A construção da *Web3*: O desenvolvimento da nova web descentralizada baseada na tecnologia *Blockchain*

Anderson Henrique da Rosa[1], **Udo Fritzke Junior**[1]

[1]Ciência da Computação, PUC Minas *Campus* de Poços de Caldas – MG, Brasil

andersonhrosa@outlook.com, udo@pucpcaldas.br

Abstract. *With the emergence of new demands for security, privacy and user empowerment, new proposals have emerged for the web as we know it. Web3 is a possible new phase of the web based on Blockchain technology, built on decentralized peer-to-peer algorithms and protected by cryptography. Given its evolution, from the Ethereum Blockchain platform it is possible to write and execute smart contracts capable of carrying out transactions in a public, immutable and decentralized way. On the other hand, it is possible to integrate the Ethereum network with the web browser through an interface, allowing the development of decentralized applications. Based on these technologies, new applications have emerged that have been changing the way people use the internet and that propose a break with the current model of web browsing. In this way, despite the financial and regulatory challenges, Web3 shows itself as a new alternative for the development of new solutions for today's society.*

Resumo. *Com o surgimento de novas demandas por segurança, privacidade e empoderamento dos usuários, surgiram novas propostas para a web que conhecemos. A Web3 se trata de uma possível nova fase da web baseada na tecnologia Blockchain, construída sobre algoritmos descentralizados peer-to-peer e protegidos por criptografia. Dada a sua evolução, a partir da plataforma Blockchain Ethereum é possível escrever e executar contratos inteligentes capazes de realizar transações de forma pública, imutável e descentralizada. Por outro lado, é possível integrar a rede Ethereum com o navegador web através de uma interface, permitindo o desenvolvimento de aplicativos descentralizados. Baseado nestas tecnologias, surgiram novas aplicações que vem mudando a forma como as pessoas utilizam a internet e que propõem uma ruptura com o modelo atual de navegação na web. Deste modo, apesar dos desafios financeiros e de regulamentação, a Web3 se mostra como uma nova alternativa para o desenvolvimento de novas soluções para a sociedade atual.*

1 INTRODUÇÃO

É notável que a *World Wide Web* passou por muitas evoluções desde que Tim Berners-Lee a propôs em 1989. Na sua primeira versão a navegação era unidirecional, com o usuário experimentando apenas o acesso de leitura do conteúdo, então referida como "*Web* 1.0" [4]. A evolução da capacidade de processamento dos computadores, maior largura de banda da rede e o surgimento de novas tecnologias que permitiram a interação com o conteúdo através do navegador, culminou na fase que estamos atualmente, conhecida como "*Web* 2.0" [3]. No cenário atual, grandes corporações dominam parte considerável da internet, tendo controle dos dados usuários, o que leva a uma centralização da navegação nas mãos de poucas empresas, destoando da visão original de quando a *web* foi concebida [4][5].

Com o então surgimento do *Bitcoin*, se introduziu o conceito de criptomoedas, que utilizando a tecnologia do *blockchain*, foi possível armazenar dados de forma imutável, pública e

distribuída através de algoritmos de consenso que garantem estas propriedades [1][6]. Baseado nestas premissas, foi proposto o *Ethereum*, uma infraestrutura de computação descentralizada capaz de executar quaisquer tipos de programas, conhecidos assim como *smart contracts*, ou contratos inteligentes [2]. Os aplicativos descentralizados, surgiram logo em seguida, quando se passou a utilizar o *smart contract* e uma interface com o usuário no navegador *web*, o que culminou na criação de aplicações da chamada "*Web* 3.0" ou então *Web3* [5]. Esta nova *web* ainda está em construção e sua proposta é permitir o desenvolvimento inteligente e a disseminação de conteúdo customizado, sem ter que abrir mão da privacidade para acessar a rede, permitindo de forma segura uma integração entre o mundo natural e o virtual [4][7].

2 FUNDAMENTAÇÃO TEÓRICA

A base teórica deste artigo se fundamenta nos trabalhos recém realizados no desenvolvimento da chamada *Web3*, se baseando na tecnologia *blockchain* atrelada ao conceito das criptomoedas, que por sua vez utiliza a plataforma *Ethereum* e os conceitos de contratos inteligentes, desenvolvidos através da linguagem de programação *Solidity* e conjunto de bibliotecas *Javascript Web3.js*.

2.1 Blockchain

O conceito da tecnologia por trás da *blockchain* foi inicialmente proposto em 1991, sendo definida como uma cadeia de blocos protegida com criptografia capaz de armazenar dados de forma imutável [9]. Porém a tecnologia só se tornou conhecida e tomou forma após o pseudônimo Satoshi Nakamoto fazer a publicação do artigo *Bitcoin: A Peer-to-Peer Eletronic Cash System* [1].

A *blockchain* presente no *Bitcoin* se constitui por um *ledger* (livro-razão) distribuído em uma cadeia de blocos, que utiliza uma rede *peer-to-peer* protegido e conectados por criptografia, *append-only* (estritamente incremental), imutável, e atualizável apenas por consenso ou acordo entre pares de blocos [10]. Outra definição menos formal expõe que a *blockchain* é um livro razão compartilhado e imutável que facilita o processo de registro de transações e rastreamento de ativos em uma rede de negócios [8]. O livro razão está presente em todas as máquinas dos usuários que participam desta rede e qualquer alteração é feita de forma simultânea em todos os participantes, garantindo a segurança e aumentando a confiança do sistema, além de inibir fraudes [11]. A **figura 1** apresenta uma visualização da estrutura da *blockchain*, incluindo a ligação dos blocos por *hash*.

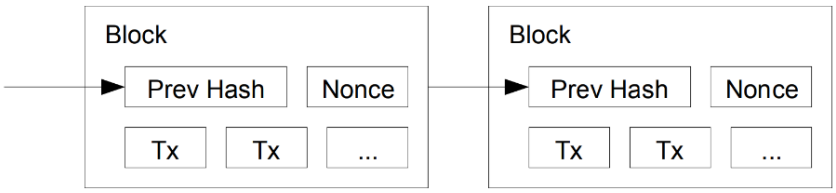


Figura 1: Estrutura da *Blockchain* [1]

Cada bloco representa um conjunto de dados armazenados, que pode variar de acordo com cada implementação, que no caso do *Bitcoin*, guarda o *timestamp* de cada transação, a chave pública do dono da atual criptomoeda e uma assinatura da chave privada do usuário anterior. Assim sendo, utilizando a chave privada, a chave pública do bloco anterior e o valor do *hash* do bloco é possível determinar se a transação é válida [6]. A *hash* de cada bloco é feita com base em dois parâmetros, o bloco anterior e um valor arbitrário, conhecido como *nonce*, que será então utilizado para verificar se o *hash* é válido. Isto impossibilita a alteração do valor de uma *hash*

em qualquer bloco sem tornar os blocos seguintes inválidos, garantindo a segurança dos dados na *blockchain* [6].

Para garantir a segurança e imutabilidade do sistema, são utilizados alguns métodos de verificação, executados pelos próprios usuários da rede *blockchain* em troca de uma recompensa. *Proof-of-work* é o método utilizado pelo *Bitcoin*, onde os usuários competem entre si para encontrar a *hash* válida para o próximo bloco da cadeia, sendo que o primeiro a encontra-la é recompensado com criptomoedas [1][6]. Graças as propriedades da *blockchain*, como mostrado na **figura 2**, foi possível conceber uma nova fase da internet, de forma verdadeiramente descentralizada e confiável, facilitando o desenvolvimento da *Web3* [5].

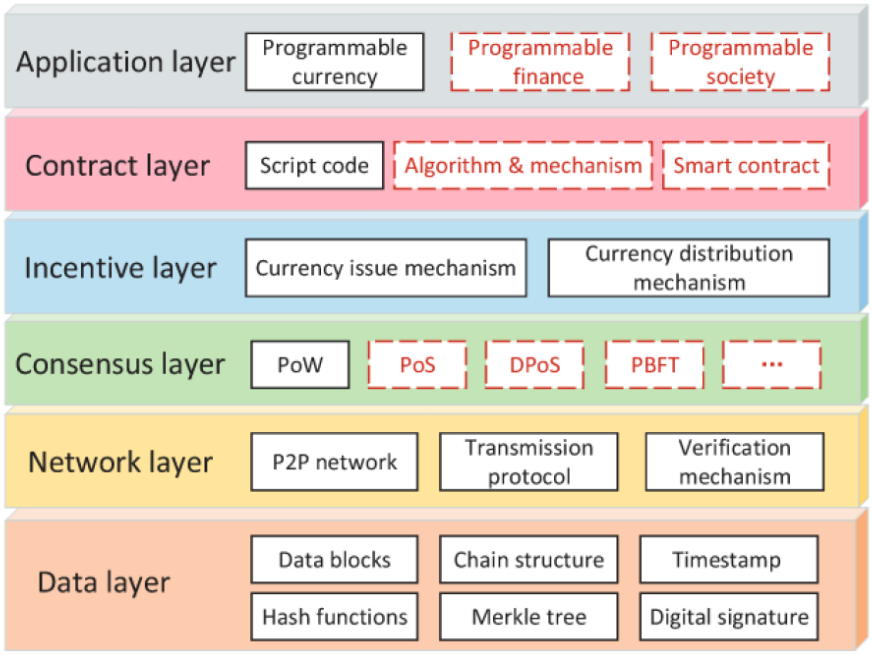


Figura 2: Arquitetura da *Blockchain*, onde o conteúdo em vermelho não faz parte da arquitetura original do *Bitcoin* [5]

2.2 Plataforma *Ethereum*

Em uma perspectiva geral, *Ethereum* é uma infraestrutura de computação global descentralizada que executa programas chamados *smart contracts* ou contratos inteligentes. Ela usa a *blockchain* para sincronizar e guardar as mudanças de estado do sistema, juntamente com uma criptomoeda chamada *Ether*, utilizada para medir e restringir os custos dos recursos de execução [12]. Já em uma perspectiva da ciência da computação, *Ethereum* é uma máquina de estados determinística, mas praticamente ilimitada, consistindo e um estado *singleton* globalmente acessível e uma máquina virtual que aplica as alterações a esse estado [12].

O *Ethereum* foi concebido por Vitalik Buterin, em 2014 e formalmente apresentado no artigo *A next generation smart contract & descentralized application platform* em 2015 [2]. Muito além de executar os *scripts* de validação das transações do *Bitcoin*, o *Ethereum* é capaz de executar qualquer programa em sua máquina virtual, conhecida como *Ethereum Virtual Machine* (EVM) [2]. Para se criar e executar um contrato inteligente na EVM, é cobrado um valor de transação, conhecido como *Gas*, que é a taxa de execução que os remetentes das transações precisam pagar para que a execução ocorra em todos os nós da rede. Sempre que um código é executado, quem solicita a execução estabelece a quantidade máxima de *Gas* que está disposto a consumir e a quantidade de *Ether* que pagará cada unidade gasta [13].

A rede *Ethereum* em sua última versão passou a utilizar o algoritmo de consenso *Proof-of-Stake*, ao invés do *Proof-of-Work*, utilizado pelo *Bitcoin*. Em setembro de 2022 a plataforma terminou o processo de migração para o novo algoritmo de consenso, que ficou conhecido como *Ethereum Merge* [14]. Diferente do *Proof-of-Work*, onde a *hash* é calculada pelo usuário mais rápido, no *Proof-of-Stake* os usuários depositam uma quantia de criptomoedas na rede, para que o sistema selecione aleatoriamente algum membro da *blockchain* para verificar o novo bloco da cadeia, e então caso se tente aprovar um bloco inválido, as criptomoedas depositadas são tomadas [15]. A **figura 3** mostra o fluxo de validação de um bloco utilizando o algoritmo *Proof-of-Stake*.

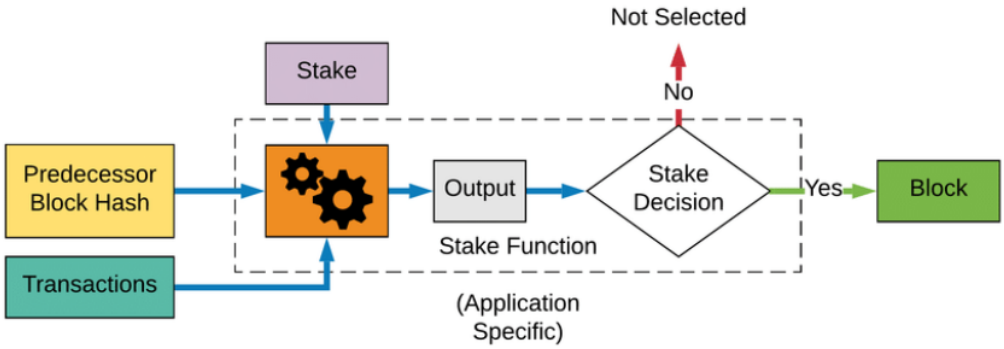


Figura 3: Fluxo do *Proof-of-Stake* [15]

No entanto, *Proof-of-Stake* recompensa com mais frequência os usuários com mais criptomoedas, pois se aprovarem blocos inválidos, mais moedas serão perdidas e por este cálculo de risco são tidos como mais confiáveis, o que cria uma espécie de monopólio na rede. Por outro lado, o algoritmo de consenso traz uma maior escalabilidade e baixo consumo de poder computacional, e consequentemente menor consumo energético para validação de novos blocos da cadeia quando comparado com o *Proof-of-Work* [12].

2.3 Contratos Inteligentes

O conceito de contrato inteligente foi inicialmente proposto por Nick Szabo em 1996, que tinha a proposta de representar digitalmente contratos convencionais de forma a reduzir a necessidade de confiança em intermediários [16]. O conceito só ganhou força após a criação do *Ethereum*, capaz de executar estes contratos em sua *blockchain*, garantindo assim a segurança entre as partes envolvidas através do armazenamento de dados de forma pública e imutável [2]. Os contratos inteligentes oferecem uma base sólida para automação, minimizando o risco de contraparte, aumentando a eficiência, propiciando corte de custos e novos níveis de transparência às operações contratuais [4].

Na *blockchain Ethereum* é possível criar contratos inteligentes com a linguagem de programação *Solidity*, orientada a contratos e desenhada para ser executada na Máquina Virtual *Ethereum* (EVM). A linguagem teve sua sintaxe influenciada por C++, Python e JavaScritpt, sendo é estaticamente tipada, com suporte a herança, bibliotecas e tipos complexos definidos pelo usuário entre outras características [17]. Um exemplo de contrato inteligente é mostrado na **figura 4.**

```
1  // SPDX-License-Identifier: GPL-3.0
2
3  pragma solidity >=0.7.0 <0.9.0;
4
5  contract Storage {
6
7      uint256 number;
8
9      function store(uint256 num) public {
10         number = num;
11     }
12
13     function retrieve() public view returns (uint256){
14         return number;
15     }
16 }
```

Figura 4: Um contrato inteligente simples escrito na linguagem de programação Solidity

2.4 Aplicações Descentralizadas e a *Web3*

Com as novas possibilidades do desenvolvimento de aplicações na rede *Ethereum*, rapidamente se ampliou a visão sobre os contratos inteligentes, fazendo da plataforma uma base para o desenvolvimento de *Decentralized applications* ou *DApps* (aplicações descentralizadas). Podemos definir um *DApp* como uma aplicação baseada em um contrato inteligente e uma interface com o usuário através do navegador *web*. Mais amplamente, os *DApps* devem ser construídos sobre plataformas e protocolos de armazenamento e de mensagens *Peer-to-Peer* (P2P) descentralizados [12].

Para que o navegador *web* possa interagir com a *blockchain*, é utilizado a coleção de bibliotecas *JavaScript Web3.js*, que permite se conectar com um nó da rede *Ethereum*, seja local ou remoto, utilizando o protocolo HTTP, como mostra a **figura 5** [18].

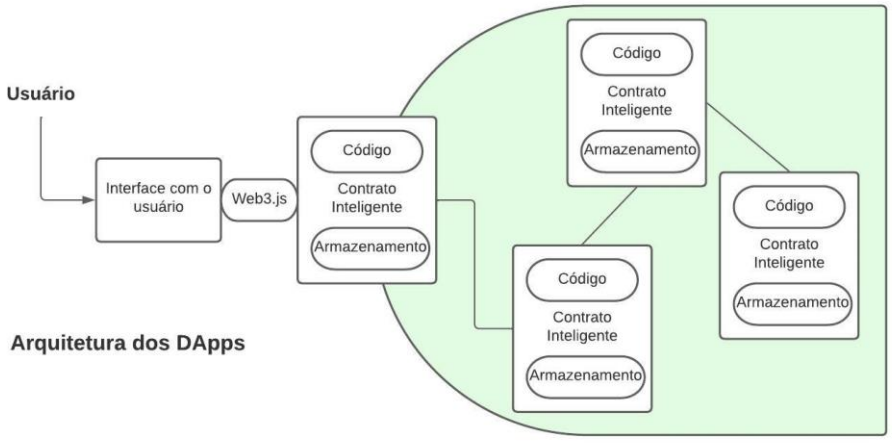


Figura 5: Diagrama com a arquitetura dos *DApps*

O *Web3.js* permite criar, ler e gravar dados de contratos inteligentes, além de transferir *Ether* entre contas, por meio de uma interface de comunicação RPC (*Remote Procedure Call)* implementado por um arquivo JSON (*JavaScript Object Notation)* [18]. O conjunto de bibliotecas também inclui uma interface para o armazenamento de rede P2P chamado *Swarm* e um serviço de mensagens P2P chamado *Whisper*. Com estes componentes executando em um navegador *web*, desenvolvedores tem o arcabouço de desenvolvimento de aplicações completo

para construir aplicações descentralizadas [12].

Para se conectar a uma aplicação *Web3* é necessário estar conectado com uma carteira de criptomoedas. A *MetaMask* é um exemplo de carteira, que conecta a *blockchain Ethereum* com a página *web* descentralizada através de uma extensão para o navegador. Por meio da *Web3.js*, a extensão se conecta a uma instância de nó *backend*, que então se comunica com a *blockchain*, permitindo recebimento e envio de *Ether*, além de ler e escrever dados usando contratos inteligentes [13].

3 CENÁRIOS DE APLICAÇÃO

De forma geral, a *Web3* refere-se à uma possível próxima geração da *web*, com novos recursos técnicos, jurídicos e infraestrutura de pagamentos, que se baseia respectivamente na *blockchain*, contratos inteligentes e criptomoedas. O caráter *peer-to-peer* de *web3* representa uma visão mais equitativa para a *web* do que seu atual estado, a *Web 2.0*, que é dominada pelas grandes empresas de tecnologia [19]. Dado isto, a *Web3* representaria uma ruptura da estrutura centralizada atual da *web*, fazendo emergir uma nova gama de aplicações e junto a ela uma nova forma de economia.

Neste cenário, as atuais aplicações existentes da *Web3* se encaixam nos seguimentos de finanças descentralizadas ou *Decentralized Finance* (*DeFi*), serviços digitais ou colecionáveis. *DeFi* é caracterizado por serviços financeiros *peer-to-peer* baseados, em sua maioria, na plataforma *Ethereum*, que inclui poupança, empréstimos, pagamentos e pontuações de crédito. Já os serviços digitais incluem o provisionamento de serviços de internet descentralizados, como armazenamento em nuvem, infraestrutura *web*, análise de dados e gerenciamento de identidade. E por fim, os colecionáveis incluem artes digitais, lembranças colecionáveis de esporte e produtos virtuais, que se baseiam nos *tokens* não-fungíveis ou *Non Fungible Tokens* (*NFT*) [19]. Um NFT, é um contrato feito com a tecnologia *blockchain* que garante a propriedade, autenticidade e exclusividade de um ativo digital.

Um exemplo de aplicação *DeFi* é a plataforma *Aave*, que é um protocolo de liquidez não custodial descentralizado, no qual os usuários podem participar como depositantes ou tomadores de empréstimo [20]. Outros exemplos são o *Chainalysis*, uma plataforma de serviços digitais de análise de dados, gerenciamento de risco e investigações de crimes cibernéticos, e o *OpenSea*, um mercado de colecionáveis digitais [19].

Um último exemplo é a plataforma *Creatokia*, que permite comprar Originais Digitais (*e-books*, audiolivros) e cunhar, trocar e colecionar livros NFT. A proposta da plataforma é que autores possam publicar seus trabalhos e receber uma parcela direta da receita das vendas, as editoras publiquem edições especiais limitadas e os leitores podem colecionar obras e revende-las assim que desejar [21].

4 DISCUSSÃO

A *Web3* apresenta oportunidades, bem como riscos. Para que esta tecnologia possa evoluir, é cada vez mais necessário que fundos de investimentos compreendam este potencial desta forma aumentar a oferta de capital e talentos disponíveis para empreendimentos *web3* em estágio inicial. Para isto, ainda se faz necessário um arcabouço jurídico e regulatório para dar segurança e atenuar os riscos, de forma a possibilitar os investimentos nesta área [19]. Desta forma, será possível que a tecnologia evolua mais rapidamente, passando a ser uma fonte de investimentos e trazendo soluções mais robustas para o mercado de tecnologia.

Neste cenário, identificou-se que as aplicações se encontram ainda em um estado bastante prematuro, devido ao curto espaço de tempo em que as tecnologias apresentadas ganharam

forma. No entanto, devido ao caráter disruptivo da tecnologia do *blockchain*, em pouco tempo algumas aplicações ganharam notoriedade e relevância perante ao mercado, com algumas delas chegando a valer mais de um bilhão de dólares de valor de mercado [19]. Assim sendo, a *Web3* e as tecnologias derivadas do *blockchain* se despontam como uma fonte de inovação para a indústria e consequentemente uma peça chave para o desenvolvimento tecnológico.

5 CONSIDERAÇÕES FINAIS

Este trabalho apresentou o estudo em torno das tecnologias e aplicações da *Web3*, levando-se em conta os mais recentes trabalhos desenvolvidos na área. Com isto, foi apresentado todo o embasamento teórico e suas tecnologias, que dão suporte ao desenvolvimento de aplicações descentralizadas. Por fim, se analisou alguns exemplos reais já em funcionamento, que vem se destacando pelo seu caráter inovador e disruptivo.

Neste sentido, foi demonstrado que a tecnologia apesar de ser bastante nova, contou com uma série de aperfeiçoamentos, que oferecem uma base bastante sólida para a construção de novos tipos aplicações. Ademais, a maior divulgação no setor de investimentos juntamente com a criação do arcabouço jurídico necessário, impulsionará o desenvolvimento da tecnologia nos próximos anos.

REFERÊNCIAS

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2009.

[2] Vitalik Buterin. A next generation smart contract & decentralized application platform. 2015.

[3] T. O'Reilly, "What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 1008839, Aug. 2007.

[4] GOEL, Amit Kumar; BAKSHI, Rahul; AGRAWAL, Krishna Kant. Web 3.0 and decentralized applications. Materials Proceedings, v. 10, n. 1, p. 8, 2022.

[5] KORPAL, Gaurish; SCOTT, Drew. Decentralization and web3 technologies. 2022.

[6] KASSUYA, Danilo Yudi Futata; BONIFACIO, Adilson Luiz. Verificação de Contratos Inteligentes para Solidity/Ethereum. 2022.

[7] MAZIERI, Marcos Rogério; SCAFUTO, Isabel Cristina; DA COSTA, Priscila Rezende. A TOKENIZAÇÃO, BLOCKCHAIN E WEB 3.0 COMO OBJETOS DE PESQUISA EM INOVAÇÃO. International Journal of Innovation, v. 10, n. 1, p. 1-5, 2022.

[8] What is blockchain technology? IBM, 2021. Disponível em: https://www.ibm.com/topics/what-is-blockchain/. Acesso em: 15 de outubro de 2022.

[9] HABER, S.; STORNETTA, W. S. How to time-stamp a digital document. J. Cryptol., Springer-Verlag New York, Inc., Secaucus, NJ, USA, v. 3, n. 2, p. 99–111, jan. 1991. ISSN 0933-2790.

[10] BASHIR, I. Mastering blockchain. 1a. ed. [S.l.]: Packt Publishing Ltd, 2017. ISBN 9781787125445.

[11] SOUSA, Suzane Carvalho de. Uso da blockchain do Ethereum para a realização de leilões de energia elétrica através da criação de ferramenta WEB. 2019.

[12] ANTONOPOULOS, A. M.; WOOD, G. Mastering ethereum: building smart contracts and dapps. [S.l.]: O'Reilly Media, 2018.

[13] GOULART, Bruno Brigido. Aplicação da tecnologia blockchain no armazenamento de documentos. 2021.

[14] Ethereum's Merge Has Finally Been Completed. Time. 2022. Disponível em: https://time.com/6213329/ethereum-merge-done/. Acesso em: 22 de outubro de 2022.

[15] NATOLI, Christopher; YU, Jiangshan; GRAMOLI, Vincent; VERÍSSIMO, Paulo. Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure. 2019.

[16] SZABO, N. Smart Contracts: Building Blocks for Digital Free Markets. Extropy Journal of Transhuman Thought, 1996.

[17] Solidity, 2016. Disponível em: https://solidityportuguese.readthedocs.io/pt/latest/solidity-by-example.html/. Acesso em: 22 de outubro de 2022.

[18] SIQUEIRA, Pedro Caetano Diniz; DUQUE, José Walmir Goncalves. Get together: estudo e implementação de uma aplicação Blockchain usando Smart Contracts. Revista H-TEC Humanidades e Tecnologia, v. 4, n. Edição Esp, p. 203-219, 2020.

[19] GILBERT, Sam. Crypto, web3, and the Metaverse. 2022. Disponível em: https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2022/03/Policy-brief-Crypto-web3-and-the-metaverse.pdf.

[20] Aave, 2022. Disponível em: https://docs.aave.com/hub/. Acesso em: 14 de novembro de 2022.

[21] Creatokia, 2022. Disponível em: https://www.creatokia.com/en/s/what-is-creatokia/. Acesso em: 15 de novembro de 2022.