Capítulo 2

Provendo Segurança em Cidades Inteligentes: Aplicações, Desafios e Tendências em Mobilidade Elétrica e Tarifação Inteligente com NFTs

Paulo Mann (UFF), Guilherme Scofano (UFF), Yona Lopes (UFF), Helio N. Cunha Neto (UFF), Diogo M. F. Mattos (UFF) e Natalia C. Fernandes (UFF)

Abstract

This theoretical-practical short course presents the principles, applications, main challenges, and trends in electric mobility and smart charging with NFT (Non-Fungible Token). In the theoretical part of the short course, the main challenges and motivations related to electric mobility and dynamic pricing for the use of blockchain and NFT are addressed. The main concepts about NFT and its commercial applications, such as games, health, artistic productions, and certificates, are described. Specific applications in electric mobility and dynamic pricing, such as carbon credit management, are detailed, highlighting how NFTs allow the management of device identities, the generation of billing tokens, and the recording of activities in a secure, private, and legal way. The main research challenges in this area, such as anonymization and the high number of transactions, will be discussed in detail. Finally, to bring practical knowledge on the subject, we present a hands-on for issuing NFTs with the participants of the short course.

Resumo

Este minicurso teórico-prático apresenta os princípios, as aplicações e os principais desafios e tendências em mobilidade elétrica e tarifação inteligente com token não-fungível (Non-Fungible Token - NFT). Na parte teórica do minicurso, são abordados os principais desafios relacionados à mobilidade elétrica e tarifação dinâmica e as motivações para o uso de blockchain e NFT neste contexto. Os principais conceitos sobre NFT e suas aplicações comerciais, como jogos, saúde, produções artísticas e certificados, são descritos. São detalhadas aplicações específicas em mobilidade elétrica e tarifação dinâmica, como a gestão de crédito carbono, destacando como os NFTs permitem a gestão de identidades de dispositivos, a geração de tokens de cobrança e o registro de atividades de forma segura, privada e em consonância com a LGPD. Os principais desafios de pesquisa nessa área, como a anonimização e o número elevado de transações serão discutidos em detalhes. Por fim, visando trazer conhecimento prático sobre o assunto, é apresentado um hands-on sobre emissão de NFTs para ser realizado com os participantes do minicurso.

Este capítulo foi realizado com recursos do CNPq, CAPES, FAPERJ e FAPESP.

2.1. Introdução

A transição energética envolve mudanças que vão desde a geração de energia limpa até seu consumo consciente e eficiente. A transformação digital do sistema elétrico envolve a modernização do sistema, impulsionando a criação de novas aplicações com potencial para melhorar a confiabilidade, eficiência, flexibilidade e controle de recursos energéticos cada vez mais distribuídos e renováveis.

Nesse cenário, são introduzidas quatro forças motrizes da indústria de energia para a transformação do sistema, conhecidos como os "quatro Ds", descarbonização, descentralização, digitalização e desregulamentação (ou democratização). Os avanços tecnológicos em sistemas de geração e armazenamento de energia, internet das coisas, inteligência artificial, dentre outros, prometem acelerar a transição energética nesses quatro eixos. A mobilidade elétrica e a tarifação inteligente são elementos essenciais neste cenário e os pilares de destaque para o desenvolvimento de soluções nestes eixos são a garantia de segurança, interoperabilidade, singularidade e proveniência.

- A **descarbonização** é o elemento chave para limitar o aquecimento global. A redução das emissões de gases de efeito estufa da sociedade, principalmente dióxido de carbono, é uma estratégia real para desacelerar as mudanças climáticas. Uma vez que não se pode parar ou reverter o aquecimento global, tem-se que criar estratégias para retardá-lo. Nesse sentido, quanto mais rápido a energia for estruturalmente descarbonizada, melhor. Em um primeiro momento, a ampla utilização de Fonte de Energia Renovável (FER) é o que se aborda quando se trata de descarbonizar o setor de energia. O crescimento constante da utilização de fontes de energia renováveis permite que um recorde seja alcançado, chegando a um quarto da geração total de energia global segundo a *International Energy Agency* (IEA)[2]. No entanto, apenas esse crescimento não é suficiente, sendo primordiais a adoção de tecnologias associadas às FERs, como o armazenamento de bateria e veículos elétricos, e medidas para remover ou compensar o carbono inerente presente em nossa infraestrutura, como o crédito carbono. Nesse contexto, espera-se que a ampla adoção de Veículos Elétricos (VE) leve a uma importante eletrificação do transporte. Soluções de crédito carbono com a implementação destes modais de transporte com baixo impacto ambiental quando alinhados a serviços de economia compartilhada trazem ganhos e mudanças de paradigma importantes no setor de mobilidade.

- A **descentralização** da energia refere-se a produção de energia mais eficiente, flexível e resiliente por meio de Geração Distribuída (GD) e armazenamento em uma arquitetura de rede descentralizada. Esse modelo pode ser viabilizado através de microrredes locais autônomas, usinas elétricas locais limpas, como fazendas solares. A descentralização do fornecimento de energia de uma região traz muitos benefícios. A implantação de usinas solares locais, pequenos parques eólicos, armazenamento de baterias e usinas combinadas de calor e energia tornam o mercado de energia mais competitivo, reduzindo os preços para o consumidor. A utilização de geração distribuída para apoio a mobilidade elétrica por exemplo, pode trazer redução de custos ao se alimentar os postos de recarga de VEs com energia limpa. Sis-

[2]Disponível em https://www.iea.org/fuels-and-technologies/renewables

temas renováveis descentralizados não são apenas melhores para o meio ambiente, mas também tendem a ser mais confiáveis do ponto de vista elétrico. Problemas que ocorrem no sistema local permanecem locais, de modo que as falhas podem ser reparadas mais rapidamente resultando um fornecimento de energia mais confiável. Ressalta-se que a redução das emissões de gases de efeito estufa também envolve uma produção de energia mais eficiente, flexível e resiliente.

- A **digitalização** do setor de energia envolve o aumento do uso de tecnologia para melhor controlar, gerenciar e proteger o sistema de energia. Uma indústria de energia descentralizada exige que os dados sobre a produção, transmissão, distribuição e o consumo de energia sejam disponibilizados em tempo real e em vários pontos da rede de maneira acessível e confiável. Para viabilizar a digitalização, iniciativas como as da norma IEC 61850 [IEC TC 57, 2022], visam padronizar todo o sistema de automação de energia garantindo interoperabilidade e reusabilidade. Para isso, cada elemento/função do sistema é representado logicamente — através dos chamados nós lógicos — de forma única com um modelo de dados padronizado. Efetivamente, para que um sistema elétrico digitalizado, como uma microrrede de VEs, seja implementado, a garantia de interoperabilidade entre seus elementos é essencial. Afinal, para averiguar que as inciativas de mudança climática implementadas estão funcionando, é necessário que a quantidade de energia utilizada seja medida, e que a quantidade de carbono que esta sendo economizado possa ser calculada.

- A **democratização** é a ação de tornar o setor de energia mais justo para os consumidores. Em um mercado de energia regulado, o governo tem controle sobre os preços da eletricidade, o que deixa pouco espaço para concorrência e pouca escolha para os clientes. No entanto, com o aumento da demanda global de energia, em algumas jurisdições, novos atores podem participar do mercado de energia. Neste cenário, novamente a mobilidade elétrica sustentável aparece como solução para democratizar o setor e impulsionar soluções de tarifação inteligente descentralizadas e seguras.

Existe uma sobreposição entre os conceitos dos quatro Ds, principalmente quando se observa aplicações em mobilidade elétrica e tarifação inteligente. A mobilidade elétrica engloba a eletrificação dos veículos, toda a infraestrutura de recarga necessária para que estes sejam abastecidos e as iniciativas propostas para solucionar problemas da mobilidade urbana, como o compartilhamento de VEs. No conceito de mobilidade elétrica a infraestrutura de carregamento é externa, onde os postos de recarga podem ser associados a geração distribuída. Para que esta infraestrutura seja implementa é necessário um sistema de tarifação inteligente, seguro e eficiente que inclui a gestão da energia gerada, a forma com que é comercializada e a relação do usuário com a tarifação. Sendo assim, a mobilidade elétrica e a tarifação inteligente estão fortemente presentes nas quatro forças motrizes da industria de energia para transformação do sistema, sendo grande foco da indústria e do governo atualmente.

Essas tecnologias prometem mudar disruptivamente o mercado de energia tradicional, seja em nível de infraestrutura, aplicações ou serviços. O potencial advindo dessas tecnologias disruptivas, no entanto, introduzem novas implicações e desafios de segurança

cibernética para os operadores de serviços públicos e de mercado. Sendo assim, melhorar a segurança, a disponibilidade e principalmente a integridade dos dados da rede elétrica e é imprescindível para atender aos requisitos emergentes dos sistemas elétricos modernos, oferecendo operações seguras e confiáveis.

A maioria das soluções existentes em mobilidade elétrica [Ruggieri et al., 2021] se concentra no manuseio e compartilhamento seguro dos dados. Desafios como o uso de dados pessoais sem o consentimento ou conhecimento do proprietário até o acesso ou manipulação de dados por partes não autorizadas são recorrentes.

Neste minicurso, a tecnologia de cadeia de blocos (*blockchain*) é apresentada como uma opção para prover segurança em mobilidade elétrica e tarifação inteligente, pois permite a construção de soluções transparentes e descentralizadas de forma segura quando combinada a contratos inteligentes. A cadeia de blocos garante que transações sejam executadas de forma autônoma.

Visando garantir a singularidade, surgiram os *Non-Fungible Token*s (NFTs), que são registros/direitos negociáveis de ativos digitais únicos, tais como imagens, músicas, vídeos, entre diversos outros, onde a propriedade é registrada em contratos inteligentes em uma cadeia de blocos [Dowling, 2022]. Portanto, funcionam como certificados exclusivos de autenticidade registrados na cadeia de blocos e, usualmente, emitidos pelos criadores dos ativos, que podem ser de natureza digital ou física [Ante, 2022]. Por suas características como unicidade, interoperabilidade e também por sua rastreabilidade, que permite que o histórico completo de transações seja mantido, o NFT tem sido apontado como opção revolucionária em novos domínios, apesar de ter sua origem e destaque no mercado de ativos digitais relacionados à arte e aos jogos. O NFT permite o registro de proveniência, com características sobre o ativo que está sendo registrado e vendido, tais como origem, data de origem, tecnologia utilizada, entre outros. Tais características permitem solucionar desafios de segurança relacionados às áreas de controle, de mercado e tecnológicos de diversas aplicações dos sistemas de energia e de cidades inteligentes.

O objetivo deste minicurso teórico-prático é apresentar os princípios, as aplicações e os principais desafios e tendências em mobilidade elétrica e tarificação inteligente com NFTs. Na parte teórica do minicurso, serão abordados os principais desafios relacionados à mobilidade elétrica e tarifação dinâmica e às motivações para o uso das cadeias de blocos e NFTs em redes elétricas inteligentes. Os principais conceitos sobre NFTs e suas aplicações comerciais como jogos, saúde, produções artísticas e certificados serão descritos. Serão detalhadas aplicações específicas em mobilidade elétrica e tarifação dinâmica, como a gestão de crédito carbono, destacando como os NFTs permitem a gestão de identidades de dispositivos, a geração de *tokens* de cobrança e o registro de atividades de forma segura, privada e em consonância com a Lei Geral de Proteção de Dados Pessoais (LGPD). Os principais desafios de pesquisa nessa área, como a anonimização e o número elevado de transações serão discutidos em detalhes. Por fim, visando trazer conhecimento prático sobre o assunto, será realizada um *hands-on* de emissão de NFTs com os participantes do minicurso.

Espera-se que ao final do minicurso os participantes sejam capazes de (i) conhecer os principais fundamentos de NFT e cadeias de blocos, (ii) conhecer as principais aplicações comerciais de NFTs, (iii) conhecer as possíveis aplicações de NFTs para mobilidade

elétrica e tarifação inteligente, (iv) compreender os principais desafios de pesquisa e tendências no assunto, (v) aprender, de forma prática, como é realizada a emissão de um NFT.

O restante desse minicurso está organizado como descrito a seguir. Na Seção 2.2, são apresentados os principais conceitos sobre cadeias de blocos, enquanto que a Seção 2.3 conceitua os NFTs. As aplicações tradicionais de NFT são discutidas na Seção 2.4, enquanto que as novas aplicações em mobilidade elétrica e tarifação são discutidas na Seção 2.5. Na sequência, a Seção 2.6 traz os desafios e tendências de pesquisa. Por fim, a Seção 2.7 apresenta uma exemplificação prática da criação de NFTs, enquanto que a Seção 2.8 traz as considerações finais do texto.

2.2. Conceitos gerais da tecnologia de cadeias de blocos

A cadeia de blocos é uma tecnologia de registro distribuído sem a necessidade de uma autoridade confiável. Essa tecnologia possibilita o desenvolvimento de aplicações distribuídas seguras em cenários nos quais há desconfiança mútua entre entidades [Nofer et al., 2017]. Dois elementos principais definem a tecnologia: i) a estrutura de dados distribuída e ii) a rede par-a-par formada pelos nós participantes da rede. A estrutura de dados distribuída é formada por uma sequência imutável de registros encadeados, que originam um livro-razão digital compartilhado, distribuído e descentralizado. Sendo assim, a cadeia de blocos funciona como um banco de dados distribuído seguro, permitindo o armazenamento da informação. É importante destacar que a estrutura de dados sozinha não é suficiente para garantir que haja o acordo entre todos os participantes do sistema sobre a versão mais atual da cadeia de blocos. Porém, a estrutura de dados provida pela cadeia de blocos possui papel essencial para garantir o ordenamento das transações e evitar o gasto duplo nos sistemas de pagamento distribuídos. Também não há garantia de acordo entre os participantes sobre qual é o bloco atual que deve ser inserido na cadeia de blocos.

O acordo entre os participantes do sistema de pagamento sobre a correta versão dos blocos a serem inseridos na cadeia de blocos é um desafio dos mecanismos de consenso do sistema. Mecanismos de consenso são algoritmos que permitem alcançar um acordo sobre um único dado ou sobre o estado de um sistema distribuído [Rebello et al., 2019]. O encadeamento dos registros associados aos mecanismos de consenso garante a integridade da informação e permitem que todos os participantes da rede possuam uma réplica idêntica da cadeia de blocos, criando uma visão global da informação armazenada.

A solução proposta para alcançar o consenso no sistema de pagamento da criptomoeda Bitcoin é que o primeiro participante que resolva um desafio computacional seja o responsável por adicionar o bloco por ele proposto na cadeia de blocos divulgada para todos os demais participantes. O desafio computacional corresponde à adição de um número aleatório ao bloco candidato a ser adicionado na cadeia de blocos, porém, após a adição desse número aleatório, o resumo criptográfico do bloco deve ser iniciado com um número predeterminado de zeros. Como as funções *hash* de resumo criptográfico têm um comportamento pseudo-aleatório, não é possível correlacionar os valores de entrada aos valores de saída. Assim, não é possível ter pistas de qual valor aleatório deva ser adicionado ao bloco candidato para que se possa ter a condição de saída necessária para finalizar o desafio. Dessa forma, a busca pelo número aleatório que cumpre o desafio proposto pelo

sistema é necessariamente baseada em tentativas e erros. O desafio computacional para provar que um participante realmente comprometeu seu trabalho computacional e, portanto, é quem detém o direito de adicionar um novo bloco à cadeia é chamado de Prova de Trabalho (*Proof of Work* - PoW).

É importante ressaltar que os participantes da rede não podem falsificar o quanto de poder computacional dispõem. Portanto, a proposta de consenso se baseia em um desafio computacional que envolve o cálculo consecutivo de valores *hash* através de tentativas e erros. Ademais, o poder computacional está intimamente ligado a questões físicas que impõe custos reais ao sistema, como aquisição de equipamento e custos energéticos. Logo, é necessário que haja incentivos aos participantes que comprometem seu poder de computação para adicionar blocos à cadeia de blocos. O Bitcoin implementa a política de que, se um participante pode mostrar que satisfez a condição, então realizou uma quantidade de trabalho e, portanto, tem o direito de adicionar um bloco novo à cadeia e receber uma recompensa. O trabalho realizado pelo participante é pago em criptomoedas Bitcoin. A prova de trabalho desencoraja o desperdício do recurso compartilhado. Nota-se que o desafio criptográfico não é uma proposta restrita à cadeia de blocos Bitcoin, mas antecede as criptomoedas sendo previamente usado em protocolos de autenticação [Nita et al., 2018] ou mecanismos de prevenção de spam (mensagens de e-mail não solicitadas) [Yoon et al., 2010].

A argumentação pelo uso do desafio computacional para realizar o consenso da rede é que o custo real para atacar o sistema é grande o suficiente para que o atacante que estiver disposto a atacar seja o maior prejudicado [Oliveira et al., 2020]. Contudo, diferentes sistemas de livro-razão distribuídos têm necessidades distintas em garantir o consenso sobre os ativos transacionados e, portanto, outros mecanismos de consenso também são propostos para diferentes plataformas de cadeias de blocos.

A base criptográfica da estrutura de dados da cadeia de blocos é fortemente baseada em duas premissas criptográficas: as funções de resumo criptográfico (*hash*) e o algoritmo de assinatura digital. A partir dessas premissas, desenvolvem-se os conceitos de estruturas de dados baseadas em *hash*, prova de comprometimento, *Proof of Work* (PoW) e endereçamento de participantes na cadeia de blocos. A função de resumo criptográfico tem como objetivo realizar o mapeamento de uma cadeia de bytes (*string*) de tamanho arbitrário em uma nova cadeia de bytes com um tamanho fixo e, possivelmente, menor que a cadeia de bytes original. O tamanho da *string* de saída é fixo e, para funções *hash* atuais, tal como a SHA256, tem comprimento de 256 bytes na saída, independentemente do comprimento da entrada. Já os algoritmos de criptografia assimétrica permitem criptografar uma mensagem para que apenas o destinatário específico seja capaz de lê-la, garantindo a propriedade da confidencialidade. Além disso, é possível gerar uma assinatura digital para comprovar que uma origem específica gerou aquela mensagem, garantindo as propriedades do não-repúdio e da autenticidade.

Outro conceito importante em cadeia de blocos é a rede par-a-par. A rede par-a-par é responsável por interconectar os participantes de uma cadeia de blocos; transações, que são mensagens geradas pelos participantes que contêm alguma instrução, como a transferência de ativos digitais; bloco, que é formado por um conjunto de transações; conta, que é uma entidade capaz de gerar transações; e a carteira, que são aplicações que

permitem um usuário interagir com a conta.

Não obstante o Bitcoin apresenta uma revolução tecnológica e financeira, suas limitações rapidamente emergiram. Em particular, o Bitcoin permitia apenas a troca de ativos fungíveis, e apenas de um tipo, a moeda $BTC. Com o passar do tempo, os desenvolvedores perceberam a necessidade de criar suas próprias moedas digitais — criptomoedas — que poderiam residir também dentro da cadeia de blocos, lado a lado com outras moedas. Uma das aplicações mais bem-sucedidas que implementou este conceito foi a cadeia de blocos Ethereum.

O Ethereum elaborou e consolidou uma nova primitiva para as cadeias de blocos, revolucionando todo o mercado de criptomoedas desde sua concepção. O Ethereum permitiu que *scripts* fossem escritos e executados em linguagem de programação de alto nível dentro da cadeia de blocos por meio de transações [Saingre et al., 2022]. Na prática, esses *scripts* são chamados de "contratos inteligentes", que também possuem um endereço único. O contrato é executado ao enviar uma transação que chama uma determinada função com os parâmetros corretos para o endereço do contrato [Saingre et al., 2022]. Essa capacidade de executar código na cadeia de blocos conferiu a criação de aplicações descentralizadas - *Distributed Application*s (DApps) - que podem utilizar a rede para efetuar cálculos arbitrários. O termo "contrato" também pode ser visto como um pedaço de código que implementa um algoritmo para o qual todos da rede que o utilizam estão mutuamente de acordo.

Um dos contratos inteligentes mais utilizados no Ethereum é o *Ethereum Request for Comments - 20* (ERC-20), criado em 2015[3]. Este contrato habilitou a criação de novas moedas que podem coexistir com a moeda dita nativa do Ethereum — o Ether. Essas moedas que podem ser criadas pelos usuários recebem o nome de *tokens*. O resultado disso é visto em diversas aplicações cujos *tokens* possuem alta capitalização de mercado atualmente — como o *token* $UNI do DApp Uniswap[4]. Além disso, a criação de um *token* próprio concede um maior controle sobre a emissão e destruição deste *token*, isto é, da economia do DApp. O maior controle pode estar em dissonância com o conceito de descentralização, mas isso também pode ser resolvido por meio da criação de um sistema *Decentralized Autonomous Organization* (DAO). O DAO irá representar de maneira democrática os interesses individuais dos usuários para opinar sobre quais direções o DApp deve tomar. O DAO permite que as pessoas, em posse de uma quantia de *tokens*, tenham poder sobre o futuro da aplicação. Além disso, muitas vezes, também é possível investir em um projeto apenas comprando o seu *token*, o que representaria algo similar a comprar ações de uma empresa na bolsa de valores.

O contrato ERC-20 foi importante por adotar uma padronização de alto nível para todos os *tokens* criados no Ethereum. Em princípio, qualquer pessoa poderia criar um padrão que define a governança de *tokens*. Entretanto, a ideia de que haja apenas um único padrão tem o objetivo de aumentar a interoperabilidade e facilitar o desenvolvimento de DApps. Isso, no entanto, incorre em alguns problemas, caso haja alguma limitação com o padrão adotado.

[3] https://eips.ethereum.org/EIPS/eip-20
[4] https://uniswap.org/

O cômputo das instruções de um contrato inteligente no Ethereum tem um custo associado. A taxa de transação — ou popularmente chamado de "gás" — é coletada pelos mineradores que mantêm a rede em funcionamento. Essa taxa é o incentivo financeiro que proporciona uma vantagem para os mineradores emprestarem seu poder computacional. A taxa de transação é calculada como $taxa\_transacao = custo\_gas \cdot preco\_gas$ [Saingre et al., 2022]. O *preco_gas* é definido por quem inicia a transação — em geral o usuário. O *custo_gas* é igual à soma do custo de cada instrução do contrato inteligente que é executada na função chamada do contrato [Saingre et al., 2022]. Isso significa que quanto maior o número de instruções a serem executadas maior será o custo do gás, e portanto maior a taxa de transação. O usuário tem um papel ativo na definição do *preço do gás*, pois a rede também possui um limite de transações por bloco, ou até transações por segundo. Com o maior número de pessoas utilizando a rede, ocorre um efeito de "afunilamento" ou "congestionamento", onde passam apenas algumas transações, sobretudo aqueles que tiverem um maior *preco_gas* definido pelo usuário. De maneira geral, os mineradores priorizam as transações que têm maior recompensa financeira. Em outras situações, o usuário também pode querer que a sua transação seja processada rapidamente, e portanto, quanto maior o *preco_gas* definido, maior a prioridade.

Um dos problemas das cadeias Bitcoin e Ethereum é o mecanismo de consenso, que consome muita energia. De fato, a maior parte dos mineradores utiliza *hardware* dedicado, como *Graphics Processing Unit*s (GPUs) ou *Application Specific Integrated Circuit*s (ASICs), para obter lucros significativos, aumentando ainda mais os danos ecológicos. O rápido crescimento das criptomoedas baseadas em PoW chamou a atenção da imprensa, academia e da indústria, devido às iniciativas políticas internacionais recentes para a redução de emissões de gases que causam o efeito estufa. As cadeias de bloco passaram a ser mal vistas, tanto pela alta necessidade de energia, quanto pelo lixo eletrônico que será gerado pelos altos investimentos em fazendas de mineração [Platt et al., 2021, Miraz et al., 2021]. Para superar esse problema, foi proposto um mecanismo de consenso chamado de Prova de Participação - *Proof of Stake* (PoS), que fornece a possibilidade de "validadores" participarem do consenso de uma transação com um consumo mínimo de energia. No Prova de Participação, não é necessário usar um hardware dedicado, mas apenas ter a criptomoeda nativa e um computador simples. Quanto maior a quantidade de criptomoedas, mais chance o validador tem de validar um bloco e receber uma recompensa por isso. Pelo fato da recompensa estar associada com a maior quantidade de criptomoedas que o validador possui, os validadores são estimulados a captarem usuários com o objetivo de aumentar a recompensa total. Dessa forma, os usuários podem "delegar" suas criptomoedas para um validador em troca de receberem parte das recompensas que o validador recebe. Delegar é vantajoso para usuários que não queiram ter o trabalho de gerenciar um validador. Caso o validador valide dados fraudulentos, eles podem perder parte de suas moedas e/ou recompensas — a depender da implementação. O mecanismo de consenso Prova de Participação também pode ser visto à luz de uma pessoa que investe em sua poupança: quanto mais dinheiro a pessoa guardar, maior a recompensa.

Como resultado, a tecnologia de cadeia de blocos está em constante desenvolvimento. O Bitcoin cementou e viabilizou o uso de um sistema financeiro sem a necessidade de uma autoridade confiável — como um banco. O Ethereum desenvolveu esse

conceito e popularizou a criação de aplicações totalmente descentralizadas. Atualmente, embora de difícil execução, é possível criar aplicações que sejam governadas pelos usuários, armazenadas em serviços descentralizados, e cujo futuro é sobretudo determinado pela comunidade. Por outro lado, tem-se serviços altamente centralizados em que as funcionalidades são desenvolvidas por um grupo muito seleto que irão impactar a vida de milhões de usuários.

Dentro desse contexto de rápida evolução das cadeias de bloco, surge a tecnologia dos NFTs. Antes, todos os *tokens* das cadeias de blocos eram fungíveis, de forma que não era possível garantir, com a cadeia, a unicidade e a posse de um determinado bem digital com características únicas. A Seção 2.3 aborda como foi a primeira tentativa de criar ativos não fungíveis no Bitcoin. Em seguida, é apresentado o funcionamento dos NFTs no Ethereum, sua concepção e evolução até os dias atuais.

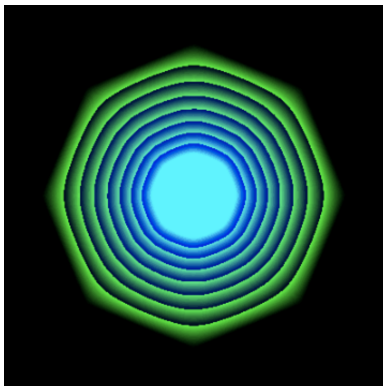
2.3. *Non Fungible Tokens* (NFT)

Um *token* não fungível (*Non-Fungible Token*) é um tipo especial de *token* criptográfico que representa um bem cuja singularidade, identidade e proveniência são cruciais [Apolinário, 2019]. Para entender esse conceito, pode-se considerar que o valor de 1 $BTC não difere de outro 1 $BTC. Igualmente, é possível trocar 1 $BTC por dois 0.5 $BTC sem prejuízos, uma vez que um bem fungível é passível de ser substituído por outro bem da mesma espécie, qualidade, quantidade e valor. Diferentemente de uma criptomoeda, um NFT não pode ser substituído por outro da mesma natureza: uma arte digital emitida por um artista nunca será igual a outra arte digital também emitida pelo mesmo artista. Ainda que o artista utilize o mesmo conteúdo digital, o NFT ainda terá outra identificação na cadeia de blocos. O NFT pode assumir qualquer tipo de conteúdo digital ou físico, como música, código, ou qualquer produção implementada como código, tal como arte generativa, jogos, páginas web ou outras.

Num cenário com quatro forças motrizes da industria de energia, temos em especial consonância a descentralização e digitalização com os NFTs. A representação digital "tokenizada" dos nós lógicos na cadeia de blocos é uma das possíveis formas de criar maior interoperabilidade no setor de energia, facilitando a tarifação inteligente. Essa seção discute a história dos NFTs, sua motivação, os padrões adotados em algumas das cadeias de blocos disponíveis, a criação e o uso de NFTs, a reusabilidade de NFTs em contextos da descentralização e o consumo de energia para emitir e negociar NFTs.

A discussão sobre a origem dos NFTs é uma área cinzenta de difícil definição. Contudo, há certo consenso que os NFTs atuais são desdobramentos da proposta *Colored Coins* [Rosenfeld et al., 2012]. A proposta das *Colored Coins* visava colorir determinadas moedas da rede bitcoin ($BTC) pelo rastreamento de sua proveniência, o que naturalmente implicaria na sua distinção, através de cores, de outras moedas da rede. As moedas coloridas eram assim definidas por terem um propósito distinto das moedas não coloridas, seja para serem usadas como moedas alternativas, certificados de *commodities* ou para representar outros instrumentos financeiros, como ações [Rosenfeld et al., 2012]. A coloração determina que a propriedade da moeda é de um bem não fungível, isto é, de identidade singular, indivisível e insubstituível. No entanto, as limitações do Bitcoin impossibilitaram o uso prático das *Colored Coins*. Na época, embora restrito apenas a uma

(a) Um *rare pepe*



(b) Um quadro de Quantum, por Kevin McCoy.

Figura 2.1. Dois dos NFTs mais antigos já emitidos.

aplicabilidade teórica, os fundamentos estabelecidos pelas *Colored Coins* deflagraram um movimento de ideias que culminou em aplicações práticas e funcionais, inclusive, no que entende-se como NFT atualmente. Por outro lado, existem pessoas que consideram o NFT Quantum — criado em maio de 2014 na rede Namecoin por Kevin MacCoy — como a origem dos NFTs. Um exemplo de quadro do NFT Quantum é mostrado na Figura 2.1b. A hipótese é que a obra Quantum foi a primeira implementação prática e funcional na rede principal (*mainnet*) pública da rede Namecoin, e portanto, poderia ser livremente negociada e oficialmente chamada de "a origem dos NFTs".

Em seguida, vários eventos se desdobraram a partir de 2015 no mundo de NFTs. A fundação do Counterparty, uma plataforma financeira distribuída cujo protocolo foi construído em cima da rede do Bitcoin, possibilitou a criação de NFTs que poderiam ser negociados livremente pela plataforma. Com efeito, dois jogos de cartas emitiram parte de seus conteúdos via NFTs: *Spells of Genesis*[5] e *Force of Will*. Ambos os jogos foram pioneiros na aplicabilidade de recursos digitais escassos emitidos via NFTs em jogos digitais. Além disso, em 2016, usuários do Counterparty começaram a criar NFTs de memes, em particular o que atualmente é conhecido como *rare pepes*, como exemplificado na Figura 2.1a, onde os usuários se especializaram em reconhecer a raridade dos *pepes* e a negociá-los livremente. Discutivelmente, esse poderia ter sido o primeiro rastro da comercialização de NFTs como colecionáveis digitais escassos. Isso demonstrou que existia não apenas uma demanda, mas também erigiu um novo nicho onde colecionadores de raridades digitais se encontravam e discutiam sobre as produções artísticas e culturais emitidas como NFTs.

No entanto, a despeito dos esforços em criar ativos que poderiam representar recursos digitais ou físicos dentro da cadeia de blocos, um problema começou a surgir por meio do excesso de heterogeneidade. A heterogeneidade é um problema porque cria um ambiente de desconfiança e de não interoperabilidade. Considere, portanto, que a em-

[5]Um *Trading Card Game* (TCG) cujos desenvolvedores se autointitulam "o primeiro jogo mobile baseado em cadeia de blocos criado" [Spells of Genesis, 2022].

presa A criou um padrão P_A de certificação digital, enquanto as empresas B e C criaram os padrões P_B e P_C. Nesse cenário, existe uma grande dificuldade de intercâmbio de produtos digitais emitidos, por exemplo, no padrão P_A para o padrão P_B ou P_C. Para haver interoperabilidade, as empresas A, B e C devem ter consenso e confiança mutua que todas as certificações digitais são válidas. Essa situação exige uma confiança e reconhecimento dos diferentes padrões adotados pelas diferentes empresas, que, no entanto, frequentemente têm dificuldade de cooperarem entre si. Com efeito, a adoção de um padrão único de emissão de NFTs foi crucial para o desenvolvimento e adoção dos NFTs, onde, às vezes, dentro de uma mesma cadeia de blocos existiam um ou mais padrões diferentes que eram usados simultaneamente.

Dessa forma, um ponto de inflexão deflagrou uma grande mudança no que hoje entende-se por NFT, iniciando-se com o padrão EIP-721[6], criado em 2017 na rede Ethereum. O EIP-721, uma implementação específica de contratos inteligentes, possibilitou a emissão e negociação de NFTs na rede Ethereum. Em seguida, os padrões EIP-1155[7] e EIP-2981[8] foram desenvolvidos com o propósito de abranger os casos de uso do EIP-721. O EIP-1155 insere um novo paradigma de uso para NFTs com a adoção do padrão *multi-tokens* e operações menos custosas — menor uso de gás — que reduzem a emissão de carbono em 90% [Valeonti et al., 2021]. Um *multi-token* permite a existência de NFTs semi-fungíveis, que implica a existência de uma classe de ativo que possui uma ou mais edições. Para todas as edições de um mesmo NFT, é possível trocá-los entre si, pois são equivalentes; mas entre classes diferentes de ativos — de *multi-token* para *multi-token* — ainda podemos considerar o ativo insubstituível.

Com os padrões EIP-721 e EIP-1155, os *royalties* são distribuídos de maneira individualizada por cada plataforma de negociação — não há uma padronização. Com efeito, o EIP-2981 cria uma maneira universal de garantir o direito financeiro dos *royalties* por meio do contrato que o NFT foi gerado. Isso garante que, a despeito de como a plataforma irá lidar com *royalties*, o criador do NFT irá receber os *royalties*. Originalmente, na ausência de um padrão que habilitava o uso de NFTs, o padrão mais adotado no Ethereum era a implementação ERC-20, que representa a emissão de moedas[9] fungíveis. Embora este padrão não seja capaz de emitir NFTs, foi uma evolução perante ao bitcoin — pois limitava-se à uma única moeda na cadeia de blocos, o $BTC.

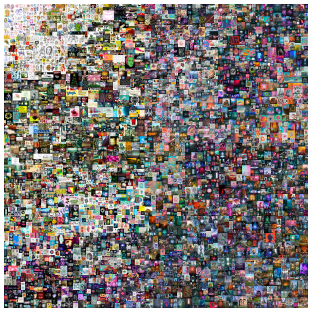
Uma das primeiras aplicações de sucesso que usou o padrão ERC-721 foi o CryptoKitties, um jogo cujo objetivo é reproduzir gatos digitais, onde os filhotes criados terão as características herdadas dos gatos pais. O jogo permitia ao jogador ter a posse dos gatos como NFT, o que, por consequência, habilitava o jogador a negociá-lo em uma plataforma de negociação, ou até mesmo trocar com seus amigos. O sucesso do jogo fez com que fosse gerado um número imenso de transações na rede Ethereum, congestionando-a e aumentando o preço necessário para processar uma transação — popularmente conhecido como gás. Embora a proposta do jogo não fosse para obter ganhos financeiros, o

[6] `https://eips.ethereum.org/EIPS/eip-721`

[7] `https://eips.ethereum.org/EIPS/eip-1155`

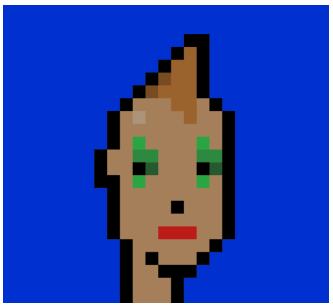
[8] `https://eips.ethereum.org/EIPS/eip-2981`

[9] Essas moedas muitas vezes recebem o nome de "*tokens*", e são moedas emitidas e controladas livremente pela pessoa — ou a organização — que os criaram, o que difere particularmente da moeda nativa do Ethereum — Ether.



(a) 5000 *Everydays*' por Beeple.

(b) Diamante destruído por Tascha Che.



(c) CryptoPunk #7610 comprado pela VISA Inc.

Figura 2.2. Em (a), um dos NFTs mais caros já vendidos. Em (b), um diamante físico que foi destruído para emitir um NFT. Em (c), um colecionável chamado CryptoPunks comprado pela VISA Inc.

mercado secundário (revenda dos gatos a outros interessados) estava super aquecido enquanto os gatos eram vendidos por altos preços; um gato chegou a ser vendido por US$ 170,000 [Valeonti et al., 2021].

Os efeitos do sucesso do ERC-721 ainda são sentidos atualmente, uma vez que cerca de 97% das vendas de NFTs ainda são realizadas no Ethereum [CoinTelegraph Research, 2021]. Com efeito, a partir de 2021, ocorreu uma sucessão de vendas de alto valor de NFTs. Em Fevereiro de 2021, ocorreu a venda de um meme popularmente conhecido como "Nyan Cat" por aproximadamente US$ 590,000 no dia da venda [Etherscan, 2021b]. Em seguida, a Christie's, uma famosa casa de leilões de arte, vendeu o NFT "5000 Everydays" do artista popularmente conhecido como Beeple por US$ 69.3 milhões [Beeple, 2021]. A arte vendida por Beeple é a união de 5000 mil artes individuais produzidas diariamente em seu perfil do Instagram por mais de treze anos, como pode ser observado pela Figura 2.2a. Em uma outra situação, a VISA Inc. comprou um NFT colecionável chamado CryptoPunks, mostrado na Figura 2.2c, por US$ 150,000 [Browne, 2021, VisaNews, 2021]. Além disso, outras utilidades inovadoras surgiram ao migrar o conteúdo físico para o digital por meio dos NFTs. Como exemplo, a Tascha Che comprou um diamante de US$ 5.000,00 e o destruiu para emitir um NFT com uma imagem e o certificado de compra do diamante [Che, 2021], mostrada na Figura 2.2b. Como resultado, o NFT que representa o diamante foi vendido por 5.5125 Ether (equivalente a US$ 18,009.28 no valor do dia da venda) no OpenSea [Etherscan, 2021a]. Em outra situação, a obra Fumeur V (1964) de Pablo Picasso foi queimada para ser emitida como um NFT [Yahoo, 2021], embora não tenha sido vendida. A obra Fumeur V original pode ser observado pela Figura 2.3a, enquanto a obra destruída (incinerada) pode ser observada pela Figura 2.3b.

Há, no entanto, uma discussão entorno do quanto um NFT consegue funcionar como uma reserva de valor em face da perda da utilidade física. O diamante possui valor pela sua utilidade física, raridade, durabilidade, mas também como reserva de valor porque existe um consenso social e financeiro que habilita o seu valor. Ao destruí-lo, a utilidade física é perdida, enquanto, em tese, a raridade, durabilidade e consenso social são transmitidos diretamente ao NFT. Porém, isso é apenas verdade enquanto o consenso

(a) Fumeur V, obra original de Pablo Picasso.

(b) Fumeur V queimado, obra original de Pablo Picasso.

Figura 2.3. Fumeur V, por Pablo Picasso em (a). A mesma obra, porém queimada em (b).

social e a confiança sustentarem o que chamamos atualmente de NFT. Mas uma coisa é inegável: é muito mais simples transferir um NFT que representa a propriedade de uma casa para outra pessoa do que passar pela burocracia para realizar a mesma tarefa sem NFTs.

Qualquer tipo de investimento ou ativo financeiro possui seus riscos inerentes, sobretudo algo tão emergente como NFTs. Entretanto, pode-se observar que todas essas aplicações inovadoras ou altos valores de vendas não somente sinalizam a adoção dos NFTs, mas também põe em pauta a presença institucional no processo de comercialização de NFTs, o que em última instância promove sua seriedade e utilidade.

2.3.1. Consumo de energia

Com o crescente número de pessoas interessadas em NFTs, particularmente inclinadas pela promessa de lucros exorbitantes, somado ao fato de Ethereum ser uma rede de alta capitalização de mercado, e portanto de maior confiabilidade, houve um crescimento vertiginoso no número de transações na rede Ethereum entre 2019–2022. Com um maior número de transações, mas com a mesma capacidade de processamento de blocos de outrora, a rede tornou-se congestionada, que por consequência fez o preço da transação (gás) aumentar em função da alta demanda. Em outras palavras, havia um número muito maior de pessoas tentando fazer transações do que a cadeia de blocos poderia suportar; a maneira, portanto, de ter sua transação processada seria aumentar o valor pago como uma forma de "suborno" aos mineradores para processar sua transação com maior prioridade na fila de transações. Isso, no entanto, fez com que o gás inviabilizasse o uso da rede para uma parcela dos usuários, já que para ter sua transação processada, frequentemente, era necessário pagar US$10–US$50, como mostrado na Figura 2.4. Pagar este valor para usuários de países subdesenvolvidos é, na maioria dos casos, uma quantia muito alta para apenas processar uma transação, causando uma grave exclusão social e econômica das tecnologias emergentes de cadeia de blocos. Além disso, como a taxa de gás é variável em função do uso da rede, o uso se torna imprevisível e portanto não confiável para determinadas aplicações.

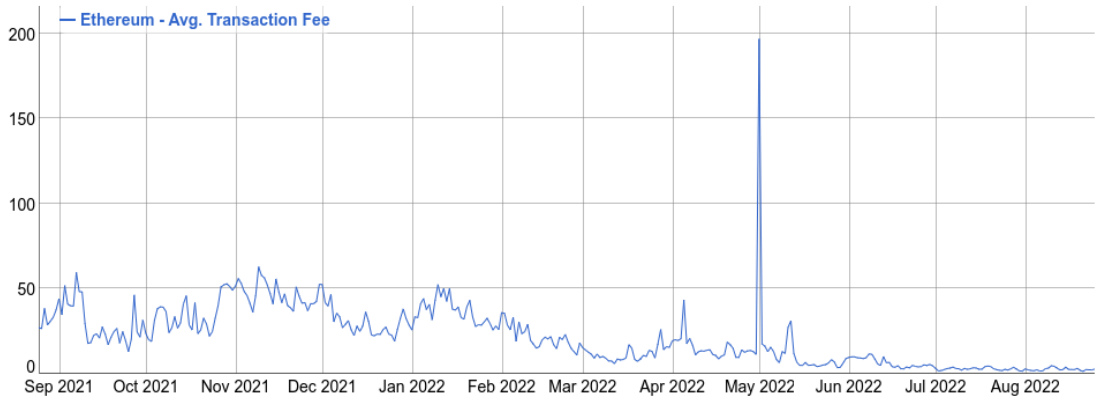


Figura 2.4. Preço de gás médio das transações do Ethereum em US$ de Setembro de 2021 até Agosto de 2022. Fonte: Bitinfocharts.

Ao mesmo tempo que o alto valor de gás dificulta o uso da rede, também propicia maiores recompensas financeiras para os mineradores. Esse maior incentivo resulta em mais pessoas participando da rede de mineração, o que em geral implica no aumento de consumo de energia da rede por meio do maior uso de GPUs — que são utilizadas para minerar criptomoedas cujas redes utilizam o consenso de Prova de Trabalho. Com o recente declínio no valor e uso das criptomoedas, houve uma queda no valor das placas de vídeo da NVIDIA de 50% no mercado secundário [Bloomberg, 2022]. Isso indica uma certa correlação do interesse das pessoas em manter suas GPUs enquanto as recompensas financeiras forem vantajosas ao minerar criptomoeda; ou vendê-las caso contrário.

Em 2018, uma pesquisa comparou o consumo de energia de mineração das redes Bitcoin e Ethereum com o consumo da mineração de metais convencionais como alumínio, cobre, ouro e platina durante o período de 2016 até 2018. Nesse estudo, foi estimado que minerar Bitcoin e Ethereum consomem em média 17 e 7 MJ respectivamente para gerar US$1, enquanto os materiais da mineração convencionais consomem em média 122, 4, 5, e 7 MJ respectivamente para gerar US$1 [Krause e Tolaymat, 2018]. O Bitcoin apenas consome menos energia do que a produção de alumínio. Por outro lado, estima-se que o Bitcoin consumiu a mesma energia que a Angola ou Panamá em 2017 [Krause e Tolaymat, 2018]. Enquanto isso, o Ethereum, que é a principal rede usada para negociação de NFTs, consumiu cerca de 2.4x menos energia do que o Bitcoin para o mesmo período. Em 26 de agosto de 2022, o índice de consumo de energia do Ethereum (*Ethereum Energy Consumption Index*), criado por Alex de Vries, aponta que o consumo de energia anualizado do Ethereum equivale ao consumo de energia do Chile [Digiconomist, 2022]. Ainda segundo o Digiconomist, a emissão de carbono de uma única transação do Ethereum equivale a 251,954 transações financeiras da VISA Inc. ou ao equivalente a 19 mil horas de vídeos assistidos no YouTube [Digiconomist, 2022]. O gráfico do consumo anualizado do Ethereum pode ser visto na Figura 2.5. Ademais, a taxa de *hash* das redes estão em tendência de alta, o que implica na necessidade cada vez maior de poder de processamento para a mineração, e portanto, maior consumo de energia com o passar do tempo [Krause e Tolaymat, 2018].

Com efeito, o problema do alto valor de gás aliado ao grande consumo de energia proporcionado pelo mecanismo de consenso Prova de Trabalho transformou o Ethereum

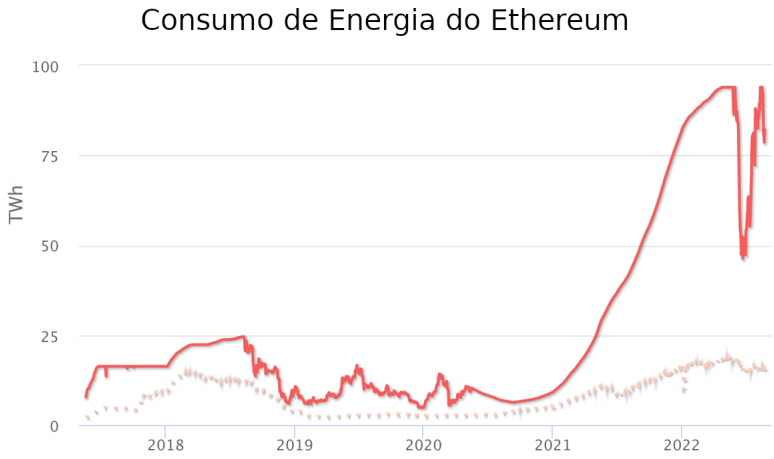


Figura 2.5. Índice de consumo de energia do Ethereum. O eixo vertical representa o consumo em TWh por ano. A linha pontilhada representa o mínimo de consumo em TWh por ano. A linha não pontilhada representa a estimativa. Adaptado de [Digiconomist, 2022].

em um grande vilão. O consumo de energia, e por consequência a emissão de carbono, é um tema que é frequentemente discutido ao falar sobre cadeias de blocos ou NFTs. O Ethereum ainda é a referência principal para emissão e negociação de NFTs. No entanto, o Ethereum, no momento de escrita deste texto, ainda é regido pelo mecanismo de consenso Prova de Trabalho. A promessa de que o Ethereum irá se tornar Prova de Participação com a atualização chamada "*The Merge*" implicaria numa redução de 99,95% do consumo de energia de toda a rede [Ethereum.org, 2022]. Mas enquanto essa solução ainda não é efetivamente implementada na rede principal do Ethereum, outras cadeias de blocos que já adotaram a Prova de Participação se movimentaram para criar seus próprios padrões de NFT, alegando serem amigáveis ao meio ambiente com o *slogan* "*green NFTs*". Este foi o caso da rede Tezos, uma cadeia de blocos que implementa a Prova de Participação, cujo padrão para NFTs é intitulado de FA2[10] e implementado como um contrato inteligente. Diferentemente do Ethereum, o FA2 é capaz de operar sobre uma miríade de tipos de *tokens*: *multi-tokens*, *tokens* fungíveis, e *tokens* não fungíveis. O consumo de energia da rede Tezos anualizado é estimado em 0.001 TWh [Tezos Foundation, 2022], tornando-se uma alternativa mais ecologicamente sustentável para o uso de NFTs com baixas taxas de transação. A rede Solana também se demonstrou eficiente em termos de uso de energia, consumindo apenas 2,707 J por transação (em comparação, uma única busca no Google consome cerca de 1,080 J [Solana, 2022]). O consumo de energia anualizado do Solana está estimado em 0.01105 TWh [Flow, 2022b]. Além disso, Solana também possui um padrão definido para *multi-tokens*, *tokens* fungíveis e não fungíveis implementados via contratos inteligentes. Uma outra rede em que as transações também possuem baixo custo e baixo consumo de energia é a rede Flow, originalmente concebida pelos mesmos criadores de CryptoKitties [Flow, 2022a]. O consumo anualizado da rede Flow está estimado em 0.00018 TWh [Flow, 2022b], ou seja, uma única busca no Google é equivalente à emissão de 12.5 NFTs no Flow.

[10]https://gitlab.com/tezos/tzip/-/blob/master/proposals/tzip-12/tzip-12.md

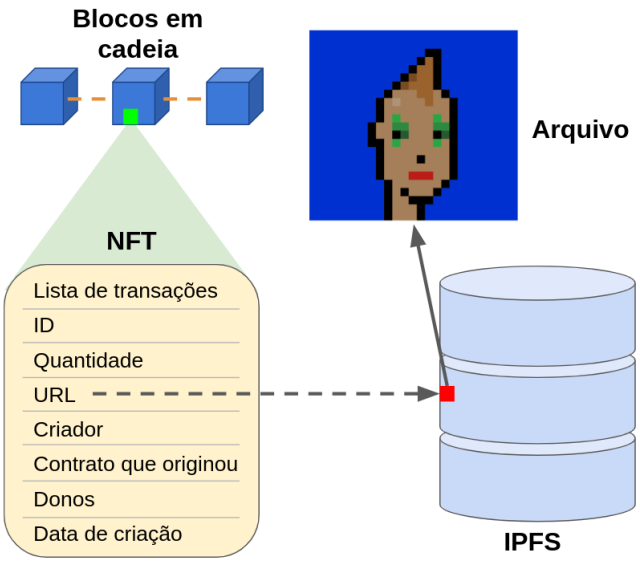


Figura 2.6. Esquema genérico do conteúdo do NFT armazenado na cadeia (url, id, quantidade, etc.) vs. o conteúdo armazenado fora da cadeia — o documento digital em si.

Embora as redes que implementam um mecanismo de consenso mais ecologicamente sustentável sejam uma boa solução para o consumo de energia e para a emissão de carbono, ainda resta um problema a ser discutido. Em linhas gerais, os NFTs armazenam metadados associados ao dado digital em questão, mas o arquivo digital não é salvo na rede de blocos. Isso ocorre em função do alto custo para armazenar até um dado muito pequeno na rede; por exemplo, no Ethereum, em julho de 2020, armazenar apenas 1 MB de dados custava mais de US$ 13,000 em taxas [Valeonti et al., 2021]. Para tanto, é necessário salvar o arquivo digital fora da cadeia de blocos em algum serviço de armazenamento, que poderia ser, por exemplo, o *InterPlanetary File System* (IPFS), ou um serviço próprio de armazenamento — frequentemente centralizado. Na prática, o NFT terá apenas uma referência (link) para o dado salvo no serviço de armazenamento escolhido. Como exemplo, alguns dos possíveis dados salvos na cadeia de blocos podem ser observados na Figura 2.6, como a URL que irá apontar para o conteúdo digital fora da cadeia; o número de edições (quantidade) que o NFT possui; o registro de todos, e quem, transferiu este NFT; os donos do NFT; a sua data de criação; o contrato cujo NFT foi emitido — aquele que rege seu comportamento; quem é o criador deste NFT, e mais outras possíveis informações a depender da cadeia de blocos ou do padrão adotado.

Embora aparentemente desprezível, o consumo de energia e a emissão de carbono associados ao uso de uma tecnologia fora da cadeia não deve ser desprezado. Para o caso de aplicações de uso prático com grandes emissões de NFTs, o armazenamento pode se tornar um grande consumidor de energia sobretudo em situações de alta escalabilidade. Além disso, o armazenamento do conteúdo digital em uma plataforma terceirizada levanta questionamentos sobre o quão descentralizado os NFTs realmente são. Por um lado, o IPFS seria a alternativa mais descentralizada, que no entanto não garante a disponibilidade do dado; por outro lado, um servidor de armazenamento pago pelo criador do NFT pode deixar de disponibilizar o dado assim que o pagamento do serviço for suspenso.

Com efeito, surgiram outras cadeias de blocos que são especializadas em armazenar os dados que, em tese, ficariam fora da cadeia original. Dessa forma, tornou-se possível armazenar o dado do NFT de uma cadeia em outra cadeia, garantindo uma maior capacidade de descentralização. O Filecoin é uma cadeia cujo propósito é fornecer uma rede de operadores que compartilham e armazenam os conteúdos requisitados pelos usuários por incentivo financeiro — a criptomoeda $FIL [Filecoin, 2022]. O Filecoin é orquestrado em cima da tecnologia do IPFS, com a exceção que no IPFS não há incentivo financeiro. Por outro lado, também existe a possibilidade de fazer cálculos computacionais fora da cadeia e acessar dados do mundo real de maneira segura por meio da cadeia Chainlink, que também oferece incentivos financeiros aos participantes [Chainlink, 2022a]. Contudo, o uso dessas cadeias em paralelo também deve ser incluído no cálculo do consumo de energia e de emissão de carbono.

2.3.2. NFTs, armazenamento e portabilidade

Uma situação particularmente interessante de casos de uso de NFTs é a reusabilidade no contexto de descentralização. O NFT emitido por uma aplicação reside na cadeia independentemente da existência da aplicação. No contexto em que a aplicação deixe de existir por motivos diversos, o NFT pode ser utilizado em outras aplicações que sejam compatíveis, ou desenvolvidas para serem compatíveis. Por outro lado, a aplicação que uma vez já existiu poderia ser recriada pela comunidade — um exemplo dos benefícios de código aberto, sobretudo em contextos de redes de blocos. Mais recentemente, o criador do *marketplace* Hic et Nunc[11] descontinuou o desenvolvimento da plataforma, delegando o código para a comunidade de desenvolvedores. A comunidade se reuniu e criou um sistema DAO para controlar a governança da plataforma de maneira livre e aberta entre os membros da comunidade. O resultado pode ser diretamente observado pelo relançamento da plataforma sob o nome Teia[12]. Embora o Hic et Nunc tenha deixado de existir por um breve período, a posse dos NFTs ainda pertenciam às pessoas que inicialmente os compraram ou emitiram. Contudo, o armazenamento da mídia digital, em geral, é controlado pela plataforma de negociação em que o artista originalmente emitiu o NFT. Isto é, a plataforma de negociação de NFTs é frequentemente responsável por pagar o serviço de armazenamento das artes criadas na mesma, que, em geral, são subsidiadas pelos *royalties* cobrados pela plataforma. No entanto, quando o desenvolvimento da plataforma é descontinuado, fica a critério dos usuários — compradores ou artistas e desenvolvedores — de manterem o conteúdo digital persistido. Isso ocorre pois a disponibilidade do conteúdo digital, que é normalmente armazenado no IPFS, depende da existência de pelo menos uma máquina na rede IPFS que armazene o conteúdo. Existem serviços pagos que garantem, com certa probabilidade, a persistência do conteúdo no IPFS. Embora o conteúdo possa não estar disponível, o IPFS garante o armazenamento da impressão digital (do inglês, *fingerprint*) do conteúdo; isso permite que o conteúdo, embora não persistido, possa eventualmente ser religado à rede, como evidenciado pela seta na Figura 2.6.

A maneira que o conteúdo digital é armazenado levanta diversos questionamentos. Em primeiro lugar, é possível criar um NFT com o mesmo conteúdo digital de um outro NFT já existente. Neste cenário, o que diferenciará um NFT do outro serão os metadados

[11] Aplicação descentralizada da rede de bloco Tezos.

[12] `https://teia.art/`

associados ao NFT, sobretudo o endereço de quem o criou, como mostrado na Figura 2.6. Um "NFT falso" terá o endereço do criador falso, que em geral aponta para o mesmo conteúdo digital armazenado no IPFS que o NFT original. Com efeito, usuários são regularmente vítimas de golpes (também conhecidos como *scam*), onde os perpetradores criam NFTs fraudulentos ao copiar as artes de artistas famosos. De maneira semelhante, os NFTs que residem em redes de blocos diferentes mas que apontam para o mesmo conteúdo digital também são outra forma de cópia fraudulenta. Ademais, é trabalho dos colecionadores (ou usuários) verificar os direitos autorais da obra que eles se propõem a negociar. Portanto, os usuários devem estar atentos à proveniência do NFT antes de negociá-lo.

Além disso, um outro problema se cria com relação à posse e propriedade do NFT. Ao alugar um apartamento, o locatário tem a posse mas não a propriedade do apartamento — de exclusividade do locador. Caso um bem seja roubado, é senso comum que a propriedade ainda seja daquele que foi roubado, embora o perpetrador tenha a posse do bem. No caso dos NFTs, não existe distinção — para a maioria das cadeias de blocos, sobretudo para o Ethereum — entre posse e propriedade. Isso implica que, ao roubar um NFT, o perpetrador tem automaticamente a posse e propriedade do NFT, o que dificulta o processo de reversão do crime.

No entanto, como já discutido anteriormente, a característica de posse e propriedade garante que o NFT possa ser utilizado por uma aplicação, ou até mesmo reutilizado em outra aplicação. Ao passo que esta portabilidade constitui um potencial de interoperabilidade, ela também é de difícil execução. Por exemplo, o modelo 3D de um personagem confere uma série de dificuldades para proporcionar a portabilidade. Uma simples mudança de motor de jogos que leia os eixos X, Y ou Z diferentemente de quem emitiu o NFT já resulta em incompatibilidade. Podemos ainda mencionar as texturas e *shaders* que irão depender dos formatos das entradas, saídas, parâmetros e *buffers*, o que dificulta ainda mais a portabilidade. Por outro lado, existem projetos inovadores que propõem o uso de um conteúdo simples e genérico que pode ser utilizado e projetado de diferentes formas em diferentes aplicações (ou jogos). Nesse cenário, Loot[13] propõe o uso de NFTs que representam equipamentos para aventureiros em um jogo — qualquer jogo que implemente as diretrizes do NFT. O projeto propositalmente omite quaisquer outras informações com a intenção de promover a criação de jogos que façam implementações individualizadas e inovadoras com poucas diretrizes, como apenas fornecer os nomes dos equipamentos. Cabe destaque, que, dentro do contexto de aplicações de energia e de cidades inteligentes, muito pouco foi discutido sobre interoperabilidade dos NFTs entre diferentes plataformas, muito embora esse seja um dos problemas em aberto para pesquisa.

Embora os NFTs forneçam uma série de benefícios, ainda pode-se dizer que é uma tecnologia incipiente. Como todo avanço tecnológico na história da humanidade, o produto pode ser utilizado de maneira eticamente questionável. Com NFTs, isso não é diferente. Contudo, num contexto de colaboração mundial, independente e de código aberto, acredita-se que o desenvolvimento da tecnologia de criptomoedas e NFTs andará a passos largos para evitar os diversos problemas existentes atualmente. As tecnologias de bancos e comércios digitais também tiveram seu período de fricção em suas primeiras

[13] `https://www.lootproject.com/`

versões, cujos problemas de segurança geraram centenas de fraudes. Ainda assim, os benefícios de tais tecnologias eram tão evidentes que a segurança da informação evoluiu para assegurar o uso dessas aplicações. Assim, é forte a possibilidade que a evolução da tecnologia de cadeias de blocos pode levar a uma adoção em massa da tecnologia. Nesse contexto, a próxima seção mostra como aplicações comerciais estão gerando receita e demanda a partir de ideias inovadoras.

2.4. Aplicações comerciais de destaque baseadas em NFT

Os NFTs ganharam muita atenção das pessoas, em particular da indústria financeira, entre 2020 e 2021, sobretudo com vendas de artes digitais como NFTs de alto valor. Diferentemente, outras formas de NFT também podem ser comercializadas, como música digital (Doja Cat), conteúdo de jogos digitais (CryptoKitties, Axie Infinity), ou ainda para bem-estar, como um aplicativo cujo objetivo é encorajar as pessoas a correr com incentivo financeiro (STEPN). Essa seção demonstra como a identificação inequívoca de um bem não fungível na cadeia de blocos pode ser utilizada em diversos cenários da indústria para fomentar a descentralização e prosperar aplicações da chamada Web 3.0.

2.4.1. Aplicações em jogos digitais

O NFT possui grande potencial para a indústria de jogos digitais. Atualmente existem cripto jogos como Axie Infinity[14], Stepn[15], [16], Gods Unchained[17], TradeStars[18] e Decentraland[19]. Nesses jogos, o jogador pode colecionar, negociar e fazer reprodução de criaturas digitais.

No jogo Axie Infinity, o jogador coleta criaturas chamadas de Axies. Com essas criaturas, o jogador pode realizar batalhas, criar e construir reinos para os Axies. Além disso, o jogador pode reproduzir seus Axies e criar espécies. Semelhantes ao Axie Infinity, no jogo CryptoKitties, o jogador compra um gato disponível no catálogo e esse gato será guardado em sua carteira. A comercialização dos gatos no jogo é feita através da criptomoeda Ethereum e alguma plataforma de negociação que opere com o EIP-721. Em posse dos gatos, o jogador pode reproduzir, selecionando dois de seus gatos, ou utilizar um genitor público para a reprodução. A Figura 2.7 mostra alguns CryptoKitties colecionáveis.

Já o jogo Gods Unchained é um jogo de cartas tático, onde o jogador tem a propriedade de seus itens do jogo, possibilitando a negociação desses itens em plataformas de negociação de NFT. O jogo possui sua própria criptomoeda chamada $GODS para negociação de itens.

A proposta do Stepn é manter as pessoas em movimento. Foi o primeiro projeto que implementou com sucesso o conceito de movimente-se para ganhar. Os jogadores que caminham ou correm ao ar livre, ganham a criptomoeda do jogo, chamada de $GMT,

[14]https://axieinfinity.com/
[15]https://stepn.com/
[16]https://www.cryptokitties.co/
[17]https://godsunchained.com/
[18]https://tradestars.app/
[19]https://decentraland.org/

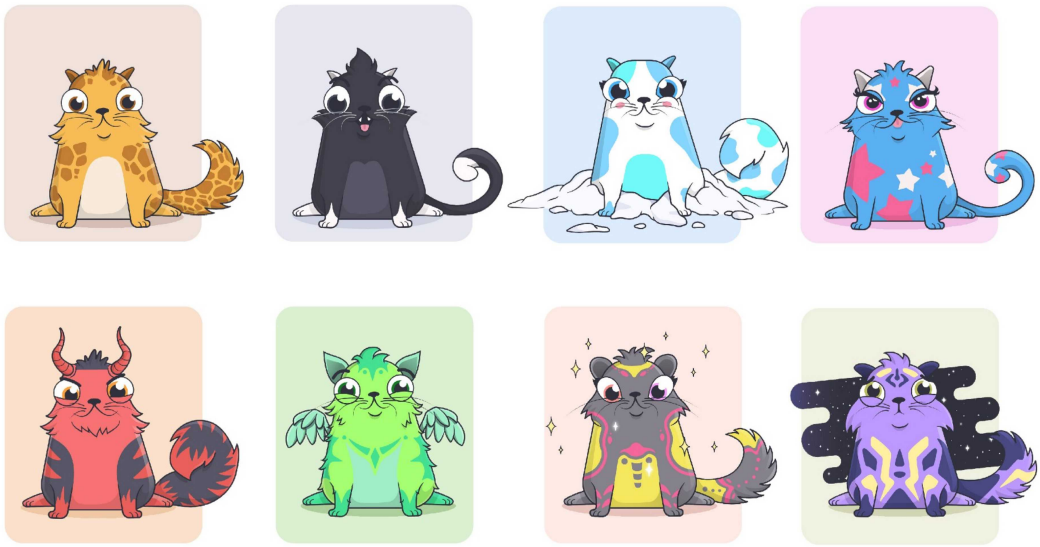


Figura 2.7. Em CryptoKitties é possível procriar novas raças de gatos.

que pode ser usada no próprio jogo ou vendida para obter lucro em moedas fiduciárias. A moeda do jogo é utilizada como mecanismo de controle da própria economia do jogo. Para participar, é preciso comprar um tênis — que é um NFT — apto a registrar seus passos, o qual é vendido pelos criadores.

O TradeStart é jogo social descentralizado onde o conhecimento dos jogadores sobre esporte é avaliado. O jogo utiliza estatísticas reais do mundo do esporte. A plataforma do jogo não é controlada por uma organização individual. A plataforma foi construída utilizando cadeia de blocos, logo, nenhum agente do jogo pode modificar as regras do jogo, os valores dos ativos ou impedir que um jogador acesse a plataforma.

O Decentraland é um jogo estilo Sandbox, onde os jogadores são livres para modificar e explorar o mundo virtual. O jogo é governado por uma organização autônoma descentralizada e foi desenvolvido na cadeia de blocos do Ethereum. O diferencial do Decentraland é que os jogadores podem ser "donos" de suas terras. O jogo também possui sua própria criptomoeda chamada de $MANA. Os ativos e terras dentro do jogo são negociadas utilizando a $MANA. O Decentraland foi um dos primeiros metaversos descentralizados que foi construído, governado por meio da participação de seus usuários.

O metaverso é um espaço compartilhado virtual coletivo que permite todos os tipos de atividades digitais. Geralmente, abrange um conjunto de técnicas como a realidade aumentada e a internet para estabelecer o mundo virtual. O conceito vem das últimas décadas e tem um grande progresso com o desenvolvimento da cadeia de blocos. A cadeia de blocos fornece um ambiente descentralizado ideal para o mundo virtual online. Os participantes dessas realidades alternativas conectadas pela cadeia de blocos podem ter muitos tipos de casos de uso intrigantes, como desfrutar de jogos, exibir artes feitas por eles mesmos, negociar ativos e propriedades virtuais, como, por exemplo artes, terras, vídeos e vestimentas. Além disso, os usuários também têm oportunidades de obter lucros

com a economia virtual. Além do Decentraland, existem outros metaversos que utilizam cadeia de blocos, como, por exemplo, [20], Somnium Space[21], MegaCryptoPolis[22] e Sandbox[23]. A descentralização nesses espaços virtuais é imprescindível para que não haja um monopólio financeiro e político que domina e controla todos os participantes, como ocorre com as grandes empresas de tecnologia atualmente.

2.4.2. Aplicações em produções artísticas e culturais

Além dos jogos, existem também os cripto colecionáveis como Meebit[24] e CryptoPunks[25]. Os CryptoPunks foi classificado pela OpenSea[26] como a maior coleção de NFT de todos os tempos por volume de negociação (2,2 bilhões de dólares). Os CryptoPunks são dez mil figuras únicas em pixel art. As figuras foram geradas aleatoriamente através de um algoritmo. Por mais que alguns CryptoPunks compartilhem algumas características, nenhum compartilha todas as características de outro. Já os Meebit, são modelos 3D estilo voxel. Existem 20 mil Meebits, onde aproximadamente 11 mil foram distribuídos gratuitamente para donos de CryptoPunks.

O comércio de produções artísticas e colecionáveis pode ser potencializado com NFT. Tradicionalmente, os artistas possuem poucos canais para exibir seus trabalhos. Os preços não refletem o verdadeiro valor das obras devido à falta de recursos. Além do mais, plataformas e anúncios cobram seus trabalhos publicados nas redes sociais com taxas intermediárias. Os NFTs transformam esses trabalhos em formatos digitais com identidades integradas. Os artistas não precisam transferir a propriedade e o conteúdo para os agentes. Isso lhes dá impulso com muitos lucros. Exemplos típicos incluem o REPLICATOR de Mad Dog Jones [27] (vendido por 4,1 milhões de dólares), os trabalhos de Grimes [28] (movimentando, no total, cerca de 6 milhões de dólares) e outros como o Trevor Jones. Além disso, por meios tradicionais, os artistas em geral não recebem royalties de vendas futuras de suas obras; ou quando recebem, o depósito ocorre semestralmente, trimestralmente, ou até anualmente. Em contraste, os NFTs podem ser programados para que o artista receba uma taxa de royalties predeterminada toda vez que sua obra de arte digital for negociada. Sendo assim, uma maneira eficiente de gerenciar, proteger e negociar obras-primas digitais. Além disso, várias plataformas como Mintbase[29] e Mintable[30] estabeleceram ferramentas para apoiar pessoas comuns a criar seus próprios trabalhos NFT de modo facilitado. A Figura 2.8 mostra alguns CryptoPunks e um Meebit.

[20] https://www.voxels.com/
[21] https://somniumspace.com/
[22] https://mcp3d.com/
[23] https://www.sandbox.game/en/
[24] https://meebits.app/
[25] https://www.larvalabs.com/cryptopunks
[26] Plataforma de negociação de NFTs online sediada em Nova Iorque.
[27] https://www.phillips.com/detail/mad-dog-jone
[28] https://www.theverge.com/2021/3/1/22308075/grimes-nft-6-million-sales-nifty-gateway-warnymph
[29] https://www.mintbase.io/
[30] https://mintable.app/

(a) CryptoPunks.

(b) Meebit.

Figura 2.8. Os CryptoPunks e Meebits foram criados aleatoriamente por um algoritmo na Larva Labs.

2.4.3. Certificados e *tickets* de eventos

Eventos tradicionais contam com empresas centralizadas que são provedores do meio tecnológico. Embora a cadeia de blocos esteja presente em diversos tipos de atividades, como arrecadação monetária, suas aplicações ainda são restritas a uma pequena gama de eventos. Os NFTs estendem o escopo das aplicações de cadeia de blocos com a ajuda de suas propriedades adicionais (*e.g.*, singularidade, propriedade, liquidez). Isso permite que cada indivíduo se vincule a um evento específico, assim como os padrões em nossa vida real. Ao comprar ingressos para eventos de maneira tradicional, o consumidor deve confiar em terceiros. Portanto, existe o risco da compra de bilhetes fraudulentos ou inválidos, que podem ser falsificados ou cancelados. O mesmo ingresso pode ser vendido múltiplas vezes ou obtido através de imagens de ingressos publicados online.

Um ingresso baseado em NFT representa um ingresso emitido pela cadeia de blocos para demonstrar o direito de acesso a qualquer evento, como cultura ou esportes. Um bilhete baseado em NFT é único e escasso, que embora possa ser revendido, é possível limitar sua negociação via contratos inteligentes, caso seja assim desejado. O contrato inteligente baseado em cadeia de blocos fornece uma plataforma transparente de negociação de ingressos para as partes interessadas. Os consumidores podem comprar e vender o bilhete criptográfico do contrato inteligente em vez de depender de terceiros de maneira eficiente e confiável.

Empresas como Oveit e Seatlab comercializam ingressos baseados em NFT para eventos. A Oveit fornece também um produto chamado *Ticket Addons*, onde qualquer ticket sobre um evento pode ser centralizado em um único lugar. Por exemplo, o cliente pode comprar o *ticket* do evento, as bebidas que serão consumidas, camisetas e outro souvenir, com todos esses itens registrados como *tickets*, centralizados no aplicativo do evento. Assim, o cliente pode ir ao evento apenas com o celular, evitando perda de seus pertences.

2.4.4. Aplicações de saúde

O NFT também possui um grande potencial para aplicações da saúde [Musamih et al., 2022]. Uma aplicação potencial é o uso do NFT para cunhar informações de pacientes. Em aplicações tradicionais um paciente deixa suas informações clínicas com o hospital ou uma clínica. O hospital pode vender esses dados genéticos a terceiros para fins de pesquisa. No entanto, ao vender esses dados a empresa pode ganhar muito dinheiro que nunca será compartilhado com os donos desses dados. Além disso, à medida que esses dados confidenciais são transmitidos ao longo de uma cadeia de transações, o risco de manuseio incorreto das informações aumenta. Agora, se esses dados são cunhados como NFTs, a informação virá com uma característica inerente a ser rastreada. O paciente seria capaz de ver onde o dado foi utilizado e responsabilizar aqueles que o usaram sem sua permissão, pois é o único proprietário dos dados. Além disso, o proprietário do NFT pode habilitar um recurso para ganhar dinheiro sempre que ocorrer uma transação com os dados.

Com uma abordagem NFT, as empresas podem oferecer serviços de saúde digital incentivando os pacientes a participar de estudos contribuindo com seus dados e ganhando com eles. Outros terceiros interessados em utilizar os dados para pesquisa ou desenvolvimento de novos produtos podem entrar em contato diretamente com os pacientes em uma plataforma digital. A principal diferença em comparação com a abordagem tradicional é que os pacientes realmente têm a opção de compartilhar seus dados de maneira transparente.

Embora muito sobre NFT na área da saúde ainda seja especulativo neste momento, existem algumas empresas que estão explorando esse potencial. Uma dessas empresas é a Aimedis, que possui um mercado NFT médico onde os pacientes podem participar de transações envolvendo seus dados de saúde. O aplicativo de monitoramento de saúde Go!, desenvolvido pela Enjin e Health Hero, pode coletar dados individuais de atividades e bem-estar de aplicativos populares como Apple Health, Google Fit e Fitbit. Estes podem até ser negociados no mercado aberto.

No entanto, existem diversos potenciais obstáculos para a adoção em massa da tecnologia de NFTs, especialmente na área da saúde. Tal como está, a tecnologia NFT atualmente funciona de forma bastante ineficiente, com grandes quantidades de energia necessárias para pequenas transações. Como tal, os NFTs podem não ser comercialmente viáveis em um futuro próximo. Mas alternativas para a cunhagem de NFT estão em andamento e podem usar uma fração do poder de computação atualmente envolvido em suas transações. Outro ponto é a falta de interesse na adoção do NFT pelas empresas que oferecem serviços de saúde digital. Essas empresas podem não ser particularmente atraídos pela ideia de compartilhar seus lucros com os pacientes, de quem tradicionalmente lucram e não o contrário.

2.5. Aplicações do NFT em mobilidade elétrica e tarifação

Embora o uso mais amplamente difundido dos NFTs seja destinado a jogos e obras de arte, vislumbra-se, atualmente, que essa tecnologia tem grandes potenciais para aumentar a segurança das aplicações de energia e de cidades inteligentes baseadas em cadeias de blocos. Os NFTs auxiliam na gestão de identidade e no controle seguro e transparente

de uso de créditos. A seguir, são apresentadas algumas das principais aplicações de NFTs dentro do contexto de mobilidade elétrica e tarifação.

2.5.1. Gestão de identidade de veículos e estações de recarga

A mobilidade elétrica depende fortemente do uso deveículos elétricos e da geração distribuída [Lopes et al., 2015] em estações de recarga. Nesse sentido, para fins de criação de contratos inteligentes e registros de dados nas cadeias de blocos, há a necessidade da associação de uma identidade de forma inequívoca a um objeto dentro da cadeia. Para esse fim, vem-se utilizando os *Identity Non-Fungible Token*s (I-NFTs), que permitem a utilização de componentes criptográficos e operações protegidas para dar suporte aos ativos da rede em todas as etapas da atividade [Gourisetti et al., 2021].

Um I-NFT consiste de um registro NFT que visa armazenar dados sobre a identidade de uma pessoa, um dispositivo ou uma entidade do sistema. Esse NFT é, então, utilizado em contratos inteligentes como forma de identificar a origem do pedido. A posse da chave criptográfica associada ao NFT já é suficiente para a realização da autenticação. Um ponto interessante para o uso de NFTs para esse tipo de processo é manter as informações pessoais fora da cadeia de blocos, mas autenticáveis pelo uso da cadeia. Gourisetti *et al.* sugerem a criação de I-NFTs a cada transação, a fim de evitar que o usuário ou o dispositivo possam ser rastreados ao longo de suas atividades por quem tem acesso aos blocos da cadeia [Gourisetti et al., 2021].

Arcenegui *et al.* generalizam os I-NFTs para a autenticação de dispositivos. Os autores colocam a necessidade de associar a identidade virtual ao dispositivo de forma inequívoca. Assim, os autores propõem o uso de *Physical Unclonable Function*s (PUFs), que é um método que permite a associação difícil de quebrar entre *tokens* e dispositivos. Dessa forma, os registros e tokens relacionados ao dipositivo passam a poder ser rastreados durante a vida útil do dispositivo, permitindo, entre outros, o registro autenticado e seguro de mudanças de propriedade [Arcenegui et al., 2021]. A proposta vai além da representação do dispositivo *Internet of Things* (IoT) na cadeia de blocos, contemplando também sua interação com outros endereços na cadeia de blocos, sejam esses endereços associados a pessoas, organizações ou outros dispositivos IoT. O dispositivo IoT passa a ser capaz de receber e prover informações e assinar transações. Carros, semáforos, câmeras e quaisquer elementos que devam participar da reconstrução digital do sistema físico de forma a manter sua fidedignidade podem ser representados por seus NFTs e as interações entre esses componentes do sistema de transporte podem ser realizadas por meio de contratos inteligentes executados na cadeia de blocos.

Gao *et al.* citam algumas formas de se implementar uma PUF. Uma delas, particularmente interessante para implementação em sistemas embarcados, baseia-se no projeto de *chipsets* de memória RAM estática [Gao et al., 2020]. Essas possibilidades remontam ao conceito de NFTs inteligentes mencionados por Arcenegui *et al.* [Arcenegui et al., 2021], no qual o NFT é fisicamente interligado ao seu dispositivo IoT respectivo graças ao PUF.

Outros trabalhos também ressaltam a necessidade da identificação segura dos dispositivos na cadeia de blocos [Karger et al., 2021]. Yuan e Wang tratam diretamente a gestão de identificadores de veículos elétricos, propondo um modelo conceitual organi-

zado em camadas para *Sistema de Transporte Inteligente*s (STIs) baseados em cadeias de blocos. O modelo contém uma camada física composta por entidades tais como veículos, câmeras, semáforos e demais componentes da malha de transportes [Yuan e Wang, 2016].

Uma aplicação mais objetiva das cadeias de blocos em sistemas de transportes pode ser encontrada em [Zhang e Wang, 2019]. Nesse trabalho, os autores trazem conceitos de *Vehicular Ad Hoc Network*s (VANETs) e as associam a cadeias de blocos com o intuito de realizar o controle inteligente do tempo de luz verde dos semáforos a partir das condições de trânsito. Para tal, é necessário que os veículos sejam equipados com *Unidade de Bordo*s (UBs) e que as estradas tenham *Unidade de Acostamento*s (UAs) espalhadas. As UBs, as UAs e o departamento de trânsito ingressam na cadeia de blocos. As UAs se comunicam com as UBs dos veículos e registram dados criptografados relativos às condições de trânsito na cadeia de blocos. O departamento de trânsito, por sua vez, recolhe, descriptografa e analisa as informações de tráfego registradas na cadeia de blocos e dispara a execução de contratos inteligentes que regulam a duração do tempo de luz verde dos semáforos de forma dinâmica. A representação dos componentes do sistema de trânsito como NFTs na cadeia de blocos também se faz coerente se aplicada neste trabalho. O autor de [Zhang e Wang, 2019] propõe, ainda, que o departamento de trânsito conceda recompensas por veículos "honestos", que fornecem informações precisas quanto à sua localização, e exponha na rede informações de veículos maliciosos. Os incentivos podem se concretizar na forma de certificados digitais únicos que, por sua vez, também podem ser implementados por meio de um NFT associado ao NFT do veículo, atestando que tal veículo fornece informações corretas.

Indo além das propostas de [Zhang e Wang, 2019], é possível, ainda, que as VANETs registrem na cadeia de blocos infrações cometidas por veículos, tais como exceder um limite de velocidade ou cruzar um semáforo fechado, na forma de NFTs. O NFTs da infração, embora não seja físico como o veículo ou o semáforo, é uma indicação de que a violação foi cometida e pode ser associada a um veículo, um semáforo, uma câmera de monitoramento e até mesmo a um vídeo documentando a ocorrência.

2.5.2. Gestão segura de créditos de carbono

Outras atividades importantes dizem respeito à geração de *tokens* de **créditos de carbono** a serem negociados entre entidades que promovam a redução de emissão de gases do efeito estufa e empresas poluidoras. Para essas aplicações, é possível o uso de sistemas baseados em NFT ou ainda, híbridos, mesclando NFT e *Fungible Token* (FT) [Karandikar et al., 2021].

2.5.2.1. Créditos de carbono

O crédito de carbono foi criado dentro do contexto do Protocolo de Kyoto, visando reduzir as emissões de gases que aumentam o efeito estufa. A pegada de carbono de um indivíduo ou uma empresa é o total de gases do efeito estufa geradas por todas as suas atividades. Dentro dos protocolos internacionais contra o aquecimento global, as empresas devem reduzir ou compensar a sua pegada de carbono. As reduções e compensações são medidas como crédito de carbono. Portanto, o crédito de carbono é a moeda utilizada no

mercado de carbono, sendo equivalente a uma tonelada de dióxido de carbono ou gases equivalentes. Nesse contexto, empresas que possuem um nível de emissão de gases que causam o efeito estufa muito alto e poucas opções para a redução da emissão desses gases devem optar pela compra de créditos de carbono para compensar suas emissões, conforme mostrado na Figura 2.9.

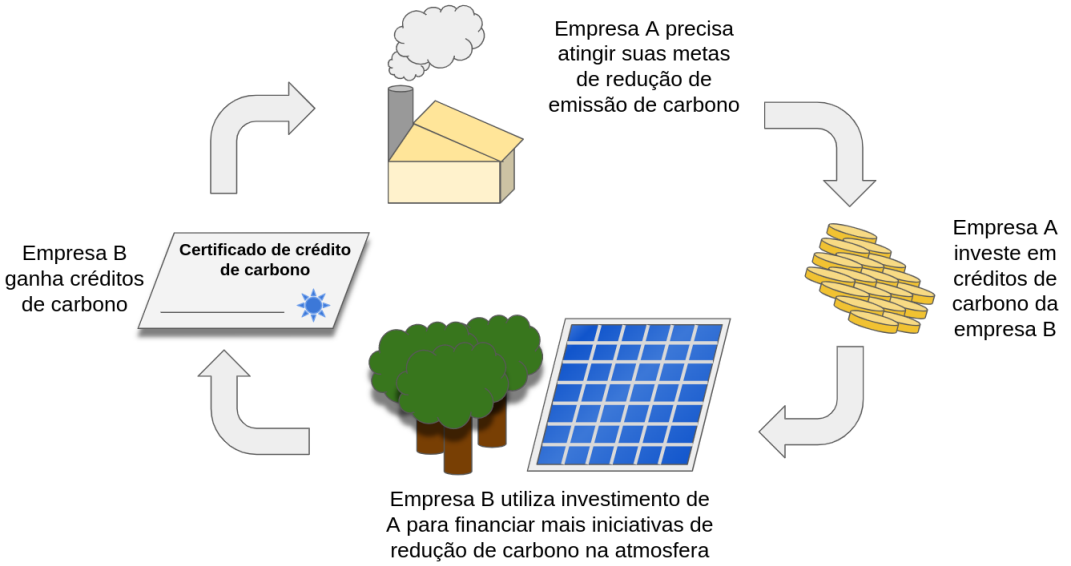


Figura 2.9. Geração e utilização dos créditos de carbono. Adaptado de [Save Planet Earth, 2021].

Existem dois tipos de crédito de carbono: redução de emissões voluntária - *Voluntary Emissions Reduction* (VER) e redução de emissões certificada - *Certified Emissions Reduction* (CER). O VER é aplicável no mercado de créditos voluntário - *Voluntary Carbon Market* (VCM), onde indivíduos ou empresas investem em projetos de redução ou sequestro de carbono de forma voluntária. O CER é emitido por meio de arcabouços regulatórios [Carbon Credits, 2021].

2.5.2.2. NFTs para créditos de carbono

Os mercados de carbono transformam as emissões de CO2 em um ativo ambiental negociável, dando-lhe um preço. Com isso, os Mercados Voluntários de Carbono - VCM - cresceram, atingindo movimentações da ordem US$ 1 bilhão em 2021, com expectativas de crescer 15 vezes até 2030 [Thomason, 2022].

Um crédito de carbono pode ser revendido várias vezes até que seja retirado pelo usuário final que deseja reivindicar o impacto da compensação. Para tanto, é necessário que os registros de créditos de carbono sejam emitidos por verificadores terceirizados, independentes e certificados internacionalmente. As cadeias de bloco e os NFTs entram como a forma de registrar a geração, as transações e o uso do crédito para compensação. Esse tipo de esquema aumenta a transparência e o monitoramento dos créditos de carbono, evita falsas alegações de eficiência energética e uso de créditos ineficazes, além de evitar a dupla contagem dos créditos de carbono devido à falta de protocolos contábeis completos

e alinhamento entre as jurisdições do mercado [Thomason, 2022]. Outra vantagem é a redução de custos em toda a cadeia.

2.5.3. Gestão segura da geração de energia

O aumento no uso de veículos elétricos está diretamente relacionado a impactos na rede elétrica, que deverá passar a suprir a energia necessária para uma atividade que outrora era suprida pela queima direta de combustíveis fósseis. Além do aumento de capacidade nas unidades de consumo e do aumento do fluxo de potência circulando pela rede elétrica para atender essa nova demanda, há de se considerar que, num contexto de popularização da GD, essa carga pode ser parcialmente atendida por uma FER. Ademais, as baterias automotivas conectadas à rede elétrica trazem a possibilidade de armazenar energia, podendo mitigar uma das principais deficiências de geradores eólicos ou fotovoltaicos, que é a intermitência, através do fornecimento *Vehicle to Grid* (V2G) [Gao et al., 2014]. Esse contexto de grandes modificações no sistema traz desafios e oportunidades que podem ser solucionados e explorados por cadeias de blocos, criptomoedas e NFTs.

Em [Li et al., 2020] o autor apresenta um gêmeo digital utilizado para estimar o estado de carga e a degradação de baterias. O gêmeo digital recebe os dados das baterias sob análise por meio de dispositivos IoT e é executado na nuvem, podendo usufruir de uma capacidade de processamento mais alta e executar algoritmos mais sofisticados para realizar suas estimativas. Em contribuições futuras, uma bateria veicular pode ser representada digitalmente por um NFT na cadeia de blocos de forma similar ao trabalho de [Arcenegui et al., 2021], bem como os dispositivos IoT físicos, e a interação entre eles se concretizaria por meio de contratos inteligentes.

Em um contexto de popularização da tecnologia V2G, as representações digitais por meio de NFTs das baterias e dos demais ativos elétricos em uma cadeia de blocos podem participar de uma reconstrução virtual do sistema de potência, garantindo ao operador maior observabilidade sobre o sistema. Dados de operação podem ser coletados e o despacho da geração pode levar em consideração a quantidade de FERs e baterias conectadas dispostas a participar do V2G. Em [Karandikar et al., 2021], o autor descreve um sistema de potência com diversos atores, cada qual com diversas capacidades, representados em uma cadeia de blocos. Tais capacidades variam entre gerenciamento pelo lado da demanda, disponibilidade de bancos de baterias, capacidade de geração a partir de fontes renováveis, dentre outros.

Um sistema de compra e venda de energia entre veículos elétricos baseado em cadeias de blocos foi proposto em [Kang et al., 2017]. Uma das inovações propostas era a figura de nós autorizados a estabelecer o livro-razão distribuído intitulados agregadores locais. A cadeia de blocos baseada nos agregadores locais era capaz de auditar e verificar registros de transações entre os veículos elétricos. Um mecanismo de leilão duplo iterativo maximiza o bem-estar comunitário otimizando o preço da energia e o estado de carga das baterias dos veículos. Neste artigo, são registrados dados, incluindo pseudônimos dos veículos, na cadeia de blocos proposta. O autor desenvolveu a moeda "energy coin" para representar digitalmente um bem utilizado para trocar energia.

Dentro desse contexto de mercado de energias renováveis controladas por cadeias de bloco, existe a tendência dos certificados de energia renovável - *Renewable Energy*

Certificate (REC), criados como *tokens*, por meio de NFTs. Um REC é um contrato único emitido por algum gerador que não emite gás carbônico, o qual é vendido a multinacionais e geradores fósseis. Na forma tradicional de gerenciar os RECs, isso demanda muitos contratos e processos complexos.

O problema associado aos RECs é a natureza dos sistemas elétricos, nos quais não é possível saber de onde a energia que está sendo consumida efetivamente veio, ou ainda, se veio de uma fonte renovável. Para sobrepor esse problema e incentivar a energia renovável, Certificados de Atributo de Energia - *Energy Attribute Certificate*s (EACs) começaram a ser emitidos, permitindo ao consumidor comprar a energia a partir do tipo de geração. Um EAC especifica um megawatt hora de energia produzida em uma determinada localização, marcando também o tipo de tecnologia e o mês de produção. Contudo, os EACs não tem a granularidade temporal ideal para demonstrar as variações na geração de energia renovável, a qual depende da força do vento ou da intensidade do sol. Assim, passou-se a considerar a necessidade de EAC que representam não apenas o mês, mas também o dia e a hora de geração. Esses EAC ou REC são, então, registrados digitalmente em um NFT [Rossi, 2022].

Um exemplo prático de NFTs para energia renovável é provido pela plataforma RESpring[31], que provê EAC com granularidade de hora para criar um mercado de energia renovável imutável e certificável. Outro exemplo é da *Restart Energy Democracy* (RED), que lançou uma plataforma descentralizada de fornecimento de energia para recompensar certificados de energia verde para consumidores de energia renovável. Essa plataforma permite o comércio direto ponto a ponto entre consumidores e fornecedores por meio de RECs em NFTs [RED, 2021]. A REX também criou a REX NFT[32], uma coleção de NFTs para REC, desenvolvida sob a plataforma Polygon, com a moeda REX Coin.

2.5.4. Tarifação dinâmica e tokens de cobrança/premiação

O registro seguro de valores para tarifação dinâmica e para crédito de carbono para diferentes tipos de atividade ao longo do tempo já é possível por meio da associação entre NFT e *Decentralized Finance* (DeFi), permitindo a desassociação entre a criptomoeda e o valor aplicado ao ativo registrado na transação. Essa nova tecnologia, ainda imatura, permite também a criação de *tokens* de cobrança basedos em NFT, que podem permitir diversos tipos de ação em plataformas de negociação de energia, como a criação de *Virtual Power Plant*s (VPPs) [Lopes et al., 2015].

Outro uso interessante é a aplicação de *tokens* para premiar usuários que participam de programas de gerenciamento pelo lado da demanda - *Demand Side Management* (DSM) [Chainlink, 2022b]. Ações de gerenciamento de energia pelo lado da demanda, permitem, entre outros, que determinadas cargas do sistema usuário sejam reduzidas ou desconectadas em momentos em que haja dificuldades em manter o balanço entre geração e demanda a um preço economicamente atrativo. No caso, o NFT gerado e atribuído ao usuário comprova o seu comportamento favorável à redução do consumo de energia, e, consequentemente, registrando a redução da pegada de carbono do usuário. A facilitação da participação de um cliente, em especial, os de grande porte, em progra-

[31] https://www.flexidao.com/respring
[32] https://www.rexcreditnft.io/

mas de gestão pelo lado da demanda é de particular interesse para a concessionária e para o operador do sistema elétrico. Tal carga se torna sensível ao preço da energia, sendo conectada somente em períodos em que haja disponibilidade de uma fonte geradora de energia de baixo custo.

Em [Karandikar et al., 2021], o autor propõe *tokens* fungíveis para representar energia trocada entre pontos do sistema e *tokens* não fungíveis para representar que um cliente foi capaz de: i - participar de uma ação de gestão pelo lado da demanda; ii - estimar sua demanda com precisão; e/ou iii - disponibilizar um de banco de baterias para armazenamento de energia do sistema. Os *tokens* recebidos podem, por sua vez, ser trocados por criptomoedas.

2.6. Desafios e tendências de pesquisa

Dado o grau de inovação que permeia as cadeias de blocos, os contratos inteligentes e os NFTs, é necessário avaliar os resultados obtidos com as primeiras implementações desses conceitos e observar possíveis pontos de aprimoramento. Esta seção discorre sobre os desafios associados a essas tecnologias e projetos de que as utilizam como forma de soluções de pesquisa.

2.6.1. Desafios relacionados ao uso de NFTs

Os principais desafios das aplicações em cadeia de blocos e da tecnologia de NFT dentro do contexto de mobilidade elétrica e cidades inteligentes são descritos nesta seção. Entre os desafios abordados, tem-se questões como o congestionamento da rede e o seu impacto sobre as aplicações, a anonimização e a legislação, os impactos dos ataques, entre outros.

2.6.1.1. Riscos associados aos contratos inteligentes

Apesar de os contratos inteligentes serem amplamente utilizados, eles ainda apresentam diversos desafios em aberto relacionados à privacidade, ataques e ao próprio gasto de energia das principais cadeias de bloco [Medeiros et al., 2019]. Esses riscos ficam ainda mais claros em aplicações de amplo uso dos contratos inteligentes, tais como o DeFi e os NFTs. Com base nas observações sobre os usos nas diversas áreas, é possível discutir algumas questões sobre o uso dos contratos e dos NFTs em sistemas de energia. As aplicações de contratos inteligentes incluem coordenação de carregamento de veículos elétricos inteligentes, resposta automatizada pelo lado da demanda, comércio de energia ponto a ponto e alocação de tarefas de controle entre os operadores de rede [Kirli et al., 2022].

Um dos principais problemas associados aos contratos inteligentes é a existência de códigos maliciosos ou com erros, os quais podem gerar impactos que, nos piores casos, podem levar a uma exaustão dos fundos de um ou mais participantes. Hoje, já existem diversos exemplos desse tipo de problemas em contratos de DeFi e de venda de NFTs, onde os desenvolvedores dos contratos deixaram *backdoors* que permitem a manipulação fraudulenta de *tokens*. Dentro do contexto dos NFTs, existem exemplos de contratos de vendas parciais de NFTs que definem códigos auto-executáveis que especificam que em

novas re-vendas, parte do preço de venda deve ser transferido para o vendedor inicial de forma não explícita, resultando em uma perda para o comprador [Kirli et al., 2022]. Ataques que permitem o vazamento de criptomoedas para entidades não autorizadas durante a execução do contrato inteligente são chamados de Ataques de Vazamento, enquanto que ataques que permitem ao atacante finalizar o contrato quando do seu interesse são chamados de Ataques Suicidas [Liu et al., 2021].

Cabe ressaltar que, até o momento, ainda não existem relatos de fraudes em contratos inteligentes para o sistema elétrico, mas isso se deve ao fato de essas aplicações ainda serem poucas e com pequena escala, além de muitas delas serem executadas em cadeias privadas ao invés de nas cadeias públicas.

Os contratos inteligentes também podem apresentar problemas relacionados à programação. Por exemplo, eventos conhecidos como Desordem de Exceção são caracterizados quando ocorrem problemas no tratamento das exceções. Quando um contrato A chama uma função de um contrato B e, por alguma razão, essa função não está disponível, o comportamento correto do contrato A seria reverter todas as transações já realizadas. Contudo, se existir uma ou mais chamadas de função de baixo nível, tal como *call()* ou *send()*, a reversão das transações para na última chamada de função de baixo nível, deixando todas as chamadas subsequentes sem reversão. Com isso, as transações restantes não serão revertidas, gerando prejuízos para quem chamou o contrato A [Liu et al., 2021]. Outra vulnerabilidade conhecida está relacionada às funções reentrantes. Tais funções podem mudar o estado de um contrato. Contudo, se uma função não reentrante for chamada como uma função reentrante, isso pode levar ao roubo de criptomoedas [Liu et al., 2021]. Um exemplo famoso da ocorrência desse tipo de ataque foi o "The DAO" na rede Ethereum, que permitiu o roubo de mais de 3,64 milhões de unidades de Ether, o equivalente à 45 milhões de dólares na época (2016) [Zhao et al., 2017].

Além da preocupação com padrões de ataques já conhecidos contra os contratos, outro ponto importante, em especial para o contexto das redes elétricas inteligentes e cidades inteligentes, é que se use sistemas de autenticação e autorização fortes. Além disso, os diversos aspectos de segurança tradicionais devem ser considerados, incluindo uma análise detalhada do código do contrato antes da sua disponibilização e uso na cadeia de blocos.

2.6.1.2. Congestionamento da rede e escalabilidade da cadeia de blocos

A escalabilidade é um dos principais problemas atuais para o uso das cadeias mais populares, em especial as que são baseadas em prova de trabalho. Em comparação, uma rede de cartões de crédito consegue processar milhares de transações por segundo, enquanto que as cadeias de bloco mais populares, como o Ethereum e o Bitcoin, são bastante limitadas em quantas transações por segundo podem fazer.

A rede Ethereum cresceu muito rapidamente e se tornou uma das mais importantes cadeias de bloco, tendo importância equivalente ao Bitcoin no mercado. Esse rápido crescimento se deu pela possibilidade de criar contratos inteligentes e também a criação dos NFTs. O aparecimento do DeFi e do NFT criou uma segunda onda de uso do Ethereum, causando congestionamentos na rede e, consequentemente, alta no preço do gás

para uso da rede. Tal crescimento gera problemas de escalabilidade para a rede. Esses problemas são associados a um "trilema", que coloca que não é possível ter descentralização, escalabilidade e segurança simultaneamente [Kiong e Xiang, 2021]. O uso do mecanismo de consenso prova de trabalho garante os requisitos de descentralização e segurança, mas também implica em uma baixa escalabilidade, já que esse tipo de consenso limita o número de transações por segundo (*Transactions per Second* (TPS)).

O trilema da escalabilidade ganhou visibilidade em 2017, quando a aplicação CryptoKitties foi capaz de praticamente congelar o uso da Ethereum em seu primeiro pico de popularidade em vendas de NFTs. Com o rápido aumento do número de requisições de transações, os mineradores ficam sobrecarregados, implicando em filas e no aumento do custo em gás para realizar uma determinada operação. Eventos similares ocorrem com certa frequência com novos lançamentos de NFTs por aplicativos populares, entre outros eventos, fazendo com o que o custo das redes mais populares cresça muito rapidamente.

Entre as soluções para esse problema, estão as chamadas soluções de camada um, soluções de camada dois e a utilização de novos protocolos de consenso tais como Prova de Participação e Tolerância a Falhas Bizantinas, que substituem o ambiente energeticamente caro e pouco amigável do Prova de Trabalho. As soluções de camada um implicam na construção de uma nova cadeia de blocos, visando sobrepujar os desafios encontrados nas cadeias originais, tais como as cadeias Polkadot[33], Solana[34], Cosmos[35], Theta[36], Algorand[37], Fantom[38], Avalanche[39], NEAR[40], TRON[41] e CELO[42]. As soluções de camada dois são construídas sobre a cadeia já existente, como um *overlay*. Outro tipo de solução implica na criação de uma segunda cadeia de blocos que funciona em paralelo com a original, como é o caso do *Binance Smart Chain*[43] e da *Huobi Eco Chais* (HECO)[44], que são *forks* da cadeia Ethereum.

Entre as soluções de camada dois, tem-se:

1. *Rollups* de camada 2 – São soluções que realizam transações fora da cadeia principal (cadeia de camada um) antes de submeter uma transação para a cadeia de camada um. Com isso, existe uma redução da carga sobre a cadeia de camada um, reduzindo também os custos associados para a manutenção do serviço (já que espera-se que os custos de camada um sejam maiores que os de camada dois). Nesse modelo, a segurança continua sendo provida pelo registro dos dados na cadeia de camada um. Existem dois tipos de *rollups*: os *rollups* de conhecimento zero, que executam operações que demandam poder computacional fora da cadeia de camada

[33]https://polkadot.network/
[34]https://solana.com/
[35]https://cosmos.network/
[36]https://www.thetatoken.org/
[37]https://www.algorand.com/
[38]https://fantom.foundation/
[39]https://www.avax.network/
[40]https://near.org/
[41]https://tron.network/
[42]https://celo.org/pt
[43]https://www.binance.com/pt-BR
[44]https://www.hecochain.com/

um e apenas registram nessa cadeia as provas de validade das operações; e o *rollup* otimista, que assume que as transações são válidas por padrão e apenas executam cálculos na cadeia de camada um em eventos de desafio, como uma prova contra fraudes [Kiong e Xiang, 2021].

2. Canais de Estado (*State Channels*) – São canais de comunicação bidirecionais entre os participantes, por meio do qual eles podem realizar inúmeras transações fora da cadeia e, ao final, ambos registram o resultado final na cadeia de camada um [Kiong e Xiang, 2021]. Com esse tipo de abordagem, aumenta-se a velocidade de transações e reduz-se a sobrecarga da cadeia de camada um. Exemplos incluem o Connext[45], Kchannels[46], Perun[47] e Raiden[48].

3. Cadeias Paralelas (*Sidechains*) – São cadeias de blocos independentes da cadeia de camada um (em oposição às soluções por *fork* da cadeia principal), mas conectadas com ela por uma ponte bidirecional. Essas cadeias paralelas usualmente utilizam seus próprios algoritmos de consenso menos custosos, como Prova de Autoridade, Prova de Participação, Tolerância de Falhas Bizantinas, entre outros. Exemplos de cadeias paralelas incluem Skale[49], POA Network[50] e xDai[51].

4. Plasma – Essa solução foi criada para a rede Ethereum, funcionando como uma cadeia filha (cadeia de nível 2) para a cadeia pai (cadeia de nível 1) [Poon e Buterin, 2017]. As cadeias pai e filha coexistem independentemente, de forma que a cadeia filha pode ter os seus próprios contratos inteligentes, criando as suas próprias regras de negócio sem estar presa a taxa de transações ou ao preço de transação da cadeia principal. A segurança é aplicada pelo monitoramento da cadeia de nível 1 e da cadeia de nível 2, de tal forma que comportamentos fraudulentos na cadeia de nível 2 são penalizados. No Plasma, cadeias filhas podem criar filhas, gerando uma árvore que confere maior flexibilidade na criação do modelo de negócio, como mostrado na Figura 2.10. Iniciativa semelhante também foi criada no Bitcoin para resolver os problemas de escalabilidade, sendo chamada de *Lightning Network* [Poon e Dryja, 2016].

2.6.1.3. Anonimização

A anonimização é um dos pontos chaves para o uso de cadeias de blocos para aplicações de energia e de cidades inteligentes. Nesse contexto, é importante garantir que as chaves públicas e transações não possam ser associadas a um determinado usuário, expondo sua privacidade, especificamente, os locais por onde anda ou seu padrão de consumo de energia.

[45] https://www.connext.network/
[46] https://www.kchannels.io/
[47] https://perun.network/
[48] https://raiden.network/
[49] https://skale.space/
[50] https://www.poa.network/
[51] https://developers.gnosischain.com/

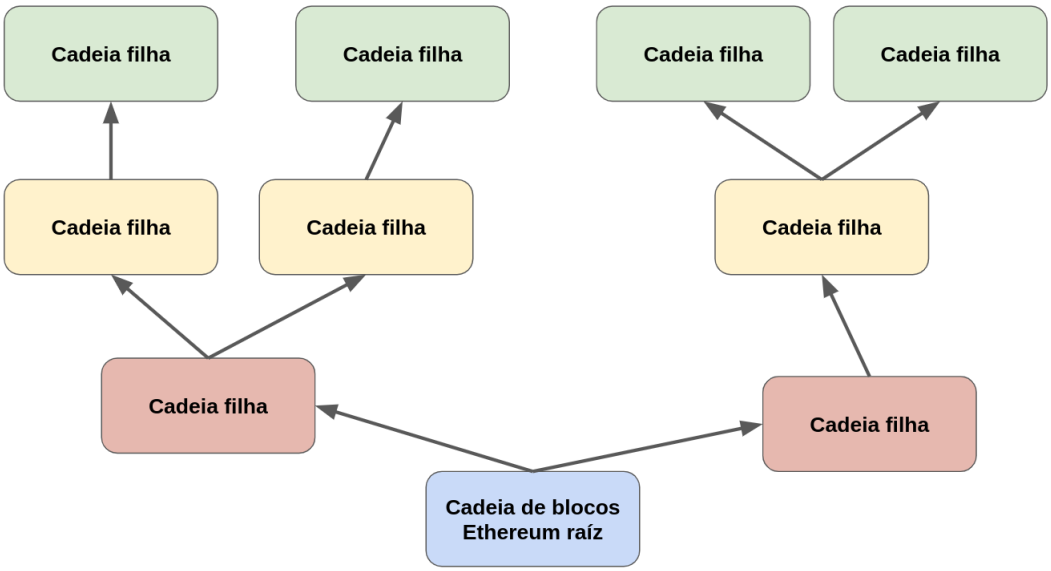


Figura 2.10. Estrutura em árvore de cadeias, gerada com a proposta do Plasma sobre a cadeia Ethereum.

A anonimização é especificamente difícil de se manter em cadeias de blocos públicas, aonde todos os registros são expostos a todos os usuários. Uma vez descoberta a identidade de um usuário, associando um nome a uma chave pública, todas as atividades daquele usuário são automaticamente expostas. Dessa forma, embora seja interessante armazenar transações e créditos de carbono na cadeia de blocos, não é recomendável, mesmo com o uso de criptografia, registrar dados pessoais, tais como consumo de energia, uso de veículos elétricos, entre outros.

Dessa forma, todas as aplicações baseadas em cadeias de blocos devem prover soluções concretas e bem estruturadas para evitar expor dados do usuário, seja pelo uso de cadeias privadas paralelas às públicas ou banco de dados paralelos. Além disso, tanto o controle de acesso quanto o sistema de armazenamento precisam ser cuidadosamente projetados para evitar vazamentos de dados e para permitir a remoção de dados pessoais sempre que necessário, conforme determinam as legislações vigentes, tais como a LGPD no Brasil.

Indo em uma direção contrária a da necessidade de anonimização dos usuários, existe a necessidade de se criar sistemas fortes de gestão de identidades para IoT, pois aplicações como o registro de créditos de carbono ou transações comerciais de energia demandam que os equipamentos e entidades que fazem registros nas cadeias de bloco sejam verificáveis e resistentes à violações (*tamper proof*). Portanto, aplicações de mobilidade elétrica e tarifação inteligente precisam ser capazes de identificar a origem dos dados e autenticar as informações contra violações, especialmente por questões legais associadas a esses tipos de aplicações.

2.6.1.4. Ataques contra a blockchain

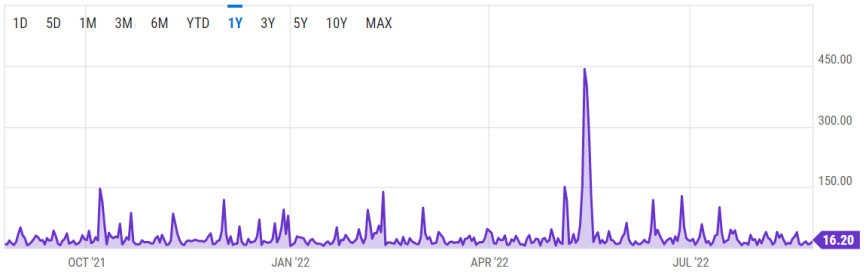
Uma das principais áreas para pesquisa e desenvolvimento para cadeias de blocos aplicadas ao sistema elétrico é a segurança cibernética. Especificamente, existem ataques que podem corromper as lógicas de negócio sendo executadas por meio de contratos inteligentes e NFTs.

Entre os principais ataques já conhecidos que podem afetar as aplicações do setor elétrico e das cidades inteligentes, destacam-se:

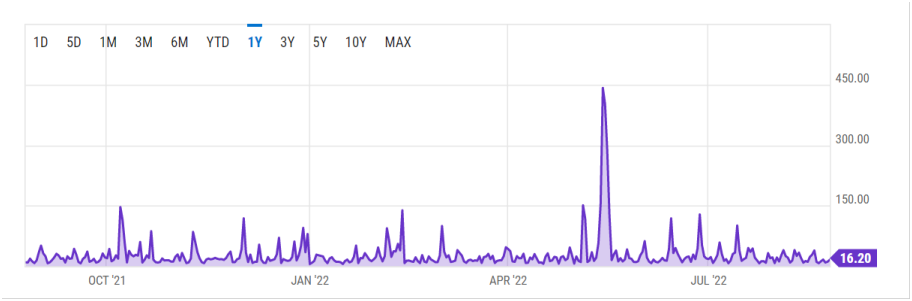
1. Ataque da Vivacidade (*Liveness Attack* - atrasa o tempo de confirmação da transação, visando obter vantagens. Esse ataque, que depende de um maior poder computacional do atacante, ocorre em três etapas: preparação, negação de transação e atraso de cadeia. Primeiramente, na preparação, o atacante tenta obter uma vantagem potencial contra usuários honestos para construir sua cadeia privada. Nesse caso, está se assumindo o uso de algoritmos de consenso que privilegiam o poder computacional do minerador. Em seguida, inicia-se a fase de negação da transação, na qual o atacante tenta atrasar um bloco genuíno que contém a transação alvo do ataque. Quando o invasor decide que o atraso não pode ser maior sem levantar suspeitas dos demais mineradores, ele prossegue para a fase de renderização da cadeia de blocos, onde tenta diminuir a taxa de transações na cadeia [Singh et al., 2021]. Atrasos em transações de leilões ou transações relacionadas a preços variáveis podem causar prejuízos significativos ao alvo.

2. Ataques de gasto duplo: busca utilizar o mesmo fundo para realizar mais de uma transação rápida sem validação. Esse ataque pode ocorrer em cadeias que tem um tempo de validação da transação lento, ou mais lento que a velocidade da transação no mundo real. Seria o caso, por exemplo, de uma transação de pagamento em um mercado, no qual o cliente paga e vai embora, sem esperar alguns minutos até confirmar que transação foi validada na cadeia. Em cenários como esse, o usuário poderia fazer diversas compras rápidas com o mesmo crédito, aproveitando-se de que não seria viável validar a transação em tempo real [Karame, 2012]. Essa possibilidade acaba por tornar a implementação de muitas aplicações inviáveis em cadeias de blocos, pois não validar a transação em tempo real permite a realização de fraudes. Como ilustração, a Figura 2.11 mostra o tempo de validação em minutos de transações na Bitcoin e no Ethereum, mostrando que são tempos relativamente longos e altamente variáveis. Dada essa realidade, existem esforços em pesquisa para reduzir e homogenizar o tempo de validação de transações em novas cadeias de bloco, possibilitando o uso de cadeias de bloco em aplicações com transações de validação rápida.

3. Roubo da Chave Privada: Todas as transações e acesso a fundos em cadeias de blocos são feitas por meio do uso de criptografia assimétrica. A perda de uma chave privada leva a perda de acesso ao fundo, sem possibilidade de recuperação. Assim, muitos ataques a computadores recentes visam encontrar e roubar chaves privadas armazenadas pelos usuários, o que permite o acesso à cadeia pelo agente malicioso [Singh et al., 2021].



(a) Tempo de confirmação de uma transação no Bitcoin em minutos.



(b) Tempo de confirmação de uma transação no Ethereum em minutos.

Figura 2.11. Estatísticas do último ano de tempo de transação nas duas principais cadeias de bloco atuais. Fonte: [Ycharts.com, 2022a, Ycharts.com, 2022b]

4. Ataque de Colisão: Esse ataque se aplica a cadeias de bloco baseadas em Prova de Trabalho. Nesse caso, se o atacante possuir mais de 50% do poder de mineração na rede, ele pode redefinir a cadeia da forma que achar mais vantajosa para si, realizando outros ataques, como por exemplo, a realização de Ataques de Gasto Duplo, por meio da criação de ramos na cadeia. Uma versão diferente do ataque se aplica a cadeias baseadas no consenso Tolerância de Falhas Bizantinas. Nesse caso, se o atacante controla pelo menos 50% dos nós de validação escolhidos pelo líder de consenso, ele pode validar algo errado ou não validar algo correto, trazendo problemas para as aplicações e regras de negócios executadas sobre a cadeia de blocos [Liu et al., 2021].

5. Ataque Sybil: Nesse ataque, o atacante cria um grande número de identidades falsas, visando levar vantagem em algoritmos de consenso baseados em votação, tais como os grupos de validação *Practical Bizantine Fault Tolerant* (PBFT), ou sistemas DAO.

6. Inserção de dados falsos: As aplicações no domínio de sistemas de energia e de cidades inteligentes podem se beneficiar das propriedades de segurança que as cadeias de blocos trazem em inúmeros sentidos. Contudo, as cadeias de bloco, seus contratos inteligentes e os NFTs apenas garantem a segurança dos registros no mundo virtual. Não existe, na tecnologia, uma garantia que os registros cibernéticos de fato correspondem aos eventos do mundo real. Assim, atacantes podem fabricar/falsificar dados e enviá-los para a cadeia de blocos [Gourisetti et al., 2021]. Dessa forma, há que existir uma camada de segurança ciber-física que garanta, entre

outros, a não-violação dos dispositivos aptos a fazer registros na cadeia de blocos em uma determinada aplicação.

Cabe destacar que qualquer ataque que possa influenciar as regras de negócio ou levar a perdas financeiras são potencialmente negativos para as aplicações do setor energético e de cidades inteligentes. Nesse sentido, vários esforços em pesquisa vem sendo aplicados para tentar minimizar os impactos desses ataques, assim como em melhorar o desempenho das cadeias de blocos.

2.6.1.5. Regulamentação

Embora as cadeias de blocos tenham grande potencial para moldar novos modelos no mercado de energia, ainda existe uma grande restrição no que diz respeito à legislação e regulamentação.

Usualmente, o setor elétrico dos países costuma ser altamente regulamentado, com órgãos de operação, regulação e controle de mercado, que definem um vasto conjunto de regras e normas de operação. Essas regulações visam garantir que o acesso à energia seja confiável, seguro e acessível [Stanwell, 2022].

Dentro desse contexto, as cadeias de bloco ainda não são vistas com bons olhos dentro do setor, por serem consideradas como uma tecnologia emergente, ainda pouco testada e não suficientemente estável. Essa desconfiança acaba por retardar significativamente a regulação e a integração dessa nova tecnologia ao mercado de energia. Além disso, observa-se que a natureza descentralizada das cadeias de bloco dificultam o desenvolvimento de estruturas e modelos legais que regulamentem o seu uso, tornando-se um desafio para os setores regulatórios [World Economic Forum, 2018]. Por exemplo, não é possível responsabilizar ou punir um responsável por ataque em uma cadeia de bloco que venha a prejudicar consumidores e geradores de energia se não for possível identificá-lo no mundo físico.

Outro ponto crucial relacionado à legalização das cadeias de blocos, contratos inteligentes e NFTs para aplicações de energia diz respeito à questão da anonimização e da persistência dos dados. Leis como a *European General Data Protection Regulation* (GDPR), na Europa, e a Lei Geral de Proteção de Dados (LGPD), no Brasil, trazem questões desafiadoras para o contexto das cadeias de bloco [Zemler e Westner, 2019, Morte et al., 2020]. Essas leis determinam fortes restrições protegendo dados privados e confidenciais de usuários, exigindo a garantia de privacidade e dando ao usuário o direito de deletar dados privados quando achar apropriado. Uma vez que a cadeia de blocos é imutável, não é possível apagar registros. Além disso, para o caso de cadeias públicas, todos os registros ficam abertos para todos os nós da cadeia.

Portanto, a legalização e regulamentação das cadeias de bloco passam não só pela maturidade da tecnologia, como também pelo forte investimento em pesquisa em mecanismos que permitam garantir a privacidade e a deleção de dados sem, com isso, ter que alterar a estrutura da cadeia [Sahmim et al., 2019].

2.6.2. Projetos de pesquisa e tendências futuras

2.6.2.1. Tendências de pesquisa

Uma das principais tendências de pesquisa está relacionada aos mercados de carbono. Com o aumento do interesse na redução do aquecimento global, diversos fóruns mundiais passaram a propagar iniciativas de compensação de emissão de gás carbônico por créditos de carbono advindos de atividades que reduzem a emissão de carbono.

Dentro das iniciativas já existentes, tem-se a da *Universal Protocol*, que lançou um crédito de carbono negociável no varejo, permitindo que projetos certificados transformem suas reduções de gases de efeito estufa em créditos de carbono negociáveis. Esse créditos são definidos como tokens fungíveis, chamados de *Universal Carbon* (UPCO2)[52]. A empresa criou ainda o *Bitcoin Zero*, que é um *token* construído como contrato inteligente do tipo ERC-20 baseados no UPCO2. O *Bitcoin Zero*[53] é um *wrapper* que combina um Bitcoin com a retirada de 10 toneladas de carbono obtidos a partir dos projetos de floresta tropical baseados no instrumento REDD+, criado pela Convenção-Quadro das Nações Unidas sobre Mudança do Clima - *United Nations Framework Convention on Climate Change* (UNFCCC). Esses créditos de carbono são certificados por organismos internacionais, validando o que seria um Bitcoin "verde".

A *SavePlanetEarth*[54], uma empresa inglesa, está disponibilizando uma plataforma para NFTs inteligentes de crédito de carbono certificados na cadeia de blocos *Phantasma*. O ciclo de funcionamento desses tokens é apresentado na Figura 2.12.

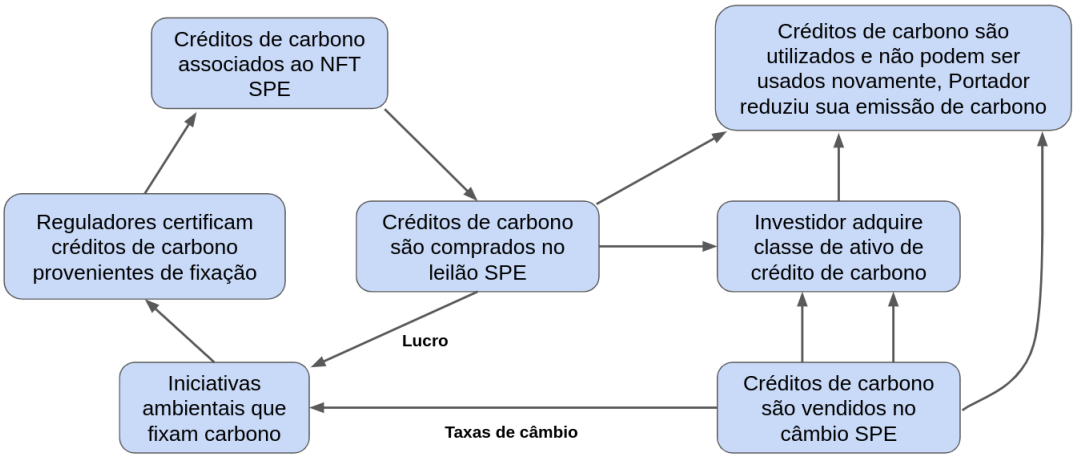


Figura 2.12. Ciclo de vida dos NFTs da organização *Save Planet Earth*, os quais são tokens de carbono negociáveis. Adaptado de [Save Planet Earth, 2021].

A *First Carbon*[55] desenvolveu uma plataforma chamada de *Mint Carbon*[56], que permite a negociação de créditos de carbono como NFTs criados na cadeia de bloco Poly-

[52]https://universalcarbon.com/
[53]https://www.universalprotocol.io/bitcoinzero
[54]https://saveplanetearth.io/
[55]https://www.firstcarbonsolutions.com/
[56]https://mintcarbon.io/

gon[57], fornecendo aos emissores de crédito de carbono acesso a cadeia de blocos e permitindo que os usuários rastreiem e negociem seus créditos.

Outros estão usando as cadeias de bloco para financiar soluções regenerativas. Por exemplo, o projeto NFTree[58], criado pela parceria entre a *Crown Platform* e a *Micorriza Association* na Espanha, está criando NFTs de pegadas de carbono na cadeia de blocos Crown[59]. A proposta é financiar o progresso ecológico por meio de certificados de carbono com validade mundial, transparentes e de fácil acesso. Já a *Carbonland Trust*[60] criou um ativo de créditos de remoção de carbono tokenizados como NFTs baseado em conservação florestal, chamado de *Carbonland Trust ESG NFTs*. Outra iniciativa é da *Cambridge Centre for Carbon Credits* (4C)[61], que promove uma solução para comprar créditos de carbono para financiar soluções "verdes" que busquem preservar biodiversidade. A *ClimateCoin Foundation*[62] incentiva a compensação de emissões de carbono, transformando registros de crédito de carbono oficiais em NFTs. Pessoas que plantam árvores ou reduzem as emissões de gás carbônico recebem tokens.

Dentro desse contexto, ficam claras as oportunidades de pesquisa dentro dos VCM, permitindo soluções mais seguras, com maior controle de mercado e que consideram novas formas de geração de crédito de carbono.

Existem ainda inciativas dentro da área de geração de energia distribuída. Nesse caso, as cadeias de blocos surgem como forma de melhorar a gerência dos mercados de energia descentralizados, aumentando a confiabilidade e a transparência dos serviços. Entre as iniciativas de mercado já disponíveis, tem-se a Powerledger[63] que permite a compra, venda ou troca do excesso de eletricidade renovável gerada por meio de uma rede par-a-par. O projeto Solstroem[64] foca na aceleração da transição energética em países em desenvolvimento e emergentes, fornecendo créditos de microcarbono pela geração em rede solar ao invés de pelo uso de combustível. Os créditos, que são georreferenciados e com carimbo de data/hora, podem ser vendidos para indivíduos ou empresas que precisem realizar compensações de crédito de carbono.

Entre os mercados de energia baseados em cadeia de blocos, destaca-se o *Grid Singularity*[65], que é uma plataforma ciente da grade energética para o mercado de energia descentralizado. Outra plataforma similar é a *TransActive Grid*[66], que usa as cadeias de bloco para criar um mercado de energia produzida em casa em uma escala local.

Com a tokenização dos RECs, gerou-se um novo modelo de negócios, simplificando o processo e evitando a possibilidade de dupla contagem e outras formas de fraude [Nova, 2021]. A transparência trazida pelos RECs tokenizados e negociados por

[57] https://polygon.technology/
[58] https://nftree.org/
[59] https://www.crownplatform.com/
[60] https://www.carbonlandtrust.com/
[61] https://4c.cst.cam.ac.uk/
[62] https://www.climateaction.org/directory/climate-coin-foundation?supplier=Climate%20Coin%20Foundation#products-and-services
[63] https://www.powerledger.io/
[64] https://www.solstroem.com/
[65] https://gridsingularity.com/
[66] http://www.solutionsandco.org/project/transactive-grid/

meio de contratos inteligentes e NFTs abre a oportunidade de criar novos tipos de REC, relacionados com variáveis como tempo, local da geração de energia, tipo de geração e até mesmo outras formas de redução de emissões de gás carbônico. Com isso, existe uma ampla gama de oportunidades de pesquisa em modelos de mercado e desenvolvimento tecnológico para viabilizar esses novos modelos de forma segura e inteligente.

É importante destacar que a principal proposta de valor dos NFTs para RECs é a garantia de não duplicidade, natural aos NFTs, e de integridade garantida pelo contrato inteligente acionado pelos próprios dispositivos geradores de energia.

2.6.2.2. Projetos de pesquisa

Existem diversos projetos de pesquisa e desenvolvimento pelo mundo relacionando as cadeias de blocos com aplicações do setor de energia. Andony *et al.*, em sua pesquisa, mostram uma classificação percentual dos casos de uso de cadeias de bloco no setor energético. A Figura 2.13 mostra esses dados, evidenciando que uma parcela significativa dos investimentos se aplica à geração de tokens e de certificados verdes [Andoni et al., 2019].

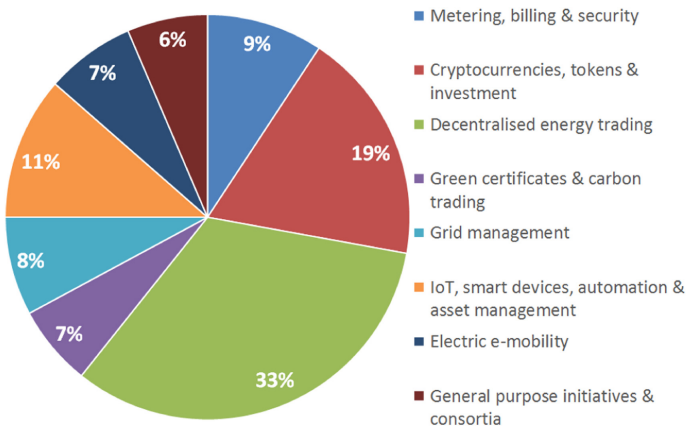


Figura 2.13. Estudo da distribuição entre áreas de 140 iniciativas de uso de cadeias de blocos no setor de energia, promovidas por empresas e instituições de pesquisa. Fonte: [Andoni et al., 2019].

Cabe destacar que projetos de pesquisa relacionadas ao mercado de energia e de carbono estão surgindo por todo mundo, em consonância com as evoluções e o surgimento de *startups*.

Entre os projetos existentes nos EUA, pode-se citar o *Brooklyn Microgrid*, que desenvolveu uma plataforma para comercialização de energia solar [67], sendo um dos primeiros programas de engenharia aplicada com cadeias de blocos utilizadas no setor de energia. Nesse projeto, que envolvia dez residências, cinco residências eram geradoras de energia, enquanto que as demais residências compravam o excedente, por meio de transações par-a-par [Zhao et al., 2019]. Outros projetos incluem o *Filament*, que usa cadeias de blocos para gerenciamento de informações de dispositivos IoT para dar suporte a soluções

[67] https://www.brooklyn.energy/

de falha na rede elétrica [Tripathy et al., 2020]. Outro projeto, desenvolvido por empresas de carregamento de baterias de carro americanas e alemãs, visou o desenvolvimento de estações de carregamento de veículos elétricos compartilhados baseado em cadeias de blocos. Com essa plataforma, é possível vender energia gerada e também carregar o carro por meio do aplicativo JuiceNet [Yaqub et al., 2020, Zhao et al., 2019].

Na Irlanda, tem-se o projeto EnerPort, promovido pelo governo irlandês, em parceria com indústrias, para criar uma rede par-a-par colaborativa, baseada em cadeias de blocos. Nesse projeto, visa-se promover o mercado de energia par-a-par entre microgrids [Verma et al., 2018].

No Chile, a *Comisión Nacional de Energía*, do Ministério das Energias, criou o portal *Energía Abierta Beta*. Esse serviço é baseado nas cadeias de blocos e visa dar maior transparência ao mercado de energia no país [Pareti e Núñez, 2021].

Na África do Sul, em 2015, foi desenvolvido o *Sun Exchange's*, um *marketplace* baseado em cadeia de blocos para microgrids. O projeto usa tokens para a energia gerada [Jackson, 2022].

Na China, o projeto ECO2 Ledger usa cadeias de blocos para controlar créditos de carbono, tornando-os mais confiáveis e rastreáveis[68]. O sistema permite ainda que pessoas consigam medir a sua redução de pegada de carbono, no aplicativo MyCarbon[69], e vender esses créditos. O serviço rapidamente alcançou mais de 500 mil usuários e acumulou mais de 100 mil toneladas de crédito de carbono.

A empresa Nori [70] propõe um sistema em que um NFT intitulado NRT é emitido na rede Polygon para um usuário que foi capaz de implementar, com sucesso, um projeto para remover uma tonelada de CO2 da atmosfera por ao menos dez anos. A mecânica requer que uma empresa independente verifique o projeto e ateste sua validade por meio da metodologia US Croplands. Uma vez em posse do NFT, seu dono pode trocá-lo na cadeia de blocos com um usuário que tenha demanda por créditos de carbono. A empresa alega que, antes desse sistema, para fazer uma transação de crédito de carbono, era necessário uma série de contratos e intermediários. Com a sua utilização, a cadeia de blocos se torna um canal único de transação entre o usuário que gerou o crédito de carbono e o usuário que deseja adquiri-lo.

No Brasil, o projeto "Implantação de um Modelo de Negócio para Compartilhamento de Veículos Elétricos Usando como Estudo de Caso o Sistema de Transporte Coletivo da UFF", em desenvolvimento na Universidade Federal Fluminense (UFF), visa utilizar uma cadeia de blocos para a tarifação no compartilhamento de veículos elétricos da UFF de forma sustentável e com incentivos sociais aos alunos. Esta proposta prevê o desenvolvimento de um sistema de compartilhamento de veículos elétricos, compreendendo toda a cadeia de produção, desde o controlador veicular presente nos veículos elétricos, até a plataforma online de monitoramento, controle e tarifação dos veículos. Ainda, este sistema será testado em um ambiente operacional, constituído pelo sistema de transporte coletivo da UFF, resultando em testes, demonstrações e avaliações que qua-

[68] https://www.eco2.cc/

[69] https://eco2.cc/MyCarbon.html

[70] https://nori.com/

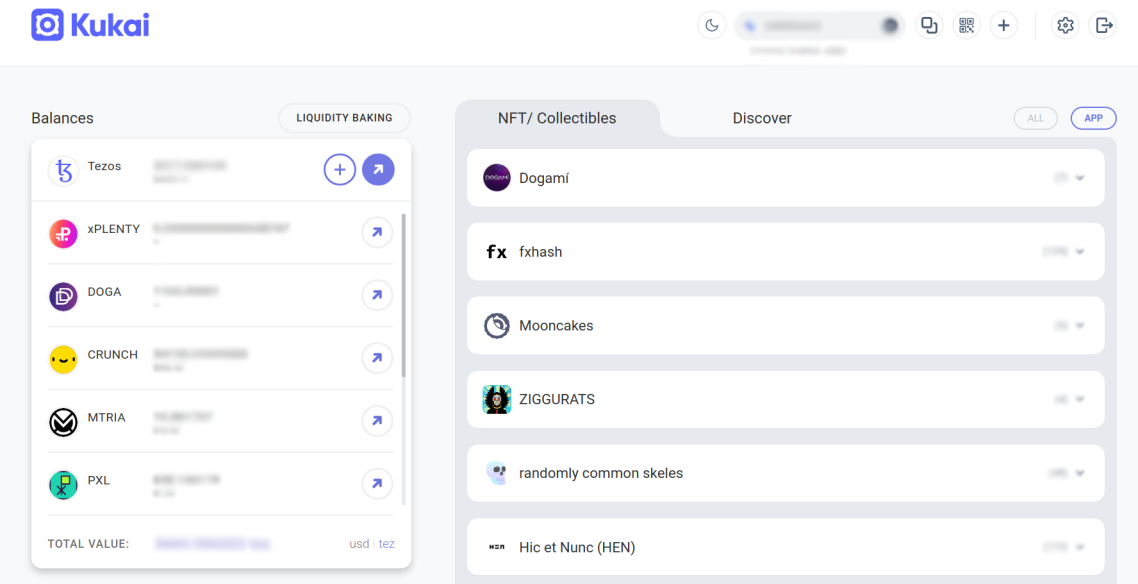


Figura 2.14. Aplicativo da carteira que habilita o acesso à rede de bloco Tezos.

lifiquem o sistema de compartilhamento com elevado grau de maturidade (TRL7). Por fim, será construído um modelo de negócios para o sistema proposto, de modo a permitir a extensão para todo o território nacional. Entre os objetivos, tem-se o uso de NFTs para gerenciamento de identidades e créditos de carbono.

A aplicação de cadeias de bloco para sistemas de energia é um tema altamente discutido e que está movimentando altíssimas quantias por todo o mundo. Os projetos apresentados visam trazer uma amostragem do que está sendo feito e a capilaridade das iniciativas.

2.7. Hands-on - Emissão e transferência de NFTs

Uma parte fundamental desta proposta de aplicação de mobilidade elétrica são as operações de emissão e transferência de propriedade de NFTs. Nesse cenário, o *hands-on* permite o contato direto com essas operações por meio de duas cadeias de blocos amplamente utilizadas no mercado: Ethereum e Tezos. A emissão permite os participantes do minicurso criarem um NFT utilizando qualquer tipo de mídia digital. A transferência de propriedade permite que os participantes vislumbrem a troca ou venda de um NFT com outros pares. Essas operações, em conjunto, viabilizam o livre mercado de NFTs que motivam o seu uso em diversas esferas.

Em primeiro lugar, é demonstrado como criar uma carteira na cadeia de blocos Tezos. A carteira é um aplicativo descentralizado (ou DApp), neste caso, web, que cria uma interface amigável para acessar as informações da carteira que está armazenada na cadeia de blocos. Além disso, a carteira também permite a interação com a cadeia de blocos, como submeter uma transação à cadeia. É adotada a plataforma Kukai[71] para a demonstração e criação da carteira. A carteira pode ser observada pela Figura 2.14.

[71] `https://wallet.kukai.app/`

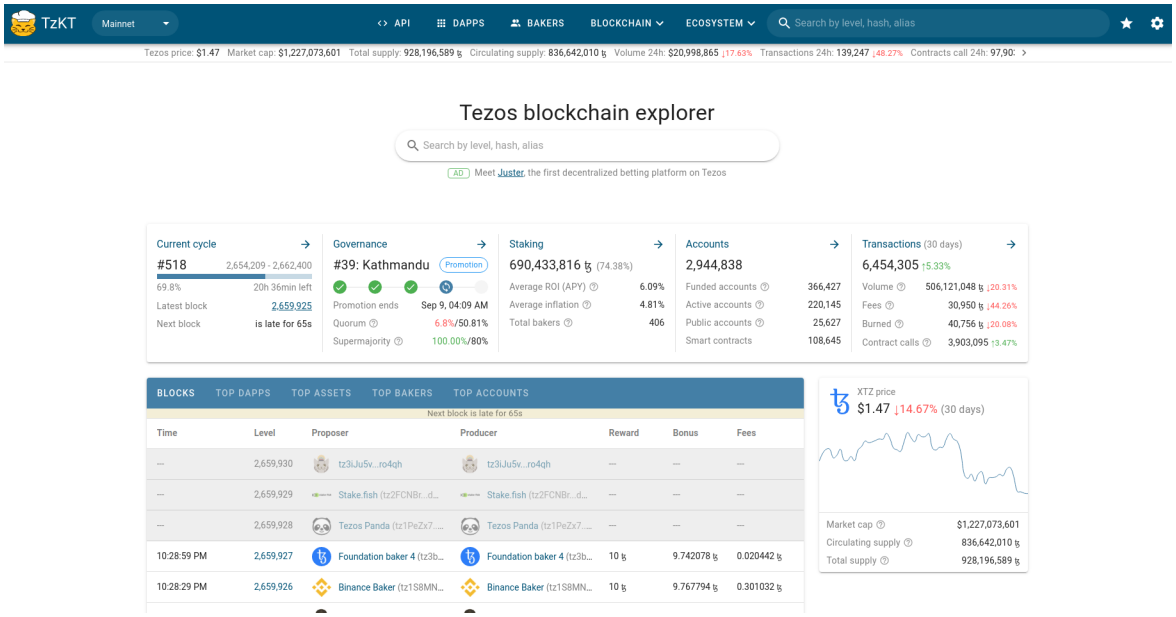


Figura 2.15. Indexador da cadeia de blocos Tezos.

Ao lado esquerdo da Figura, se encontram as moedas fungíveis, onde aparecem suas respectivas logos e a quantidade que a carteira possui. Ao lado direito da Figura, são as coleções e quantos NFTs a carteira possui para cada coleção. Como exemplo, Ziggurats é uma coleção criada pelo Mike Shinoda, o cantor da banda Linkin Park. Essa carteira da figura possui ao menos um NFT de cada coleção listada.

Em seguida, é demonstrado um indexador e explorador de cadeia de blocos — Tezos e Ethereum. Cada cadeia de blocos possui um meio de consultar informações históricas de maneira eficiente. Trabalhar diretamente com a cadeia de blocos para buscar informações históricas seria demorado. Portanto, a plataforma TzKT[72], ou o Etherscan[73] no Ethereum permitem diversas consultas, como exemplo: (1) quais foram todas as transações efetuadas para um NFT específico?; (2) qual o saldo de $XTZ de uma determinada carteira?; (3) quem criou determinado NFT? Além disso, o indexador também permite identificar outras informações gerais como quais as transações foram processadas em determinado bloco, ou a quantidade de gás uma determinada transação consumiu, ou ainda o total de gás consumido pelo bloco. É possível acompanhar as recompensas históricas obtidas por meio do consenso de Prova de Participação, ver qual foi o nó que processou o bloco, ou ainda buscar por carteiras, contratos inteligentes, ou até por aplicações. É possível observar pela Figura 2.15 a interface do indexador TzKT da cadeia de blocos Tezos.

Com efeito, a plataforma Objkt[74], que é a maior plataforma de negociação de NFTs de propósitos gerais na cadeia de blocos Tezos, será demonstrada. Neste momento, serão identificadas as informações associadas ao NFT na plataforma, tal como royalties, colecionadores, coleções, transações, volume, etc. Em seguida, será demonstrado como

[72] https://tzkt.io/
[73] https://etherscan.io/
[74] https://objkt.com/

negociar NFTs por meio da compra de um NFT. O NFT comprado será demonstrado via carteira web ou pelo explorador da cadeia de blocos por meio da transação ou pelo NFT em si. Será avaliado como o conteúdo digital do NFT está armazenado: se ocorre por meio do IPFS, e quais metadados estão associados e armazenados fora da cadeia.

Em seguida, será demonstrado como criar um NFT. O NFT criado será distribuído para todos os participantes. Pode-se dizer que o NFT distribuído funcionará como um mecanismo de POAP (*Proof of Attendance Protocol*), isto é, um NFT que irá representar a experiência física do minicurso de maneira digitalizada. Ou ainda, representará a prova de comparecimento ao minicurso. Os participantes serão encorajados a criarem suas carteiras durante o minicurso para poderem receber o POAP.

Com efeito, todas as tarefas de exploração do indexador da cadeia de blocos, emissão de NFT e busca por informações na plataforma de negociação de NFTs serão repetidas para a cadeia de blocos Ethereum — exceto a parte de emitir e comprar NFTs em função do alto custo das transações no Ethereum. Para esta cadeia de blocos, serão adotadas as plataformas de negociação OpenSea[75] e Foundation[76] durante o hands-on.

2.8. Considerações finais e perspectivas futuras

O padrão NFT tem sido utilizado em vários domínios, tais como cadeias de suprimentos, rastreabilidade de dados e manufatura, para representar bens físicos na forma de tokens digitais por conta de suas características de unicidade e rastreabilidade durante todo clico de vida do ativo. Entretanto, cada abordagem tem uma metodologia diferente para representar e sincronizar as informações entre o mundo físico e o digital.

O NFT é uma tecnologia ainda recente e com diversos desafios de pesquisa. Um dos principais desafios é sobre segurança e privacidade. No estágio atual, o anonimato e a privacidade dos NFTs ainda são pouco estudados. A maioria das transações NFT depende da plataforma Ethereum, que fornece apenas pseudo-anonimato. Os usuários podem ocultar parcialmente suas identidades se os links entre suas identidades reais e os endereços correspondentes forem desconhecidos pelo público. Caso contrário, todas as atividades dos usuários sob o endereço exposto são visíveis. As soluções existentes de preservação de privacidade, como, por exemplo, criptografia homomórfica [Wang et al., 2020], prova de conhecimento zero [Wang e Kogan, 2018], assinatura em anel [Noether et al., 2016], computação multipartidária [Neto et al., 2020], ainda não foram aplicadas aos esquemas relacionados a NFT devido à sua complexidade. Semelhante a outros tipos de sistemas baseados em cadeia de blocos, diminuir os custos computacionais torna-se característica chave para implementação de esquemas de privacidade do usuário.

Nos principais projetos de NFT, um *hash* criptográfico como identificador será marcado com o *token*, em vez de uma cópia do arquivo, e depois registrado na cadeia de blocos para economizar consumo de energia. Isso faz com que o usuário perca a confiança no NFT porque o arquivo original pode ser perdido ou danificado. Vários projetos de NFT integram um sistema de armazenamento de arquivos especializado, como o IPFS [Benet, 2014], no qual os endereços IPFS permitem que os usuários encontrem um conteúdo

[75] `https://opensea.io/`
[76] `https://foundation.app/`

desde que algum cliente da rede IPFS o hospede. Inevitavelmente, tais sistemas têm falhas. Quando os usuários carregam metadados NFT para nós IPFS, não há garantia de que seus dados serão replicados entre todos os nós. Os dados podem ficar indisponíveis se o ativo estiver armazenado no IPFS e o único nó que o armazena estiver desconectado da rede. Este problema foi relatado por `decrypto.io` [77] e `checkmynft.com`. Além disso, um NFT pode apontar para um endereço de arquivo incorreto. Se for esse o caso, um usuário não pode provar que ele realmente possui o NFT. Portanto, contar com um sistema externo como componente central de armazenamento para um sistema NFT é vulnerável.

De toda a forma, apesar de ainda existirem riscos associados, os NFTs já mostraram de forma concreta o seu potencial como instrumento para revolucionar mercados digitais. As vantagens trazidas são muito grandes e reduzem significativamente a burocracia e os custos no registro e negociação de bens não-fungíveis. Os NFTs representam ainda uma forma de tornar o processo mais seguro e transparente para os usuários, tornando toda a cadeia de processo mais segura.

As oportunidades em termos de aplicações trazidas pelos NFTs ainda estão longe de serem exauridas, existindo diversas possibilidades de criação de novos negócios com potencial para revolucionar no mercado. As oportunidades de pesquisa, em especial na área de segurança, para essas aplicações também são inúmeras, representando um tema que ainda será abordado na academia pelos próximos anos.

Referências

[Andoni et al., 2019] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P. e Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, 100:143–174.

[Ante, 2022] Ante, L. (2022). The Non-Fungible Token (NFT) market and its relationship with Bitcoin and Ethereum. *FinTech*, 1(3):216–224.

[Apolinário, 2019] Apolinário, W. d. A. (2019). Implementação de smart contracts e tokens não-fungíveis na geração e aquisição de certificados de energia renovável no brasil. B.S. thesis, Universidade Federal do Rio Grande do Norte.

[Arcenegui et al., 2021] Arcenegui, J., Arjona, R., Román, R. e Baturone, I. (2021). Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFs. *Sensors*, 21(9):3119.

[Beeple, 2021] Beeple, C. (2021). Everydays: The first 5000 days. `https://onlineonly.christies.com/s/beeplefirst-5000-days/beeple-b-1981-1/112924?ldp\_breadcrumb=back`. Acessado em 24 de agosto de 2022.

[Benet, 2014] Benet, J. (2014). IPFS-content addressed, versioned, P2P file system - Draft 3. *arXiv preprint arXiv:1407.3561*, p. 1–11.

[Bloomberg, 2022] Bloomberg (2022). Nvidia game card prices fall along with crypto mining demand. `https://www.bloomberg.com/news/articles/2022-06-30/nvidia-game-card-prices-plunge-along-with-crypto-mining-demand`. Acessado em 26 de agosto de 2022.

[77] Disponível em `https://decrypt.co/62037/missing-or-stolen-nfts-how-to-protect`. Acessado em 01/09/2022

[Browne, 2021] Browne, R. (2021). Visa jumps into the NFT craze, buying a 'CryptoPunk' for $150,000. https://www.cnbc.com/2021/08/23/visa-buys-cryptopunk-nft-for-150000.html. Acessado em 24 de agosto de 2022.

[Carbon Credits, 2021] Carbon Credits (2021). The ultimate guide to understanding carbon credits. https://carboncredits.com/the-ultimate-guide-to-understanding-carbon-credits/. Acessado em 31 de agosto de 2022.

[Chainlink, 2022a] Chainlink (2022a). Chainlink. https://chain.link/. Acessado em 27 de agosto de 2022.

[Chainlink, 2022b] Chainlink (2022b). New report highlights how blockchains and oracles are redefining the energy industry. https://blog.chain.link/blockchains-and-oracles-are-redefining-the-energy-industry/. Acessado em 31 de agosto de 2022.

[Che, 2021] Che, T. (2021). The world's 1st destroyed diamond NFT: Who, what, when, where, why & how. https://taschalabs.com/the-worlds-1st-destroyed-diamond-nft-who-what-when-where-why-how/. Acessado em 23 de agosto de 2022.

[CoinTelegraph Research, 2021] CoinTelegraph Research (2021). Blockchains vie for NFT market, but Ethereum still dominates. https://cointelegraph.com/news/blockchains-vie-for-nft-market-but-ethereum-still-dominates-report. Acessado em 24 de agosto de 2022.

[Digiconomist, 2022] Digiconomist (2022). Ethereum energy consumption index. https://digiconomist.net/ethereum-energy-consumption. Acessado em 26 de agosto de 2022.

[Dowling, 2022] Dowling, M. (2022). Is non-fungible token pricing driven by cryptocurrencies? *Finance Research Letters*, 44:102097.

[Ethereum.org, 2022] Ethereum.org (2022). Ethereum energy consumption. https://ethereum.org/en/energy-consumption/. Acessado em 26 de agosto de 2022.

[Etherscan, 2021a] Etherscan (2021a). Transação de compra do diamante no Ethereum. https://etherscan.io/tx/0xb3eb6a51c740f3a9532d9f38ea874be377d08cf28a73135602d3e134cffa410e. Acessado em 23 de agosto de 2022.

[Etherscan, 2021b] Etherscan (2021b). Transação de compra do Nyan Cat no Ethereum. https://etherscan.io/tx/0xa1042c7dac0750c48049a5556d42553cec6f90d9ff1ec9bfe3b4574265d9ac2f. Acessado em 24 de agosto de 2022.

[Filecoin, 2022] Filecoin (2022). Filecoin. ipns://filecoin.io/. Acessado em 26 de agosto de 2022.

[Flow, 2022a] Flow (2022a). Flow. https://flow.com/. Acessado em 26 de agosto de 2022.

[Flow, 2022b] Flow (2022b). Sustainability built to be green: Leading web3 to a more eco-friendly future. https://flow.com/sustainability. Acessado em 26 de agosto de 2022.

[Gao et al., 2014] Gao, S., Chau, K. T., Liu, C., Wu, D. e Chan, C. C. (2014). Integrated energy management of plug-in electric vehicles in power grid with renewables. *IEEE Transactions on Vehicular Technology*, 63(7):3019–3027.

[Gao et al., 2020] Gao, Y., Al-Sarawi, S. F. e Abbott, D. (2020). Physical unclonable functions. *Nature Electronics*, 3(2):81–91.

[Gourisetti et al., 2021] Gourisetti, S. N. G., Ümit Cali, Choo, K.-K. R., Escobar, E., Gorog, C., Lee, A., Lima, C., Mylrea, M., Pasetti, M., Rahimi, F., Reddi, R. e Sani, A. S. (2021). Standardization of the distributed ledger technology cybersecurity stack for power and energy applications. *Sustainable Energy, Grids and Networks*, 28:100553.

[IEC TC 57, 2022] IEC TC 57 (2003-2022). IEC 61850 - communication networks and systems in substations. Relatório técnico, IEC - TC 57 (Technical Committee on Power systems management and associated information exchange).

[Jackson, 2022] Jackson, J. (2022). The blockchain projects making renewable energy a reality. `https://cointelegraph.com/magazine/2022/03/18/blockchain-projects-making-renewable-energy-reality`. Acessado em 23 de agosto de 2022.

[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.

[Karame, 2012] Karame, G. O. (2012). Two Bitcoins at the price of one? Double-spending attacks on fast payments in Bitcoin. Em *In Proc. of Conference on Computer and Communication Security*.

[Karandikar et al., 2021] Karandikar, N., Chakravorty, A. e Rong, C. (2021). Blockchain based transaction system with fungible and non-fungible tokens for a community-based energy infrastructure. *Sensors*, 21(11):3822.

[Karger et al., 2021] Karger, E., Jagals, M. e Ahlemann, F. (2021). Blockchain for smart mobility—literature review and future research agenda. *Sustainability*, 13(23):13268.

[Kiong e Xiang, 2021] Kiong, L. e Xiang, L. (2021). *Investing in DeFi and NFT projects on alternative blockchains: A Beginner's Guide to Investing in DeFi and NFT Projects on Alternative Blockchains other than Ethereum*. Liew Voon Kiong.

[Kirli et al., 2022] Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D. e Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, 158(112013).

[Krause e Tolaymat, 2018] Krause, M. J. e Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. *Nature Sustainability*, 1(11):711–718.

[Li et al., 2020] Li, W., Rentemeister, M., Badeda, J., Jöst, D., Schulte, D. e Sauer, D. U. (2020). Digital twin for battery systems: Cloud battery management system with online state-of-charge and state-of-health estimation. *Journal of Energy Storage*, 30:101557.

[Liu et al., 2021] Liu, C., Zhang, X., Chai, K., Loo, J. e Chen, Y. (2021). A survey on blockchain-enabled smart grids: Advances, applications and challenges. *IET Smart Cities*, 3:56–78.

[Lopes et al., 2015] Lopes, Y., Fernandes, N. C. e Muchaluat-Saade, D. C. (2015). Geração Distribuída de Energia: Desafios e Perspectivas em Redes de Comunicação. Em *Minicursos do XXXIII SBRC*, p. 55–109. SBC.

[Medeiros et al., 2019] Medeiros, D. S. V., Fernandes, N. C. e Mattos, D. M. F. (2019). Smart Contracts and the Power Grid: A Survey. Em *1st Blockchain, Robotics and AI for Networking Security Conference (BRAINS)*, p. 140–194.

[Miraz et al., 2021] Miraz, M. H., Excell, P. S. e Sobayel, K. (2021). The Non-Fungible Token (NFT) market and its relationship with Bitcoin and Ethereum. *Annals of Emerging Technologies in Computing (AETiC)*, 5(4):54–59.

[Morte et al., 2020] Morte, A. B., Meira, A., Costa, R. e Mariz, D. (2020). Uma análise sobre o uso de DLTs no tratamento de dados pessoais: Aderência aos princípios e direitos elencados na LGPD. Em *Anais do III Workshop em Blockchain: Teoria, Tecnologia e Aplicações*, p. 74–87, Porto Alegre, RS, Brasil. SBC.

[Musamih et al., 2022] Musamih, A., Salah, K., Jayaraman, R., Yaqoob, I., Puthal, D. e Ellahham, S. (2022). NFTs in healthcare: Vision, opportunities, and challenges. *IEEE Consumer Electronics Magazine*, p. 1–14.

[Neto et al., 2020] Neto, H. N. C., Mattos, D. M. F. e Fernandes, N. C. (2020). Privacidade do usuário em aprendizado colaborativo: Federated learning, da teoria à prática. Em *Livro de Minicursos do SBSEG 2020*. Sociedade Brasileira de Computação.

[Nita et al., 2018] Nita, S. L., Mihailescu, M. I. e Pau, V. C. (2018). Security and cryptographic challenges for authentication based on biometrics data. *Cryptography*, 2(4).

[Noether et al., 2016] Noether, S., Mackenzie, A. et al. (2016). Ring confidential transactions. *Ledger*, 1:1–18.

[Nofer et al., 2017] Nofer, M., Gomber, P., Hinz, O. e Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3):183–187.

[Nova, 2021] Nova, A. (2021). A token improvement: The rise of non-fungible tokens. `https://www.powerledger.io/media/a-token-improvement`. Acessado em 29 de agosto de 2022.

[Oliveira et al., 2020] Oliveira, M. T., Reis, L. H., Medeiros, D. S., Carrano, R. C., Olabarriaga, S. D. e Mattos, D. M. (2020). Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications. *Computer Networks*, 179:107367.

[Pareti e Núñez, 2021] Pareti, S. e Núñez, I. (2021). Blockchain as an information system in Chile: The case of Open Energy Project - Chilean's Ministry of Energy. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 1(E39):554–568.

[Platt et al., 2021] Platt, M., Sedlmeir, J., Platt, D., Xu, J., Tasca, P., Vadgama, N. e Ibañez, J. I. (2021). The energy footprint of blockchain consensus mechanisms beyond proof-of-work. Em *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, p. 1135–1144.

[Poon e Buterin, 2017] Poon, J. e Buterin, V. (2017). Plasma: Scalable autonomous smart contracts. Relatório técnico, Plasma.io, `https://plasma.io/plasma.pdf`.

[Poon e Dryja, 2016] Poon, J. e Dryja, T. (2016). The Bitcoin lightning network: Scalable off-chain instant payments. Relatório Técnico Draft 0.5.9.2, Bitcoin Lightning, https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf.

[Rebello et al., 2019] Rebello, G., Camilo, G., Silva, L., Souza, L., Guimarães, L., Alchieri, E., Greve, F. e Duarte, O. (2019). Correntes de blocos: Algoritmos de consenso e implementaçao na plataforma Hyperledger Fabric. Em *Jornada de Atualização em Informática (JAI) - XXXIX Congresso da Sociedade Brasileira de Computação*.

[RED, 2021] RED (2021). Restart energy democracy platform - user guide. Relatório Técnico Version 1.0, RED.

[Rosenfeld et al., 2012] Rosenfeld, M. et al. (2012). Overview of colored coins. *White paper, bitcoil. co. il*, 41:94.

[Rossi, 2022] Rossi, E. (2022). NFTs for renewable energy certification - a solid use case. https://www.flexidao.com/post/nfts-for-renewable-energy-certification-a-solid-use-case. Acessado em 31 de agosto de 2022.

[Ruggieri et al., 2021] Ruggieri, R., Ruggeri, M., Vinci, G. e Poponi, S. (2021). Electric mobility in a smart city: European overview. *Energies*, 14(2).

[Sahmim et al., 2019] Sahmim, S., Gharsellaoui, H. e Bouamama, S. (2019). Edge computing: Smart identity wallet based architecture and user centric. *Procedia Computer Science*, 159:1246–1257.

[Saingre et al., 2022] Saingre, D., Ledoux, T. e Menaud, J.-M. (2022). Measuring performances and footprint of blockchains with BCTMark: a case study on Ethereum smart contracts energy consumption. *Cluster Computing*, 25(4):2819–2837.

[Save Planet Earth, 2021] Save Planet Earth (2021). Save planet earth official white paper - the cryptocurrency response to reversing the effects of climate change. Relatório Técnico v4, Save Planet Earth.

[Singh et al., 2021] Singh, S., Hosen, A. S. M. S. e Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access*, 9:13938–13959.

[Solana, 2022] Solana (2022). Solana's energy use report: March 2022. https://solana.com/news/solanas-energy-use-report-march-2022. Acessado em 26 de agosto de 2022.

[Spells of Genesis, 2022] Spells of Genesis (2022). Spells of genesis. https://spellsofgenesis.com/. Acessado em 23 de agosto de 2022.

[Stanwell, 2022] Stanwell (2022). How blockchain can impact the energy market. https://whatswatt.com.au/how-blockchain-can-impact-the-energy-market/. Acessado em 23 de agosto de 2022.

[Tezos Foundation, 2022] Tezos Foundation (2022). Sustainability through innovation. https://tezos.com/carbon/. Acessado em 26 de agosto de 2022.

[Thomason, 2022] Thomason, J. (2022). Blockchain and GreenFi - tools for climate action. https://thepaypers.com/expert-opinion/blockchain-and-greenfi-tools-for-climate-action--1257628. Acessado em 23 de agosto de 2022.

[Tripathy et al., 2020] Tripathy, R. P., Mishra, M. R. e Dash, S. R. (2020). Next generation warehouse through disruptive IoT blockchain. Em *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, p. 1–6. IEEE.

[Valeonti et al., 2021] Valeonti, F., Bikakis, A., Terras, M., Speed, C., Hudson-Smith, A. e Chalkias, K. (2021). Crypto collectibles, museum funding and OpenGLAM: challenges, opportunities and the potential of non-fungible tokens (NFTs). *Applied Sciences*, 11(21):9931.

[Verma et al., 2018] Verma, P., O'Regan, B., Hayes, B., Thakur, S. e Breslin, J. G. (2018). Enerport: Irish blockchain project for peer- to-peer energy trading. *Energy Informatics*, 1(14).

[VisaNews, 2021] VisaNews (2021). #newprofilepic. https://twitter.com/VisaNews/status/1430185056098820105. Acessado em 26 de agosto de 2022.

[Wang et al., 2020] Wang, Q., Qin, B., Hu, J. e Xiao, F. (2020). Preserving transaction privacy in Bitcoin. *Future Generation Computer Systems*, 107:793–804.

[Wang e Kogan, 2018] Wang, Y. e Kogan, A. (2018). Designing confidentiality-preserving blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, 30:1–18.

[World Economic Forum, 2018] World Economic Forum (2018). Fourth industrial revolution for the earth series - building block(chain)s for a better planet. Relatório técnico, World Economic Forum.

[Yahoo, 2021] Yahoo (2021). The burned picasso nft to digitally preserve artistic legacy. https://finance.yahoo.com/news/burned-picasso-nft-digitally-preserve-173000064.html. Acessado em 23 de agosto de 2022.

[Yaqub et al., 2020] Yaqub, R., Ahmad, S., Ali, H. e Asar, A. u. (2020). AI and blockchain integrated billing architecture for charging the roaming electric vehicles. *IoT*, 1(2):382–397.

[Ycharts.com, 2022a] Ycharts.com (2022a). Bitcoin average confirmation time. https://ycharts.com/indicators/bitcoin_average_confirmation_time. Acessado em 26 de agosto de 2022.

[Ycharts.com, 2022b] Ycharts.com (2022b). Ethereum average confirmation time. https://ycharts.com/indicators/ethereum_average_block_time. Acessado em 26 de agosto de 2022.

[Yoon et al., 2010] Yoon, J. W., Kim, H. e Huh, J. H. (2010). Hybrid spam filtering for mobile communication. *Computers & Security*, 29(4):446–459.

[Yuan e Wang, 2016] Yuan, Y. e Wang, F.-Y. (2016). Towards blockchain-based intelligent transportation systems. Em *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, p. 2663–2668. IEEE.

[Zemler e Westner, 2019] Zemler, F. e Westner, M. (2019). Blockchain and GDPR: Application scenarios and compliance requirements. Em *Portland International Conference on Management of Engineering and Technology (PICMET)*, p. 1–8.

[Zhang e Wang, 2019] Zhang, X. e Wang, D. (2019). Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain. *IEEE Access*, 7:97281–97295.

[Zhao et al., 2017] Zhao, X., Chen, Z., Chen, X., Wang, Y. e Tang, C. (2017). The DAO attack paradoxes in propositional logic. Em *2017 4th International Conference on Systems and Informatics (ICSAI)*, p. 1743–1746.

[Zhao et al., 2019] Zhao, Y., Peng, K., Xu, B., Liu, Y., Xiong, W. e Han, Y. (2019). Applied engineering programs of energy blockchain in US. *Energy Procedia*, 158:2787–2793.

