Blockchain e Sistemas Distribuídos: conceitos e implicações

Maurício Witter

Departamento de Tecnologia da Informação
Universidade Federal de Santa Maria - Campus Frederico Westphalen

14 de novembro de 2023

Resumo - A tecnologia Blockchain emergiu como uma necessidade da descentralização dos meios de pagamento e transações, mas que trouxe consigo muitas propriedades de sistemas distribuídos que a tornaram uma tecnologia primordial para superar alguns dos desafios da sociedade, especialmente no contexto de descentralização dos serviços, transparência das informações, disponibilidade e segurança. Sua arquitetura e formas de comunicação, embora, possuem algumas nuances complexas de entender, especificamente para o público leigo no assunto de sistemas distribuídos, protocolos e redes de computadores. Neste artigo iremos explorar alguns tópicos de sistemas distribuídos relacionados à tecnologia Blockchain.

Keywords: Blockchain; Peer-to-Peer; RPC

1 INTRODUÇÃO

A tecnologia *Blockchain* nasceu como uma tecnologia disruptiva que logo conquistou holofotes, principalmente por sua envoltura aplicação em ativos digitais, logo conhecida como o *Bitcoin*. O termo "Blockchain" é usado para descrever uma estrutura de dados, as vezes o sistema como um todo (XU et al., 2017, p. 244), mas para este contexto definimos como uma estrutura de dados, onde "Block" se refere a um bloco de transações e "chain" refere-se a cadeia que conecta os blocos por meio de uma *hash*. Assim, a *Blockchain* é uma cadeia de blocos ordenada e encadeada, onde o bloco subsequente contém um *hash* da representação do bloco anterior, como mostra a figura 3.

A tecnologia Blockchain faz uso de uma rede *Peer-to-Peer*(XU et al., 2017, p. 243), essa rede é definida como uma rede *overlay* (rede sobreposta). As redes *Peer-to-peer* (P2P) são sistemas distribuídos por natureza, sem qualquer organização hierárquica ou controle centralizado. Os pares formam topologias de redes virtuais sobrepostas auto-organizadas acima da topologia de rede física (LUA et al., 2005, p. 1). Essencialmente, os nós da rede formam uma rede virtual que utiliza protocolos gerais para atuar sobre o Protocolo de Internet (IP) e, assim, fazer a conexão entre os pares na rede.

No contexto de arquitetura de software, a tecnologia Blockchain permite novas formas de arquiteturas de software distribuídas, onde o acordo sobre o estado compartilhado para dados descentralizados e transacionais pode ser estabelecido através de uma grande rede de participantes não confiáveis (XU et al., 2017, p. 243). Ou seja, não há um estabelecimento de confiança entre nenhuma das partes, o nó da rede pode ser um individuo bem-intencionado, uma entidade ou um individuo mal-intencionado, não há o estabelecimento de uma conexão de confiança prévia pois o algoritmo de consenso garante a validade e segurança nas transações, o que é realmente importante para cenários descentralizados.

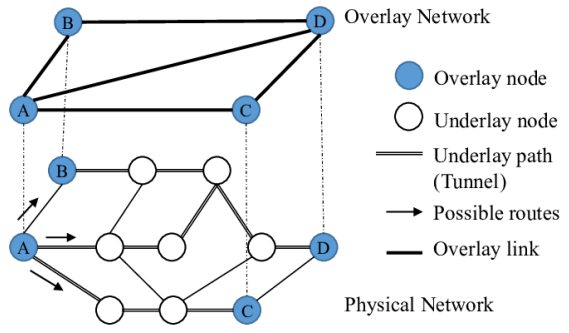
Este artigo tem como objetivo analisar a

arquitetura da tecnologia *Blockchain* e como ela incorpora conceitos de sistemas distribuídos para tornar as aplicações robustas, resilientes, tolerantes a falhas, decentralizadas e seguras. Este trabalho pode ser utilizado futuramente para desenvolver aplicações práticas ou servir como um guia de entendimento a alguns dos conceitos das tecnologias blockchains.

2 PEER-TO-PEER

Diferentemente do modelo cliente-servidor, conhecido também como *Three-Tier Architecture*, que realiza a comunicação diretamente com o modelo TCP/IP, as redes *Peer-to-Peer* são redes virtuais implementadas acima do modelo TCP/IP. A figura 1 apresenta uma conceituação visual de como a rede sobreposta interage com a rede física. Por exemplo, se o nó de sobreposição **A** tiver tráfego para o nó **D**, ele poderá roteá-lo diretamente usando o túnel de **A** a **D** ou retransmiti-lo através de outro nó de sobreposição **B** ou **C** (RAI; SINGH; MODIANO, 2016).

Figura 1: Arquitetura de rede sobreposta.

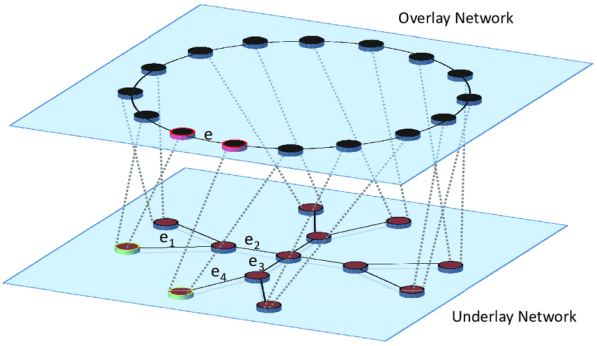


Fonte: Rai, Singh e Modiano (2016).

É importante destacar que, a comunicação real entre dois nós conectados por um link na sobreposição é realizada por meio de conexões que existem em uma ou mais camadas de rede subjacentes. A rede física ainda é responsável pelos mecanismos básicos de transporte, endereçamento e roteamento. Os serviços de nível superior como redes de sobreposição utilizam esses mecanismos como meio para a internet (SCHOLTES, 2011, p. 17–18).

Enquanto a rede física faz o trabalho de roteamento e transporte para a internet, no nível superior podem ser implementados esquemas de endereçamento e roteamento personalizados para os nós da rede, o que acontece na maioria das aplicações *Peer-to-Peer*, como a *Blockchain*. Assim, sobreposições de alto nível podem ser usadas para desenvolver novos serviços e aplicações sem a necessidade de implantar novos dispositivos ou protocolos na base (SCHOLTES, 2011, p. 18).

Figura 2: Topologia Overlay (acima) e Topologia Underlay (abaixo)



Fonte: Scholtes (2011).

Conforme Lua et al. (2005, p. 1), as redes de sobreposição possuem uma combinação de vários recursos, como arquitetura robusta de roteamento de área ampla, pesquisa eficiente de itens de dados, seleção de pares próximos, armazenamento redundante, permanência, nomenclatura hierárquica, confiança e autenticação, anonimato, escalabilidade massiva e tolerância a falhas.

Embora pareça, a seleção de pares não é simplesmente aleatório. Segundo (LUA et al., 2005, p. 72–73), a topologia da rede de sobreposição P2P é rigidamente controlada e o conteúdo é colocado em locais específicos que farão com que consultas subsequentes sejam mais eficientes. Tais sistemas P2P es-

truturados usam a Tabela Hash Distribuída (DHT), na qual as informações de localização do objeto de dados (ou valor) são colocadas deterministicamente, nos pares com identificadores correspondentes à chave exclusiva do objeto de dados.

Os sistemas baseados em DHT têm uma propriedade que atribui consistentemente *NodeIDs* aleatórios uniformes ao conjunto de pares em um grande espaço de identificadores. Então, cada par mantém uma pequena tabela de roteamento que consiste nos *NodeIDs* e endereços IP de seus pares vizinhos. Consultas de pesquisa ou roteamento de mensagens são encaminhadas através de caminhos de sobreposição para pares de maneira progressiva, com os *NodeIDs* que estão mais próximos da chave no espaço do identificador (LUA et al., 2005, p. 73).

Conforme (EISENBARTH; CHOLEZ; PERRIN, 2023, p. 76-79), o Ethereum e o Sistema de Arquivos Interplanetário (IPFS) fazem uso do algoritmo de DHT *Kademlia*. *Kademlia* é um algoritmo de tabela de hash distribuída (DHT) usado em redes *peer-to-peer* (P2P). Este algoritmo é usado principalmente para manter uma lista de nós em uma rede P2P de maneira eficiente e escalável. Ele é conhecido por sua capacidade de pesquisar nós e dados na rede de forma rápida e eficaz. Assim, ele usa *IDs* de nós e *IDs* de recursos para organizar os nós em uma estrutura de árvore binária.

Cada nó na rede *Kademlia* é identificado por um *ID* único, que é uma sequência binária de tamanho fixo, geralmente de *160 bits*. Os nós são organizados em uma árvore binária, e a proximidade entre dois nós é calculada usando a distância *XOR* entre seus *IDs*. Quanto mais próximos são os *IDs*, mais próximos os nós estão na árvore (LUA et al., 2005, p. 79–80).

Assim, o uso de redes *overlay* possibilitou novas formas de criar sistemas distribuídos, as novas tecnologias como a Blockchain permitem criar um ecossistema colaborativo e altamente escalável. Os pares compartilham seus recursos computacionais e, além de cliente, torna-se um servidor. Ou seja, cada par da rede atua por uma via bidirecional fazendo ambos os papéis, o que elimina a necessidade de servidores centralizados e contratação de serviços de *cloud computing*.

Cabe ressaltar que, a implementação de redes *overlay* é de alta complexidade, uma vez que não existe de fato uma RFC (*Request for Comments*) ou padronização internacional de implementação, os modelos de endereçamento e roteamento podem ser customizados na rede *overlay*, o que lhe concede liberdade mas também lhe da complexidade.

3 BLOCKCHAIN

A *Blockchain* como um sistema distribuído possui muitos elementos, como já citado, funciona em uma rede *overlay* e utiliza o poder de processamento, a largura de banda e a capacidade de armazenamento das máquinas dos pares da rede. Ademais, possui cadeias e blocos para armazenar os dados com segurança. Mas não obstante, a *Blockchain* é um construto de algoritmos criptográficos, de consenso e de execução de código (*Smart Contracts*).

A primeira geração de Blockchain veio com o Bitcoin (NAKAMOTO, 2009). Essa geração elementar possuía muitas limitações que foram sendo aprimoradas ao longo do tempo. Mas, especialmente, a segunda geração de Blockchain trouxe uma revolução ao permitir a implantação e execução de código por usuários em uma Blockchain (*turing-complete*) (XU et al., 2017, p. 244).

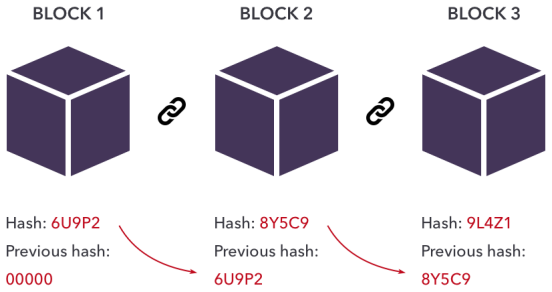
Uma Blockchain implementa um *ledger* (livro-razão) distribuído, que pode, em geral, verificar e armazenar qualquer tipo de transação (XU et al., 2017 apud TSCHORSCH; SCHEUERMANN, 2016, p. 1–2). Cada nó da rede possui uma cópia idêntica do livro-razão, com isso, os nós da rede podem verificar a partir de algoritmos de consenso as transações de forma transparente e confiável, o que elimina a necessidade de um servidor central confiável.

O livro-razão é o banco de dados de uma

Blockchain elementar, estruturado pela cadeia de blocos, conforme mostra a figura 3. Esse livro-razão registra todas as transações feitas pelos pares da rede da *Blockchain* e são públicos.

A figura 3 mostra uma representação de como são os blocos de cadeias de uma *Blockchain*. Elementarmente, tem-se uma cadeia linear de blocos, onde o bloco possui seu *hash* e o *hash* do conteúdo anterior.

Figura 3: Estrutura de dados utilizada para representar os blocos e cadeias da Blockchain.



Fonte: Dimitriadis et al. (2022).

As transações são constituídas de uma carga útil, em outras palavras, pacotes de dados que armazenam parâmetros como valor monetário, endereço do destinatário e resultados de chamadas de função (como contratos inteligentes) (XU et al., 2017).

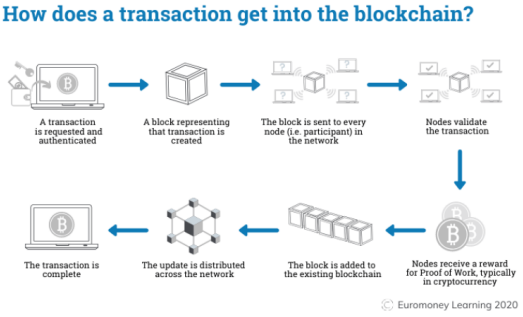
Uma transação passa por uma série de etapas até ser registrada de fato no livro-razão, como mostra a figura 4. Conforme Xu et al. (2017), uma transação é assinada por quem a iniciou, para autorizar a carga útil de dados de uma transação ou a criação e execução de um contrato inteligente (*smart contract*).

O remetente assina a transação com sua chave privada (*private key*) para provar que é proprietário da transação. A transação é propagada para os nós conectados à rede *Blockchain*, que fazem a validação inicial a fim de checar se a transação atende as regras do protocolo. Quando a maioria dos pares concorda que a transação é válida, a transação é enviada ao grupo de transações válidas (*mempool*).

Os mineradores da rede (*mining nodes*) fazem a mineração dos blocos através do algoritmo *Proof-of-work* (PoW), quando um nó cria um bloco, esse bloco é propagado para outros nós na rede, onde também passa por uma validação que requer que a maioria dos pares entre em consenso que é um bloco válido (XU et al., 2017, p. 244). Assim, quando o bloco for considerado válido pelos pares, ele é adicionado à sua cópia da *Blockchain* e propagado aos outros nós da rede.

As transações que estavam no *mempool* são escolhidas pelos mineradores, essa escolha é feita usualmente pela taxa que o remetente pagou, ou seja, quanto maior a taxa, mais rápido a transação será confirmada pelos mineradores. As transações são recolhidas do *mempool* e inseridas nos blocos válidos e propagadas aos pares da rede. Ao final, as transações estão registradas de forma imutável e permanente na *Blockchain*. Conforme, Xu et al. (2017), o consenso garante que todas as transações armazenadas sejam válidas e que cada transação válida seja adicionada apenas uma vez.

Figura 4: Etapas que uma transação passa até ser considerada válida e registrada no livro-razão.



Fonte: Singh e Chakraverty (2022).

4 SEGURANÇA

A segurança é outro ponto crucial em Sistemas Distribuídos. A *Blockchain* implementa muitos algoritmos criptográficos para garan-

tir que as transações sejam seguras. Grande parte da segurança é feita pelos algoritmos de consenso, onde todas as transações e blocos precisam passar pela validação da maioria dos nós da rede *blockchain*. De acordo com Xu et al. (2017), a integridade de uma transação é verificada por regras algorítmicas e técnicas criptográficas.

O histórico de transações na *Blockchain* não podem ser excluídas ou alteradas sem invalidar a cadeia completa de *hashes*. Combinado com restrições computacionais e esquemas de incentivos à criação de blocos, isso evita a adulteração e revisão das informações armazenadas na *Blockchain* (XU et al., 2017, p. 244).

A criptografia de chave pública e as assinaturas digitais são normalmente utilizadas para identificar contas e garantir a autorização de transações iniciadas em uma blockchain (XU et al., 2017, p. 244).

Também existem outras técnicas utilizadas em Sistemas Distribuídos que são utilizadas por blockchains, como o *Byzantine fault tolerance* (BFT), uma alternativa ao algoritmo de consenso PoW de Nakamoto (2009). De acordo com Xu et al. (2017, p. 250), o BFT exige que todos os participantes concordem com a lista de participantes da rede, por isso, normalmente é utilizado para blockchains privadas, ele é uma abordagem mais convencional em sistemas distribuídos e oferece uma garantia de consistência muito mais forte e menor latência, mas para um número menor de participantes. Conforme Xu et al. (2017, p. 250), o BFT garante consenso apesar do comportamento arbitrário de alguma fração dos participantes.

5 CONSENSO

A escolha do protocolo de consenso impacta a segurança e a escalabilidade. Assim que um novo bloco é gerado por um minerador, o minerador propaga o bloco para seus pares conectados na rede *blockchain*. No entanto, os mineradores podem encontrar diferentes novos blocos concorrentes e resolver isso usando os mecanismos de consenso da *blockchain*(XU et al., 2017). A abordagem fundamental proposto por Nakamoto (2009, p. 1) foi o algoritmo de consenso *Proof-of-Work* (*PoW*).

No Bitcoin, que utiliza o algoritmo PoW, novos blocos são gerados através do mecanismo de prova de trabalho (*Proof-of-Work*). Os mineradores de Bitcoin competem entre si para resolver cálculos matemáticos simples, mas demorados para decompor, isso é feito para cada bloco, usando grandes quantidades de energia computacional (XU et al., 2017, p. 248). Os blocos, assim como as transações, precisam passar pelo consenso e aprovação da maioria dos pares. Na mineração de blocos, os mineradores concorrem para gerar blocos, os blocos concorrem para se tornarem parte de uma das cadeias de blocos. No Bitcoin, o princípio de consenso é a de que a cadeia mais longa é escolhida, as outras cadeias são abandonadas pelos nós e apenas uma delas é validada. Ao final, o minerador que gerou a bloco vencedor recebe a sua recompensa de mineração somado com as taxas pagas por outros usuários para validarem as transações.

Os sistemas descentralizados que utilizam validadores anônimos precisam de proteção contra ataques *Sybil*, onde os atacantes criam muitos nós anônimos hostis. O *Bitcoin* protege parcialmente contra isso usando seu mecanismo de prova de trabalho, de modo que não é o número total de nós que é importante para a integridade, mas sim a quantidade total de poder computacional. Embora seja fácil para um invasor criar nós anônimos, não é fácil para ele acumular grandes quantidades de poder computacional (XU et al., 2017 apud EYAL; SIRER, 2014, p. 245).

6 SMART CONTRACTS

Smart Contracts (contratos inteligentes) é uma forma de programar contratos (algoritmos) por qualquer pessoa com intuito de executar em uma blockchain *turing-complete*

(XU et al., 2017, p. 248). Conforme Khan et al. (2021, p. 116675), um contrato inteligente é definido como um programa de computador que faz cumprir as promessas acordadas pelas partes interagentes na ausência de intermediários confiáveis. Assim, a computação em um sistema baseado em blockchain pode ser realizada na cadeia, por exemplo, por meio de contratos inteligentes (*on-chain*) ou fora da cadeia (*off-chain*).

Com o desenvolvimento do ecossistema *Ethereum*, o contrato inteligente se torna um ponto central para alavancar blockchains a máquinas de estado programáveis, introduzindo a execução de aplicativos descentralizados (*dApps*) (KHAN et al., 2021, p. 116675).

Desde a introdução de contratos inteligentes, as aplicações de blockchains não estão mais limitadas à criação e gerenciamento de *tokens* e ativos digitais; surgiram diversas plataformas com recursos de *smart contracts* para conectar blockchains (KHAN et al., 2021, p. 116673).

Contratos inteligentes podem ser desenvolvidos com a linguagem de programação Solidity, está é uma linguagem *turing-complete* e orientada a objetos desenvolvida pela plataforma *Ethereum* para executar contratos inteligentes na Máquina Virtual Ethereum (EVM) (KHAN et al., 2021, p. 116673).

Não é necessário ser um nó da rede para interagir com a blockchain. Em vez disso, quando um usuário adiciona uma nova entrada ao livro-razão de uma blockchain, ele envia uma transação para um nó existente usando um protocolo de Chamada de Procedimento Remoto (RPC). Este par retransmite a transação para o resto da rede para inclusão em um bloco futuro. Isto significa que as partes envolvidas numa transação, como o remetente e o destinatário, não estão diretamente envolvidas na execução dessa transação. Em vez disso, esta tarefa cabe aos pares da rede, confirmarem e validarem a transação (KOLB et al., 2020, p. 4). Assim, os nós da rede fornecem uma interface *JSON-RPC* que permite a qualquer cliente interagir com a blockchain por meio dessa interface de comunicação.

O armazenamento de dados fora da cadeia (*off-chain*) pode ser uma nuvem privada na infraestrutura do cliente ou um armazenamento público fornecido por terceiros ou rede. Alguns armazenamentos de dados *peer-to-peer* são projetados para serem compatíveis com blockchain, como o *IPFS* e o *Storj* (XU et al., 2017, p. 248).

Alguns desafios dos contratos inteligentes é que, uma vez implantados a rede principal de uma blockchain, ele não pode mais ser alterado, devido a princípio fundamental de imutabilidade de blockchains.

7 TRANSPARÊNCIA

A transparência é um fator muito importante para sistemas distribuídos. A blockchain como um desses sistemas possui algumas dessas propriedades, tal como a transparência de acesso, onde os participantes têm acesso aos dados e transações registradas na cadeia de blocos por meio de operações padronizadas.

A transparência de concorrência nos algoritmos de consenso como PoW de Nakamoto (2009) e PoS permitem transações simultâneas sem interferência entre elas.

A rede *peer-to-peer* é uma forma de transparência de replicação, onde cada nó da rede possui uma cópia do livro-razão, as transações e inserção de blocos e cadeias são retransmitidas aos nós da rede a todo tempo para garantir que todos tenham uma mesmo cópia, atributos que garantem a disponibilidade e resistência a falhas, assim os usuários finais não precisam se preocupar com a replicação dos dados.

A transparência de falhas é um dos principais problemas de servidores centralizados que a blockchain e redes *peer-to-peer* resolvem, pois mesmo que alguns nós da rede falhem dada uma catástrofe hipotética, há muitos outros nós ativos, o que não irá impactar na indisponibilidade da rede.

Também atende a transparência de mobilidade, os nós da rede podem se conectar e desconectar de forma transparente, sem qualquer impacto aparente a rede *peer-to-peer*.

8 REFLEXÃO CRÍTICA

A análise do artigo e a pesquisa realizada durante este estudo proporcionaram uma visão mais profunda e crítica sobre a interseção entre sistemas distribuídos e a redes peer-to-peer, bem como a tecnologia Blockchain. Fiquei impressionado com a complexidade e a riqueza de possibilidades que a integração dessas duas áreas oferece.

Através desta exploração, tornou-se evidente que os sistemas distribuídos desempenham um papel fundamental na sustentação da segurança e confiabilidade das redes peer-to-peer. Conceitos como consenso, tolerância a falhas e escalabilidade se tornaram mais claros e tangíveis, à medida que observei suas aplicações reais em projetos de blockchain. No entanto, também ficou evidente que a área de interoperabilidade entre diferentes blockchains e questões de escalabilidade em larga escala ainda são desafios em aberto que requerem estudos adicionais e inovação.

9 CONCLUSÃO

As redes *peer-to-peer* tornaram-se muito populares nos últimos anos, devido principalmente a necessidade de decentralizar a web como um todo. O serviços centralizados, apesar de serem maioria, tem algumas desvantagens como a de servidores centralizados, o que implica em complexidades de disponibilidade, em caso de um servidor cair no ponto central, quando não houver meios para recuperação de falhas, o serviço fica *off-line*.

Ademais, conforme Xu et al. (2017), em um sistema centralizado, todos os utilizadores dependem de uma autoridade central para mediar as transações. As rede *peer-to-peer*, no entanto, não sofrem com esse problema, uma vez que utilizam os recursos dos nós da rede e podem ficar disponíveis a todo momento e as transações são autônomas e baseadas no consenso. Por exemplo, transações em redes *Blockchain* podem ser feitas a qualquer momento, seja em feriados ou fins de semana, dada sua automação. Já serviços centralizados não-autônomos ficam *off-line* durante períodos eventuais ou rotineiros.

Mas, apesar de todos esses benefícios, há algumas limitações, tal como sistemas em tempo real, tamanho dos dados na *Blockchain*, a latência na confirmação das transações e custos (XU et al., 2017). As *Blockchains* de primeira geração como o *Bitcoin* e o *Ethereum* tem altos custos de transações e as validações podem demorar entre segundos a minutos. Além disso, quanto maior a transação no sentido de tamanho da carga útil (MB/s), maior a taxa cobrada para os nós validarem. Uma prática comum para gerenciamento de dados em sistemas baseados em *blockchain* é armazenar dados brutos fora da cadeia (*off-chain*) e armazenar na cadeia apenas metadados, pequenos dados críticos e *hashes* (XU et al., 2017, p. 247).

Alumas *Blockchains* de nova geração como a *Solana* e a *Fantom* possuem outros algoritmos *Proof-of-Stake* (PoS) e estruturas de dados *Directed acyclic graph* (DAG) para organizar e validar as transações de forma mais eficiente sem perder a segurança.

Neste artigos discutimos sobre como conceitos de sistemas distribuídos são aplicados a sistemas reais para fornecer aplicações de alta disponibilidade, distribuídas por meio de redes *overlay* e algoritmos criptográficos para fornecer um sistema seguro para aplicações, onde o desafio está em ter confiança em pares sem conhecimento de boa fé prévia.

Trabalhos futuros podem explorar com maior profundidade os protocolos de comunicação entre redes *overlay*, redes físicas e também explorar as *blockchains* de terceira geração com novas estruturas de livro-razão e algoritmos de consenso, onde chega-se a interoperabilidade entre diversas *blockchains* e governança descentralizada.

REFERÊNCIAS

DIMITRIADIS, V. et al. Uncuffed: A blockchain-based secure messaging system. In: *Proceedings of the 25th Pan-Hellenic Conference on Informatics*. New York, NY, USA: Association for Computing Machinery, 2022. (PCI '21), p. 340–345. ISBN 9781450395557. Disponível em: <https://doi.org/10.1145/3503823.3503886>.

EISENBARTH, J.-P.; CHOLEZ, T.; PERRIN, O. Avoiding the 1 tb storage wall: Leveraging ethereum's dht to reduce peer storage needs. In: *Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure*. New York, NY, USA: Association for Computing Machinery, 2023. (BSCI '23), p. 75–84. ISBN 9798400701986. Disponível em: <https://doi.org/10.1145/3594556.3594625>.

EYAL, I.; SIRER, E. G. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, ACM New York, NY, USA, v. 61, n. 7, p. 95–102, 2014.

KHAN, S. et al. Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability. *IEEE Access*, v. 9, p. 116672–116691, 20 ago. 2021. ISSN 2169-3536.

KOLB, J. et al. Core concepts, challenges, and future directions in blockchain: A centralized tutorial. *ACM Comput. Surv.*, Association for Computing Machinery, New York, NY, USA, v. 53, n. 1, fev. 2020. ISSN 0360-0300.

LUA, E. K. et al. A survey and comparison of peer-to-peer overlay network schemes. *IEEE Communications Surveys Tutorials*, v. 7, n. 2, p. 72–93, abr. 2005. ISSN 1553-877X.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. p. 1–9, mai. 2009. Disponível em: <http://www.bitcoin.org/bitcoin.pdf>.

RAI, A.; SINGH, R.; MODIANO, E. A distributed algorithm for throughput optimal routing in overlay networks. dez. 2016. Disponível em: <https://www.researchgate.net/publication/311715170_A_Distributed_Algorithm_for_Throughput_Optimal_Routing_in_Overlay_Networks>.

SCHOLTES, I. Harnessing complex structures and collective dynamics in large networked computing systems. p. 17–18, mai. 2011. Disponível em: <https://www.researchgate.net/publication/230774628_Harnessing_Complex_Structures_and_Collective_Dynamics_in_Large_Networked_Computing_Systems>.

SINGH, S.; CHAKRAVERTY, S. Implementation of proof-of-work using ganache. In: *2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*. [S.l.: s.n.], 2022. p. 1–4.

TSCHORSCH, F.; SCHEUERMANN, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, v. 18, n. 3, p. 2084–2123, mar. 2016.

XU, X. et al. A taxonomy of blockchain-based systems for architecture design. *2017 IEEE International Conference on Software Architecture (ICSA)*, p. 243–252, 18 abr. 2017.