Arquitetura de Aplicações Descentralizadas Baseadas em Blockchain

Noelí Antonia Pimentel Vaz
Instituto de Informática - Universidade Federal de Goiás
{noeli.vaz@discente.ufg.br}

1. Introdução

O desenvolvimento de aplicações no contexto da Web 2.0 utiliza, de forma predominante, a arquitetura cliente servidor para gerenciamento do *front-end*, *back-end,* e também, para o armazenamento dos dados. Esse tipo de arquitetura, fortemente centralizada, depende da disponibilização de serviços por terceiros para que a aplicação seja utilizada pelos usuários.

No âmbito da Web descentralizada, também conhecida como Web 3.0, a principal premissa é a retirada do agente centralizador. Essa descentralização pode ser proporcionada nos blocos de construção que compõem uma aplicação (back-end, front-end e armazenamento de dados), ou somente para parte deles. Ao eliminar o agente intermediário entre o usuário e a aplicação, as aplicações descentralizadas (*Decentralized Application* - dApp) utilizam as tecnologias da Web 3.0, para prover a descentralização.

Neste cenário, redes Blockchains se apresentam como um recurso chave para o desenvolvimento de dApps. Blockchain é uma rede composta por nós distribuídos e descentralizados, que possibilitam a execução de operações/ transações autônomas, com garantias pertinentes ao desenvolvimento de aplicações como estado global do sistema, segurança, imutabilidade e a capacidade de auditoria das transações realizadas, entre outras. Blockchain tem se apresentado como tecnologia inovadora e com potencial disruptivo, considerando seu potencial para dar suporte às relações de interações na sociedade. A arquitetura de dApp baseada em blockchain, envolve a utilização de tecnologias voltadas para sistemas descentralizados nas camadas que compõem a aplicação, mantendo, nos contratos inteligentes, a interação entre a lógica de negócio e a própria blockchain.

Este trabalho apresenta uma pesquisa exploratória relacionada aos fundamentos e as tecnologias utilizadas para o desenvolvimento de dApps, visando apresentar uma arquitetura para aplicações descentralizadas baseadas em blockchain. Serão apresentadas arquiteturas e tecnologias utilizadas para o desenvolvimento de dApps baseados em blockchain, visando a proposta de uma arquitetura com o detalhamento dos blocos de construção que a compõem.

As seções a seguir são organizadas da seguinte forma: seção 2 apresenta alguns principais fundamentos de sistemas distribuídos relacionados com a proposta, a seção 3 apresenta a estrutura de redes e plataformas blockchain e, na seção 4 são apresentados fundamentos de dApps baseados em blockchain e a arquitetura proposta. Finalmente, na seção 5 são apresentadas as considerações finais sobre a arquitetura de dApp proposta.

2. Fundamentos de Sistemas Distribuídos

Sistemas Distribuídos são compostos por componentes que realizam tarefas pré determinadas de forma colaborativa, com a comunicação baseada no envio de mensagens. Os componentes de sistemas distribuídos podem ser referenciados como máquinas físicas ou processos de software rodando em rede/ nuvem. A colaboração entre os componentes é requisito básico em sistemas distribuídos, visto que os nós computacionais autônomos necessitam colaborar para realizar suas tarefas. Nesse contexto, os sistemas descentralizados possuem características dos sistemas distribuídos, portanto serão minimamente discutidas as redes par a par (*Peer to Peer* - P2P), coordenação e consenso, protocolos de comunicação e questões relacionadas a escalabilidade, que apresentam conhecimentos relevantes dentro de aplicações descentralizadas.

2.1 Redes Peer-to-Peer

Em redes P2P, dados e recursos computacionais são oriundos da colaboração de muitas máquinas na Internet de maneira semelhante. Sistemas P2P derivam da necessidade de prover recursos compartilhados a um grande número de dispositivos conectados à internet (COULOURIS et al, 2013). Redes P2P modificam o paradigma de comunicação, considerando cenários em que existe um único agente centralizador de serviços. Em uma arquitetura descentralizada, utilizando uma rede P2P, não há servidores dedicados e cada nó pode atuar tanto como cliente ou como servidor. A comunicação nesse ambiente, pode ser realizada utilizando métodos de comunicação distribuída para realizar a troca de informações. O protocolo *gossip* é um exemplo.

2.2 Coordenação e Consenso

Em sistemas distribuídos é necessário que os processos coordenem suas ações e entrem em acordo sobre os valores que serão distribuídos pela rede, para garantir o estado da rede. Algoritmos de eleição e consenso distribuído são utilizados para garantir a coordenação dos processos para garantir a consistência dos dados, além do estado do sistema.

2.3 Protocolos de consenso

Os protocolos de consenso permitem que um conjunto de processos independentes concorde sobre um mesmo valor proposto. É um bloco básico de construção de sistemas tolerantes a faltas, comunicação em grupo, entre outras aplicações. Protocolos de consenso são utilizados em sistemas de cadeia de blocos com o objetivo de garantir uma decisão descentralizada e uniforme sobre qual bloco deve ser adicionado à cadeia de blocos.

Estratégias podem ser adotadas para esta tomada de decisão. As principais abordagens são listadas:

- Qualquer nó da rede pode propor blocos, e o protocolo verifica qual bloco, dentre os propostos, deve ser incluído na cadeia.
- Primeiro o protocolo define quais nós poderão propor outros nós à rede.

A decisão pela escolha do bloco não pode ser resolvida por um pequeno conjunto de participantes, visto que isso implicaria problemas relacionados à escalabilidade. A seguir, são apresentados os principais protocolos de consenso:

Prova de Trabalho (PoW - *Proof-of-Work*) - Neste protocolo nós chaves, denominados mineradores, competem entre si para ganhar o direito de produzir novo bloco, desta forma, esses nós podem colotar recompensas e taxas de transação, pela tarefa realizada de produzir um novo nó. Neste processo é proposto a resolução de um desafio computacional. A dificuldade para resolver este desafio sofre ajustes a cada 10 minutos, em média. O desafio é basicamente a busca por um valor, denominado nonce, que produza uma Hash para o bloco iniciando com um determinado número de bits em 0. O nonce é um campo de 32 dígitos, necessitando de muitas tentativas até que o número n de bits 0 seja alcançado. O nome Prova de Trabalho é devido ao grande esforço computacional que é necessário para alcançar a tarefa. Quando mais de um bloco consegue resolver o desafio criptográfico e propõem um bloco para uma mesma posição da cadeia, a decisão final é pela cadeia mais longa, que exprime maior esforço computacional. O nível de dificuldade da prova de trabalho aumenta ou diminui de acordo com o tempo de mineração dos blocos.

Prova de Participação (PoS - *Proof-of-Stake*) -Realiza o processo de de consenso com menor esforço computacional que o PoW, por isso se apresenta como uma alternativa. Nesse

protocolo, qualquer usuário pode realizar um tipo especial de transação. É atribuído um validador a qualquer usuário que enviar um valor x de unidade monetária, que ficará retido, como garantia de honestidade. Esse valor é chamado de participação. Em certos tipos de sistemas, quanto maior a participação, maior será a chance de ser eleito líder e propor um novo bloco na rede.

2.4 Protocolos de Comunicação

Comunicação entre os blocos que compõem as DApps são realizadas por meio de troca de mensagens. São utilizados nas aplicações, formatos de dados padronizados e APIs como JSON-RPC, RESTful APIs, GraphQL.

3. Blockchain

Blockchain é uma rede que permite o compartilhamento de dados e transações em uma rede estruturada de forma descentralizada, que não requer um ponto central de confiança. Blockchains são projetadas para atender objetivos em ambientes descentralizados e, são constituídas pela junção de tecnologias clássicas (ou elementares) da ciência da computação, como: computação distribuída, estruturas de dados, criptografia e hashing, algoritmos de consenso, redes peer-to-peer (P2P), entre outras.

A infraestrutura necessária para suportar uma rede Blockchain pode variar dependendo da sua implementação. Em geral, uma rede Blockchain requer uma rede distribuída de nós com poder computacional suficiente para processar e validar as transações, levando-se em conta que o objetivo da Blockchain é a transferência de valores de forma segura, aberta e imutável. A rede pode utilizar protocolos para facilitar a comunicação e a coordenação entre os nós, como mencionado, e necessitar de soluções de armazenamento seguro para proteger os blocos do acesso não autorizado ou de adulteração. Por fim, a rede pode exigir alguma forma de mecanismo de incentivo, como, por exemplo, recompensas na forma de criptomoeda, para incentivar novos nós a participar da validação e manutenção dos blocos, além da expansão da cadeia de blocos.

A evolução das plataformas blockchain são geralmente classificadas em gerações que compreendem as evoluções do Bitcoin até as blockchains atuais. A primeira geração, denominada Bitcoin, possui foco no caso de uso de criptomoedas e possui foco no registro de suas transações. Na segunda geração de plataformas blockchain, sua utilização é evoluída para além das criptomoedas, pois a criação dos contratos inteligentes (*smart contracts*) permite a escrita de código para o registro de interações dentro de outros cenários,

possibilitando assim a construção de aplicações descentralizadas (decentralized application - dApp). A terceira geração tem foco na criação de plataformas blockchain para aplicações corporativas (CONNORS e SARKAR, 2023).

Blockchains permitem novas formas de arquiteturas de softwares distribuídos. Sistemas baseados em Blockchain requerem arquiteturas que possibilitam a interação entre a aplicação e as tecnologias da Web 3.0 e seus protocolos, conforme apresentado na Figura 1.

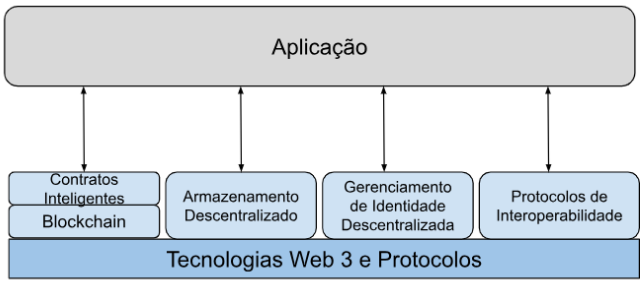

Figura 1: Interação entre aplicação e tecnologias Web 3 e protocolos.

As tecnologias Web 3 incluem Blockchain e os smart contracts, armazenamento descentralizado, gerenciamento de identidade descentralizada e os protocolos de interoperabilidade. Para Ray (2023), as tecnologias Web 3 e protocolos, permitem a criação de sistemas seguros, transparentes e descentralizados, que permitem maior confiança e inovação. Blockchain é a tecnologia base para o desenvolvimento de Aplicações Descentralizadas (Decentralized Application - DApp) no âmbito da Web 3.

Um exemplo de um dApp poderia ser uma aplicação que acumula tokens ou alguma moeda específica, à medida que o usuário realiza ações que promovam seu auto cuidado em saúde, como consultas de rotina, atividades físicas com frequência, consumo de alimentos saudáveis, entre outros. O dApp seria integrado a algum órgão de gestão governamental que seria responsável pela validação e troca dos tokens dos usuários por incentivos de diferentes tipos, como: redução de impostos, priorização de serviços e indicação de atividades em ações governamentais, entre outros.

Greve et al. (2018) destacam que o consenso da blockchain é fortemente voltado ao tipo de rede a que se destina. Redes blockchain podem ser classificadas em: pública, privada/ federada, permissionada (*permissioned*) e não permissionada (*permissionless*).

Em redes blockchain públicas os nós são desconhecidos e é permitida a entrada e a saída aleatórias de nós da rede. Neste tipo de rede, não há controle dos seu participantes, e a rede pode funcionar em escala mundial. São exemplos de redes deste tipo as plataformas

Bitcoin, Ethereum e Solana. As redes públicas podem exigir alguma forma de mecanismo de incentivo aberto e baseado em mineração, com recompensas na forma de criptomoeda. Nós denominados mineradores entram em uma competição com base no poder computacional (e.g., PoW da Bitcoin), poder de posse (e.g., PoS da Ethereum) ou outras capacidades relevantes para a eleição e que não podem ser monopolizadas.

Em blockchains privadas os nós da rede são identificados, autorizados e autenticados por nós com autoridade previamente conferida. As entradas e saídas de nós estão condicionadas por permissões e, em geral, funcionam em escala menor abrangendo corporações ou organizações em que os participantes possuem papéis bem definidos. Exemplos são os protocolos PoA (proof of authority) ou Prova de Autoridade, disponíveis no Hyperledger Fabric e Hyperledger Besu.

Nas redes híbridas ou consorciadas existe um conjunto de participantes (nós) da rede trabalhando como validadores com algum nível de confiança. O uso do consenso PoA é uma vantagem, visto que os nós validam transações de forma mais otimizada, trazendo mais velocidade ao processo de consenso. Iniciativas como a Rede Blockchain Brasil (RBB) se enquadram nesse tipo de rede.

A escolha do mecanismo de consenso dependerá dos requisitos, objetivos específicos e decisões do projeto em desenvolvimento. Alguns projetos podem preferir eficiência e velocidade (PoA), enquanto outros podem optar por descentralização e segurança (PoS). WÜST & GERVAIS, 2018 realizaram a proposta de decisões relacionadas ao tipo de redes blockchain, que podem ser visualizadas na Figura 2 e que consideram questões relevantes relacionadas ao projeto da aplicação, que ao serem respondidas, realiza o direcionamento para o tipo de rede adequado para o projeto.

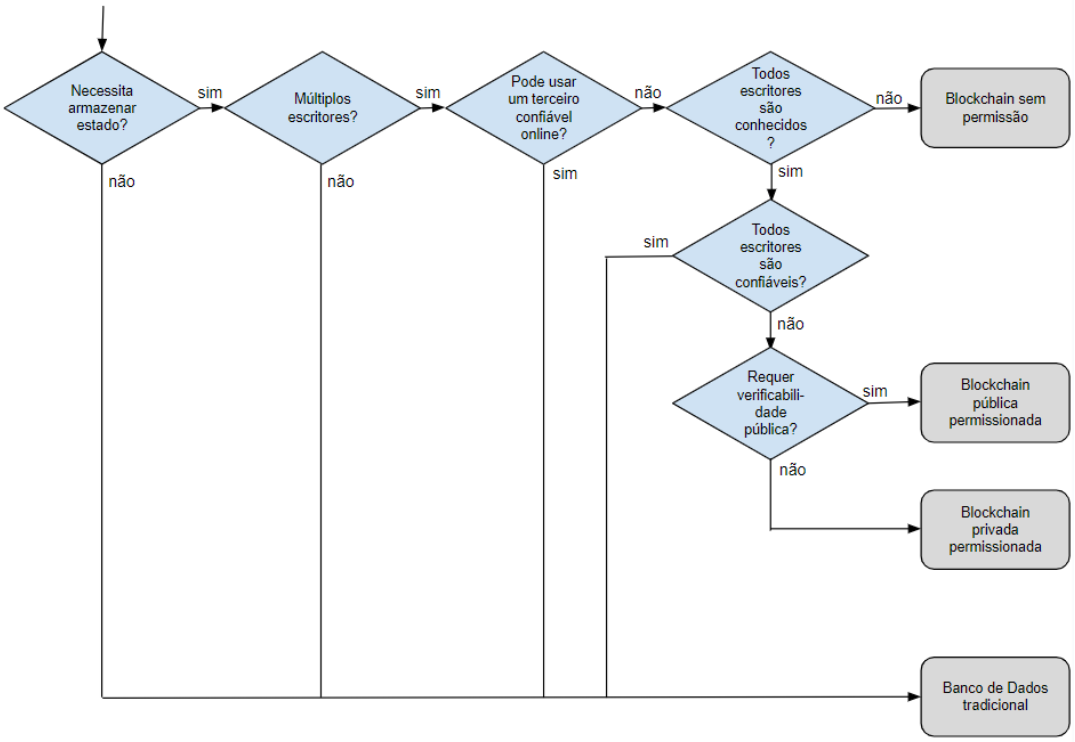

Figura 2 - Fluxograma com decisões sobre o tipo de blockchain. Fonte: Adaptado de WÜST & GERVAIS, 2018.

Após a definição do tipo de rede, é necessário conhecer iniciativas de plataformas blockchain disponíveis e adequadas ao tipo de rede selecionado para o projeto.

3.1 Plataformas Blockchain

As principais iniciativas de plataformas blockchain passam pelos projetos Ethereum e Hyperledger. Serão apresentadas características das principais plataformas blockchains utilizadas no desenvolvimento de dApps: Ethereum e Hyperledger.

3.1.1 Ethereum

Ethereum é uma plataforma de blockchain open source usada para criar dApps utilizando contratos inteligentes (*smart contracts*). A plataforma ferece uma rede pública, sem necessidade de controle de seus participantes e, portanto, caracterizada por uma rede em que não há qualquer confiança entre os nós. A Ethereum já utilizou o consenso PoW e, atualmente, usa o consenso PoS. Embora esse mercado esteja em grande atividade em que diariamente surgem novas técnicas, ferramentas e plataformas, a tomada de decisão passa pelas duas plataformas de referência.

3.1.2 Hyperledger

A Hyperledger é uma plataforma de blockchain de código aberto projetada para uso empresarial. Foi iniciada pela Linux Foundation em 2015 e atualmente é uma das principais iniciativas colaborativas nesse campo. Ao contrário de outras plataformas de blockchain, a Hyperledger não se concentra em criptomoedas, mas sim em oferecer um framework flexível e modular para o desenvolvimento de aplicativos e soluções empresariais baseadas em blockchain.

A Hyperledger é construída com base em alguns princípios fundamentais que a diferenciam de outras plataformas de blockchain:

a) Código aberto e colaborativo: A Hyperledger é uma iniciativa de código aberto que incentiva a colaboração entre empresas e desenvolvedores. Isso permite uma maior transparência e promove a inovação e a adoção generalizada da tecnologia.

b) Foco em casos de uso empresarial: Ao contrário de outras plataformas de blockchain, a Hyperledger se concentra em resolver problemas específicos enfrentados pelas empresas. Ela fornece ferramentas e recursos para o desenvolvimento de soluções empresariais eficientes e seguras.

c) Modularidade e flexibilidade: A arquitetura da Hyperledger é modular, permitindo que os desenvolvedores escolham os componentes específicos que melhor atendam às necessidades de seus projetos. Isso garante uma maior flexibilidade e adaptabilidade da plataforma.

Graduated Hyperledger Projects:

a) Hyperledger Fabric: É o principal framework da Hyperledger e oferece um ambiente para o desenvolvimento de redes de blockchain empresariais. Ele suporta a criação de contratos inteligentes e permite a configuração de diferentes políticas de governança.

b) Hyperledger Sawtooth: Outro framework da Hyperledger, o Sawtooth, é projetado para fornecer escalabilidade e modularidade. Ele apresenta uma arquitetura flexível e suporta a implementação de algoritmos de consenso personalizados.

c) Hyperledger Indy: Esse componente da Hyperledger é focado na identidade digital descentralizada e fornece recursos para criar e gerenciar identidades digitais confiáveis.

Diariamente surgem novas técnicas, ferramentas e plataformas de blockchain, devido à grande atividade deste mercado. Porém, a tomada de decisão para o qual plataforma blockchain utilizar no desenvolvimento de dApps, passa pelas duas plataformas de referência. Há, por exemplo, plataformas como a Solana, Polygon, Avalanche, Hyperledger Besu que

são compatíveis com a EVM, a máquina virtual da Ethereum que permite a execução dos contratos inteligentes e a construção de aplicações.

4. dApps baseadas em Blockchain

Uma aplicação descentralizada pode ser considerada, portanto, uma aplicação web aberta, desenvolvida sobre serviços de infraestrutura P2P (Antony & Wood, 2018).

Conhecer as principais plataformas blockchain disponíveis e seus requisitos de implantação se faz necessário para projetar aplicações descentralizadas baseadas em blockchain. Xu et. al. (2017) afirmam que ao criar aplicativos baseados em blockchains, precisamos considerar sistematicamente os recursos e as configurações de blockchains e avaliar seu impacto na qualidade e atributos para os sistemas globais e, para isso, os autores desenvolveram um processo para auxiliar a tomada de decisão relacionada ao uso de blockchain em sistemas. A Figura 3 é baseada no processo proposto em Xu et. al. (2017).

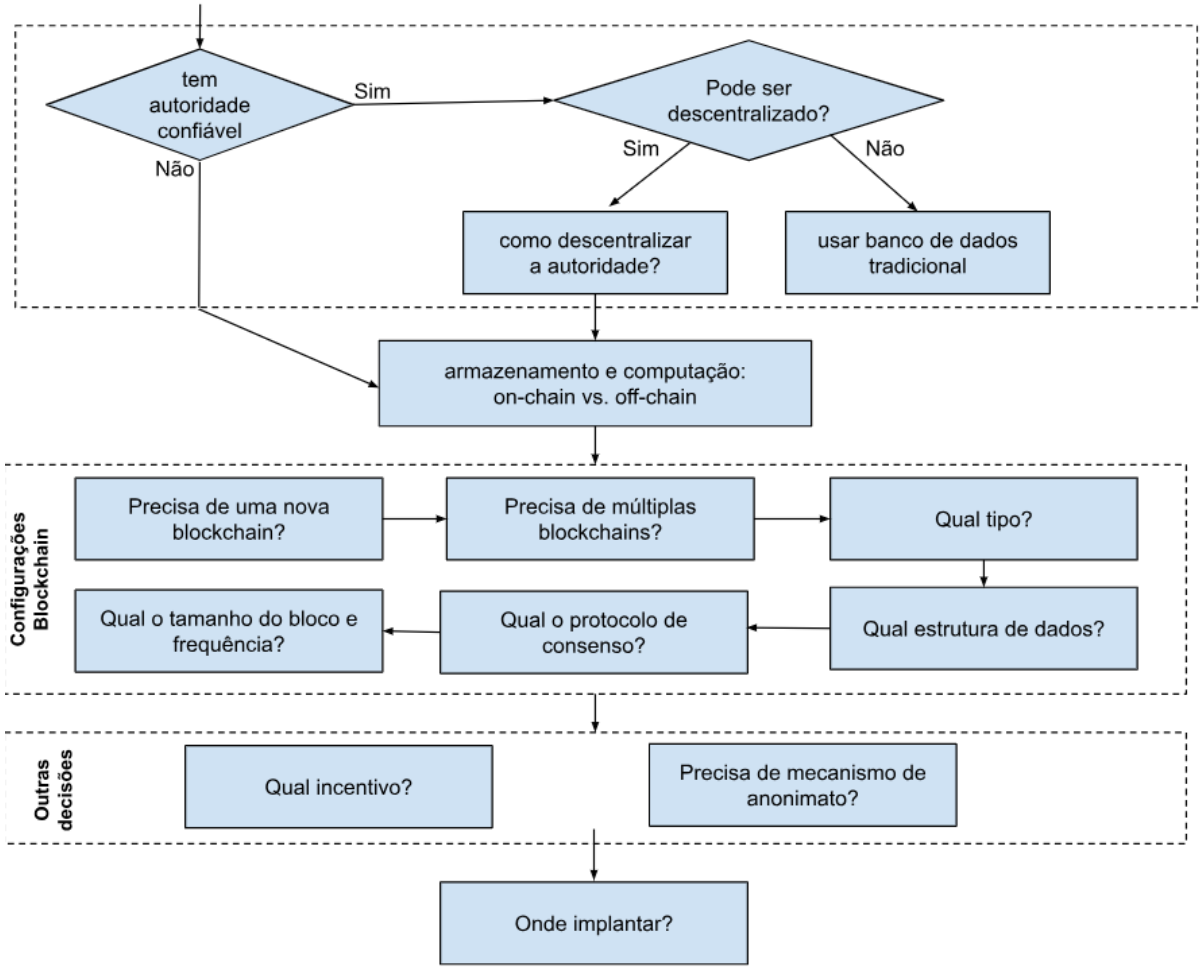

Figura 3: Design process para sistemas baseados em blockchain. Adaptado de Xu et. al. (2017)

Um dos requisitos para criar essas aplicações ou serviços tem sido o uso de plataformas de blockchain descentralizadas, como é o caso da Ethereum (Buterin, 2014).

4.1 Arquitetura de dApps

Em termos de concepção arquitetural das aplicações descentralizadas, há uma discussão em relação ao grau de descentralização (total ou parcial) que se deseja de tais aplicações, envolvendo eminentemente duas dimensões: operacional e de dados.

Quando se trata da dimensão operacional, o grau de descentralização é analisado tendo-se como pressuposto o tipo de rede blockchain envolvida e o emprego de contratos inteligentes (Xu et al., 2017). Nesta vertente, aplicações baseadas em rede blockchain pública são consideradas totalmente descentralizadas, dada a natureza de tais redes em que não há nós centralizadores. Diferentemente, aplicações baseadas em redes blockchain privadas são consideradas apenas parcialmente descentralizadas, pois tem-se como premissa a existência (muitas vezes previamente definida, como no caso das redes consorciadas) de nós com algum grau de confiança e, portanto, com potencial de centralização por serem responsáveis pela validação das atividades da rede.

Ao tratar da dimensão de dados, o grau de descentralização é também analisado considerando-se o serviço de armazenamento usado pelas aplicações. Aqui, a tecnologia que vem sendo utilizada de suporte às aplicações totalmente descentralizadas, entre outras, é a IPFS, um sistema de arquivos descentralizado e baseado na estrutura de uma rede P2P (Zheng et al., 2023.

Portanto, uma aplicação totalmente descentralizada requer uma rede blockchain do tipo pública e, ainda, a descentralização do armazenamento por meio de uma rede P2P como a oferecida pela tecnologia IPFS (*Interplanetary File System*)). Uma aplicação parcialmente descentralizada significa aquela, ou baseada em uma rede blockchain do tipo privada, ou cujo armazenamento seja centralizado.

A Figura 4 propõe uma arquitetura geral para dApps baseadas em blockchain para redes públicas. Essa visão envolve a utilização, no nível da aplicação, de blocos de construção e de tecnologias subjacentes, como protocolos, APIs, carteira e, no nível mais baixo, da própria blockchain e o seu funcionamento.

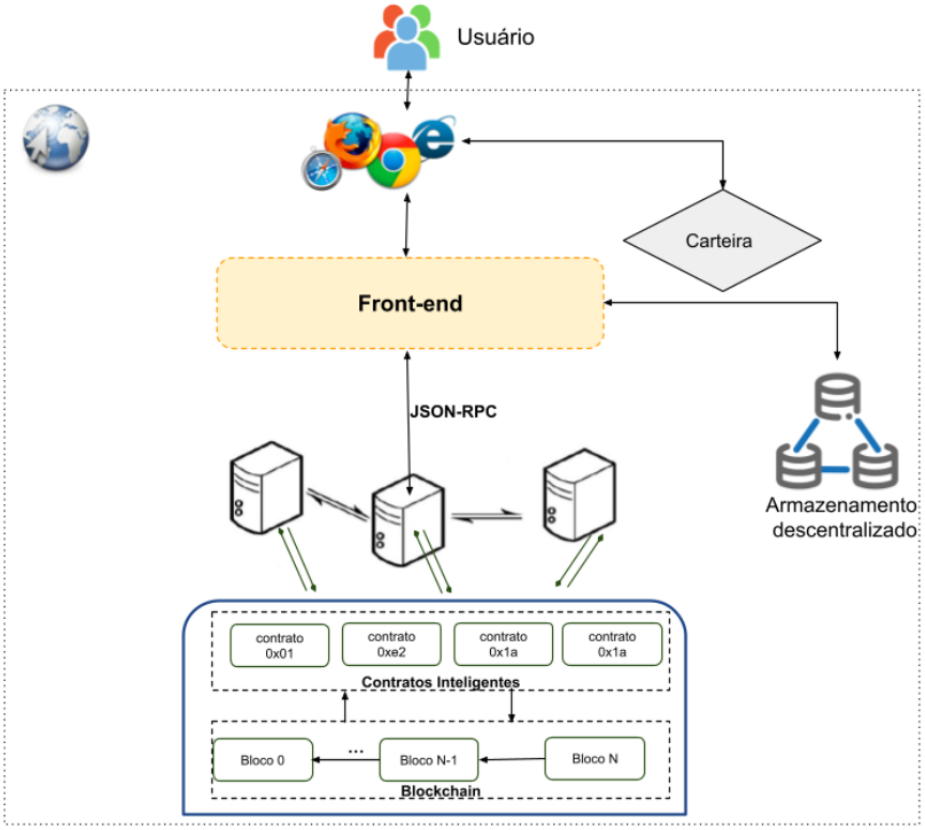

Figura 4: Arquitetura de dApp baseada em blockchain públicas

Os blocos de construção que compõem dApps baseada em blockchain são detalhados a seguir.

- Front-end : define a interface do usuário, que se comunica com a lógica da aplicação, por meio dos contratos inteligentes. Para a construção de interfaces, são utilizadas bibliotecas Javascript como React.js , Node.js. Bibliotecas são utilizadas para prover a interação da aplicação com a blockchain Ethereum como web3.js7, ether.js, dentre outras.
- Carteira: possibilita que usuários assinem transações utilizando sua chave privada, antes que sejam transmitidas para a blockchain. Além disso, auxilia o gerenciamento de permissões que seja possível o compartilhamento de dados, armazenamento de criptomoedas, NFTs e outros. Metamask e Taho são exemplos de carteiras.
- JSON-RPC: protocolo de comunicação da aplicação com a blockchain, que provê a interação, sem a necessidade de participar da rede. Muitas vezes esse papel é denominado provider, como por exemplo a Infura.

- Armazenamento descentralizado: conforme citado, IPFS é um exemplo desta tecnologia.
- Contratos Inteligentes: definem a lógica de negócio das mudanças que são executadas na blockchain. Linguagens de programação de alto nível como Solidity e Vyper, são utilizadas para escrever contratos inteligentes.

Importante observar que a estrutura proposta é adequada para dApps implementadas sobre uma estrutura de rede blockchain pública EVM ou baseadas.

5. Considerações Finais

O estudo apresentado buscou pavimentar o caminho para um entendimento mais amplo das dApps baseadas em blockchain, buscando identificar as principais decisões relacionadas às características da plataforma blockchain para melhorar a visão arquitetural de uma dApp baseadas em blockchain. Foi possível observar que a arquitetura da dApp está relacionada às principais decisões tomadas durante seu projeto, visto que existem características peculiares a redes blockchain pública e privada que direciona fortemente a estrutura da aplicação descentralizada. Como continuidade do estudo será realizada a definição da stack voltada para principais decisões de projeto para cada tipo de rede (pública e privada) e, por fim, a implementação de uma aplicação para cada stack proposta.

6. Referências

A. M. Antony e G. Wood, Mastering Ethereum: Building Smart Contracts and DApps, 2nd ed. O'Reilly Media, 2018.

COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim; et al. Sistemas distribuídos. Grupo A, 2013. E-book. ISBN 9788582600542. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788582600542/. Acesso em: 18 jun. 2023.

CONNORS, Collin; SARKAR, Dilip. Survey of prominent blockchain development platforms. Journal of Network and Computer Applications, p. 103650, 2023.

[166] J. Zarrin, H. Wen Phang, L. Babu Saheer, e B. Zarrin, "Blockchain for decentralization of internet: prospects, trends, and challenges," Cluster Computing, v. 24, n. 4, p. 2841–2866, 2021.

WÜST, Karl; GERVAIS, Arthur. Do you need a blockchain?. In: **2018 crypto valley conference on blockchain technology (CVCBT)**. IEEE, 2018. p. 45-54.

A. M. Antony e G. Wood, Mastering Ethereum: Building Smart Contracts and DApps, 2nd ed. O'Reilly Media, 2018.

COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim; et al. Sistemas distribuídos. Grupo A, 2013. E-book. ISBN 9788582600542. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788582600542/. Acesso em: 18 jun. 2023.

GREVE, Fabíola Greve et al. Blockchain e a Revolução do Consenso sob Demanda. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos, 2018.

V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," Bitcoin Magazine, v. 20, 2014. [Online]. Available: https://bitcoinmagazine.com/technology/ethereum-next-generation-smart-contract-and-decentralized-application-platform-1390528211

X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, e P. Rimba, "A taxonomy of blockchain-based systems for architecture design," in 2017 IEEE international conference on software architecture (ICSA). IEEE, 2017, p. 243–252.

ZHENG, Peilin et al. Blockchain-based Decentralized Application: A Survey. IEEE Open Journal of the Computer Society, 2023.