ao executar contratos inteligentes. Assim, no caso de um ciclo morto, a execução é interrompida quando esgotam-se os créditos da conta usada [Merz, 2016].

[1]Acessível em http://ir.nasdaq.com/news-releases/news-release-details/nasdaq-linq-enables-first-ever-private-securities-issuance.

Objetivos do Capítulo

O objetivo principal deste capítulo é apresentar como a tecnologia de cadeia de blocos (*blockchain*) melhora a segurança, provendo a confiabilidade, a privacidade e a auditoria, em sistemas críticos, como as redes elétricas inteligentes. O capítulo foca na aplicabilidade da tecnologia de cadeia de blocos no setor elétrico, a fim de aprimorar os processos de monitoramento e faturamento da rede de geração e transmissão de energia elétrica. O uso da tecnologia de cadeia de blocos e contratos inteligentes tem o potencial de prover segurança ao sistema elétrico e reduzir os erros de armazenamento e processamento das medições no sistema. Adicionalmente, essa tecnologia reduz o risco de fraudes através de uma auditoria confiável e da garantia de execução dos contratos inteligentes. O capítulo conta com uma abordagem teórica sobre o tema, apresentando uma visão geral sobre a tecnologia de cadeia de blocos e o uso dos contratos inteligentes, discutindo especificamente os desafios encontrados no setor elétrico para monitorar ativos e realizar o faturamento entre empresas parceiras e consumidores de forma confiável. Apresentam-se, ainda, as tendências e contribuições da tecnologia de cadeia de blocos particularmente para essa nova área de pesquisa. Compara-se o desempenho do modelo baseado nessa tecnologia e dos modelos atuais utilizados para monitoramento e faturamento no sistema elétrico. Por fim, o capítulo também analisa e discute os desafios em aberto para motivar os participantes a desenvolver pesquisas na área de segurança para redes elétricas.

Organização do Capítulo

O restante do capítulo está organizado da seguinte forma. A Seção 4.2 discute os principais desafios em segurança e privacidade nas redes elétricas inteligentes. A Seção 4.3 apresenta as principais tecnologias para o desenvolvimento de aplicações sobre cadeia de blocos. O controle distribuído e a necessidade de se atingir o consenso em uma cadeia de blocos com nós não confiáveis são analisados na Seção 4.4. Os contratos inteligentes e a sua aplicação no mercado de energia elétrica são explorados na Seção 4.5. As aplicações de cadeias de blocos em redes elétricas inteligentes são abordadas na Seção 4.6. A Seção 4.7 discute as principais tendências e desafios de pesquisa da tecnologia de cadeia de blocos em redes elétricas inteligentes. A Seção 4.8 conclui o capítulo.

4.2. Segurança e Privacidade em Redes Elétricas Inteligentes

Novas vulnerabilidades são inseridas quando se introduzem as técnicas de comunicação nas redes elétricas inteligentes. Nesse novo cenário, dispositivos autônomos, como medidores inteligentes, tornam-se susceptíveis a ataques. Os atacantes de uma rede elétrica inteligente podem ser atacantes individuais; grupos criminosos; desenvolvedores de *spyware* / *malware*; *phishers*; espiões; sabotadores; terroristas ou agentes de serviços de inteligência estrangeiros [Guimarães et al., 2013, Lopes et al., 2016]. Os principais requisitos de segurança para as redes elétricas inteligentes são a disponibilidade, a integridade, a privacidade, a autenticação, a autorização, a auditoria, o não repúdio e a confiança entre os componentes da rede [Mo et al., 2012, Wang e Lu, 2013]. No contexto das aplicações de cadeia de blocos para redes elétricas inteligentes, destacam-se as propriedades de privacidade, auditoria e não repúdio que são garantidas naturalmente pelas caracterís-

ticas de formação da cadeia de blocos. Ademais, como a confiabilidade entre nós da rede não é garantida, a cadeia de blocos fornece mecanismos para execução de código entre pares que não possuem confiança mútua através dos contratos inteligentes.

A rede de comunicação das redes elétricas inteligentes interconecta os diversos atores do sistema elétrico, como consumidores, concessionárias, distribuidoras, entre outros. Assim, um ataque à rede de comunicação pode se originar de qualquer dispositivo conectado à rede [Igure et al., 2006]. A interconexão dos atores do sistema ocorre tanto por enlaces de rede cabeada quanto por enlaces de rede sem-fio, para reduzir os custos de implantação e manutenção [Zhu et al., 2011]. Dessa forma, além dos diversos pontos de entrada para um atacante[2], os ataques às redes elétricas inteligentes passam a poderem ser realizados de duas maneiras: (1) o acesso direto a um dispositivo físico, como o medidor inteligente de uma residência; ou (2) através da comunicação sem-fio, devido à natureza compartilhada do meio de transmissão da tecnologia. Portanto, para dificultar ações maliciosas nesse ambiente hostil proveniente da introdução das redes de comunicações, deve-se levar em conta os requisitos de segurança para as redes elétricas inteligentes.

A **disponibilidade** refere-se ao tempo e à acessibilidade aos dispositivos da rede. Através de uma falha na rede ou um ataque intencional [Neuman e Tan, 2011], um servidor pode tornar-se indisponível, interrompendo assim os serviços providos por este e implicando danos em equipamentos eletrônicos ou perda financeira [Rahman et al., 2013]. Um nó malicioso, por exemplo, pode comprometer o medidor inteligente de uma residência para interromper o serviço de coleta de informações de energia. Ainda em serviços críticos que necessitam da troca de mensagens dentro de um tempo mínimo aceitável, um simples ataque DoS que degrade a qualidade da comunicação pode gerar o atraso necessário no envio dos pacotes para causar danos à infraestrutura da rede elétrica [Guimarães et al., 2013].

A **integridade** refere-se à consistência e à exatidão do dado durante todo seu ciclo de vida, ou seja, a confiança de que uma mensagem enviada pela fonte chegou em seu destino sem sofrer alterações indevidas no meio do caminho. Um exemplo de quebra de integridade é a modificação das informações de cobrança por uso da energia elétrica [Neuman e Tan, 2011]. Um atacante poderia, por exemplo, modificar o valor de consumo enviado para a distribuidora de energia, a fim de se beneficiar reduzindo o valor da cobrança do seu consumo. Um ataque de vulnerabilidade para a adulteração das informações pode impactar também a disponibilidade de outros dispositivos ou serviços da rede e, portanto, deve-se adotar métodos para impedir ataques à integridade.

A **privacidade** é outro ponto importante nas redes elétricas inteligentes. Por exemplo, os medidores inteligentes mantêm informações sobre a utilização de energia por parte do consumidor [McDaniel e McLaughlin, 2009], que descrevem partes de sua rotina como os horários em que o consumidor esteve em casa ou os cômodos que ele mais utiliza. É possível descobrir quais equipamentos elétricos um consumidor possui, em qual horário usou o chuveiro elétrico, ou qual é o nível de carga do veículo elétrico desse consumidor ao chegar em casa, podendo calcular possíveis destinos, entre outros dados pessoais. Esse conjunto de informações pode facilitar ações criminosas contra re-

[2]Atacante, entidade maliciosa e nó malicioso são termos usados intercaladamente como sinônimos neste capítulo.

sidências ou fornecer inteligência de negócios para os concorrentes [Hadley et al., 2010]. A cadeia de blocos pode proporcionar uma solução confiável para garantir a privacidade dessas informações.

A **autenticação** diz respeito à identificação de uma entidade, certificando que o indivíduo é quem realmente diz ser. A autenticação assegura a integridade das ações tomadas e mensagens compartilhadas na rede, uma vez que sistemas sensíveis podem sofrer ataque de injeção de dados resultando em dano a equipamentos, perda financeira ou, até mesmo, roubo de energia [Hadley et al., 2010]. No cenário de redes elétricas inteligentes com geração distribuída, a confiança entre os nós da rede é um desafio.

A **autorização** tem como objetivo liberar o acesso de um dispositivo a um limitado conjunto de políticas. Nas redes elétricas inteligentes, as políticas de autorização são responsáveis por garantir que os serviços, de leitura ou de gerenciamento, sejam executados apenas por um seleto grupo de dispositivos. É importante ressaltar que autenticação e autorização são conceitos diferentes, mas intrinsecamente relacionados. Enquanto a autenticação garante a identidade do usuário, a autorização, após a autenticação, concede acesso às funções específicas do seu nível de permissão. Uma rede sem políticas bem definidas é suscetível a ataques à privacidade. Por exemplo, uma política de acesso que permite a leitura de informações partindo de qualquer entidade autenticada [Yan et al., 2011] facilitaria ações criminosas. O mesmo vale para políticas de gerenciamento dos dispositivos da rede elétrica, um atacante (com autorização de gerenciamento, ou por falta de políticas bem definidas) pode desligar remotamente o fornecimento de energia de uma residência [Neuman e Tan, 2011].

A **auditoria** diz respeito à capacidade de averiguar a integridade dos dispositivos e o registro de suas ações na rede elétrica inteligente [Hadley et al., 2010]. Uma área que se beneficia do requisito da auditoria é a documentação de eventos incomuns. Esse registro é importante para análise e elucidação de eventuais falhas ou tentativas de ataques à rede elétrica, podendo atribuir uma pontuação para cada dispositivo de acordo com suas ações na rede [Wang e Lu, 2013].

O requisito de **não repúdio** é importante nas redes elétricas inteligentes para garantir que ações acordadas entre as partes não possam ser contestadas futuramente. Um ataque direcionado ao não repúdio pode se aproveitar de vulnerabilidades do dispositivo para alteração dos dados auditáveis e contestação de cobranças por consumo de energia elétrica [Neuman e Tan, 2011]. Em cenários de geração distribuída de energia, esse é um grande desafio devido às transações de compra e venda de energia ocorrerem sem um intermediador. O histórico de transações permite a validação e o estudo das operações, podendo criar estratégias para maximizar o lucro ou minimizar o gasto [Ramachandran et al., 2011].

A **confiança** diz respeito à crença entre os dispositivos da rede elétrica inteligente de que os dispositivos se comportam da forma esperada. Este requisito considera que os dispositivos da rede estão autenticados e autorizados de forma correta e suas ações são bem intencionadas [Wang e Lu, 2013]. Em um ataque direcionado à confiança, o atacante aproveita-se da crença dos outros dispositivos da rede para efetuar ações danosas como a injeção de informações incorretas que podem causar interrupções de energia em menor escala [Hadley et al., 2010].

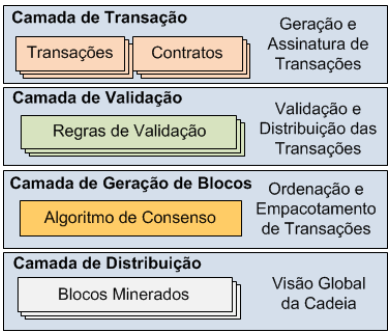
É evidente a necessidade de tecnologias para evitar ou reduzir possíveis falhas e ataques à rede. Através da tecnologia de cadeia de blocos, é possível atender aos requisitos de segurança, em especial nas redes de geração distribuída, nos quais não existe uma organização centralizadora para garantir a legitimidade das transações. Uma das características das cadeias de blocos é a garantia de imutabilidade dos dados contidos nos blocos. Assim, todas as ações dos usuários ficam gravadas na cadeia, formando um histórico incontestável. Através da auditoria dos blocos, é possível detectar falhas ou ataques e tomar as devidas ações para correção destes problemas, evitando a probabilidade de reocorrência no futuro. Os contratos inteligentes possibilitam a integridade, confiança e não repúdio, garantindo que as transações sejam concluídas apenas se ambas as partes atenderem aos requisitos acordados anteriormente, reforçados pela rede, e assegurando que, após finalizada, a transição não é desfeita.

4.3. Tecnologia de Cadeia de Blocos

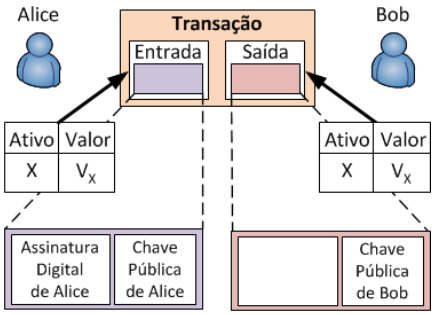
A tecnologia de cadeia de blocos consiste em uma rede par-a-par com uma estrutura de dados capaz de armazenar transações de forma ordenada e distribuída. Dessa forma, a tecnologia de cadeia de blocos é definida por dois elementos básicos, a estrutura de dados de encadeamento dos blocos e a rede par-a-par composta pelos nós participantes. O diferencial que a tecnologia de cadeia de blocos oferece em relação aos sistemas de dados distribuídos é a não necessidade da terceira entidade centralizadora, âncora de confiança, para garantir a segurança entre transações na rede [Nakamoto, 2008]. Ao se introduzir uma terceira entidade centralizadora gera-se um ponto único de falha que prejudica a segurança e a privacidade das transações realizadas, quando são considerados os conflitos de interesses entre as partes envolvidas. Assim, a tecnologia de cadeia de blocos tem sido amplamente empregada em diversos ramos de negócios, a fim de garantir disponibilidade, integridade, privacidade e não repúdio sem a necessidade de uma organização centralizadora controlando os dados.

A tecnologia de cadeia de blocos beneficia a **transparência** das transações, pois permite velocidades de liquidação próximas a tempo real e construindo a base para a auditoria, rastreabilidade e confiança entre participantes; a **confiança** entre os pares, pois elimina os intermediários e garante que a base de dados nos nós participantes converge para uma única versão coerente; a **eficiência** do sistema, já que, com a eliminação de intermediários, há a redução de custos com reconciliação e conformidade, assegurando a viabilidade de transacionar quantias menores; o **controle** e a **segurança** dos ativos transacionados ao reduzir os riscos de fraude e de liquidação, pois usa inerentemente funções criptográficas e evita a criação de pontos de centralização do controle [Dütsch e Steinecke, 2017].

A primeira geração de cadeia de blocos, representada pela *Bitcoin* [Nakamoto, 2008], foi idealizada para transferências monetárias entre nós em uma rede pública, que representam transações de pequenas quantidades de dados em uma rede hostil, em que os nós não confiam uns nos outros. Posteriormente, a segunda geração de cadeia de blocos, representada pela rede *Ethereum*, propôs que a estrutura de dados da cadeia de blocos fosse usada para representar transações mais complexas que executam um determinada aplicação, os chamados contratos inteligentes. Contratos inteligentes são estruturas de computação de mensagens de objeto confiável, autoexecutáveis. Um



(a) A tecnologia de cadeia de blocos em camadas.



(b) Exemplo de transação de transferência de ativos.

Figura 4.3. Elementos que compõem a tecnologia de cadeia de blocos. a) Divisão da cadeia de blocos em camadas. As transações dos usuários são geradas nas camada de transação, validadas pela rede na camada de validação, inseridas em blocos na camada de geração de blocos e os blocos são distribuídos na camada de distribuição. b) Transação típica em que Alice transfere um ativo da sua posse para Bob. A transação é identificada pelas chaves públicas e validada pela assinatura digital de Alice. Adaptado de [de Oliveira et al., 2018].

contrato inteligente é determinístico. Isso quer dizer que, para uma mesma entrada, sempre produzirá uma mesma saída. Caso contrário, um contrato não determinístico geraria resultados aleatórios para os diferentes nós da rede [Christidis e Devetsikiotis, 2016], impossibilitando o alcance de uma consenso sobre dados que devem ser armazenados na cadeia de blocos. A característica determinística dos contratos inteligentes é o que garante a convergência da visão global da rede. O contrato inteligente reside na cadeia de blocos e, como tal, seu código pode ser inspecionado por todos os participantes da rede. Como todas as interações com um contrato ocorrem via mensagens assinadas, é possível rastrear todos os participantes envolvidos na operação do contrato. Sendo assim, a aplicação de contratos inteligentes possibilitou a automatização de regras executáveis com o consentimento das várias partes envolvidas [Wood, 2014].

A segurança oferecida pela tecnologia de cadeia de blocos reside em todos os nós participantes da rede par-a-par acessarem uma réplica idêntica da cadeia de blocos armazenada localmente, mesmo em um ambiente de desconfiança mútua entre participantes. Portanto, é necessário adotar mecanismos de validação e de consenso para realizar a distribuição e a réplica coerente dos dados e adotar mecanismos de assinatura digital e resumos criptográficos para garantir a auditoria distribuída sobre as transações executadas na rede.

Para que as transações sejam efetivadas como parte da cadeia, as transações são processadas por quatro camadas, transações, validação, geração de blocos e distribuição, mostradas na Figura 4.3(a) [de Oliveira et al., 2018].

A camada de **transações** representa a geração da informação que se deseja armazenar em uma cadeia de blocos. Estas informações são por natureza não editáveis, isto é, contratos, transferências bancárias, compra e venda etc. Assim como em bancos de dados tradicionais, na cadeia de blocos, as transações seguem a semântica ACID (Atomicidade, Consistência, Isolamento e Durabilidade) [Dinh et al., 2017]. Além disso, a interação direta dos usuários com a cadeia ocorre na camada de transações. O controle de acesso à rede acontece a partir da concessão de um par de chaves assimétricas para que o

usuário possa assinar digitalmente uma transação na rede. Os usuários são identificados somente pelas chaves públicas geradas ao ingressarem na rede, permitindo uma pseudo-anonimização dos participantes [Nakamoto, 2008]. Vale ressaltar que, por padrão, não há um esquema para autenticação de usuários, já que os usuários são apenas identificados por suas chaves públicas, não há um mecanismo que relacione uma chave pública com uma entidade conhecida, como realizado por uma infraestrutura de chaves públicas (*Public Key Infrastructure* - PKI). Assim, o usuário assina suas transações com a chave privada e pode ser endereçado na rede por meio da chave pública. Seguindo critérios definidos na rede, como organização e linguagem de codificação pré-estabelecidas para a elaboração da transação e a assinatura, o usuário transmite a transação para todos os nós vizinhos, conforme mostrado na Figura 4.3(b). A camada de **validação** é determinada pela verificação das transações. Os nós vizinhos são responsáveis por verificar se as transações seguem os critérios predeterminados pela rede. A validação analisa se a transação obedece a todas as regras da rede no desenvolvimento da cadeia de blocos. Por exemplo, na *Bitcoin*, a regra fundamental para executar uma transação é a disponibilidade da quantia enviada em posse da chave pública que a emite. As transações são somente transmitidas para os nós seguintes se forem consideradas válidas pelos nós que realizam o processo de validação das novas transações. Caso a transação descumpra algum dos critérios da rede, deve ser descartada e não passada adiante.

Na camada de **geração de blocos**, as transações validadas na camada de validação estão disponíveis para a formação do novo bloco da cadeia, *pool* de transações válidas. Essas transações são coletadas, ordenadas e empacotadas em um bloco candidato a ser inserido na cadeia, com a estampa de tempo correspondente (*timestamp*). A geração do bloco é chamada de processo de mineração, no qual o nó minerador toma a responsabilidade de gerar o bloco e introduzi-lo efetivamente na cadeia. Contudo, a escolha do nó minerador depende diretamente do mecanismo de consenso empregado na rede. Cada bloco minerado contém uma referência ao bloco antecessor, formando assim o encadeamento de blocos. Essa referência é feita através de resumos criptográficos (*hash*) [Nakamoto, 2008, Chicarino et al., 2017, Christidis e Devetsikiotis, 2016], como ressaltado na Figura 4.4. O bloco inicial da cadeia é o bloco *genesis*, que armazena um valor de resumo criptográfico determinado na pela regra de formação da cadeia de blocos. O bloco B_n, com transações válidas, possui junto ao seu conteúdo o resumo criptográfico do bloco anterior B_{n-1}. O conteúdo completo do bloco B_n será usado para gerar o resumo criptográfico que será incluído como referência no próximo bloco B_{n+1}. Como o algoritmo que computa o resumo criptográfico é unidirecional, é improvável a recuperação dos dados originais a partir do resumo gerado, assim como é improvável a geração de um novo conteúdo que gere o mesmo resumo. Isso garante a integridade dos dados na cadeia. Caso haja uma mudança indevida no conteúdo de um dos blocos armazenados em um nó, tal mudança é evidenciada pela alteração do valor do *hash* desse bloco que, por sua vez, é propagada para todos os demais blocos da cadeia, devido ao encadeamento de valores dos *hashes* do blocos seguintes, a exemplo do $Bloco_{n-2}$ no *Nó 2* da Figura 4.4.

Na camada de **distribuição**, o bloco minerado é adicionado à estrutura de dados da cadeia de blocos de cada nó da rede par-a-par. Destaca-se a necessidade da réplica atualizada da cadeia localmente para que seja alcançado o consenso na rede. Assim sendo, as transações associadas aos blocos são executadas para atualizar a visão global da cadeia.

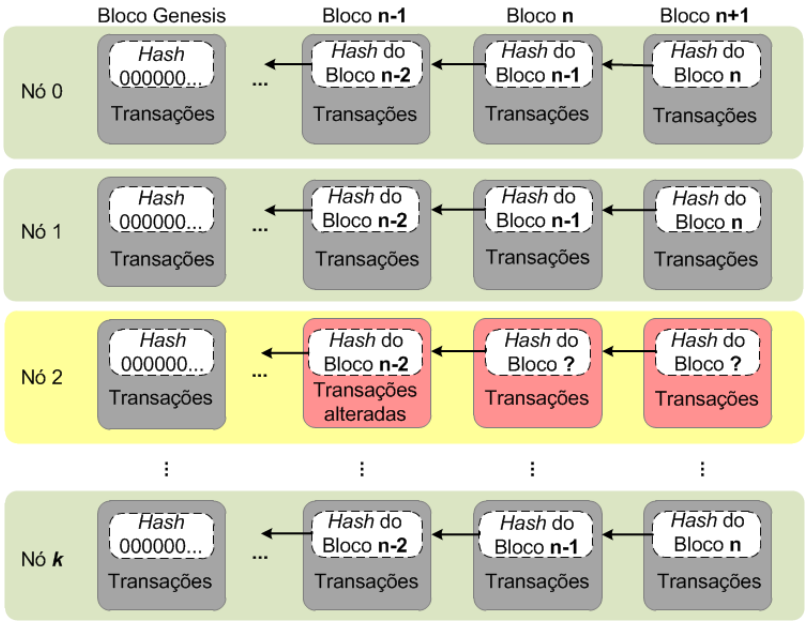


Figura 4.4. Visão esquemática da estrutura de dados em uma cadeia de blocos. O bloco *genesis* representa o primeiro bloco da cadeia. Cada bloco tem o resumo criptográfico do bloco anterior, gerando um encadeamento de resumos criptográficos. A alteração de um bloco gera a inconsistência de todos os blocos seguintes da cadeia.

Ressalta-se que a execução das transações determina uma mudança de estado global na cadeia, seja a transferência de ativos, seja a execução de um contrato inteligente. Contudo, o encadeamento de um novo bloco só ocorre nos nós adjacentes se o resumo criptográfico do bloco minerado estiver correto. Essa verificação é feita pela comparação entre o conteúdo do bloco e o resumo criptográfico apresentado. Caso contrário, o bloco minerado é descartado. Se todos os nós da rede possuírem o mesmo estado global da cadeia, com o mesmo conteúdo e blocos organizados na mesma ordem, os nós estão em consenso. Ao atingi-lo, todos os nós passam a ter acesso à mesma informação. A visão global distribuída da cadeia permite a disponibilidade e a auditoria das informações.

4.3.1. Taxonomia de Plataformas de Cadeia de Blocos

Christidis e Devetsikiotis classificam as cadeias de blocos segundo os aspectos de controle de acesso ao conteúdo da cadeia e quanto às permissões sobre as funções que os nós da rede exercem [Christidis e Devetsikiotis, 2016]. Contudo, não há um consenso sobre uma definição formal de taxonomia para classificar as redes de cadeia de blocos. Outros trabalhos classificam as redes como pública, privada, permissionada e híbrida [Pilkington, 2016, Gupta e Sadoghi, 2018]. Apesar dos conceitos de rede pública e privada serem bem conhecidos e antagônicos, os conceitos de rede permissionada e híbrida não são autoexplicativos. Neste capítulo, adota-se a taxonomia em diferentes tipos de visão da rede, *pública não permissionada*, *pública permissionada*, *privada não permissionada* e *privada permissionada*, como evidenciado na Figura 4.5.

Redes públicas e privadas se distinguem em relação ao controle de acesso à rede e ao conteúdo da cadeia, visto que uma vez que o nó é participante da rede par-a-par, o nó acessa a sua réplica da cadeia armazenada localmente. Em uma rede pública, de conteúdo

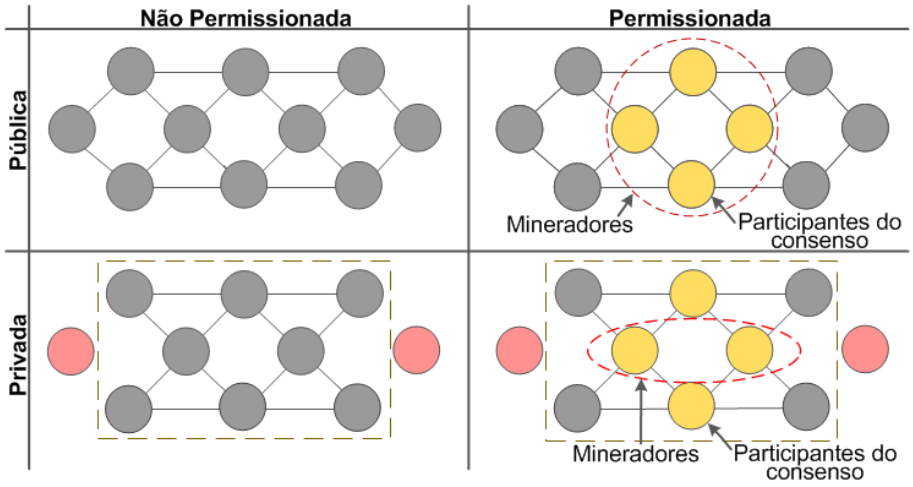


Figura 4.5. Taxonomia aplicada a redes de cadeia de blocos. A classificação entre pública e privada relaciona-se com a participação de nós na rede. A classificação entre permissionada e não permissionada relaciona-se com o papel desempenhado pelos nós da rede nos mecanismos de consenso e de geração de novos blocos.

aberto, não há qualquer mecanismo de controle de acesso e os nós podem ingressar e deixar a rede sem qualquer prejuízo para o mecanismo de consenso ou para a geração de novos blocos. Em redes privadas, em que o conteúdo é fechado, há medidas de controle de acesso e apenas nós autorizados podem acessar a rede par-a-par e ter acesso ao conteúdo da cadeia. Em paralelo, redes permissionadas e não permissionadas se diferenciam pelo critério de atividades desempenhadas na rede. Em redes não permissionadas, todos os nós desempenham o mesmo papel na rede, podendo gerar transações, competirem na mineração de blocos e participarem do mecanismo de consenso. Em contraste, nas redes permissionadas, os nós podem possuir papéis distintos, de acordo com a necessidade da aplicação, como por exemplo, uma aplicação em que todos os nós podem criar transações, um grupo de nós da rede é responsável por realizar o consenso e apenas um subgrupo é autorizado a minerar novos blocos.

Em **redes públicas não permissionadas** de cadeias de blocos há desconfiança mútua entre os usuários da rede e, por isso, os mecanismos de consenso são rígidos. A fim de evitar ataques de personificação (*Sybil Attack*) [Douceur, 2002], o consenso em redes públicas não permissionadas é oneroso, exigindo-se a resolução de um desafio computacional como prova da participação no consenso e, assim, evitando que um nó apresente diversas identidades. O incentivo aos nós a participarem desse mecanismo de consenso consiste em um incentivo econômico dado aos nós mineradores na forma de criptomoeda. Isso é justificável pelas características principais de uma rede pública não permissionada, tais como conteúdo aberto e igualdade entre os nós. Todo nó pode ingressar e sair da rede. O participante da rede gera um par de chaves criptográficas para assinar e realizar transações quando ingressa pela primeira vez na rede. Além disso, qualquer nó pode ser um minerador e fazer parte do mecanismo de consenso da rede. Os problemas associados às redes públicas não permissionadas estão relacionados à escalabilidade e ao tempo efetivo desde a emissão da transação até a execução na cadeia. Essas redes constituem ambientes colaborativos e, portanto, dependem do comportamento benigno dos nós. Além disso, a

competição entre os nós mineradores pelas recompensas da geração do bloco torna o processo mais lento e custoso. *Bitcoin* e *Ethereum* são exemplos de plataformas que oferecem configuração de rede pública não permissionada.

As **redes públicas permissionadas** foram desenvolvidas para aplicação de mecanismos de consenso menos custosos em redes públicas. A diferença entre as redes públicas não permissionadas e as permissionadas é a desigualdade de atuação dos nós na rede. Em uma rede pública permissionada, todos os dados são disponíveis para auditoria pública e não se restringe a entrada de novos nós. Contudo, um nó só participa da rede após a verificação adequada de sua identidade e, assim, alocam-se as permissões que determinam quais atividades o nó pode executar na rede. Este tipo de rede é utilizada para gerenciar transações entre empresas ou em processos que envolvem várias entidades, permitindo que somente alguns nós de cada entidade fiquem responsáveis pela geração de blocos, aplicando mecanismos de consenso mais eficientes e sustentáveis.

As **redes privadas não permissionadas** se diferenciam das redes púbicas por restringirem a entrada de nós e, portanto, só fornecem a réplica da cadeia a nós identificados por uma chave pública autorizada. Existe uma ou um conjunto de instituições que determinam quem são os nós autorizados a participarem da rede. Destaca-se que o conceito de rede privada se delimita ao controle de acesso aos dados da cadeia. Os nós que participam da rede têm funções iguais e exercem a mesma importância na rede, pois não se determinam permissões diferenciadas aos nós da rede. Uma vez autorizado a participar da rede, o nó pode gerar transações, gerar blocos e participar do consenso. Esta característica é interessante às aplicações em que nós, mesmo autorizados a participarem da rede, oferecem um comportamento hostil. Nesses casos, empregam-se mecanismos de consenso tolerantes a falhas Bizantinas (*Byzantine-Fault Tolerant* - BFT), exigindo que todos os nós participem do consenso. O *Hyperledger Fabric* é um exemplo de plataforma com opção de configuração de redes privadas não permissionadas.

As **redes privadas permissionadas** oferecem a oportunidade de aplicações de mecanismos de consenso mais eficientes e menos custoso em termos de processamento. A característica privada limita a entrada e permanência de nós indesejáveis na rede. As permissões possibilitam configurar diferentes papéis para os nós participantes da rede como, por exemplo, oferecer flexibilidade para aplicações permitirem que apenas alguns nós façam parte do processo de consenso e apenas um subconjunto desses nós possam gerar o próximo bloco. As aplicações de cadeia de blocos em redes elétricas inteligentes podem aproveitar esta flexibilidade para poupar processamento e energia de dispositivos simples, como medidores inteligentes, impedindo a participação desses nós em mecanismos de consenso e geração de blocos. Dispositivos com mais processamento e segurança exercem essas atividades na rede. A *Parity* e a *MultiChain* são exemplos de plataformas que permitem configurações de redes privadas permissionadas.

4.3.2. Plataformas para Desenvolvimento de Cadeias de Blocos

A **Bitcoin**[3] é uma plataforma para desenvolvimento de aplicações para cadeias de blocos proposta por Satoshi Nakamoto [Nakamoto, 2008]. Ela permite a criação de redes públicas não permissionadas nas quais um nó pode participar e exercer qualquer

[3]Disponível em https://bitcoin.org/.

função na rede. Essa característica faz com que certos critérios de confiabilidade sejam exigidos de seus participantes, por isso esta plataforma utiliza a Prova de Trabalho como mecanismo de consenso. Antonopoulos define que as funções exercidas por cada nó podem ser divididas em: (i) cliente de referência que possuem todas as funções, (ii) nó completo que não exerce a função de mineração, (iii) nó leve que apenas interage com a rede para enviar e receber transações e (iv) nó minerador que é apenas responsável por executar a prova de trabalho [Antonopoulos, 2014].

A Bitcoin permite aos seus usuários criarem regras que restringem o modo como os valores enviados através das transações são gastos. Apenas usuários capazes de satisfazer essas regras podem ter acesso aos valores a eles relacionados. Para expressar essas regras, a Bitcoin implementa uma linguagem denominada *Script*. Um usuário ao criar uma transação acrescenta um código executável que define as condições para gastar aquele valor. Ao utilizar esse valor para criar outra transação, deve-se acrescentar outro código executável que, quando executado juntamente ao anterior, resulte em uma execução bem sucedida. A *Script* é uma linguagem baseada em pilha e não é do tipo *Turing* completa, ou seja, ela não possui estruturas de laços. Essa restrição se faz necessária para impedir que ataques de negação de serviço sejam feitos contra um nó através da criação de laços infinitos. A regra mais utilizada para criar transações é a que atrela um dado valor à chave pública de outro usuário e, assim, garante que apenas ele possa gastá-lo. Em suas primeiras versões, a Bitcoin permitia somente a criação de soluções financeiras baseadas na troca de valores. No entanto, as versões mais recentes da plataforma permitem o envio de dados no lugar de apenas valores. Aplicações não financeiras foram propostas sobre a Bitcoin, como o *FairAccess* [Ouaddah et al., 2016], cujo objetivo é prover controle de acesso a recursos, utilizando a estrutura das transações como meio para enviar as permissões. A linguagem *Script* é usada para expressar as condições de acesso aos recursos.

A **MultiChain**[4] é uma plataforma para desenvolvimento de aplicações utilizando cadeias de blocos, cujo projeto foi desenvolvido baseado na implementação da Bitcoin. A plataforma é totalmente compatível com o protocolo e capaz de funcionar como um nó da rede Bitcoin. A MultiChain permite a criação de redes privadas permissionadas [Greenspan, 2015], o que exige a participação de um administrador na rede, que é responsável por permitir a entrada e gerenciar as permissões dadas aos nós. As permissões variam desde capacidade de executar buscas na cadeia, até permissão para um nó ser minerador ou tornar outro nó administrador. O papel de administrador é concedido ao nó responsável por criar o bloco *gênesis* da rede. Sempre que um administrador concede ou revoga uma permissão de um nó, esse evento fica registrado na cadeia através de uma transação especial. Dessa forma, todos os demais nós são capazes de verificar quais permissões estão vinculadas a cada chave pública da rede.

Usuários de uma rede MultiChain são capazes de criar e gerenciar seus próprios ativos, através de uma transação especial, chamada "Transação Gênesis", que contém os metadados necessários para registrar o canal na cadeia de blocos [Greenspan, 2015]. Para tanto, o usuário deve possuir a permissão concedida por um administrador da rede. Após a criação do canal, o criador assume o papel de administrador, podendo decidir quem pode

[4]Disponível em https://www.multichain.com/.

enviar, receber e criar novos ativos naquele canal. A criação de canais privados permite que apenas os usuários que tenham interesse em um certo tipo de ativo obtenham acesso ao canal e às informações presentes na cadeia relativa ao ativo.

Ao contrário da plataforma Bitcoin, a MultiChain não possui suporte à criação de regras através da linguagem *Script*. Logo, um usuário é apenas capaz de enviar e receber ativos pela rede. No entanto, quando utilizada para se conectar à rede Bitcoin, a plataforma fornece suporte à criação de regras através da *Script*. O mecanismo de consenso oferecido pela MultiChain permite que, através da configuração de parâmetros no momento da criação da rede, o consenso funcione como uma prova de trabalho ou que cada minerador alterne na criação de um novo bloco, sem a necessidade de haver competição. Isso permite que haja maior flexibilidade na criação de novas redes e elimina os altos custos computacionais da prova de trabalho. A manutenção da prova de trabalho permite a retrocompatibilidade com a rede Bitcoin.

A **Ethereum**[5] é uma plataforma criada e mantida pela *Ethereum Foundation* e representa o início da segunda geração das plataformas de cadeias de blocos [Buterin et al., 2013]. Essa plataforma foi desenvolvida com o intuito de possibilitar a realização de novas transações além de somente as transações de trocas de posse de ativos. A plataforma possibilita a criação de aplicações que, através da invocação de contratos inteligentes, podem exercer diferentes funções na redes. A utilização de contratos inteligentes estabeleceu uma nova geração de aplicações de cadeias de blocos, pois o desenvolvedor de aplicações na plataforma Ethereum é capaz de criar aplicações que interagem com a rede Ethereum de maneira transparente ao usuário final. Essas aplicações usufruem de todas as vantagens das cadeias de blocos, porém sem a necessidade de conhecimento específico sobre a tecnologia. A principal proposta da plataforma Ethereum é a criação de aplicações que utilizam a cadeia de blocos da própria rede Ethereum. Contudo, a plataforma possibilita a criação de redes públicas não permissionadas e, assim como na rede Bitcoin, a rede Ethereum possui sua própria moeda corrente, o *Ether*. A plataforma possibilita a realização de transações financeiras simples, sem a necessidade da utilização de contratos complexos. O mecanismo de consenso utilizado pela Ethereum é prova de trabalho, mas a versão implementada por esta plataforma impede a utilização de *hardware* especializado para a otimização do tempo de resolução do desafio computacional. Isso garante uma melhor distribuição das capacidades de mineração através da rede [Buterin et al., 2013]. Segundo seus desenvolvedores, em uma versão futura, será acrescentado suporte à utilização da prova de participação (*Proof of Stake*) como uma alternativa à prova de trabalho.

A **Parity**[6] inicialmente foi proposta como um meio de interação com a rede Ethereum. Assim, a Parity possui todas as características presentes na plataforma Ethereum. Além disso, a Parity agrega uma ferramenta para desenvolvimento e depuração de aplicações baseadas em contratos inteligentes utilizando a linguagem nativa da Ethereum, a *Solidity*, além de possuir suporte para a utilização de carteiras digitais e para o gerenciamento de chaves de usuários. A Parity estende as funções padrão da plataforma Ethereum permitindo a criação de redes privadas permissionadas, que possuem compati-

[5]Disponível em https://www.ethereum.org/.
[6]Disponível em https://www.parity.io/.

bilidade com a rede Ethereum e permitem que aplicações desenvolvidas para a Ethereum funcionem normalmente na rede privada Parity. Para a criação de redes privadas, a Parity fornece suporte ao mecanismo de consenso original da Ehtereum, a prova de trabalho, porém também possui uma implementação do mecanismo baseado na prova de autoridade. Nessa implementação, os nós mineradores se revezam para criar blocos dentro de uma janela de tempo determinada no momento da criação da rede.

O **Hyperlegder**[7] é um projeto formado por diversas corporações, como a Linux Foundation, a IBM e a Intel, que visam desenvolver soluções para promover a aplicação comercial e incentivar os estudos sobre a tecnologia de cadeia de blocos [Greve et al., 2018]. Um dos desdobramentos do projeto é a plataforma **Hyperledger Fabric**, proposta pela IBM [Cachin, 2016]. A plataforma permite a criação de soluções empresariais baseadas no uso de cadeias de blocos privadas permissionadas. A arquitetura modular permite que serviços específicos de rede sejam distribuídos entre nós especializados, o que permite que sejam oferecidos altos graus de confiabilidade, resiliência, flexibilidade e escalabilidade [Greve et al., 2018]. Os nós da rede podem fornecer serviços de validação, consenso, controle de credenciais e armazenamento. Nós que fornecem serviços de validação são responsáveis por conectar clientes aos serviços de consenso, através da emissão de transações. Esses nós não possuem capacidade para executar as transações, apenas de verificá-las. O serviço de consenso é oferecido pelos nós responsáveis por executarem o mecanismo de consenso, que nesta plataforma consiste de uma implementação do modelo prático de tolerância a falhas bizantinas (*Practical Byzantine Fault Tolerance* - PBFT). Esses nós também são responsáveis por validar as transações. O serviço de consenso também é responsável por atualizar o estado da cadeia de blocos. O controle de credenciais é o serviço responsável por criar os certificados que identificam os usuários da rede. Através dessa identificação, é possível exercer o controle de permissão da rede. Ao realizar uma transação, um usuário deve obrigatoriamente se identificar através de seu certificado. O serviço de armazenamento é oferecido por todos os nós da rede, com exceção dos nós que realizam controle de credenciais. O serviço consiste em armazenar uma cópia da cadeia de blocos e permitir a realização de consultas. As informações da cadeia de blocos são armazenados em um banco de dados não relacional e apenas as referências aos dados ficam na cadeia. Esse procedimento torna a rede escalável, pois reduz o espaço necessário para armazenar uma cópia local da cadeia e reduz o tempo para realizar buscas por informações. A Hypeledger Fabric possui suporte para a criação de contrato inteligente, denominado *ChainCode*. Esses contratos ficam armazenados na cadeia e, quando invocados, são executados pelos nós que implementam o serviço de consenso. A linguagem utilizada para o desenvolvimento dos contratos é a GO[8]. Para adicionar um contrato a uma cadeia, um usuário executa uma transação, ficando assim também registrado o momento da criação do contrato.

A plataforma **R3 Corda**[9] foi desenvolvida com o propósito de se diferenciar das demais plataformas de desenvolvimento de cadeias de blocos, já que propõe o isolamento dos dados de seus usuários. O isolamento ocorre através da criação de canais de comunicação entre usuários que estejam interessados em realizar transações entre si, formando

[7]Disponível em http://www.hyperledger.org.
[8]Disponível em https://golang.org/.
[9]Disponível em http://www.corda.net/.

pequenas cadeias de blocos acessíveis apenas entre eles. A Corda possibilita a criação de cadeias privadas permissionadas. Para que um usuário possa fazer parte de uma rede, é necessário que ele possua os certificados gerados pela entidade responsável por administrar aquela rede. Uma vez na rede, o usuário pode se associar a canais com participantes com os quais deseja realizar transações. Contratos inteligentes são tratados de maneira diferente pela Corda, uma vez que esse contratos são disponibilizados na forma de aplicativos (*Cordapps*) que podem ser instalados em nós específicos da rede, sem a necessidade de estarem disponíveis em todos os nós. Esse aplicativos são responsáveis por realizarem a interação dos usuários com a rede. Para o desenvolvimento das aplicações, a Corda oferece bibliotecas nas linguagens *Java* e *Kotlin*, porém qualquer linguagem compatível com a máquina virtual Java (JVM) pode ser utilizada. O desenvolvedor pode criar uma interface gráfica e disponibilizá-la através de um servidor *web* integrado à sua aplicação. Isso torna a utilização das aplicações mais amigáveis aos usuários. Na versão atual, versão 3.0, a Corda disponibilizada três opções para mecanismos de consenso, o *Raft*, o *bftSMaRt* e o consenso personalizado. O *Raft* é um protocolo de consenso por votação simplificado, mas que não resiste a falhas bizantinas [Ongaro e Ousterhout, 2014]. O *bftSMaRt* consiste de uma implementação do modelo prático de tolerância a falhas bizantinas [Bessani et al., 2014]. A aplicação (*Cordapp*) pode fornecer uma implementação própria de um mecanismo de consenso personalizado. O armazenamento dos dados da rede é feito através da utilização de bases de dados externas à cadeia em cada nó. As bases de dados armazenam apenas as transações em que eles tiveram participação, restringindo os acesso aos dados apenas a usuários que utilizam os canais aos quais o nó pertence.

4.4. Controle Distribuído e Consenso em Cadeias de Blocos

Os nós participantes de um sistema que utilize cadeia de blocos devem possuir uma visão global comum sobre a rede, para que não existam divergências nas cópias das cadeias de blocos presentes em cada nó. Os blocos da cadeia são compostos por uma sequência de transações a serem executadas. Antes de serem executadas, os nós precisam alcançar um consenso, concordando com as transações inseridas no bloco e com a ordem em que serão executadas. O consenso consiste em regras para validação e difusão de transações e blocos, resolvendo potenciais conflitos [Xu et al., 2017], e alcançando uma consistência eventual da informação presente na rede. Ao se alcançar o consenso, garante-se a integridade, a consistência e a imutabilidade da cadeia de blocos.

O consenso é alcançado de forma distribuída, eliminando a necessidade de um agente central intermediário confiável. O tipo de mecanismo de consenso utilizado depende do tipo de rede de cadeia de blocos e do tipo de vetor de ataque esperado. São duas as principais classes de mecanismos de consenso: protocolos probabilísticos de consistência eventual e protocolos baseados em votação por maioria [Christidis e Devetsikiotis, 2016, Cachin e Vukolic, 2017]. Nos mecanismos baseados em consistência eventual, não é necessário saber o número de participantes disponíveis no consenso e eventualmente existe convergência sobre a cadeia de blocos, com base na disseminação da informação sobre o que cada participante enxerga como verdade. Já nos protocolos baseados em votação, é necessário conhecer todos os participantes do mecanismo. Dessa forma, consenso baseado em consistência eventual é adequado para cadeias de blocos públicas, enquanto os baseados em votação são mais adequados para ca-

deias de blocos privadas [Christidis e Devetsikiotis, 2016, Cachin e Vukolic, 2017]. Dentre os mecanismos de consenso utilizados nas redes de cadeia de blocos públicas estão as provas de trabalho (*Proof of Work* - PoW), de participação (*Proof of Stake* - PoS) e de capacidade (*Proof of Capacity* - PoC). Em redes de cadeia de blocos privadas, a necessidade por mecanismos de consenso custosos em termos computacionais, como a PoW, é reduzida [Christidis e Devetsikiotis, 2016] e, portanto, outros mecanismos de consenso podem ser utilizados, como a prova de autoridade (*Proof of Authority* - PoA), o protocolo prático de tolerância a falhas bizantinas (*Practical Byzantine Fault Tolerance* - PBFT) [Castro e Liskov, 1999] e os algoritmos Paxos [Lamport, 2001], Raft [Ongaro e Ousterhout, 2014] e Ripple [Schwartz et al., 2014].

4.4.1. Prova de Trabalho – PoW

Em redes públicas, tais como *Bitcoin* e *Ethereum*, uma única entidade pode participar da rede com múltiplas identidades para influenciar a votação sobre a validação de um determinado bloco. A consequência imediata dessa possibilidade é o controle da rede por uma minoria [Christidis e Devetsikiotis, 2016]. Para desestimular essa prática, Nakamoto [Nakamoto, 2008] propõe o uso de um mecanismo de consenso denominado Prova de Trabalho (*Proof of Work* - PoW). Na PoW, para que um bloco seja inserido na cadeia de blocos, os nós mineradores devem resolver um desafio não trivial, que exige grande poder de processamento para ser resolvido, mas cujo resultado pode ser facilmente verificado por qualquer nó da rede que seja participante do consenso. O bloco candidato a ser inserido na rede é composto pelas transações que foram submetidas, mas ainda não foram validadas. Quando o desafio é solucionado, o bloco é minerado, isto é, inserido na cadeia de blocos global, e as transações são validadas e executadas. O nó minerador recebe uma recompensa por ter empenhado seu poder computacional para a resolução do desafio.

O desafio computacional exigido na PoW consiste em encontrar um número aleatório (*nonce*) que faz com que o resumo criptográfico (*hash*) do bloco tenha o número esperado de zeros iniciais para a dificuldade definida para aquela rede [Nakamoto, 2008]. O *nonce* está contido no cabeçalho do bloco, juntamente com o resumo criptográfico do bloco anterior. Quanto maior o número de zeros iniciais requeridos, mais complexo é o desafio computacional. Na *Bitcoin*, a rede ajusta a dificuldade do desafio a cada 2.016 blocos para levar em consideração mudanças no poder de processamento dos nós e para garantir que os blocos sejam gerados a uma taxa constante [Christidis e Devetsikiotis, 2016] e, atualmente, são exigidos resumo criptográfico que iniciam com 8 zeros.

Ao resolver o desafio computacional, o nó gera uma prova de trabalho e pode adicionar o novo bloco à cadeia de blocos, recebendo a recompensa pela resolução do desafio. Esse bloco é disseminado através da rede para que os outros nós possam adicioná-lo a suas cópias da cadeia de blocos. Os outros nós que estavam trabalhando para solucionar o mesmo desafio param de tentar, uma vez que não haverá mais recompensa caso resolvam o desafio após o bloco ter sido minerado [Nakamoto, 2008]. Além disso, os blocos que os outros nós estão tentando minerar agora referenciam o resumo criptográfico do bloco errado e podem ser compostos por transações que já foram mineradas, isto é, que estão no bloco recentemente inserido na cadeia pelo nó vencedor. Ao desistirem e aceitarem que o desafio foi solucionado por um minerador vencedor, o consenso é alcançado. Na PoW, é possível que vários nós reivindiquem o próximo bloco a ser adicionado à cadeia.

Isso ocorre porque a PoW é um mecanismo de consenso probabilístico, no qual cada nó tem uma determinada probabilidade de concluir o desafio computacional antes de todos os outros nós da rede. Quando mais de um nó minera um bloco, ocorre uma ramificação da cadeia de blocos. Na PoW, a ramificação que carregar a maior quantidade de trabalho deve ser seguida. A ramificação da cadeia de blocos que crescer primeiro, através da inserção de novos blocos será adotada como a cadeia correta, levando à poda dos outros ramos [Nakamoto, 2008]. Isso permite que a rede alcance novamente o consenso sobre a ordem de ocorrência dos eventos e, então, obtenha uma visão global da cadeia consistente.

Apesar de o mecanismo tender probabilisticamente à convergência, a Prova de Trabalho apresenta desvantagens como a crítica à sustentabilidade do processo de mineração, em que há um gasto exacerbado de energia para criação de um bloco. Além disso, é observada uma alta latência para alcançar o consenso na rede. Como consequência, há uma baixa vazão na quantidade de transações validadas no tempo. Além disso, o mecanismo de Prova de Trabalho pode ser comprometido, teoricamente, por um usuário que controle pelo menos mais que 50% dos recursos computacionais da rede. Apesar da PoW desestimular uma entidade única a possuir diversas identidades na rede devido ao custo computacional para gerar a prova de trabalho, um grupo de nós mineradores pode compartilhar recursos para gerar blocos mais rapidamente, distorcendo a natureza descentralizada da rede. Atualmente, quatro aglomerados de poder computacional, *BTC.com*, *SlushPool*, *AntPool* e *BTC.TOP*, são responsáveis por mais de 50% da taxa de resumos criptográficos gerados na *Bitcoin*[10].

4.4.2. Prova de Participação – PoS

A Prova de Participação (*Proof of Stake* - PoS) é uma alternativa ao alto custo computacional da Prova de Trabalho para alcançar o consenso na rede, preservando a natureza descentralizada da rede pública. Na PoW, a probabilidade de um nó conseguir minerar um bloco depende do poder computacional de cada nó. Já na PoS, essa probabilidade passa a depender da participação dos nós na rede. Os nós mineradores precisam encontrar um valor de resumo criptográfico menor ou igual a um valor alvo para que possam minerar um bloco. A dificuldade para encontrar esse resumo criptográfico é inversamente proporcional à riqueza acumulada (*coin age*) daquele nó, definida como a quantidade de recursos do nó multiplicada pelo período em que o nó reteve aquele recurso. Por exemplo, se Bob recebeu 10 recursos de Alice e manteve a posse desses recursos por 90 dias, Bob acumulou uma riqueza igual a 900 $recursos \times dias$. Quando Bob gasta esses 10 recursos provenientes de Alice, ele consumiu, ou destruiu, o valor de riqueza acumulada devido a esses 10 recursos. A consequência imediata de se utilizar o conceito de riqueza acumulada na PoS é atribuir ao nó com maior participação, riqueza acumulada, a oportunidade de gerar o próximo bloco [Tschorsch e Scheuermann, 2016].

Na PoS, é necessário que cada transação possua um campo de marcação do tempo de geração para que o valor da riqueza acumulada seja calculado. O conjunto de nós que deseja atuar como minerador precisa necessariamente bloquear seus recursos por um determinado tempo. Isso é feito através da construção de um bloco especial, *coinstake*, no qual o proprietário do recurso emite uma transação para si mesmo, adicionando uma deter-

[10]Dados disponíveis em https://www.blockchain.com/pt/pools.

minada taxa de transação como recompensa [Tschorsch e Scheuermann, 2016]. No momento em que o minerador paga a si mesmo, o valor da sua riqueza acumulada (*coin age*) é consumido. Dessa forma, na próxima rodada de mineração, outros nós têm a chance de conseguir minerar o novo bloco. A primeira entrada do bloco *coinstake* é composta por um *kernel* que deve obedecer a um protocolo de geração de resumos criptográficos específico da rede. As tentativas de geração do resumo criptográfico correto ocorrem a uma taxa de uma tentativa por unidade de riqueza acumulada. Assim, quanto mais recursos o nó disponibilizar para tentar encontrar o *kernel* correto, maior será a sua chance de reivindicar a oportunidade para minerar o próximo bloco. Por exemplo, se Alice possui uma riqueza acumulada de 100 $recursos \times dias$, para a qual se espera a geração de um *kernel* em 2 dias, então Bob, que possui uma riqueza acumulado de 200 $recursos \times dias$, pode esperar que o *kernel* seja gerado na metade do tempo. Com a PoS, a probabilidade de gerar o *kernel* independe do poder computacional dos nós da rede [King e Nadal, 2012]. Caso exista uma ramificação da cadeia, aquela que será declarada como principal é a que possui a maior soma de riqueza acumulada consumida [King e Nadal, 2012]. Existe a possibilidade de as ramificações crescerem na PoS quando a implementação não fornece incentivo para que os nós adicionem blocos à cadeia correta, originando o problema conhecido como "nada a perder" (*nothing-at-stake*) [Kiayias et al., 2017]. Dessa forma, os nós adicionam blocos a múltiplos ramos para maximizar a probabilidade de receber uma recompensa, prejudicando a obtenção de uma visão global única da cadeia de blocos.

4.4.3. Prova de Capacidade – PoC

O protocolo de consenso de prova de capacidade foi desenvolvido como uma alternativa à prova de trabalho. Introduzido com a criptomoeda *Burstcoin*[11], o algoritmo permite utilizar o espaço de armazenamento de memória secundária, ao invés de poder computacional bruto, para determinar o nó minerador. Assim, a PoC é baseada no espaço disponível do disco rígido do nó. O mecanismo funciona configurando o disco rígido para reservar um espaço de armazenamento em um processo chamado "plotagem"(*plotting*). Com a plotagem no disco rígido, os cálculos são feitos de antemão e as possíveis soluções são armazenadas em disco. Algumas dessas soluções, ou parcelas das soluções, permitem alcançar a solução final mais rapidamente do que outras e o nó que alcançar primeiro a solução final para o bloco mais recente será recompensado pela mineração. Isso essencialmente permite que o nó gere uma receita passiva utilizando o espaço de armazenamento disponível. Em outras palavras, os nós mineradores pré-geram pedaços de dados conhecidos como grafos que são salvos no disco. O número de parcelas que o nó armazena é efetivamente sua velocidade de mineração. A cada bloco, o nó minerador correrá as parcelas salvas e obterá uma quantidade de tempo até poder extrair um bloco, se outro bloco ainda não tiver sido encontrado. Depois de ler as plotagens, o *hardware* permanece ocioso até o próximo bloco. Quanto mais grafos o nó obtiver em seu disco rígido, maiores serão suas chances de resolver o próximo bloco. O algoritmo de prova de capacidade mostra um potencial para a evolução das criptomoedas, pois requer menos energia que a PoW baseada em ASIC (*Application Specific Integrated Circuits*) [Gauld et al., 2017].

[11] Disponível em https://bitcointalk.org/index.php?topic=731923.0.

4.4.4. Prova de Autoridade – PoA

No contexto das redes privadas, em vez da prova de trabalho ou de participação, propõe-se o uso da Prova de Autoridade (*Proof of Authority* – PoA). Nas redes privadas, existe uma entidade responsável pela rede que pode pré-determinar o papel de alguns nós. Assim, na prova de autoridade, a ideia é designar um conjunto de nós com autoridade para participar do consenso. Esses nós são encarregados da tarefa de gerar novos blocos e validar as transações. A PoA endossa um bloco como parte da cadeia se ele for assinado por pelo menos um nó com autoridade. O modelo de incentivo na PoA destaca que é do interesse de um nó de autoridade manter sua reputação para permanecer como nó de autoridade. Deve existir, então, um mecanismo confiável que permita a avaliação do comportamento dos nós de autoridade na rede para definir a reputação de cada nó. Vale ressaltar que PoA mantém a natureza distribuída da rede pelo fato de que todos os nós de autoridade devem concordar sobre o estado global da cadeia. Plataformas que se baseiam em PoA como mecanismo de consenso aplicam um tipo de rotação entre os nós de autoridade para que cada um tenha um tempo para gerar blocos alternadamente, sem disputa e desperdício de recursos por mais de um nó. Após o nó minerador da rodada minerar o último bloco, todos os nós de autoridade devem concordar e adicioná-lo ao final da cadeia. Caso seja observada alguma falha do nó de autoridade, é preciso que a plataforma ofereça recursos para fiscalizar e retirar a autoridade desse nó e, como consequência, desconsiderar seus blocos minerados, retornando as transações para o conjunto de transações não mineradas [Cachin e Vukolic, 2017].

4.4.5. Protocolos de Consenso Baseados em Votação

Todos os mecanismos de consenso descritos anteriormente eventualmente alcançam a consistência da visão global da cadeia de blocos existente na rede. A consistência eventual é alcançada sem a necessidade de conhecer o número de participantes do consenso. Outro grupo de mecanismos de consenso é composto por protocolos baseados em votação. Para alcançar o consenso na rede, é necessário que uma determinada fração dos participantes do consenso entrem em comum acordo quanto à adição do bloco na cadeia de blocos da rede. Para tanto, um grupo de nós da rede participa do consenso, votando a favor ou contra qualquer proposta de modificação nos dados do sistema. Alguns exemplos desse grupo de protocolos são PBFT [Castro e Liskov, 1999], Ripple [Schwartz et al., 2014], Paxos [Lamport, 2001] e Raft [Lamport, 2001].

Os protocolos baseados no **Modelo Prático de Tolerância a Falhas Bizantinas** (PBFT) consideram que os nós da rede podem exercer comportamentos arbitrariamente maliciosos ou falhas que fogem do protocolo predefinido [Bessani et al., 2014, Castro e Liskov, 2002, Alvarenga et al., 2018]. Apesar da participação de nós maliciosos, os protocolos baseados no PBFT garantem o consenso entre os nós da rede até o número limite de nós maliciosos, chamados de nós bizantinos, atingir f, em que $f \leq \frac{n+1}{3}$ e n representa o número total de nós da rede. O mecanismo de consenso PBFT pode ser resumido em quatro fases. A primeira fase é determinar o nó líder da rodada de mineração, que geralmente segue um rodízio entre os nós da rede, considerando que todos os nós são iguais e participam do consenso. Na segunda fase, o nó líder gera um novo bloco e o encaminha para todos os nós da rede. Na terceira fase, o nó líder aguarda a resposta de no mínimo $f+1$ nós com o mesmo resultado para o novo bloco. A quarta fase é a execução das tran-

sações contidas no bloco, visto que o consenso foi alcançando e os nós compartilham da mesma visão da cadeia. Como resultado final, todos os nós legítimos chegam a um acordo sobre a ordem das transações e as aceitam ou rejeitam. Além disso, algumas aplicações de PBFT oferecem opções nas quais a maioria absoluta de nós legítimos pode decidir se um líder está com defeito, ou sendo desonesto. A maioria pode votar para removê-lo da rotação de líder nas próximas rotações para a geração de blocos. Em comparação à PoW, os protocolos baseados em PBFT são vantajosos em termos de processamento. Por outro lado, estes protocolos exigem uma grande complexidade de mensagens, $O(n^2)$, o que gera um problema de escalabilidade para a rede. Consequentemente, protocolos baseados em PBFT são adequados para redes com poucos nós.

Schwartz et al. propõem o protocolo **Ripple** como mecanismo de consenso distribuído para cadeias de blocos federadas[12] [Schwartz et al., 2014]. O Ripple é tolerante a falhas bizantinas e é robusto contra ataques de conluio. Essa robustez advém da criação de subconjuntos de zonas confiáveis, nas quais não se espera uma conspiração entre os nós para atacar o sistema. Dessa forma, os nós consultam apenas o subconjunto e nós confiáveis para alcançar o consenso. Um dos problemas do Ripple é a escalabilidade quanto ao número de nós designados para alcançar o consenso [Cachin e Vukolic, 2017].

Paxos [Lamport, 2001] e **Raft** [Ongaro e Ousterhout, 2014] são protocolos equivalentes, com o objetivo de gerenciar registros replicados de entradas de dados. Primeiramente é eleito um líder, que recebe todas as propostas de modificação de dados no sistema. O líder torna-se responsável por compartilhar todas as modificações com todos os outros nós, para que eles possam votar. Em seguida, o líder compartilha a decisão coletiva com todos os outros nós participantes do consenso. Ambos os protocolos são resilientes a f falhas, em que $f \leq \frac{n+1}{2}$ e n representa o número total de nós da rede. Esses protocolos foram desenvolvidos para serem usados em ambientes confiáveis, uma vez que não consideram comportamento malicioso de nós que participam do consenso. Dessa forma, só devem ser utilizados em cadeias de blocos privadas. Variações dos protocolos Paxos e Raft consideram a redução do número de fases para alcançar o consenso com menor número de mensagens e a assinatura das mensagens trocadas permite extrapolar o uso desses protocolos em ambientes não confiáveis [Mattos et al., 2018, Cachin e Vukolic, 2017].

4.5. Contratos Inteligentes no Mercado de Energia Elétrica

A popularização dos contratos inteligentes é evidente com o crescimento exponencial do número de transações realizadas por esses contratos nos últimos anos, acarretando dezenas de milhares de contratos armazenados na plataforma Ethereum, responsáveis pelas movimentações de milhões de dólares [Luu et al., 2016]. A Figura 4.6 mostra o crescimento acelerado do número de contratos na Ethereum entre 2015 e 2018. Como consequência dessa popularização, hoje já existem diversas outras plataformas disponíveis para os contratos inteligentes [Bartoletti e Pompianu, 2017].

A primeira definição de contrato inteligente foi proposta por Nick Szabo em 1994 e colocava que o contrato inteligente se tratava de um protocolo de transação computado-

[12]Cadeias de blocos federadas são cadeias privadas sob a liderança de um grupo ou consórcio de nós.

[14]Gráfico gerado com base nos dados disponíveis em https://hackernoon.com/ethereum-smart-contracts-most-of-them-are-rarely-used-f45749730d3e.

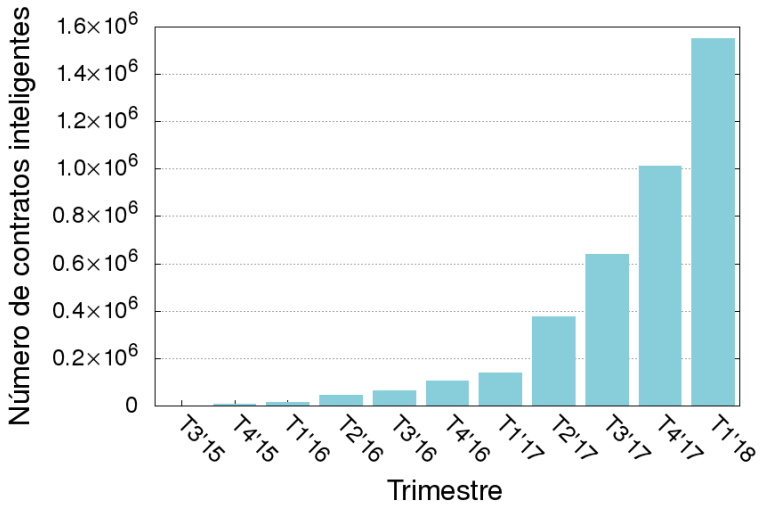


Figura 4.6. Crescimento exponencial do número de contratos inteligentes na plataforma Ethereum[14] entre os anos de 2015 e 2018.

rizado que executa os termos de um contrato. Na época, não existiam estruturas ou poder computacional para dar amplo suporte a aplicação da ideia, o que a fez cair em desuso por mais de vinte anos [Christidis e Devetsikiotis, 2016, Giancaspro, 2017].

Os contratos inteligentes oferecem transações eficientes, com baixo custo e seguras sem a necessidade de intermediários, tais como bancos e companhias de crédito, que encarecem muito o custo do negócio [Giancaspro, 2017]. Os contratos inteligentes automatizam operações, tornando a sua efetividade e as transferências de crédito mais céleres. Para tanto, o programa definido pelo contrato inteligente deve ser executado sobre uma cadeia de blocos e ser garantido por um protocolo de consenso, que pode ser o mesmo da cadeia de blocos ou definido em uma plataforma a parte. Com isso, o contrato tem acesso a movimentações financeiras por meio da criptomoeda da cadeia [Giancaspro, 2017]. O contrato deve respeitar um conjunto de regras definidas em uma linguagem de programação específica e a lógica do negócio pode ser expressa em código e validada a cada novo pedido de transação [Christidis e Devetsikiotis, 2016]. Com isso, os contratos inteligentes podem ser usados para uma vasta gama de aplicações.

O contrato inteligente possui um estado, está associado a um conjunto de dados e a uma quantidade de criptomoedas e possui um endereço próprio[15]. O endereço do contrato é usado pelas mensagens ou transações que ativam a execução do contrato. Assim, um contrato é executado ao ser invocado por uma transação ou pelo envio de uma mensagem para o seu endereço. Com isso, se a transação é aceita na cadeia de blocos, todos os mineradores executam o contrato baseados no estado atual da cadeia. Para tanto, ao se considerar o uso de cadeias públicas não permissionadas, o contrato deve ser sempre associado a uma quantidade de criptomoedas, que deve ser suficiente para financiar a execução do contrato, além de cobrir eventuais transações financeiras que sejam inerentes ao

[15]Variações nos conjunto de informações associadas ao contrato ocorrem dependendo da tecnologia utilizada. Por exemplo, diferentemente da Bitcoin, a Ethereum permite contratos com estados que podem ser modificados a cada nova transação [Luu et al., 2016].

contrato. A cada linha de execução do contrato, uma determinada quantia de criptomoedas é descontada do valor associado ao contrato. Esse mecanismo garante que o contrato só pode executar enquanto houver crédito suficiente, evitando ciclos mortos (*deadlocks*) ou execuções infinitas.

Por ser baseado em um protocolo de consenso, o contrato precisa ser determinístico. Logo, qualquer um dos mineradores que execute o contrato, com um certo conjunto de entradas, obterá o mesmo resultado como saída. Por estar armazenado na cadeia de blocos, todos os participantes da cadeia podem inspecionar o código do contrato. Além disso, como todas as transações sobre o contrato são registradas na cadeia, é possível fazer uma auditoria de todas as operações realizadas por meio daquele contrato [Christidis e Devetsikiotis, 2016]. Vale ressaltar que o contrato inteligente é armazenado dentro da cadeia e, então, após criado, ele não pode ser modificado ou cancelado [Giancaspro, 2017], o que pode trazer complicações legais. Como nenhum bloco pode ser removido ou alterado na cadeia, não é possível alterar um contrato já criado. Dessa forma, para alterar o contrato, em caso de observação de alguma falha ou vulnerabilidade, a cadeia precisaria ser reescrita, o que não é viável na maioria dos casos. Outro recurso que vem sendo usado é a utilização de contratos que guardam listas de contratos já cancelados e que são invocados para validação antes da execução de um código.

Os contratos inteligentes podem ser usados para diversos fins. Bartoletti e Pompianu propõem uma classificação das aplicações típicas dos contratos inteligentes com base em uma pesquisa nos contratos existentes na plataforma Ethereum [Bartoletti e Pompianu, 2017]. Os contratos são classificados em contratos de finanças, cartório, jogo, carteira e biblioteca.

Contratos de finanças são os que gerenciam, coletam ou distribuem criptomoedas. Alguns desses contratos verificam quem são os donos de um determinado ativo, verificam valores e lidam com a comercialização, enquanto outros realizam coleta de dinheiro para financiamento de projetos (*crowdfunding*). Nessa segunda categoria, merece destaque o DAO, que era o serviço de financiamento solidário mais proeminente da Ethereum, mas deixou de existir devido a um ataque em 2016 que desviou milhões de dólares. Existem ainda os esquemas Ponzi, nos quais os usuários investem dinheiro com a promessa de receber o valor com juros de volta no caso de novos investidores participarem do esquema (Ex. *King of the Ether Throne*). Existem ainda os contratos de seguradoras que podem ser comprovados digitalmente e ainda contratos para publicação de propaganda (Ex. *PixelMap*). Os contratos do mercado de energia são classificados nessa categoria.

Contratos de cartório servem para armazenar dados de forma permanente, registrando dados de origem e posse. Uma vez que os dados podem ser grandes, uma proposta é armazenar apenas o *hash* do documento na cadeia, o que prova a integridade e existência do documento, mas não pode garantir que o dado não será destruído, restando apenas a evidência que o documento deveria existir. Esse tipo de contrato também é usado para registro de direitos autorais (Ex. *Monegraph*), para registro de identidades por meio da associação de uma entidade com uma chave pública (Ex. *Physical Address*) e para aplicações mais livres, como o registro de mensagens por usuários para a comunidade (Ex. *Eternity Wall*). No setor elétrico, esses contratos podem ser utilizados para registrar as entidades do sistema e para registrar o consumo, a geração e o preço da energia.

Contratos de carteira lidam com chaves, enviam transações e gerenciam dinheiro e outros contratos, sendo gerenciados por um ou mais donos. Assim como os contratos financeiros, os contratos de carteira podem ser usados no setor elétrico, em especial no que diz respeito a transações relacionadas a grupos de clientes ou consórcios de empresas.

Os contratos de jogos servem para registros de apostas em jogos de azar (Ex. *LooneyLotery*) ou jogos de habilidades (Ex. *Etherization*). Já os contratos de biblioteca trazem funcionalidades de uso geral, como funções matemáticas úteis, e são exclusivamente criados para serem usados por outros contratos.

4.5.1. Plataformas de Contratos Inteligentes

Algumas das principais plataformas de contratos inteligentes, que estão atualmente disponíveis e apresentam um determinado grau de maturidade, são a Bitcoin, a Ethereum, a Counterparty, a Monax e a Lisk. As plataformas e o funcionamento de cada uma são detalhados a seguir.

O principal objetivo da **Bitcoin** é criar uma plataforma para a transferência de criptomoeda em um ambiente aberto e com conteúdo imutável. Dentro desse cenário, é possível criar formas limitadas de contratos inteligentes [Bartoletti e Pompianu, 2017]. A limitação se dá pelo fato de a Bitcoin utilizar uma linguagem de códigos executável que não é uma linguagem *Turing* completa, que permite apenas colocar algumas condições que devem ser verificadas antes de executar uma transação. A execução na Bitcoin é orientada a pilha e, portanto, não permite a execução de códigos iterativos. Entre as operações disponíveis, têm-se aritmética básica, lógica e operações criptográficas. Outra limitação importante é que apenas poucos nós da rede Bitcoin realizam o processamento de códigos executáveis que usem operações que tenham códigos que dependam de mais do que uma verificação de assinatura [Banasik et al., 2016].

A **Ethereum** é uma plataforma com mais suporte a contratos inteligentes que a Bitcoin, disponibilizando uma linguagem *Turing* completa de *bytecode* baseada em pilha para a codificação dos contratos. Para criação dos códigos, utilizam-se linguagens de alto nível, sendo a mais utilizada a *Solidity* [Ethereum, 2018]. Os usuários criam os seus códigos de contratos e os submetem, por meio de uma transação, para a cadeia de blocos. Para usar esse contrato, uma transação deve ser direcionada a esse contrato ou, ainda, pode-se chamar um contrato a partir de outro contrato da cadeia. O resultado da transação é validado pela rede. Como um outro diferencial com relação à Bitcoin, na Ethereum, tanto os usuários quanto os contratos podem armazenar, enviar e receber criptomoeda, tanto de ou para outros usuários quanto de ou para outros contratos. Vale destacar o sistema de gás (*gas*), o "combustível" para a execução do contrato. Como a execução de um contrato leva a um esforço computacional, que varia de contrato para contrato, a Ethereum paga aos mineradores uma quantia pelo processamento de um determinado contrato proporcional ao esforço aplicado. Cada instrução que pode ser usada em um contrato tem um preço em gás pré-determinado. Ao chamar um contrato, o usuário deve dizer o quanto ele quer pagar por cada unidade de gás gasto na execução do contrato (*gasPrice*) e um gasto máximo que ele aceita pagar pelo contrato (*gasLimit*). Assim, com a execução do contrato, o minerador irá receber a quantia relativa à quantidade de gás usada na execução multiplicada pelo *gasPrice*. Caso o valor exceda o *gasLimit*, a

execução é pausada e o minerador recebe *gasLimit* sem ter que enviar o resultado final do contrato ao remetente. Esses casos geram uma exceção e levam à reversão das operações realizadas até a finalização do gás [Luu et al., 2016].

O **Counterparty** [Counterparty, 2018] é um protocolo desenvolvido especificamente para criar contratos inteligentes sobre a cadeia de blocos Bitcoin. Para tanto, as informações que devem ser trocadas para a realização do contrato são inseridas em transações da Bitcoin com o prefixo CNTRPRTY, em campos que são ignorados pela Bitcoin, como, por exemplo, a saída do OP_RETURN ou como *hash* falso de chave pública. Assim, a rede Bitcoin ignora a informação, que é coletada e interpretada por nós do Counterparty. A tarifação padrão de contratos Counterparty é similar àquela proposta na Ethereum, sendo que diferentes tipos de operação serão associados a diferentes tarifas. Contudo, cabe observar que o Counterparty possui uma criptomoeda própria, o XCP, que é usada para pagar a execução do contrato por meio de *proof of burn*[16]. Além disso, os contratos utilizam a mesma linguagem que a Ethereum, sendo o diferencial a ausência de consenso na validação do resultado.

Diferentemente do Counterparty, a plataforma **Stellar** [Stellar, 2018] provê a sua própria cadeia de blocos com sua própria criptomoeda, chamada *lumen*, a qual é regida usando o acordo Bizantino federado[17]. Para a Stellar, o contrato inteligente não define uma linguagem específica e, além das contas individuais, é possível também ter contas com vários donos (*multisignature*).

A **Monax** [Monax, 2018] é uma plataforma para criar contratos da Ethereum, mas sem estar associado à cadeia ou à criptomoeda da Ethereum. A plataforma disponibiliza modelos padrão (*templates*) de contratos que podem ser configurados, facilitando a criação de novas regras de negócio. A plataforma permite a criação de cadeias privadas com regras de autorização configuradas por cada cadeia, com consenso baseado votação.

A plataforma **Lisk** [Lisk, 2018] provê a sua própria cadeia de blocos pública baseada em prova de participação, com sua própria criptomoeda. Permite a execução de contratos baseados em máquinas de Turing-completas nas linguagens *JavaScript* ou *Node.js*. Apesar de ter uma cadeia principal, cada contrato nessa plataforma é executado em uma cadeia a parte e a criptomoeda pode ser transferida entre a cadeia principal e as cadeias de contrato. Nas cadeias específicas de contrato, o dono do contrato pode especificar, entre outros, quais nós podem participar do mecanismo de consenso. A Tabela 4.1 apresenta um resumo das principais plataformas para contratos inteligentes.

4.5.2. Exemplos de Contratos Inteligentes na Ethereum

A Ethereum é o exemplo mais relevante de plataforma de contratos inteligentes e, portanto, será usada para exemplificar a estrutura de um contato inteligente. O contrato na Ethereum é uma sequência de funções que podem, entre outras ações, transferir *Ether* entre usuários e para outros contratos. As transações são usadas para criar novos contratos, chamar funções de contratos e transferir *Ether*. Um contrato pode receber *Ether*

[16]Mecanismo de consenso em que um nó envia uma determinada soma de ativos para um endereço a partir do qual não é mais possível consumir aquele ativo. Funcionamento semelhante ao *proof of stake*.

[17]O consenso é feito entre a vizinhança, a qual é composta pelos nós mais confiáveis para aquele nó. Semelhante ao protocolo Ripple.

Plataforma	Tipo de cadeia	Tamanho da cadeia	Intervalo entre blocos	Linguagem
Bitcoin	Pública	96 GB	10 minutos	Scripts Bitcoin + Assinatura
Counterparty				EVM Bytecode
Ethereum	Pública	17-60 GB	12 s	EVM Bytecode
Stellar	Pública	N/A	3 s	Cadeias de transações + Ass.
Monax	Privada	N/A	Configurável	EVM Bytecode + permissões
Lisk	Privada	N/A	Configurável	JavaScript

Tabela 4.1. Comparação entre as principais plataformas para criação de contratos inteligentes. Adaptado de [Bartoletti e Pompianu, 2017].

ou enviá-lo para outros usuários ou contratos usando a função ***pay***. Todo *Ether* recebido por um contrato é guardado na variável ***balance***, a qual não pode ser modificada pelo programador, mas apenas por funções pré-definidas na plataforma.

A Figura 4.7 exemplifica um contrato escrito na linguagem *Solidity* que tem por objetivo transferir uma quantidade de *Ether* armazenado em nome do contrato para um determinado receptor. Cada contrato é composto por campos e funções. As funções são chamadas passando a quantidade de *Ether* necessária para financiar a execução daquele conjunto de instruções pelos mineradores e, opcionalmente, alguma quantidade de *Ether* a ser transferida para outro contrato ou usuário durante a execução da função. Cabe ainda observar a existência das exceções que são tratadas de forma diferente do usual. Uma exceção, nessa linguagem, não pode ser capturada, resultando no fim da execução da função, com a reversão de todas as modificações realizadas, incluindo as transferências de *Ether*. Contudo, a taxa paga pela execução da função, o gás, é perdida [Atzei et al., 2017].

```
1  contract AWallet{
2      address owner;
3      mapping (address => uint) public outflow;
4
5      function AWallet(){ owner = msg.sender; }
6
7      function pay(uint amount, address recipient) returns (bool){
8          if (msg.sender != owner ||  msg.value != 0) throw;
9          if (amount > this.balance) return false;
10         outflow[recipient] += amount;
11         if (!recipient.send(amount)) throw;
12         return true;
13     }
14 }
```

Figura 4.7. Exemplo de contrato da Ethereum [Atzei et al., 2017].

Os contratos são construídos em estruturas semelhantes a uma classe. No exemplo da Figura 4.7, o contrato *AWallet* possui dois atributos, um que representa o dono do contrato e outro que registra quais valores já foram enviados por meio desse contrato. Na linha 5, a função *AWallet* funciona como um construtor, sendo chamada apenas na criação do contrato. Essa função, no exemplo, apenas registra que o dono do contrato é

quem o enviou para a cadeia de blocos (*msg.sender*). A função *pay* executa efetivamente a funcionalidade do contrato. Ela recebe como entradas uma determinada quantidade de Ether e um endereço para enviar essa quantia e retorna verdadeiro ou falso. A primeira ação realizada pela função *pay* é verificar se quem está chamando a função (*msg.sender*) é o dono do contrato. A função também garante que nenhum *Ether* será transferido para esse contrato. Qualquer quantia sendo transferida para uma função estaria na variável *msg.value*. Caso algum usuário diferente do dono chame a função *pay* ou algum *Ether* seja enviado quando a função é chamada, o contrato é terminado por uma exceção e o valor em *msg.value* é devolvido a quem chamou o contrato. A próxima verificação é se o contrato ainda possui recursos suficientes para fazer a transferência, o que é feito observando o valor da variável *this.balance*. Essa variável não pode ser atualizada pelo código do contrato diretamente, sendo controlada por funções próprias especificadas pela Ethereum, pois armazena a quantidade de *Ether* relacionada a cada usuário ou contrato. Caso não exista recurso suficiente, a função retorna falso. Caso exista, a transferência é registrada em *outflow* (linha 10) e, em sequência, a quantia é efetivamente enviada ao receptor. Caso a quantia não possa ser enviada, acontece uma exceção, levando a devolução do Ether e revertendo a modificação em *outflow*.

A estrutura básica de um contrato da Ethereum dá liberdade ao programador e permite sua ampla utilização em diferentes cenários, como o das redes elétricas. A plataforma desenvolvida pela *Energy Web Foundation*, embora use cadeia de blocos própria, é baseada na estrutura de contratos da Ethereum [Energy Web Foundation, 2018]. Outro exemplo é a empresa *Power Ledge*, que desenvolveu uma plataforma para controle de cobrança de energia renovável sobre a cadeia da Ethereum [Power Ledger Pty Ltd, 2018].

4.5.3. Vulnerabilidades dos Contratos Inteligentes

Contratos inteligentes trazem grandes vantagens em termos de eficiência e controle de operações, mas há que se considerar o impacto que pode ocorrer em caso de falhas na codificação ou no processamento do contrato. Um exemplo famoso de contrato atacado devido a uma vulnerabilidade foi o do DAO, que era parte da Ethereum e fazia financiamento colaborativo de projetos. O ataque realizado sobre uma falha de codificação desse contrato levou a perdas da ordem de 50 milhões de dólares, o que levou a extinção do serviço [Popper, 2016, Bartoletti e Pompianu, 2017].

Diferentemente de softwares tradicionais, quando uma falha é detectada ou é tornada pública, não é possível modificar o contrato, já que a cadeia de blocos impede que ele seja removido ou alterado, a menos que a cadeia seja reconstruída [Luu et al., 2016]. Embora seja possível reconstruir uma cadeia, essa é uma tarefa muito custosa e pouco provável de ocorrer.

Algumas características de contratos e da cadeia de blocos já vêm sendo discutidas pela sua relevância na construção e execução dos contratos inteligentes. Uma dessas características é a dependência da ordem das transações. Alguns contratos permitem que o dono modifique o valor pago pela execução de um determinado desafio proposto pelo contrato. Assim, se duas transações, uma para apresentar a solução e outra para mudar o preço da solução acontecem em tempos muito próximos, a ordem em que o minerador escolhe para construir o bloco pode alterar o resultado final e os ganhos ou perdas de

cada uma das partes. Esse é um problema especialmente relevante em contratos com alta taxa de atualização de preços [Luu et al., 2016]. Por exemplo, um mercado de energia renovável que tenha alta variação de preço poderia sofrer com esse problema. Um caso hipotético é que um "prossumidor" verifique o preço que está sendo pago pela energia renovável e decida vender a sua produção, ao invés de consumir a energia em sua própria residência. Contudo, uma transação reduzindo o preço pago pela energia é lançada um pouco depois que o "prossumidor" pede o registro da sua venda para o contrato, mas essa nova transação, por ter uma remuneração de retorno maior pela mineração que a transação gerada pelo "prossumidor", deve ser minerada antes da transação de venda de energia. Nesse cenário, é provável que o "prossumidor" tenha sua transação efetivada depois da transação reduzindo o preço e reduzindo o seu lucro. Um contrato que gera essa dependência da ordem das transações é explicitado na Figura 4.8.

```
1 contract MarketPlace{
2   uint public price;
3   uint public stock;
4   /.../
5   function updatePrice(uint _price){
6     if (msg.sender == owner)
7       price = _price;
8   }
9   function buy (uint quant) returns (uint){
10    if (msg.value < quant * price || quant > stock)
11      throw;
12    stock -= quant;
13    /.../
14  }}
```

Figura 4.8. Exemplo de contrato da Ethereum que permite que os valores recebidos pelas partes variem de acordo com a ordem que os mineradores decidem processar as transações [Luu et al., 2016].

O problema da ordem de execução pode ocorrer naturalmente ou de forma maliciosa, quando o proprietário do contrato tenta alterar a ordem de execução das transações participando da mineração, aumentando o preço que ele paga pela transação da sua atualização de preço ou pelo conluio com outros mineradores [Luu et al., 2016]. Outro problema similar pode ocorrer em contratos que dependem de marcações de tempo para iniciar uma determinada operação, como, por exemplo, enviar uma quantia de dinheiro. Ao processar um bloco, um minerador precisa adicionar uma estampa de tempo ao bloco, o que para mineradores com funcionamento correto significa estampar o tempo atual no sistema local. Contudo, variações de até 900 s são toleradas dentro do processamento da cadeia. Com isso, atacantes podem manipular a estampa de tempo do bloco para manipular o resultado de um contrato dependente de estampa de tempo [Luu et al., 2016]. Uma outra vulnerabilidade relaciona-se a contratos que lidam com exceções. Por exemplo, na Ethereum, um contrato pode chamar outro contrato. Em caso do contrato chamado gerar uma exceção, essa exceção pode ou não ser propagada para o contrato original, dependendo da forma como o contrato foi chamado, que pode ser feito pela instrução *send* ou pela chamada direta da função. Quando a chamada é feita diretamente pelo nome da função, a exceção se propaga e ambos os contratos são terminados e devolvem as quantias pendentes. Contudo, quando a chamada é feita por meio de *send*, se o contrato que fez a

chamada não verificar a resposta da função, ele pode executar assumindo que a chamada do outro contrato foi realizada com sucesso. Observou-se que aproximadamente 27% dos contratos da Ethereum usam a chamada *send* para outros contratos e não verificam a resposta recebida [Luu et al., 2016]. A Figura 4.9 mostra um exemplo de contrato real da Ethereum que tem essa vulnerabilidade e, por isso, levou ao fim do serviço *King of Ether Throne*. Nesse serviço, um usuário poderia se tornar rei, desde que pagasse uma compensação ao rei atual. Com isso, a cada troca de rei, o novo rei deve compensar o rei anterior, gerando lucro. Contudo, não existia nenhuma verificação se a função *claimThrone* estava sendo chamada por um usuário ou por um contrato. Assim, o rei poderia ser tanto um usuário quanto um contrato. Na Ethereum, transferir dinheiro para um contrato custa mais gás que transferir dinheiro para uma carteira. Como o código completo desse contrato não leva em consideração que um rei pode ser um contrato, quando o endereço do rei é um contrato, o gás para fazer a transferência da compensação é insuficiente. Com isso, o *send* falhava com uma exceção no contrato do rei atual, levando o rei atual a perder o trono sem receber a compensação [Bennett, 2018].

```
1 contract KingOfTheEtherThrone {
2   struct Monarch {
3     // address of the king.
4     address ethAddr;
5     string name;
6     // how much he pays to previous king
7     uint claimPrice;
8     uint coronationTimestamp;
9     }
10  Monarch public currentMonarch;
11  // claim the throne
12  function claimThrone(string name) {
13    /.../
14    if (currentMonarch.ethAddr != wizardAddress)
15      currentMonarch.ethAddr.send(compensation);
16    /.../
17    // assign the new king
18    currentMonarch = Monarch(
19        msg.sender, name,
20        valuePaid, block.timestamp);
21  }}
```

Figura 4.9. Contrato da Ethereum do serviço *King of Ether Throne*, que por não conferir a resposta da operação send, foi alvo de um ataque que finalizou o serviço [Luu et al., 2016].

Outras vulnerabilidades específicas da Ethereum incluem o estouro deliberado da profundidade máxima da pilha de chamadas, chamadas para destinos que não existem, exploração de estados em reentrâncias, entre outras [Luu et al., 2016, Atzei et al., 2017]. Vale notar que algumas ferramentas de análise de contratos na cadeia Ethereum mostram que a quantidade de contratos com vulnerabilidades é alarmante [Luu et al., 2016]. Assim, a elaboração de contratos inteligentes seguros é um desafio de pesquisa, especialmente para lidar com mercados com alto volume monetário como o mercado de energia.

4.6. Aplicações de Cadeia de Blocos em Redes Elétricas Inteligentes

A cadeia de blocos é uma tecnologia com grande poder disruptivo e, por isso, sua aplicação na indústria aumenta dia após dia [Dütsch e Steinecke, 2017]. Empresas cada vez mais desejam se comunicar através de interfaces de programação de aplicações (*Application Program Interfaces* - APIs), a chamada integração B2B (*Business to Business*). É necessário, para tanto, padronizar as interfaces para facilitar a comunicação entre as empresas. A padronização da integração B2B foca em três pilares: o formato dos dados, o processo empresarial e o protocolo de comunicação [Merz, 2016]. A tecnologia de cadeia de blocos satisfaz tais pilares. A cadeia de blocos define um formato de dados único em todos os nós da rede par-a-par e, por isso, todos os seus participantes seguem o mesmo formato de dados, processo empresarial e protocolo de comunicação. Consequentemente, o emprego da cadeia de blocos reduz custos de integração, uma vez que o número de comunicações aumenta exponencialmente com o número de participantes [Merz, 2016]. Elimina-se ainda a centralização de dados, pois os participantes trocam dados através da rede par-a-par. Identificam-se, por fim, fatores chave para o sucesso de uma aplicação em cadeia de blocos [Dütsch e Steinecke, 2017]:

- **Participantes acordam nas regras da negociação.** É essencial que os participantes cooperem para acordar padrões e regras para descrever as transações;
- **Um arcabouço legal e regulatório pode ser acordado.** O arcabouço legal e regulatório permite que os registros digitais sejam traduzidos em ativos e obrigações no mundo real;
- **Os papéis e permissões são definidos.** Os papéis e permissões dos nós participantes devem ser claramente definidos, no caso de uma cadeia privada, e acordados;
- **A identidade digital é associada ao mundo real**. A identidade dos atores deve ser adequada, vinculada ao mundo real e inalterável, no caso de uma cadeia privada.

4.6.1. Microrredes (*microgrids*)

Os sistemas de energia elétrica cresceram e evoluíram mantendo sua premissa inicial de construir centrais geradoras junto às fontes de energia primária e utilizar linhas de transmissão de longa distância para levar a energia produzida até os consumidores. Com as redes elétricas inteligentes, há modificações de natureza regulatória, estrutural e tecnológica no sistema de energia tradicional [Falcão, 2009]. Uma delas é a adoção de microrredes (*microgrids*), que são redes locais de energia elétrica compostas por cargas e elementos de geração e armazenamento, formando um sistema distribuído para provimento de energia elétrica. Os elementos geradores das microrredes podem estar localizados próximos aos pontos de consumo e podem ser conectados à rede elétrica da concessionária ou podem operar isoladamente, de forma totalmente independente da concessionária de energia. Essa autonomia facilita a operação, a automação e o gerenciamento dos recursos. Os elementos que compõem as microrredes agem como uma entidade única (subsistema), que pode ser operada de forma controlada e coordenada [Marnay et al., 2015]. Assim, é possível conectar um grande número de fontes geradoras de pequeno e médio porte ao sistema elétrico principal através de subestações de forma mais eficiente, segura

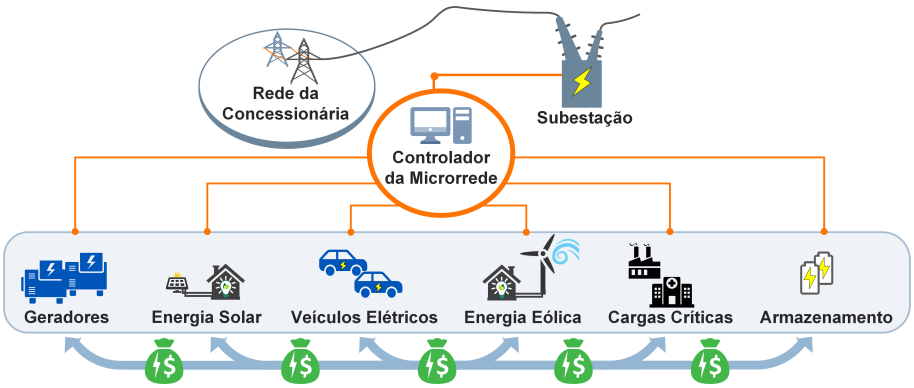


Figura 4.10. A microrrede é composta por cargas, fontes geradoras e armazenadores de energia distribuídos, que podem estar conectados a um ponto de acoplamento comum. Esses elementos são controlados e coordenados pelo controlador da microrrede, responsável por determinar se a microrrede deve operar de forma isolada ou conectada à rede da concessionária.

e gerenciável. A Figura 4.10 mostra uma microrrede e como esta se conecta à rede da concessionária. Ressalta-se que as microrredes agregam a geração de energia de fontes renováveis na rede de distribuição a média e a baixa tensão.

Os principais elementos geradores de energia nas microrredes são as fontes de energia renováveis e pequenas unidades como células a combustível, motores a diesel ou gás e pequenas turbinas a gás [Falcão, 2009]. Devido à tendência de uso de energias limpas e renováveis, diversas implementações de microrredes utilizam apenas fontes de energia renováveis como painéis fotovoltaicos e aerogeradores. Atualmente, as microrredes podem ainda se beneficiar da integração com estações de recarga e carros elétricos, capazes de exercer o papel de células distribuídas para armazenamento de energia. Em um momento crítico, os carros elétricos podem ser conectados à rede elétrica para suprir a demanda energética ou para reduzir flutuações na tensão ou frequência.

A coordenação da microrrede é feita através de equipamentos e técnicas de controle que definem a operação do sistema, determinando, por exemplo, a potência reativa e a variação da quantidade de energia adquirida da concessionária, sem perturbar o fornecimento de energia para os consumidores nem o funcionamento da rede da concessionária [Falcão, 2009]. Além disso, caso ocorram perturbações na rede da concessionária, como flutuações de frequência ou tensão, é possível desconectar totalmente a microrrede da rede principal sem cortar a alimentação das cargas [Lasseter e Paigi, 2004] alimentadas pela microrrede. Para esse fim, utiliza-se de forma intensa a tecnologia da informação e comunicação na rede elétrica, permitindo a comunicação entre os diversos componentes da rede e a otimização da sua operação.

O sistema de energia de cada cliente é controlado com o objetivo de alcançar uma solução ótima local para o consumo de energia, considerando as individualidades de cada sistema. No entanto, nem sempre a energia gerada pela microrrede nas instalações do cliente é totalmente consumida. O uso colaborativo do total de recursos disponíveis para um grupo de sistemas clientes pode resultar em uma solução global melhor. Assim, o excedente gerado pelos sistemas cliente pode ser inserido na rede da concessionária ou pode ser negociado diretamente com outros consumidores, originando o mercado de energia

das microrredes. Esse mercado tem o potencial de suprir a demanda local utilizando recursos de energia da vizinhança, reduzindo a necessidade de transporte de energia através de longas linhas de transmissão, que muitas vezes é caro e apresenta perdas substanciais no caminho [Mengelkamp et al., 2018a].

O "prossumidor" pode receber benefícios na forma de desconto nas contas de energia elétrica futuras ou pode ser pago utilizando algum tipo de moeda de troca. Para essa finalidade, é necessário existir um sistema eficiente, resiliente, igualitário e inviolável para transferência de informação, capaz de operar em um ambiente descentralizado [Cohn et al., 2017]. A estrutura descentralizada da tecnologia de cadeia de blocos vai ao encontro da mudança de paradigma em curso no mercado de energia. Essa mudança desloca o tradicional modelo de negócios centralizado para um modelo descentralizado.

A cadeia de blocos oferece um ambiente seguro e de baixo custo para transações financeiras ou operacionais serem armazenadas e validadas através de uma rede distribuída, sem a necessidade de um entidade central para controlar as transações [Power Ledger Pty Ltd, 2018]. A consistência dos dados é garantida pelo mecanismo de consenso utilizado na rede. As cadeias de bloco vêm ganhando cada vez mais espaço no setor de energia elétrica como ferramenta capaz de promover a negociação de energia. O uso das cadeias de bloco no setor de energia elétrica compõe, então, parte da solução para atualizar e melhorar os sistemas legados que operam de forma centralizada. Sistemas elétricos baseados em cadeias de bloco podem aumentar a confiabilidade e a qualidade do fornecimento de energia e promover a evolução para um sistema híbrido, no qual grandes usinas de energia coexistem com as microrredes distribuídas.

As negociações realizadas entre os "prossumidores" e consumidores são feitas de forma direta, formando uma rede par-a-par. Um dos requisitos para que negociações par-a-par locais sejam realizadas é a redução do tamanho dos lotes negociados. No comércio de energia e *commodities*, unidades padronizadas são definidas de acordo com o tamanho, a qualidade e a quantidade. A padronização dos critérios e do tamanho dos lotes é necessária para superar os custos de transação na configuração atual do mercado. Os atores não são capazes de vender nos mercados atacadistas de energia se a oferta não corresponder aos critérios padronizados. Eles são obrigados por intermediários, como corretores e bancos, a elaborar contratos. Assim, os negociantes de *commodities* são de fato grandes clientes ou especialistas [Dütsch e Steinecke, 2017]. As cadeias de blocos são capazes de reduzir os custos de transação através da padronização por contratos inteligentes e da execução automática das tarefas. A redução dos custos de transação permite lotes de energia de tamanhos menores, sendo possível eliminar os intermediários no comércio e comercializar a energia diretamente entre "prossumidores" [Dütsch e Steinecke, 2017].

Os contratos inteligentes contidos nas cadeias de blocos permitem a automatização dos pagamentos, habilitando o comércio entre "prossumidores" de forma segura e eficiente. Cada "prossumidor" deve estar equipado com um dispositivo capaz de armazenar todas as transações realizadas na rede composta pelos consumidores e produtores. Os contratos inteligentes devem ser elaborados de forma que a venda da energia excedente produzida seja automática. Ao manter um comércio local de energia, a quantidade de energia retirada da rede de transmissão na localidade é potencialmente reduzida [Cohn et al., 2017].

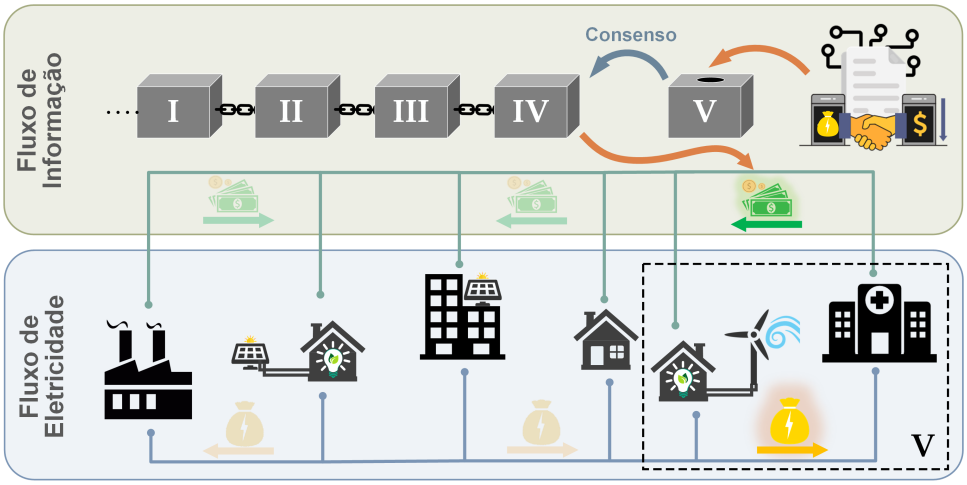


Figura 4.11. O modelo de mercado de energia baseado em cadeias de blocos é descentralizado. As negociações ocorrem de forma direta entre os pares, sem a necessidade de um agente intermediário. O fluxo de energia elétrica é transportado através da rede elétrica, enquanto o fluxo de informação passa por um sistema de tecnologia da informação e comunicação de alta capacidade.

Qualquer "prossumidor" e consumidor pode submeter um pedido de compra ou de venda ao sistema gerenciador de troca de energia da microrrede, suportado por um contrato inteligente. Esses pedidos são compostos por um lote e pelo preço do lote. O mercado pode funcionar com preços fixos, mas regulados pelo mercado, ou na forma de leilão, como na microrrede do Brooklyn, baseada em cadeia de blocos [Mengelkamp et al., 2018b]. Seja qual for o mecanismo de mercado, o lote de energia fornecido pelo "prossumidor" vencedor é inserido na microrrede, o consumidor vencedor paga ao "prossumidor" e pode, então, retirar a mesma quantidade de energia da microrrede. A Figura 4.11 exemplifica a negociação no mercado de energia de microrredes baseada em cadeia de blocos. No instante ilustrado, existe apenas um pedido de compra de energia, proveniente de uma carga crítica, por exemplo, um hospital. Esse pedido é feito através de uma chamada ao contrato inteligente que suporta o mercado de energia local. Existem diversos "prossumidores" com produção excedente que disponibilizam informações sobre o lote e o valor do lote de energia através de uma chamada para o contrato inteligente. O "prossumidor" vencedor da negociação e a carga crítica estão indicados na figura pela linha tracejada (conjunto V). A negociação realizada entre eles é incluída em um bloco candidato (bloco V), contendo as chamadas ao contrato, o valor do lote energia fornecido pelo "prossumidor" e o valor pago pela carga crítica. Após a verificação e validação do bloco através de um mecanismo de consenso, o bloco é inserido na cadeia de blocos e a compra é efetivada de fato, ocorrendo a transferência de ativos financeiros para a carteira do "prossumidor", e permitindo a retirada do lote de energia da microrrede. A principal diferença entre o modelo tradicional e o modelo baseado em cadeia de blocos é a eliminação do agente intermediário nas negociações.

Existem diversos projetos em desenvolvimento, ou que já estão sendo implementados e testados, que propõem o uso das cadeias de blocos no setor elétrico. Alguns desses projetos estão mais focados no comércio de energia entre os prossumidores das microrredes, como *PowerLedger*, *Key2Energy*, *Exergy* e *NRGCoin*. O projeto *Exergy* é uma plataforma criada pela *LO3 Energy*, utilizada na implantação da primeira microrrede

funcional do mundo, localizada no Brooklyn, em Nova York [Mengelkamp et al., 2018b]. Esses projetos são discutidos na Seção 4.7.

Existem alguns problemas que ainda precisam ser superados para que exista uma operação em larga escala das cadeias de blocos no mercado de energia elétrica. A rede da concessionária é fortemente regulamentada, assim como o comércio de energia elétrica. Negociações com cadeias de blocos também devem passar por um processo de regulamentação rígido. Um segundo problema que deve ser superado é a falta de interoperabilidade entre sistemas de diferentes empresas que estão desenvolvendo e utilizando cadeias de blocos próprias. O problema de interoperabilidade pode ser reduzido com a regulamentação do setor. Um terceiro problema é a eficiência energética das cadeias de blocos. Para que possam ser aplicadas no mercado de energia das microrredes, cadeias de blocos computacionalmente eficientes devem ser desenvolvidas [Mengelkamp et al., 2018a]. Por exemplo, em vez de utilizar mecanismos de consenso custosos em termos computacionais, é possível utilizar mecanismos de consenso baseados em identidade, nos quais cada agente possui uma única identidade que pode ser confirmada [Mengelkamp et al., 2018a]. Para que esses problemas sejam resolvidos, é necessária a existência de consórcios e organizações para cooperação entre companhias, operadores de sistema de distribuição e de transmissão e dos governos nacionais. Uma iniciativa nesse sentido é a *Energy Web Foundation* (EWF)[18], criada pela empresa GridSingularity e pelo Instituto de Rocky Mountain com o objetivo de acelerar a implementação da tecnologia de cadeia de blocos no setor elétrico. A EWF coopera com diversos parceiros do setor de energia elétrica, reguladores e órgãos de padronização e contribui com o desenvolvimento da cadeia de blocos EWF específica para aplicações no setor de energia elétrica, com diversos estudos de caso, provas de conceito e aplicações comerciais.

4.6.2. Medição Inteligente

Medidores inteligentes são dispositivos eletrônicos capazes de realizar medições do consumo de energia com mais detalhes do que os medidores comuns e com suporte a tecnologias de comunicação para reportar as medidas em tempo real [Efthymiou e Kalogridis, 2010]. A tecnologia de cadeia de blocos fortalece o papel de mercado dos consumidores e produtores individuais. Permite aos "prossumidores" comprar e vender energia diretamente, manualmente ou via automação de contratos inteligentes, com alto grau de autonomia. Os medidores inteligentes são os equipamentos responsáveis por medirem tanto o consumo como a produção de energia dos "prossumidores". No cenário de cadeia de blocos em microrredes, os medidores inteligentes passam a ser a interface entre as operações na cadeia de blocos e a realização das transações na rede elétrica. Logo, em microrredes, os medidores inteligentes são a interface entre a rede elétrica e a rede de comunicação, ou a cadeia de blocos.

No cenário de negociação de energia elétrica entre "prossumidores" com o suporte dos medidores inteligentes em uma microrrede, a compra e venda de energia elétrica se beneficiam da ausência das barreiras burocráticas, agilizando e barateando as transações por meio da tecnologia de cadeia de blocos [Bittwatt Pte.Ltd., 2018]. Com isso, os custos operacionais e tarifas de transferência são reduzidos pela automatização das transações ao

[18]Disponível em https://energyweb.org/.

aplicar os conceitos de contratos inteligentes. Com a utilização de uma carteira virtual, é possível participar de leilões de energia, em que as regras, como quantidade, tipo e preço, são levadas em conta para firmar contratos inteligentes entre ambas as partes.

Com os medidores inteligentes, os clientes podem ser alertados sobre o preço da energia quando esta ultrapassa o valor esperado, permitindo ajustes no consumo de energia nesses momentos para redução do valor da conta de energia elétrica [Bittwatt Pte. Ltd., 2018]. É possível também que os consumidores comprem energia quando esta torna-se mais barata e a armazenem para utilização posterior ou até para revender no futuro. Essa compra e venda de energia são feitas através de uma "Carteira de Energia" utilizando criptomoedas especiais [Bittwatt Pte.Ltd., 2018].

4.6.3. Gerenciamento e Negociação Automática de Energia

O crescente número de fontes de energia renováveis e intermitentes agregadas às redes elétricas levam a novas abordagens do mercado em relação à precificação e à distribuição da geração volátil e distribuída [Mengelkamp et al., 2018b]. Nesse novo cenário, um dos maiores desafios é o gerenciamento da rede elétrica inteligente [Guimarães et al., 2013]. Uma solução viável é agregar diversas fontes geradoras distribuídas de energia em uma usina de geração de energia virtual (*Virtual Power Plant* - VPP) [Pudjianto et al., 2007]. A VPP é comparável a uma usina de geração conectada diretamente à rede de transmissão, como ilustrado na Figura 4.12. Ao operarem sozinhas, muitas geradoras distribuídas de energia não têm capacidade, flexibilidade ou capacidade de controle e previsibilidade suficientes para interagir no mercado de energia elétrica de maneira rentável ou tecnicamente viável. No entanto, com a criação de uma VPP a partir de um grupo de geradoras distribuídas de energia, esses desafios são superados [Pudjianto et al., 2007]. A usina virtual é conectada diretamente à rede de transmissão e possui um perfil de características, como cronograma de geração, limites de geração, custo operacional e assim por diante, bem determinado. Com base nesse perfil, a usina virtual pode interagir diretamente com outros participantes do mercado para oferecer serviços e fazer contratos. Através da comunicação direta com o operador da rede de transmissão ou através de transações de mercado, uma unidade geradora conectada à rede de transmissão pode contribuir para o gerenciamento do sistema. A geração de energia elétrica e outros serviços associados podem ser vendidos por meio de interação no mercado atacadista ou por contato direto com concessionárias fornecedoras de energia e outras partes. O comércio ponto-a-ponto direto com agregação de fontes distribuídas em VPPs é uma solução viável e pode ser baseada na tecnologia de cadeia de blocos [Dütsch e Steinecke, 2017].

Para poder participar do mercado de compra e venda de energia, os operadores da usina virtual têm que produzir previsões para minimizar as flutuações. A complexidade envolvida na produção de previsões varia para cada tipo de instalação de geração. Derivar previsões para a produção de energia eólica e solar, por exemplo, é uma tarefa mais complexa do que para usinas controláveis, como usinas termoelétricas a gás. Caso um operador erre ao prever sua produção de energia, pode incorrer em prejuízos devido a multas e encargos pelo desequilíbrio energético provocado [Dütsch e Steinecke, 2017, Pudjianto et al., 2007]. O ator central de controle das VPPs pode ser substituído por uma implantação de uma solução baseada em cadeia de

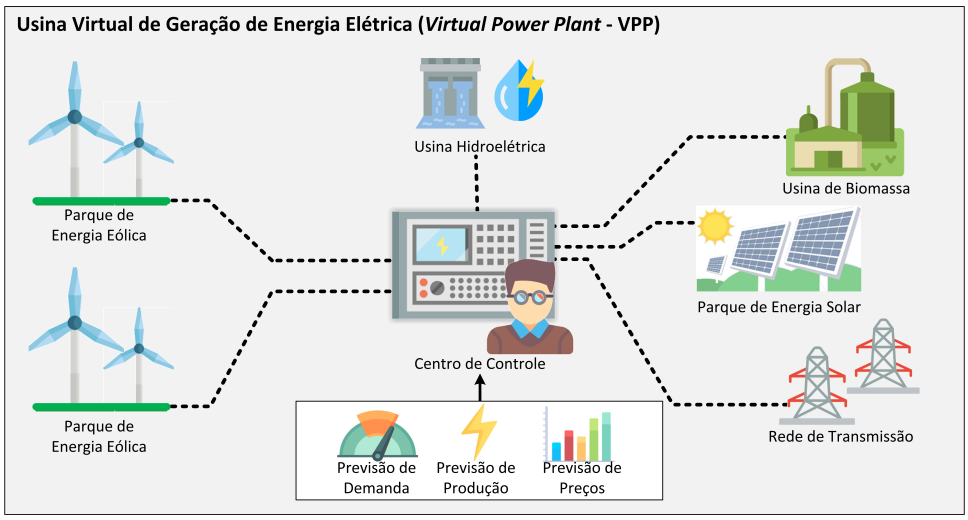


Figura 4.12. Usina virtual de geração de energia (VPP). Diversas fontes de energia renováveis são controladas por uma unidade de controle central e ligadas diretamente à rede de transmissão. A agregação de diversas fontes de energia permite gerenciar com mais previsibilidade as variações na demanda e na geração de energia. O controle centralizado pode ser substituído por contratos inteligentes em cadeia de blocos.

blocos que integra automaticamente informações locais e otimiza as redes de geração de energia. As redes locais são então agregadas à usina virtual, fornecendo capacidade de energia estável a baixo custo. Trabalhos recentes consideram o uso de cadeias de blocos para aumentar a segurança e a disponibilidade dos dados dos Sistemas de Supervisão e Aquisição de Dados (*Supervisory Control and Data Acquisition* - SCADA) [Dong et al., 2018, Liang et al., 2018]. A manutenção do sistema de supervisão distribuído e confiável é essencial para o funcionamento correto da usinas virtuais de geração.

Quanto à negociação automática de energia, vislumbra-se a tecnologia de cadeia de blocos como um canal de comunicação padronizado entre os atores do mercado de energia elétrica. O mercado de energia elétrica é composto por diversos atores, em especial geradoras, operadores de transmissão, distribuidoras, consumidores, negociante e câmara de comercialização [Merz, 2016]. Paralelamente, há ainda os órgãos de padronização e regulação do mercado. As geradoras alimentam a rede elétrica com a energia gerada, principalmente através de grandes usinas, mas atualmente também com pequenas usinas e usinas virtuais. As operadoras de transmissão são as responsáveis por manterem as redes físicas de distribuição da energia. As operadoras de transmissão são conectadas horizontalmente e trafegam a energia gerada pelas geradoras até os distribuidores e consumidores. As distribuidoras compram grandes quantidades de energia e oferecem produtos adequados aos consumidores, sejam residenciais ou industriais. Os consumidores compram os produtos correspondentes a seus perfis das distribuidoras. Vale ressaltar que os consumidores podem gerar energia e injetar diretamente na rede da distribuição, agindo assim como “prossumidores”. Os negociantes compram a energia das geradoras no mercado atacadista e revendem para outros negociantes e para distribuidoras. Muitas das vezes os negociantes compram e revendem os produtos diversas vezes, pois negociam com preços futuros sobre a energia a ser gerada. Há ainda as câmaras de negociação de energia, no Brasil, representada pela Câmara de Comercialização de Energia Elétrica

(CCEE)[19]. As câmaras de comercialização são associadas a pontos de troca de energia. A câmara de comercialização oferece o mercado no qual a energia é comercializada e, também, exerce meios para a liquidação financeira e física das transações de energia. Vale ressaltar que o mercado de energia oferece uma variedade de produtos que são negociados entre geradoras, negociantes e distribuidores. Os produtos ofertados variam de ofertas a longo prazo, para o mercado futuro, a operações *intraday*, para a liquidação no mesmo dia, com entregas escalonadas em intervalos de 15 minutos [Merz, 2016]. Nesse cenário, é necessário que as interfaces entre todos os atores sejam padronizadas e que o comportamento confiável e verificável de todos os atores seja garantido.

A abordagem de cadeia de blocos para o mercado de energia elétrica mantém todos os papéis [Dong et al., 2018]. Os negociantes continuam a realizar operações com outros negociantes e distribuidoras, corretores e a câmara de comercialização estão disponíveis como plataformas e os operadores de transmissão recebem dados de escalonamento da entrega da energia. Assim, os principais atores do mercado de energia passam a gerenciar um nó na cadeia de blocos que replica o mercado de energia elétrica. O modelo de cadeia de blocos permissionada é a que melhor se adéqua ao mercado de energia elétrica, pois assegura a comunicação entre nós, com diferentes papéis na rede, e entre participantes e nós da cadeia, no caso em que um nó representa um grupo de participantes com a mesma função na rede. O efeito mais significativo da adoção da cadeia de blocos é a padronização. Todos os participantes são forçados a ler e escrever dados exatamente no mesmo formato. Os processos de negócios são sincronizados com base nos estados e os dados estão disponíveis na cadeia de blocos. Logo, a cadeia de blocos é o veículo de transporte para distribuir dados consistentes e irrefutáveis entre todos do mercado.

Agências reguladoras passam a serem usuárias da cadeia de blocos. Ao acessarem um nó da cadeia, podem receber os dados das transações em tempo quase real, em comparação a atrasos atuais de aproximadamente 24 horas [Merz, 2016]. Vale ressaltar que ao operar sobre a cadeia de blocos, os participantes do mercado de energia não necessitam qualquer esforço extra de reportar as transações para as agências reguladoras, dado que a difusão intrínseca de informações na cadeia cumpre esse requisito legal. Dessa forma, a cadeia de blocos apresenta o potencial de diminuir o risco de fraudes, dado que um regulador pode monitorar as transações em tempo real. Portanto, se todos os que atualmente têm de relatar dados de transação às agências reguladoras registrarem esses dados na cadeia de blocos, basta que a agência reguladora também se conecte à cadeia de blocos com permissão de leitura. Cabe notar que o uso da cadeia de blocos também é vantajoso para os negociantes, pois os dados que estão armazenados na cadeia podem ser usados por várias partes como um banco de dados para as etapas de transformação posteriores. Os negociantes podem derivar o índice de certos produtos do banco de dados, que é uniforme para todos os participantes, e definir melhores estratégias de compra e venda de ativos.

4.6.4. Medição Automática em Sistemas de Transmissão

Os operadores de sistemas de transmissão precisam produzir previsões para todo o mercado de energia elétrica a cada dia. As previsões devem ser preparadas, o mais tardar, no dia anterior, com base nos chamados escalonamentos, submetidos a eles pelos

[19]Disponível em https://www.ccee.org.br/.

operadores de balanceamento do sistema energético [Hasse et al., 2016]. Cabe destacar que há as questões de quem são os responsáveis por submeterem esses escalonamentos aos operadores das redes de transmissão, a corretude dos escalonamentos e a integridade e validade irrefutáveis dos escalonamentos recebidos. Em paralelo, as medições de carga recebida e fornecida na rede de transmissão são relevantes ao operador da rede de transmissão para efeitos de compensação e liquidação. O operador da rede de transmissão coleta todos os dados para cada grupo de balanceamento e os agrega para determinar os custos de energia a serem alocados ao grupo de balanceamento.

A proposta do uso de cadeias de blocos, tanto no armazenamento das medições realizadas pelos operadores de transmissão quanto na padronização e na garantia de integridade e não repúdio nas negociações, simplifica os processos e a troca de informações entre operadores de redes de transmissão e outros atores do mercado de energia elétrica. Considerando que as operações de negociação de energia são realizadas diretamente sobre uma cadeia de blocos, mesmo que por motivos de relatórios, as transações também estarão simultaneamente disponíveis para o operador de transmissão. Assim, essa parte da tarefa da câmara de comércio, a liquidação física da entrega da energia, já é realizada pela cadeia de blocos. Quanto à liquidação financeira, o faturamento em forma de estrela, entre a câmara de comércio e os operadores, também pode ser implantado sobre a cadeia de blocos, uma vez que muitas soluções de cadeia de blocos, como a Ethereum, são equipadas com uma unidade de faturamento, os *tokens*, como o *Ether* da Ethereum. Há ainda o potencial para criação de novos *tokens* apenas para a comercialização de energia. Paralelamente à liquidação física da entrega de energia, através das entregas dos escalonamentos diárias e internos ao dia, e à liquidação financeira, é necessária a introdução de meios de verificação de que a energia negociada foi realmente entregue, tanto aos operadores de transmissão como pelos operadores de transmissão às distribuidoras e consumidores.

Atualmente, no Brasil, a medição do fluxo de energia em pontos da rede de transmissão é realizada pelo Sistema de Medição para Faturamento (SMF) composto por medidores e transformadores de potencial e de corrente elétrica. Esses equipamentos de medição são conectados ao Sistema de Coleta de Dados de Energia (SCDE) da CCEE. O sistema de coleta de dados realiza a coleta diária dos dados de todos os equipamentos de medição através da conexão com os equipamentos por meio de redes públicas, Internet, e, muitas vezes, sem o uso de proteções como Redes Privadas Virtuais (*Virtual Private Networks* - VPNs). A coleta diária impede o monitoramento preciso de variações do fluxo de energia no período de um dia, dificultando operações de planejamento e organização do sistema de transmissão. Em contrapartida, medições frequentes e com fina granularidade permitem um melhor controle do sistema. Os dados coletados são altamente sensíveis já que norteiam o quanto de energia está sendo fornecido por cada empresa geradora de energia e o quanto está sendo transmitido em uma dada linha de transmissão. No modelo atual, operadores de transmissão e geração devem realizar cópias de salvaguarda (*backup*) das medições e confiam nos valores coletados pela CCEE. Assim, nesse cenário, há a necessidade de se prover um mecanismo capaz de permitir que os dados coletados por diversas empresas sejam armazenados em uma estrutura de dados distribuída, sem controle centralizado e sem a necessidade de haver uma âncora de confiança em uma única entidade, capaz de garantir a disponibilidade, a integridade, a autenticidade, a auditabilidade e o não repúdio de todas as medições realizadas.

A cadeia de blocos satisfaz, então, as necessidades do sistema de coleta de dados. Com essa tecnologia, aumentam-se a transparência e a agilidade para comercializar energia porque as medições de fluxo de energia, assim que geradas, são disponibilizadas em um repositório distribuído e auditável [Dong et al., 2018]. Vale ressaltar que no modelo atual de coleta de dados, os pontos de medição são consultados uma vez por dia, em períodos predeterminados. Considerando a participação da CCEE na cadeia de blocos, a coleta de dados passa a ser realizada através da consulta na cadeia de blocos, recuperando as últimas transações e verificando o quanto foi registrado por cada medidor.

4.7. Discussão, Tendências e Desafios de Pesquisa

Embora se trate de uma área recente, já é possível encontrar diversas pesquisas e soluções da indústria que utilizam soluções de cadeias de blocos voltadas ao sistema elétrico. Via de regra, esses produtos visam a utilização das cadeias de blocos e dos contratos inteligentes como forma de registrar e dar suporte a operações seguras de compra e venda de energia. No entanto, o mercado alvo varia. A maioria dos sistemas envolve os consumidores finais de energia elétrica, embora haja também plataformas que dão suporte a negociações entre empresas das áreas de geração, transmissão e distribuição.

4.7.1. Soluções da Indústria

A **Bittwatt** [20], uma empresa sediada em Cingapura, desenvolveu uma plataforma de mesmo nome que funciona como um mercado digital para a troca e balanceamento energético. A plataforma baseia-se em cadeia de blocos para suporte a transações de compra e venda de energia elétrica entre vários tipos de participantes diferentes, desde os consumidores finais, até grandes empresas dos ramos de geração, transmissão e distribuição de energia. Do ponto de vista do usuário, o Bittwatt funciona como uma criptomoeda para transações no mercado de energia. Usuários, tanto fornecedores, quanto consumidores de energia, são cadastrados e a plataforma realiza o trabalho de casamento entre compradores e vendedores. As transações são consagradas através de contratos inteligentes. Segundo a empresa, o "fluxo de eletricidade é automaticamente codificado na cadeia de blocos" e os pagamentos são automaticamente disparados quando a energia é entregue.

A tecnologia da cadeia de blocos usada pelo Bittwatt é baseada na Ethereum. A solução inclui ainda a adição de medidores inteligentes na rede elétrica, tanto para consumidores, quando para produtores, de forma a permitir o monitoramento em tempo real do fluxo de energia. A empresa desenvolveu uma interface amigável que permite a cada usuário acompanhar a evolução do mercado, indicadores de preço, e gerenciar a carteira. A moeda usada na plataforma, denominada BWT, apresenta uma correspondência fixa com energia consumida/produzida: 1 BWT é equivalente a 1 kWh. A ideia é que usuários do sistema possam realizar o câmbio entre BWTs e outras moedas, o que determinaria o valor monetário da energia comercializada através da plataforma. Segundo os dados mais recentes publicados pela empresa [Bittwatt Pte.Ltd., 2018], sua solução já se encontra em fase de desenvolvimento em Londres, Bucareste e Cingapura. Segundo seu plano de negócio, a integração final de todos os componentes da plataforma será concluída em junho de 2022, data na qual a empresa antecipa operar em mais de 17 países.

[20]Disponível em http://bittwatt.com.

Diferentemente da Bittwatt, que ambiciona conectar todo tipo de participante no mercado de transação de energia, a australiana **Power Ledger**[21], criada pela Vector, tem como objetivo ser uma plataforma para negociação de energia em mercados locais de distribuição baseada em cadeia de blocos. A Power Ledger baseia-se na Ethereum e utiliza uma cadeia de blocos privada gerenciada pela própria empresa [Power Ledger Pty Ltd, 2018], embora haja planos para torná-la pública no segundo trimestre de 2019 e eventualmente gerenciada pelos próprios usuários. O mecanismo de consenso utilizado é atualmente baseado em Prova de Trabalho. No entanto, segundo a empresa, um dos objetivos futuros é transicionar a plataforma para o uso da Prova de Participação, uma das motivações para adotar a Ethereum como tecnologia. A outra é o suporte a contratos inteligentes. Um diferencial dessa plataforma é a utilização de duas criptomoedas para a realização de tipos de transações diferentes: a POWR e a Sparkz. A Sparkz é a moeda utilizada para transações efetivas de energia elétrica, enquanto a POWR é a criptomoeda usada para interconectar a plataforma com o mundo externo, como câmbio por outras criptomoedas ou por equivalentes monetários. A POWR já se encontra disponível para câmbio em diversas bolsas de criptomoedas. As transações são realizadas através de contratos inteligentes, compatíveis com o padrão ERC-20[22] de contratos inteligentes da Ethereum. Implantações da plataforma já foram testadas na Austrália e na Nova Zelândia. Segundo o plano de negócio publicado, a empresa está atualmente buscando novos parceiros comerciais e desenvolvendo novas aplicações sobre a plataforma.

Outro concorrente no setor é a **Exergy**[23], criado pela LO3 Energy. Similar às demais plataformas citadas anteriormente, a Exergy é a tecnologia base do projeto piloto *Brooklyn Microgrid*[24]. A moeda utilizada nas transações de energia nessa plataforma é chamada de XRG. Assim como as demais plataformas discutidas até aqui, a moeda é baseada no padrão ERC-20 [LO3 Energy Team, 2017].

O projeto *Brooklyn Microgrid* consiste em um mercado de energia para uma microrrede instalada no Brooklyn, em Nova York. Os participantes do piloto são residências e estabelecimentos da região que ainda estão conectados à rede elétrica de larga escala da cidade, mas fazem parte também de uma microrrede inteligente que os interconecta. Alguns desses usuários são "prossumidores", tendo, portanto, a capacidade de gerar energia renovável, através de painéis solares, por exemplo. Dessa forma, a Exergy é utilizada como uma plataforma para registrar transações de compra e venda de energia. A microrrede contém medidores inteligentes desenvolvidos pela LO3, denominados de *Transactive Meters*, capazes de interagir com a cadeia de blocos do Exergy. Essa cadeia de blocos, denominada *Transactive Grid Blockchain*, foi desenvolvida inicialmente sobre a Ethereum, mas a empresa migrou para uma solução de cadeia de blocos proprietária [Mengelkamp et al., 2018a]. A tecnologia em uso no *Brooklyn Microgrid* é baseada no *Tendermint* [Kwon, 2014]. Atualmente, a cadeia de blocos é privada.

Outra funcionalidade da plataforma é o casamento entre compradores e vendedores. Pedidos e ofertas de energia são cadastrados na cadeia de blocos na forma de

[21] Disponível em https://powerledger.io/.

[22] ERC-20 (*Ethereum Request for Comments 20*) é um padrão técnico que estabelece contratos inteligentes na cadeia de blocos da Ethereum para a implementação de *tokens*.

[23] Disponível em https://exergy.energy/.

[24] Disponível em https://www.brooklyn.energy/.

contratos inteligentes. A plataforma utiliza um sistema de leilão duplo, no qual o comprador que oferece o maior valor tem sua demanda atendida primeiro, seguido do segundo maior valor e assim por diante. Do ponto de vista do usuário, no entanto, o sistema de leilão é transparente, sendo gerenciado pela própria plataforma de acordo com preferências configuradas pelo usuário, por exemplo origem da energia desejada e valor máximo para compra. Outro aspecto interessante do projeto é a participação de instituições consideradas críticas para a sociedade, como hospitais. Essas instituições, no entanto, recebem uma parcela fixa da energia gerada pela microrrede, sem a participação no sistema de leilões.

Outra plataforma é a **PowerPeers**[25], originada na Holanda. Assim como a Power Ledger, a PowerPeers visa atuar no segmento de compra e venda de energia entre consumidores e produtores locais, explorando a popularização de tecnologias de geração de energia renovável em residências e outros tipos de consumidores finais.

A **Share & Charge**[26], por outro lado, é uma solução criada pela Motionwerk que tem como alvo o mercado de recarga de veículos elétricos. A ideia é criar uma plataforma baseada em cadeia de blocos que possa intermediar as transações entre usuários de veículos elétricos e entidades que disponibilizam postos de recarga, sejam empresas ou mesmo pessoas físicas que queiram disponibilizar uma infraestrutura de recarga própria para terceiros. A empresa conta atualmente com um projeto piloto no Reino Unido.

O número de iniciativas da indústria voltadas ao emprego das cadeias de blocos no mercado de consumo de energia elétrica é, de fato, grande. Além das plataformas já citadas nessa seção, Basden e Cottrell listam alguns outros projetos piloto pelo mundo [Basden e Cottrell, 2017]. Na Áustria, a *Wien Energie*, um conglomerado da área de energia, está atualmente testando uma solução de cadeia de blocos para gerenciar transações relacionadas à troca de energia com outras grandes empresas do setor. Também na Áustria, a *Grid Singularity* está desenvolvendo uma plataforma de troca de energia baseada em cadeia de blocos cujo diferencial é permitir, entre outras coisas, o monitoramento de equipamentos da rede elétrica. O objetivo é auxiliar no gerenciamento da rede elétrica. Na Alemanha, a empresa *Innogy* está testando uma solução piloto para a cobrança automática do consumo de carros elétricos autônomos em postos de recarga. As transações envolvidas são autenticadas por uma solução baseada em cadeia de blocos. No Reino Unido, a *startup Electron* desenvolve uma plataforma de cadeia de blocos para permitir que consumidores troquem rapidamente de empresa de fornecimento de energia.

4.7.2. Pesquisas Acadêmicas

Além das várias plataformas desenvolvidas por empresas, a aplicação de cadeias de blocos e contratos inteligentes às redes elétricas inteligentes tem gerado também bastante interesse acadêmico. Nos últimos anos, tem surgido uma massa considerável de artigos propondo plataformas ou estudando problemas pontuais nessa área.

O trabalho seminal nesse sentido é o NGRcoin [Mihaylov et al., 2014]. Trata-se de uma criptomoeda similar à Bitcoin, mas aplicada ao mercado de compra e venda de energia em mercados com geração distribuída. Embora a moeda proposta guarde muitas semelhanças com a Bitcoin, a principal diferença está na forma pela qual novas moedas

[25]Disponível em https://www.powerpeers.nl/.
[26]Disponível em https://shareandcharge.com/.

são criadas no sistema. Enquanto isso ocorre pelo processo de mineração na Bitcoin, no NRGcoin as novas moedas são criadas a partir da introdução de energia por um "prossumidor" na rede elétrica. Ao introduzir energia gerada localmente na rede elétrica, o "prossumidor" envia uma mensagem de aviso em *broadcast* para todos os demais participantes da rede NRGcoin. Por consequência, os demais participantes, em conjunto, criam uma determinada quantidade de NRGcoins e a creditam ao "prossumidor". Concomitantemente, a empresa responsável pela distribuição de energia elétrica na região transfere uma certa quantia de NRGcoins do seu próprio saldo para o "prossumidor". Por outro lado, se um "prossumidor" necessitar consumir energia da rede elétrica, ele deve pagar pela quantidade de energia consumida usando seus NRGcoins.

Ambos os preços de compra e venda de energia pelos "prossumidores" são determinados dinamicamente pela empresa distribuidora, em intervalos regulares de 15 minutos. Os autores propõem um modelo de precificação que tem como objetivo incentivar uma oferta de energia pelos "prossumidores" que case com a demanda atual. É importante destacar que os autores dissociam o processo de precificação da energia em NRGcoin do processo de câmbio entre NRGcoin e seu equivalente monetário. Tal câmbio, na proposta dos autores, seria realizado através de um mercado aberto, no qual a taxa de conversão fosse determinada pela relação entre oferta e demanda da criptomoeda.

Mais recentemente, Kang *et al.* apresentam um novo modelo de negócio para a compra e venda localizada de energia [Kang et al., 2017]. Nesse modelo, os autores assumem a popularização de veículos híbridos *plug-in* (ou PHEV, da sigla em inglês *Plug-in Hybrid Vehicule*). No modelo vislumbrado, usuários desse tipo de veículo teriam acesso a "tomadas bidirecionais", que permitiram fluxo de energia tanto da rede elétrica para o carro, como o carregamento das baterias, quanto do carro para a rede elétrica, fornecendo energia elétrica para a rede. Tais tomadas bidirecionais estariam disponíveis em estacionamentos públicos, postos de recarga ou mesmo nas casas dos usuários. Nesse cenário, veículos com baterias suficientemente carregadas eventualmente injetariam energia de volta na rede, auxiliando a suprir a demanda de energia na região onde se encontram. Segundo os autores, tal modelo ainda tem como vantagens a remoção do ponto único de falha no sistema de fornecimento de energia e reduziria a dependência do sistema de linhas de transmissão longas e redes de distribuição complexas. Os autores argumentam, no entanto, que esses benefícios só seriam alcançados caso uma parcela considerável dos usuários aderisse ao programa. Isto é, se esses usuários estivessem dispostos a permitir a descarga das baterias dos seus veículos para injeção de energia de volta à rede. Para isso, seria necessário algum tipo de incentivo que, na visão dos autores, poderia ser obtido através de um mercado de compra e venda de energia dos veículos híbridos. Mais especificamente, os autores buscam uma solução descentralizada e capaz de fornecer privacidade aos usuários participantes. Dados esses objetivos, os autores argumentam que a tecnologia de cadeia de blocos se apresenta como uma alternativa interessante. No entanto, soluções como o NRGcoin não seriam adequadas ao cenário pelas restrições energéticas dos veículos híbridos, dado o elevado custo energético dos mecanismos de consenso baseados em Prova de Trabalho. Como alternativa, os autores exploram o conceito de Consórcio de Cadeia de Blocos, no qual um grupo de nós dedicados atuam como Agregadores Locais. As transações de energia são negociadas diretamente entre os veículos, criptografadas e assinadas digitalmente pelas partes. As transações digitais resultantes

são enviadas aos agregadores locais que, por sua vez, se responsabilizam por auditá-las e registrá-las na cadeia de blocos através de um sistema de prova de trabalho. Os autores investigam também um sistema de precificação dinâmica, baseado em leilões duplos. No sistema proposto, compradores e vendedores submetem lances, os compradores submetem o valor que estão dispostos a pagar, enquanto vendedores submetem o valor pelo qual estão dispostos a vender. Com base nos lances, um preço de referência p é determinado. Vendedores cujos lances sejam menores ou iguais a p vendem, enquanto compradores cujos lances sejam maiores ou iguais a p compram.

Li *et al.* consideram outros cenários de compra e venda de energia em ambientes de geração distribuída, além do uso de veículos híbridos [Li et al., 2018]. Os autores também abordam aspectos práticos de implementação do sistema proposto, em particular, os relacionados ao estabelecimento de consenso entre os agregadores locais. O mais interessante, no entanto, é a proposta do uso de um sistema de crédito para compra de energia. Nesse sistema, cada agregador atua também como um banco com grandes reservas da criptomoeda energética. Um consumidor que precisa comprar energia, mas não possui moedas suficientes pode iniciar um pedido de empréstimo ao banco. O banco, por sua vez, avalia a capacidade de pagamento do empréstimo solicitado com base, por exemplo, o histórico de pagamentos de empréstimos anteriores do consumidor. Note que isso pressupõe que o consumidor ofereça informações de identificação para o banco, o que pode ter implicações relacionadas ao anonimato do sistema. De acordo com a capacidade de pagamento determinada, os autores apresentam um modelo derivado a partir de Teoria dos Jogos para computar os juros cobrados pelo empréstimo. Para concretizar o empréstimo, o banco cria uma carteira compartilhada com o consumidor com um saldo correspondente ao valor emprestado. As chaves criptográficas usadas para a manipulação da carteira são enviadas ao consumidor, juntamente com um certificado de autorização de uso da carteira, emitido pelo banco. O consumidor, então, pode usar a carteira para realizar compras de energia de outros participantes do sistema.

O propósito desse sistema de empréstimo é lidar com os atrasos nas verificações de operações na cadeia de blocos. Segundo experimentos conduzidos pelos autores, o atraso de verificação da cadeia de blocos proposta, baseada em consórcio, seria da ordem de dezenas de minutos. Esses valores são consideravelmente mais baixos que os atrasos de verificação encontrados em criptomoedas tradicionais, como a Bitcoin. Mesmo assim, os autores argumentam que esse atraso não é desprezível considerando-se a natureza das transações realizadas, que envolvem consumo e geração de energia elétrica. Assim, caso um consumidor precise comprar energia, mas esteja temporariamente sem moedas energéticas suficientes, um sistema tradicional baseado em câmbio a partir de outras moedas poderia incorrer em atrasos inaceitáveis.

Já Mengelkamp *et al.* consideram o cenário de um mercado local de compra e venda de energia com geração distribuída [Mengelkamp et al., 2018b]. A microrrede é ligada a uma rede tradicional de larga escala, mas "prossumidores" locais tentam suprir a demanda local com sua própria geração sempre que possível. Assim como nas demais propostas discutidas nessa seção, isso é feito através da manipulação de preços de compra e venda de energia produzida pelos "prossumidores", em um esquema de leilão duplo. Propõe-se a utilização de uma cadeia de blocos privada para registrar as operações de compra e venda. Os autores argumentam que a opção por uma cadeia de blocos privada

se deve à redução do custo do processo de consenso. O principal diferencial desse trabalho em relação aos anteriores está no uso da cadeia de blocos também para gerenciar as informações relativas ao leilão. Enquanto outros autores geralmente assumem uma infraestrutura e/ou protocolo a parte para lidar com os leilões, nesse trabalho os lances, ou seja, intenções de compra ou venda, são armazenados na própria cadeia de blocos, na forma de contratos inteligentes. Em outras palavras, o próprio lance gerado pelo consumidor, seja para compra ou para venda, constitui um compromisso de execução da transação no futuro dependente do valor de mercado a ser determinado. Uma vez que o leiloeiro determina e dissemina o valor de mercado da energia naquele momento, os contratos são executados de acordo com os lances e os saldos das carteiras são atualizados.

Em outro trabalho [Mengelkamp et al., 2018a], os mesmos autores argumentam que, em um mercado local de compra e venda de energia, os participantes do mercado são conhecidos e, por isso, o sistema de consenso baseado em prova de identidade pode ser usado. Essa seria uma alternativa mais eficiente em termos de custos de manutenção da cadeia de blocos, incluindo custos energéticos. No entanto, os próprios autores reconhecem que o sistema de prova de trabalho garante níveis mais altos de resiliência e segurança ao sistema. Dentre as outras contribuições desse trabalho, os autores propõem um modelo de sete requisitos para a viabilidade de uma microrrede baseada em cadeia de blocos. Um dos aspectos citados é a adoção da solução por um número suficiente de participantes, alguns dos quais precisam possuir a infraestrutura necessária para produção de energia. Os autores apontam ainda a escalabilidade da cadeia de blocos, em termos da taxa de verificação de transações, como um dos obstáculos técnicos ainda existentes.

Além dos aspectos técnicos relacionados a cadeias de blocos, contratos inteligentes e redes elétricas inteligentes, outros autores têm discutido os impactos regulatórios, econômicos, comerciais e políticos da combinação dessas tecnologias. Por exemplo, Green e Newman argumentam que a viabilidade dos mercados locais de troca de energia causará mudanças profundas no modelo de negócio das empresas do setor elétrico [Green e Newman, 2017]. Isso é algo que já ocorre na prática, ao menos em projetos piloto. Os autores, no entanto, alertam que a rede elétrica de larga escala ainda exercerá um papel importante no fornecimento de energia, dadas as questões de previsibilidade no consumo e das fontes de energia renováveis mais difundidas. Na prática, as grandes empresas do setor poderão acumular novos modelos de negócio, oferecendo, por exemplo, sua *expertise* na prestação de serviços de infraestrutura das microrredes. Já Bertsch *et al.* conduziram uma pesquisa de opinião na Alemanha sobre os níveis de aceitação da população em relação a diferentes tecnologias de geração de energia e aspectos relacionados [Bertsch et al., 2016]. Entre os dados levantados, aproximadamente 50% e 85% dos participantes disseram aceitar a instalação de painéis solares e turbinas eólicas se estas estiverem a ao menos 1 km de suas residências. Tais números indicam que ainda há certa resistência por parte considerável da população em relação à implantação da infraestrutura necessária a algumas das vertentes do conceito de geração distribuída.

4.8. Considerações Finais

A tecnologia de cadeia de blocos satisfaz os requisitos de segurança de aplicações em redes elétricas inteligentes, mesmo para aquelas aplicações em que não existe uma organização centralizadora para garantir a legitimidade das transações, como nas redes de

geração distribuída. A cadeia de blocos (i) assegura a confiabilidade da rede elétrica em um contexto em que não há confiança entre os pares, (ii) permite o controle e a manutenção dos dados de produção e de consumo de energia de forma distribuída, (iii) permite a auditoria do histórico de transações de compra e venda de energia elétrica de maneira irrefutável e, por fim, (iv) executa contratos de compra e venda de energia elétrica, independentemente da cooperação dos participantes.

Uma breve revisão das soluções da indústria e da literatura científica recente mostra que aplicações da cadeia de blocos e contratos inteligentes em diversos setores das redes elétricas inteligentes já se encontram próximas de estágios de produção. No entanto, também é clara a existência de obstáculos diversos a esse objetivo. Tais obstáculos são técnicos, políticos e até mesmo sociais.

Em termos técnicos, o desenvolvimento de contratos inteligentes seguros é um desafio. Há consenso de que os contratos inteligentes são necessários para a negociação segura e descentralizada entre diferentes atores do mercado de energia como, por exemplo, a compra e venda de energia entre os "prossumidores" em microrredes. Particularmente, o mercado de energia tem alto volume monetário e, nesse cenário, vulnerabilidades podem gerar enormes prejuízos financeiros. Por isso, a pesquisa nessa área é importante. Há, atualmente, vulnerabilidades tanto de codificação quanto no processamento dos contratos inteligentes que podem ser exploradas. A ordem escolhida para execução das transações e a construção do bloco pode afetar o valor a ser pago pela execução de um dado desafio causando prejuízos financeiros, por exemplo. Da mesma forma, contratos que dependem de estampas de tempo podem ter suas ordens alteradas para a ordem de execução dos blocos. Há ainda problemas identificados em contratos que geram exceções. Em particular, para a Ethereum, uma plataforma que possui cerca de 1,6 milhão de contratos inteligentes, é possível explorar o estouro deliberado da profundidade máxima da pilha de chamadas, chamadas para destinos que não existem, exploração de estados em reentrâncias, entre outras vulnerabilidades [Luu et al., 2016, Atzei et al., 2017]. O agravante é que quando uma vulnerabilidade é identificada ou é tornada pública, não é possível modificar o contrato, já que a cadeia de blocos impede que ele seja removido ou alterado, sem que a cadeia seja reconstruída. Portanto, esse é um desafio que requer um grande esforço dos pesquisadores e da indústria nos próximos anos.

Um outro desafio técnico é encontrar uma solução simultaneamente viável e totalmente descentralizada. Um dos grandes apelos da tecnologia de cadeia de blocos é fornecer um registro distribuído das transações, que não seja intermediado e dependente de uma determinada entidade. Os protótipos existentes e as propostas encontradas na literatura recente, no entanto, são soluções baseadas em cadeias privadas, gerenciadas por uma entidade central, ou um grupo pequeno responsável pela auditoria de todo o sistema. A reiterada opção por essa arquitetura é comumente justificada por problemas de escalabilidade na taxa de validação das operações e consequente aumento no atraso de verificação, em soluções de cadeias de blocos públicas. Além da questão do tempo, há também preocupação com a eficiência energética do gerenciamento da cadeia de blocos, algo particularmente importante nesse tipo de aplicação, dada a expectativa de que as redes elétricas inteligentes possam trazer menores perdas energéticas no sistema elétrico. Outra barreira técnica potencial associada à distribuição da gerência da cadeia de blocos é o custo associado à manutenção do aparato tecnológico necessário para que um usuário

participe do gerenciamento da cadeia. Esses custos podem ir de encontro à promessa de uma energia mais barata, repetidamente ecoada por empresas do setor e pesquisadores.

Do ponto de vista político, há questões regulatórias que podem afetar a viabilidade de implantação dessas soluções. No Brasil, por exemplo, atividades econômicas nos setores de geração, transmissão e distribuição de energia demandam concessões públicas atribuídas pelo governo [Ministério de Minas e Energia, 2012]. A atuação de tais plataformas no mercado brasileiro requer ajustes na legislação. Ademais, no caso de soluções que envolvam operações de compra e venda de energia diretamente entre "prossumidores", tais ajustes legislativos podem não contar com o apoio de grandes empresas já estabelecidas no setor. É importante considerar as preocupações governamentais com os processos de auditoria e recolhimento de impostos relativos às transações nesses mercados. Para que uma solução desse tipo seja legalmente introduzida no mercado brasileiro, há a preocupação de estabelecer mecanismos que permitam essas atividades.

Consideraram-se ainda os aspectos sociais dessas soluções. Embora uma solução de registro de transações através de cadeia de blocos e contratos inteligentes tenha como um de seus objetivos fornecer maior auditabilidade às operações do sistema elétrico, a adoção de cadeia de blocos só será bem sucedida se contar com a confiança dos consumidores. Isso é um desafio, especialmente considerando-se o fato de que a maior parcela de participantes do sistema será composta por usuários leigos.

Algumas das aplicações discutidas na literatura e implementadas em projetos piloto também pressupõem a popularização de veículos elétricos, o que ainda não é uma realidade em certos países, como no Brasil, onde a participação de veículos elétricos e híbridos em 2016 correspondia a cerca de 0,006% da frota total [FGV Energia, 2017]. Outro aspecto relevante é o impacto da dissociação das criptomoedas usadas para transações energéticas das suas contrapartes monetárias, algo proposto em várias das soluções encontradas na indústria e na literatura. Essa dissociação pode criar preocupação entre os consumidores acerca da volatilidade das cotações das criptomoedas e da possibilidade de manipulações nas cotações das taxas de câmbio.

Ao enumerar os desafios, conclui-se que há um vasto campo de pesquisa, ainda pouco explorado, para adoção da tecnologia de cadeia de blocos nas aplicações das redes elétricas inteligentes. Simultaneamente, há expectativa de investimento cada vez maior no desenvolvimento da tecnologia de cadeia de blocos, cujo mercado estimado é de centenas de milhões de dólares para os próximos anos. O cenário, portanto, é otimista: há demanda para pesquisa e recursos para financiá-la.

Referências

[Aitzhan e Svetinovic, 2018] Aitzhan, N. Z. e Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 15(5):840–852.

[Alvarenga et al., 2018] Alvarenga, I. D., Rebello, G. A. F. e Duarte, O. C. M. B. (2018). Securing configuration management and migration of virtual network functions using blockchain. Em *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, p. 1–9.

[Antonopoulos, 2014] Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc., 1 edição.

[Atzei et al., 2017] Atzei, N., Bartoletti, M. e Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts SoK. Em *International Conference on Principles of Security and Trust*, p. 164–186.

[Banasik et al., 2016] Banasik, W., Dziembowski, S. e Malinowski, D. (2016). Efficient zero-knowledge contingent payments in cryptocurrencies without scripts. Em Askoxylakis, I., Ioannidis, S., Katsikas, S. e Meadows, C., editors, *Computer Security – ESORICS 2016*, volume 9879 of *Lecture Notes in Computer Science*, p. 261–280. Springer International Publishing.

[Bartoletti e Pompianu, 2017] Bartoletti, M. e Pompianu, L. (2017). An empirical analysis of smart contracts: Platforms, applications, and design patterns. Em *Financial Cryptography and Data Security (FC)*, p. 494–509.

[Basden e Cottrell, 2017] Basden, J. e Cottrell, M. (2017). How utilities are using blockchain to modernize the grid. *Harvard Business Review*.

[Bennett, 2018] Bennett, E. (2018). Ethereum attacks. Disponível em `https://gist.github.com/ethanbennett/7396bf3f61dd985d3426f2ee184d8822`. Acessado em 24/08/2018.

[Bertsch et al., 2016] Bertsch, V., Hall, M., Weinhardt, C. e Fichtner, W. (2016). Public acceptance and preferences related to renewable energy and grid expansion policy: Empirical insights for Germany. *Energy*, 114:465 – 477.

[Bessani et al., 2014] Bessani, A., Sousa, J. e Alchieri, E. E. P. (2014). State machine replication for the masses with BFT-SMaRt. Em *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, p. 355–362.

[Bittwatt Pte. Ltd., 2018] Bittwatt Pte. Ltd. (2018). Bittwatt business plan. Relatório técnico, Bittwatt Pte. Ltd. Disponível em: `https://ico.bittwatt.com/static/files/Bittwatt-Business-Plan.pdf`.

[Bittwatt Pte.Ltd., 2018] Bittwatt Pte.Ltd. (2018). Bittwatt whitepaper. Relatório técnico, Bittwatt Pte. Ltd. Disponível em: `https://ico.bittwatt.com/static/files/Bittwatt-Whitepaper-EN.pdf`.

[Buterin et al., 2013] Buterin, V. et al. (2013). Ethereum white paper, 2014. Relatório técnico. Disponível em: `https://github.com/ethereum/wiki/wiki/White-Paper`.

[Cachin, 2016] Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. Em *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*.

[Cachin e Vukolic, 2017] Cachin, C. e Vukolic, M. (2017). Blockchain consensus protocols in the wild. Em *International Symposium on Distributed Computing (DISC)*, p. 1–16.

[Castro e Liskov, 1999] Castro, M. e Liskov, B. (1999). Practical Byzantine fault tolerance. Em *Symposium on Operating Systems Design and Implementation (OSDI)*, p. 173–186.

[Castro e Liskov, 2002] Castro, M. e Liskov, B. (2002). Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461.

[Chen et al., 2012] Chen, P., Cheng, S. e Chen, K. (2012). Smart attacks in smart grid communication networks. *IEEE Communications Magazine*, 50(8):24–29.

[Chicarino et al., 2017] Chicarino, V. R. L., Jesus, E. F., Albuquerque, C. V. N. e Rocha, A. A. A. (2017). Uso de blockchain para privacidade e segurança em Internet das coisas. Em *Minicursos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*, p. 100–150. Sociedade Brasileira de Computação (SBC).

[Christidis e Devetsikiotis, 2016] Christidis, K. e Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303.

[Cohn et al., 2017] Cohn, A., West, T. e Parker, C. (2017). Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids. *Georgetown Law Technology Review*, 1(2):273–304.

[Counterparty, 2018] Counterparty (2018). Protocol specification. Disponível em `https://counterparty.io/docs/protocol\_specification/`. Acessado em 20/08/2018.

[de Oliveira et al., 2018] de Oliveira, M. T., Carrara, G. R., Fernandes, N. C., Carrano, R. C., Albuquerque, C. V. N., Medeiros, D. S. V. e Mattos, D. M. F. (2018). Uma avaliação de desempenho de cadeias de blocos privadas permissionadas através de cargas de trabalho realísticas. Em *XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'2018)*, Natal/RN, Brazil.

[Dinh et al., 2017] Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C. e Tan, K.-L. (2017). Blockbench: A framework for analyzing private blockchains. Em *Proceedings of the 2017 ACM International Conference on Management of Data*, p. 1085–1100. ACM.

[Dong et al., 2018] Dong, Z., Luo, F. e Liang, G. (2018). Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. *Journal of Modern Power Systems and Clean Energy*.

[Douceur, 2002] Douceur, J. R. (2002). The sybil attack. Em *International workshop on peer-to-peer systems*, p. 251–260. Springer.

[Dütsch e Steinecke, 2017] Dütsch, G. e Steinecke, N. (2017). Use cases for blockchain technology in energy and commodity trading. Snapshot of current developments of blockchain in the energy and commidity sector.

[Efthymiou e Kalogridis, 2010] Efthymiou, C. e Kalogridis, G. (2010). Smart Grid Privacy via Anonymization of Smart Metering Data. *2010 First IEEE International Conference on Smart Grid Communications*, p. 238–243.

[Energy Web Foundation, 2018] Energy Web Foundation (2018). Buiding the grid's digital dna. https://energyweb.org/. Acessado em 24.08.2018.

[Ethereum, 2018] Ethereum (2018). Solidity. https://solidity.readthedocs.io/en/develop/index.html. Acessado em 20.08.2018.

[Falcão, 2009] Falcão, D. M. (2009). Smart grids e microredes: o futuro já é presente. Em *Anais do VIII Simpósio de Automação e Sistemas Elétricos*, SIMPASE '09.

[FGV Energia, 2017] FGV Energia (2017). Caderno de carros elétricos. Disponível em: `https://fgvenergia.fgv.br/sites/fgvenergia.fgv.br/files/caderno_carros_eletricos-fgv-book.pdf`.

[Gauld et al., 2017] Gauld, S., von Ancoina, F. e Stadler, R. (2017). The burst dymaxion: An arbitrary scalable, energy efficient and anonymous transaction network based on colored tangles. Relatório técnico.

[Giancaspro, 2017] Giancaspro, M. (2017). Is a 'smart contract' really a smart idea? insights from a legal perspective. *Computer Law & Security Review*, 33(6):825 – 835.

[Green e Newman, 2017] Green, J. e Newman, P. (2017). Citizen utilities: The emerging power paradigm. *Energy Policy*, 105:283 – 293.

[Greenspan, 2015] Greenspan, G. (2015). Multichain private blockchain—white paper. *URl: http://www. multichain. com/download/MultiChain-White-Paper. pdf*.

[Greer et al., 2014] Greer, C., Wollman, D. A., Prochaska, D. E., Boynton, P. A., Mazer, J. A., Nguyen, C. T., FitzPatrick, G. J., Nelson, T. L., Koepke, G. H., Hefner Jr, A. R. et al. (2014). NIST framework and roadmap for smart grid interoperability standards, release 3.0. Relatório técnico.

[Greve et al., 2018] Greve, F., Sampaio, L., Abijaude, J., Coutinho, A., Ítalo Valcy e Queiroz, S. (2018). Blockchain e a revolução do consenso sob demanda. Em *Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, p. 1–52. Sociedade Brasileira de Computação (SBC).

[Guimarães et al., 2013] Guimarães, P. H. V., Murillo, A., Andreoni, M., Mattos, D. M., Ferraz, L. H. G., Pinto, F. A. V., Costa, L. H. M. e Duarte, O. C. M. (2013). Comunicação em redes elétricas inteligentes: Eficiência, confiabilidade, segurança e escalabilidade. *Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (Minicursos SBRC)*.

[Gunter et al., 2008] Gunter, C. A., Nelli, R., Gross, G. e LeMay, M. (2008). An integrated architecture for demand response communications and control. Em *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)(HICSS)*, volume 00, p. 174.

[Gupta e Sadoghi, 2018] Gupta, S. e Sadoghi, M. (2018). Blockchain transaction processing.

[Hadley et al., 2010] Hadley, M., Lu, N. e Deborah, A. (2010). Smart-grid Security Issues. *IEEE Security and Privacy*, 8(1):81–85.

[Hasse et al., 2016] Hasse, F., von Perfall, A., Hillebrand, T., Smole, E., Lay, L. e Charlet, M. (2016). Blockchain–an opportunity for energy producers and consumers. *PwC Global Power & Utilities*, p. 1–45.

[Igure et al., 2006] Igure, V. M., Laughter, S. A. e Williams, R. D. (2006). Security issues in SCADA networks. *Computers and Security*, 25(7):498–506.

[Jesus et al., 2018] Jesus, E. F., Chicarino, V. R. L., de Albuquerque, C. V. N. e Rocha, A. A. A. (2018). A survey of how to use blockchain to secure Internet of Things and the stalker attack. *Security and Communication Networks*, 2018:1–28.

[Kang et al., 2017] Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y. e Hossain, E. (2017). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Transactions on Industrial Informatics*, 13(6):3154–3164.

[Kiayias et al., 2017] Kiayias, A., Russell, A., David, B. e Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. Em Katz, J. e Shacham, H., editors, *Advances in Cryptology – CRYPTO 2017*, p. 357–388.

[King e Nadal, 2012] King, S. e Nadal, S. (2012). PPCoin: peer-to-peer crypto-currency with proof-of-stake. Relatório técnico.

[Kwon, 2014] Kwon, J. (2014). Tendermint: Consensus without mining. Relatório técnico. Draft versão 6. Disponível em: `https://cdn.relayto.com/media/files/LPgoWO18TCeMIggJVakt_tendermint.pdf`.

[Lamport, 2001] Lamport, L. (2001). Paxos made simple. *ACM SIGACT News*, 32(4):18–25.

[Langner, 2011] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security Privacy*, 9(3):49–51.

[Lasseter e Paigi, 2004] Lasseter, R. H. e Paigi, P. (2004). Microgrid: a conceptual solution. Em *Anais do 35th Annual Power Electronics Specialists Conference (IEEE Cat. No.04CH37551)*, volume 6 of *PESC '04*, p. 4285–4290.

[Li et al., 2012] Li, X., Liang, X., Lu, R., Shen, X., Lin, X. e Zhu, H. (2012). Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine*, 50(8):38–45.

[Li et al., 2018] Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q. e Zhang, Y. (2018). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8):3690–3700.

[Liang et al., 2018] Liang, G., Weller, S. R., Luo, F., Zhao, J. e Dong, Z. Y. (2018). Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Transactions on Smart Grid*.

[Lisk, 2018] Lisk (2018). Access the power of blockchain. https://lisk.io/. Acessado em 20.08.2018.

[LO3 Energy Team, 2017] LO3 Energy Team (2017). Exergy: Electrical power whitepaper. Relatório técnico, LO3 Energy. Disponível em: `https://exergy.energy/wp-content/uploads/2017/12/Exergy-Whitepaper-v8.pdf`.

[Lopes et al., 2016] Lopes, Y., Bornia, T., Farias, V., Fernandes, N. C. e Muchaluat-Saade, D. C. (2016). Desafios de segurança e confiabilidade na comunicação para smart grids. *Miniursos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (Minicursos SBSeg)*.

[Luu et al., 2016] Luu, L., Chu, D.-H., Olickel, H., Saxena, P. e Hobor, A. (2016). Making smart contracts smarter. Em *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS'16, p. 254–269, New York, NY, USA. ACM.

[Marnay et al., 2015] Marnay, C., Abbey, C., Joos, G., Ash, K., Bando, S., Braun, M., Chatzivasileiadis, S., Driesen, J., Hatziargyriou, N., Iravani, R., Jimenez, G., Katiraei, F., Lombardi, P., Lynch, K., Mancarella, P., Moneta, D., Moreira, C., Oudalov, A., Khattabi, M., Morris, G., Nakanishi, Y., Reilly, J., Ross, M., Shinji, T. e von Appen, J. (2015). Microgrids 1 engineering, economics, & experience. Relatório Técnico 635.

[Mattos et al., 2018] Mattos, D. M. F., Duarte, O. C. M. B. e Pujolle, G. (2018). A lightweight protocol for consistent policy update on software-defined networking with multiple controllers. *Journal of Network and Computer Applications*. A ser publicado.

[McDaniel e McLaughlin, 2009] McDaniel, P. e McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, 7(3):75–77.

[Mengelkamp et al., 2018a] Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L. e Weinhardt, C. (2018a). Designing microgrid energy markets: A case study: The brooklyn microgrid. *Applied Energy*, 210:870 – 880.

[Mengelkamp et al., 2018b] Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D. e Weinhardt, C. (2018b). A blockchain-based smart grid: towards sustainable local energy markets. *Computer Science - Research and Development*, 33(1):207–214.

[Merz, 2016] Merz, M. (2016). Potential of the blockchain technology in energy trading. Em Burgwinkel, D., editor, *Blockchain Technology: An Introduction for Business and IT Managers*, chapter 2, p. 51–97. DE GRUYTER, Alemanha.

[Mihaylov et al., 2014] Mihaylov, M., Jurado, S., Avellana, N., Moffaert, K. V., de Abril, I. M. e Nowé, A. (2014). Nrgcoin: Virtual currency for trading of renewable energy in smart grids. Em *11th International Conference on the European Energy Market (EEM14)*, p. 1–6.

[Ministério de Minas e Energia, 2012] Ministério de Minas e Energia (2012). Concessões de geração, transmissão e distribuição de energia elétrica: Perguntas e respostas. Disponível em: http://www.mme.gov.br/documents/10584/1256596/Perguntas_e_respostas_-_Concessxes.pdf/57c8080d-eb1b-4052-9c3e-d3c4c010e974.

[Mo et al., 2012] Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A. e Sinopoli, B. (2012). Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209.

[Monax, 2018] Monax (2018). Monax - active agreements for growing businesses. https://monax.io/. Acessado em 20.08.2018.

[Nakamoto, 2008] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Relatório técnico.

[Neuman e Tan, 2011] Neuman, C. e Tan, K. (2011). Mediating cyber and physical threat propagation in secure smart grid architectures. *2011 IEEE International Conference on Smart Grid Communications, SmartGridComm 2011*, p. 238–243.

[Noce et al., 2017] Noce, J., Lopes, Y., Fernandes, N. C., Albuquerque, C. V. N. e Muchaluat-Saade, D. C. (2017). Identifying vulnerabilities in smart gric communication networks of electrical substations using geese 2.0. Em *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)*, p. 111–116.

[Ongaro e Ousterhout, 2014] Ongaro, D. e Ousterhout, J. (2014). In search of an understandable consensus algorithm. Em *Proceedings of USENIX Conference on USENIX Annual Technical Conference*, USENIX ATC'14, p. 305–320.

[Ouaddah et al., 2016] Ouaddah, A., Abou Elkalam, A. e Ait Ouahman, A. (2016). Fairaccess: a new blockchain-based access control framework for the internet of things. *Security and Communication Networks*, 9(18):5943–5964.

[Pilkington, 2016] Pilkington, M. (2016). 11 blockchain technology: principles and applications. *Research handbook on digital transformations*, p. 225.

[Popper, 2016] Popper, N. (2016). A hacking of more than $50 million dashes hopes in the world of virtual currency. https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html. Acessado em 24.08.2018.

[Power Ledger Pty Ltd, 2018] Power Ledger Pty Ltd (2018). Powerledger whitepaper. Relatório técnico, Power Ledger Pty Ltd. Disponível em: https://powerledger.io/media/Power-Ledger-Whitepaper-v8.pdf.

[Pudjianto et al., 2007] Pudjianto, D., Ramsay, C. e Strbac, G. (2007). Virtual power plant and system integration of distributed energy resources. *IET Renewable Power Generation*, 1:10–16.

[Rahman et al., 2013] Rahman, M. A., Al-Shaer, E. e Bera, P. (2013). A noninvasive threat analyzer for advanced metering infrastructure in smart grid. *IEEE Transactions on Smart Grid*, 4(1):273–287.

[Ramachandran et al., 2011] Ramachandran, B., Srivastava, S. K., Edrington, C. S. e Cartes, D. A. (2011). An intelligent auction scheme for smart grid market using a hybrid immune algorithm. *IEEE Transactions on Industrial Electronics*, 58(10):4603–4612.

[Schwartz et al., 2014] Schwartz, D., Youngs, N. e Britto, A. (2014). The Ripple protocol consensus algorithm. Relatório técnico, Ripple Labs Inc.

[Stellar, 2018] Stellar (2018). Stellar | move money across borders quickly, reliably, and for fractions of a penny. https://www.stellar.org/. Acessado em 20.08.2018.

[Sui et al., 2009] Sui, H., Wang, H., Lu, M. e Lee, W. (2009). An ami system for the deregulated electricity markets. *IEEE Transactions on Industry Applications*, 45(6):2104–2108.

[Szabo, 1997] Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2(9).

[Tschorsch e Scheuermann, 2016] Tschorsch, F. e Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, 18(3):2084–2123.

[Wang e Lu, 2013] Wang, W. e Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344 – 1371.

[Wood, 2014] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32.

[Xu et al., 2017] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C. e Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. Em *International Conference on Software Architecture*, ICSA'17, p. 243–252.

[Yan et al., 2011] Yan, Y., Qian, Y. e Sharif, H. (2011). A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. *2011 IEEE Wireless Communications and Networking Conference, WCNC 2011*, (to):909–914.

[Zhu et al., 2011] Zhu, T., Xiao, S., Ping, Y., Towsley, D. e Gong, W. (2011). A secure energy routing mechanism for sharing renewable energy in smart microgrid. *2011 IEEE International Conference on Smart Grid Communications, SmartGridComm 2011*, p. 143–148.