Uma Avaliação de Desempenho de Cadeias de Blocos Privadas Permissionadas através de Cargas de Trabalho Realísticas *

Marcela T. Oliveira[1], Gabriel R. Carrara[2], Natalia C. Fernandes[1], Célio V. N. Albuquerque[2], Ricardo C. Carrano[1], Dianne S. V. Medeiros[1], Diogo M. F. Mattos[1]

[1]Departamento de Engenharia de Telecomunicações - TET/PPGEET/UFF
[2]Departamento de Ciência da Computação - IC/UFF
Laboratório MídiaCom – Universidade Federal Fluminense (UFF)
Niterói, RJ – Brasil

Abstract. *Blockchain is a trending technology that has been used to add security to private applications in several areas of knowledge. The diversity results in the development of multiple platforms to meet the specificities of applications. Thus, a key challenge is to ensure that blockchain platforms provide security, access control, and high performance to applications. In this paper, we evaluate two frameworks for blockchain development Parity and Multichain. Our evaluation is a comprehensive comparison between platforms, analyzing the validation of transactions, the acceptance of blocks and the latency for accessing the chain. For this purpose, we deploy a peer-to-peer private network for each blockchain platform, in which we apply realistic workloads. We randomly generate workloads, following the distribution of probabilities of the inter arrival time of transactions in Bitcoin's blockchain. The results show that each platform stands out under specific criteria, and design decisions imply feature restrictions that are critical for the creation of secure and efficient blockchains.*

Resumo. *As cadeias de blocos vêm sendo utilizadas para agregar segurança a aplicações privadas em diversas áreas do conhecimento. Esta diversidade resulta no desenvolvimento de múltiplas plataformas para atender às especificidades de cada aplicação. Assim, um desafio fundamental é assegurar que essas plataformas proveem segurança, controle de permissionamento e alto desempenho às aplicações de cadeias de blocos. Este artigo avalia duas plataformas de desenvolvimento de cadeia de blocos, Parity e Multichain. A avaliação consiste na comparação entre as plataformas, analisando a vazão das transações, aceitação de blocos e a latência de acesso à cadeia. Para tanto, utiliza-se uma topologia de rede par a par privada permissionada de cadeia de blocos, na qual são aplicadas cargas de trabalho realísticas. As cargas de trabalho são geradas aleatoriamente, seguindo a distribuição de probabilidades da chegada de transações na cadeia de blocos do* `Bitcoin`*. Os resultados mostram que cada plataforma se destaca em critérios específicos. As decisões de projeto de cada plataforma resultam em restrições de funcionalidades que devem ser tratadas por desenvolvedores para a criação de cadeias mais seguras e eficientes.*

1. Introdução

A tecnologia *blockchain*, ou cadeia de blocos, é a principal tendência para prover aplicações distribuídas sem uso de uma terceira parte confiável e com requisitos de segurança

*Este trabalho foi realizado com recursos do CNPq, CAPES, RNP e FAPERJ.

como integridade, autenticidade, não repúdio e, principalmente, auditoria sobre os dados armazenados [Nakamoto, 2008]. A ideia central da tecnologia de cadeia de blocos é distribuir a validação dos dados e a responsabilidade pela inserção de novos dados na cadeia, sobre uma rede par a par que executa um algoritmo de consenso e as regras de validação dos dados. Assim, a tecnologia de cadeia de blocos é apontada como uma alternativa simples e segura para o desenvolvimento de aplicações em diversas áreas do conhecimento. Para atender às demandas dessas novas aplicações, diferentes plataformas para o desenvolvimento de cadeias de blocos personalizadas são propostas [Jesus et al., 2018, Dinh et al., 2017].

As plataformas para o desenvolvimento de aplicações seguras baseadas em cadeia de blocos variam em relação às abordagens quanto à participação de nós na rede, à responsabilidade de cada nó na cadeia, à visibilidade dos dados armazenados e ao algoritmo de consenso adotado. Os mecanismos de consenso variam desde o consenso bizantino, que resiste à ocorrência de falhas [Bessani et al., 2014], até consensos probabilísticos que executam apenas sobre uma parcela da rede [Schwartz et al., 2014]. A principal plataforma para o uso da tecnologia de cadeia de blocos é a criptomoeda *Bitcoin*, que representa o estudo de caso mais bem-sucedido de aplicação da cadeia de blocos. Paralelamente, outras plataformas como o *Ethereum* e o *Hyperledger* aparecem como soluções de cadeia de blocos apoiadas por grandes empresas. A escolha pelo uso de uma determinada plataforma deve ser pautada no desempenho de cada uma e, também, nas opções de configurações que cada uma oferece.

Este artigo apresenta a comparação de desempenho entre duas plataformas de desenvolvimento de aplicações de cadeia de blocos. As plataformas avaliadas são a *Multichain*, baseada na cadeia blocos original da *Bitcoin*, e a *Parity*, que executa sobre a cadeia de blocos da *Ethereum*. Essas plataformas são apontadas como as principais soluções para o desenvolvimento de cadeias de blocos privadas permissionadas [Dinh et al., 2017]. São comparados os tempos de validação de uma transação, de mineração de blocos e de busca por transações e blocos já inseridos na cadeia. A avaliação das plataformas é realizada através da inserção de transações geradas seguindo a probabilidade real de chegada de novas transações na rede*Bitcoin*. Por fim, o artigo propõe a modelagem da distribuição de probabilidades de cada parâmetro avaliado.

Aplicações de cadeia de blocos são propostas para armazenar dados distribuídos e executar ações distribuídas em diversos campos do conhecimento [Mettler, 2016, Zyskind et al., 2015, Guo et al., 2018]. Outras propostas visam a criação de novas ferramentas de cadeias de blocos que não se baseiam em plataformas já estabelecidas [Alvarenga et al., 2018, Rebello et al., 2018]. Ao considerar a comparação entre plataformas para a criação de cadeias de bloco, a proposta BlockBench se destaca ao propor um arcabouço de avaliação [Dinh et al., 2017]. Contudo, essas propostas não focam na modelagem do comportamento das plataformas. Neste artigo, implementa-se duas redes de testes, uma para cada plataforma avaliada, e compara-se o desempenho das plataformas. Ademais, os resultados mostram que a plataforma *Multichain* possui o melhor desempenho ao se considerar o tempo de efetivação total das transações, ao custo de permitir a execução de transações simples, quando comparada a execução de códigos complexos de contratos inteligentes.

O restante do artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. O problema de permissionamento em cadeias de bloco públicas e privadas é discutido na Seção 3. As plataformas de cadeia de blocos avaliadas são detalhadas na Seção 4. O esquema de avaliação de desempenho proposto e os resultados experimentais são evidenciados na Seção 5. Por fim, a Seção 6 conclui o artigo.

2. Trabalhos Relacionados

Inúmeras aplicações são propostas utilizando cadeias de blocos e diversas plataformas baseiam o desenvolvimento dessas novas aplicações. Na área de saúde, por exemplo, elas permitem o armazenamento seguro de dados gerais [Mettler, 2016, Guo et al., 2018], desde histórico de pacientes a informações referentes à produção de farmacêuticos. No setor comercial, as cadeias de blocos podem ser usadas para a realização de transações financeiras entre pares, sem a necessidade de uma entidade intermediadora [Zyskind et al., 2015]. A tecnologia de cadeia de blocos também é proposta para agregar segurança à comunicação máquina a máquina (*Machine to Machine* – M2M). Mengelkamp *et. al.* apresentam a aplicação em microrredes, para fiscalizar a compra e venda de energia renovável através da execução de contratos inteligentes [Mengelkamp et al., 2018]. Christidis *et. al.* investigam também o emprego de contratos inteligentes para outras aplicações em internet das coisas, além de microrredes [Christidis e Devetsikiotis, 2016]. Contudo, questões como tempo para efetivação das transações, tempo de mineração, escalabilidade e disponibilidade dos dados são desafios atuais das cadeias de blocos [Mettler, 2016]. Assim, torna-se necessário avaliar objetivamente cada plataforma antes de escolher qual aplicar em cada cenário.

Alguns trabalhos apresentam comparações qualitativas das tecnologias e propostas relativas às cadeias de blocos. Zyskind *et al.* verificam ameaças à privacidade dos dados em serviços *online*. Os autores afirmam que a necessidade de uma terceira entidade fragiliza a privacidade dos usuários, que não têm controle sobre quais dados estão sendo coletados e armazenados [Zyskind et al., 2015]. Dai *et al.* abordam o problema de escalabilidade, apresentando opções de descarte dos blocos mais antigos da cadeia e consideram a abordagem de operar sobre os resumos dos dados [Dai et al., 2018]. Pahl *et al.* comparam as características de diferentes cadeias de blocos para propor um arcabouço de auxílio à decisão sobre qual tecnologia utilizar [Pahl et al., 2018]. Wang *et al.* apresentam uma visão geral sobre as tecnologias de cadeias de blocos, enfatizando suas diferenças arquiteturais e comparando os seus algoritmos de consenso [Zheng et al., 2017]. Nessa mesma linha, Julien *et al.* realizam uma comparação entre as plataformas *Ethereum*, IBM *Open Blockchain* (OBC), Intel *Sawtooth Lake*, *BlockStream Sidechain Elements* e Eris, relacionada à usabilidade, à flexibilidade, ao desempenho e à potencialidades [Macdonald et al., 2017].

Dinh *et al.* foram pioneiros ao desenvolverem uma plataforma analisadora de desempenho para estudar e comparar plataformas de cadeia de blocos privadas. Segundo os autores, o *Blockbench* visa testar as plataformas escolhidas, implementado cargas de trabalho, em forma de contratos inteligentes. O objetivo da plataforma é comparar e compreender a fundo as diferentes organizações de cadeia de blocos privadas [Dinh et al., 2017]. Xu *et al.* realizaram uma análise de desempenho em cadeias de blocos baseadas no problema de consenso bizantino (*Practical Byzantine Fault Tolerance* - PBFT). A análise foca na questão da escalabilidade, mostrando que as plataformas *Hyperledger Fabric* v0.6 com consenso PBFT, *Ripple* com algoritmo de consenso XRP e *Hyperledger Fabric* v1.0 baseado em consenso BFT-SMaRt não escalam a mais que algumas dezenas de dispositivos [Han et al., 2018]. Uma abordagem diferente foi proposta por Zagar *et al.*, que compararam as cadeias de bloco com base em seu consumo de energia. O foco está na verificação dos blocos, analisando os algoritmos de consenso passo a passo [Bach et al., 2018].

3. Cadeias de Blocos e Estratégias de Consenso

A tecnologia de cadeia de blocos [Nakamoto, 2008] explora a distribuição do controle das redes par a par e da estrutura de dados de encadeamento de blocos para prover a execução

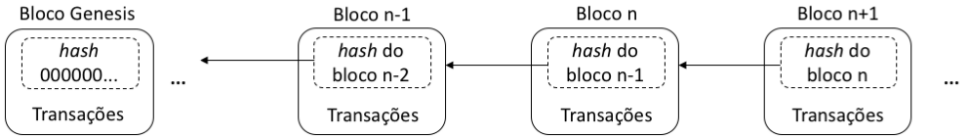
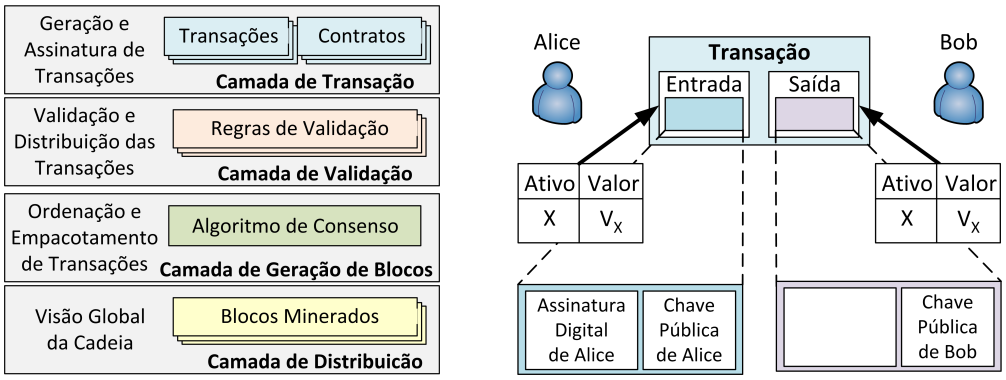


Figura 1: Visão esquemática da estrutura de dados em uma cadeia de blocos. O bloco *genesis* representa o primeiro bloco da cadeia. Cada bloco tem o resumo criptográfico do bloco anterior, gerando um encadeamento de resumos criptográficos. A alteração de um bloco gera a inconsistência de todos os blocos seguintes da cadeia.

de transações confiável, distribuída e consistente, a exemplo da linguagem *Script* proposta pela *Bitcoin*. Dessa forma, a tecnologia de cadeia de blocos é definida por dois elementos básicos, a estrutura de dados de encadeamento dos blocos e a rede par a par composta pelos nós participantes da rede. A cadeia de blocos de primeira geração, representada pela rede *Bitcoin*, permite armazenar pequenas quantidades de dados e foi idealizada para transações monetárias entre nós da rede. Posteriormente, a segunda geração de cadeia de blocos, representada pela rede *Ethereum*, propôs que a estrutura de dados da cadeia de blocos fosse usada para representar transações mais complexas, os chamados contratos inteligentes. Contratos inteligentes são estruturas de computação de mensagens de objeto confiável, que realizam cálculos não triviais dentro da própria cadeia de blocos. A aplicação de contratos inteligentes possibilitou a automatização de regras executáveis com o consentimento das várias partes envolvidas [Wood, 2014]. A Figura 1 mostra o esquema da tecnologia de cadeias de blocos. O esquema consiste no encadeamento de resumos criptográficos, em que um bloco armazena o resumo criptográfico do seu conteúdo, englobando o valor do resumo criptográfico do bloco anterior. Cada bloco na cadeia armazena uma lista de transações e o resumo criptográfico do bloco anterior. A exceção é o bloco *genesis*, o primeiro bloco da cadeia que possui um resumo criptográfico previamente determinado.

A ideia central das cadeias de blocos é garantir a confiança em redes nas quais os nós não confiam uns nos outros, são livres para ingressarem e saírem da rede e sem a necessidade de haver uma terceira entidade centralizada em que todos os nós confiem, âncora de confiança [Nakamoto, 2008]. Mesmo nesse ambiente hostil, é necessário que exista uma visão global única da cadeia de blocos distribuída e replicada entre todos os nós da rede, para que todos os nós tenham acesso à mesma informação. Dessa forma, é necessário adotar mecanismos de validação e de consenso para realizar a distribuição e a réplica coerente dos dados e garantir a auditoria distribuída sobre as transações executadas na rede. As transações em uma cadeia de blocos são sequências de operações atômicas, que seguem a semântica ACID (Atomicidade, Consistência, Isolamento e Durabilidade) [Dinh et al., 2017] como em um banco de dados tradicional. Na *Bitcoin*, por exemplo, uma transação representa a transferência da posse de uma certa quantia de moedas entre usuários. Antes de se tornarem parte da cadeia de blocos, as transações são processadas por quatro camadas da cadeia: transações, validação, geração de blocos e distribuição, conforme ilustrado na Figura 2(a). Plataformas que permitem a criação de cadeias de blocos implementam as quatro camadas.

A camada de **transações** representa o relacionamento da tecnologia de cadeia de blocos com o usuário. Assim o usuário segue os critérios definidos na rede, como organização e linguagem de codificação pré-estabelecida para a elaboração da transação. O critério fundamental de uma transação em cadeia de blocos é a assinatura dos usuários envolvidos na emissão da transação. Por isso, a interação com a cadeia de blocos é feita por meio de um par de chaves assimétricas, recebidas pelos usuários ao entrarem na rede. A Figura 2(b) exemplifica uma transação de transferência de um ativo entre dois usuários. No exemplo, os usuários são identificados por suas chaves públicas. O usuário que emite a transação, usa sua chave pri-



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

(b) Exemplo de transação de transferência de ativos.

Figura 2: Relacionamento entre elementos que compõem a tecnologia de cadeia de blocos. a) Divisão da cadeia de blocos em camadas. As transações dos usuários são geradas na camada de transação, validadas pela rede na camada de validação, inseridas em blocos na camada de geração de blocos e os blocos são distribuídos na camada de distribuição. b) Transação típica em que Alice transfere um ativo da sua posse para Bob. A transação é identificada pelas chaves públicas de Alice e Bob e validada pela assinatura digital de Alice.

vada para assiná-la. O uso da assinatura digital garante o não repúdio às transações, permite autenticação do conteúdo da transação e controle de acesso. O usuário assina suas transações com a chave privada e pode ser endereçado na rede por meio da chave pública. Após a assinatura da transação, o usuário a transmite para todos os nós vizinhos. Vale ressaltar que não há um esquema para autenticação de usuários, já que os usuários são apenas identificados por suas chaves públicas, mas não há um mecanismo que relacione uma chave pública com uma entidade conhecida, como realizado por uma infraestrutura de chaves públicas.

A verificação se as transações seguem os critérios predeterminados pela rede ocorre na camada de **validação**. A validação é a verificação feita pelos nós vizinhos e avaliam se a transação obedece a todas as regras da rede. Em caso positivo, é considerada válida e transmitida para os nós seguintes da rede. Caso contrário, a transação é descartada. Na *Bitcoin*, um dos critérios que deve ser obedecido para executar a transação é a disponibilidade da quantia enviada em posse da chave pública que a emite.

Na camada de **geração de blocos**, as transações coletadas e validadas são ordenadas e empacotadas em um bloco candidato a ser inserido na cadeia, com registro de data e hora. A geração do bloco é chamada de processo de mineração. A escolha do nó de mineração e o conteúdo do bloco dependem do mecanismo de consenso que a rede emprega. Cada bloco aprovado pelo consenso contém uma referência ao bloco antecessor, formando assim o encadeamento de blocos. Essa referência é feita através de resumos criptográficos (*hash*), conforme ilustrado na Figura 1. Um bloco B_n com transações válidas possui junto ao seu conteúdo o resumo criptográfico do bloco anterior B_{n-1}. O conteúdo completo do bloco B_n será usado para gerar o resumo criptográfico que será incluído como referência no próximo bloco B_{n+1}. Como o algoritmo que computa o resumo criptográfico é unidirecional, é improvável a recuperação dos dados originais a partir do resumo gerado, assim como é improvável a geração de um novo conteúdo que gere o mesmo resumo. Isso garante a integridade dos dados na cadeia.

Na camada de **distribuição**, o bloco minerado e validado é adicionado à estrutura de dados da cadeia de blocos de cada nó da rede par a par adjacente e as transações associadas são executadas para atualizar a visão global da cadeia. Ressalta-se que a execução das transações determina uma mudança de estado global na cadeia, seja a transferência de ativos,

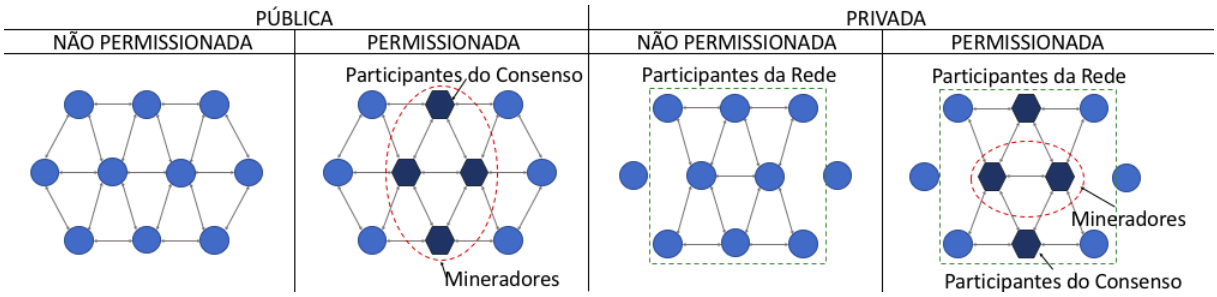


Figura 3: Taxonomia adotada para redes de cadeia de blocos. A classificação entre pública e privada relaciona-se com a participação dos nós na rede. Enquanto, permissionada e não permissionada dizem respeito ao papel desempenhado pelos nós na rede, nos mecanismos de consenso e de geração de novos blocos.

seja a execução de um contrato inteligente. O encadeamento de blocos só ocorre se o resumo criptográfico do bloco minerado estiver correto. Caso contrário, o bloco minerado é descartado. Se todos os nós da rede possuírem o mesmo estado global da cadeia, com o mesmo conteúdo e blocos organizados na mesma ordem, os nós estão em consenso. Ao atingir o consenso, todos os nós passam a ter acesso à mesma informação. A visão global distribuída da cadeia garante a disponibilidade e a auditoria das informações armazenadas.

Considerando a disponibilidade das informações na cadeia, o papel de cada nó na rede par a par e como ocorre o consenso na rede, a tecnologia de cadeia de blocos apresenta características distintas que são importantes para definir o cenário de aplicação. Trabalhos anteriores classificam as cadeias como pública, privada, permissionada e híbrida [Pilkington, 2016, Gupta e Sadoghi, 2018]. Christidis e Devetsikiotis classificam as cadeias de bloco quanto aos aspectos de controle de acesso ao conteúdo da cadeia e quanto às funções que os nós da rede exercem [Christidis e Devetsikiotis, 2016]. Neste artigo, adota-se a taxonomia de rede de cadeias de blocos em diferentes tipos de visão da rede, *pública não permissionada*, *pública permissionada*, *privada não permissionada* e *privada permissionada*, mostradas na Figura 3.

A classificação entre redes públicas e privadas define o grupo de nós que podem acessar a rede par a par adjacente à cadeia de blocos. Em uma rede pública, não há qualquer mecanismo de controle de acesso e os nós podem ingressar e deixar a rede sem qualquer prejuízo para o mecanismo de consenso ou para a geração de novos blocos. Nas redes privadas, apenas nós autorizados podem acessar a rede par a par. Paralelamente, a classificação entre redes permissionadas e não permissionadas define o papel dos nós ao participarem da rede. Em redes não permissionadas, todos os nós possuem o mesmo papel na rede, sendo responsáveis por gerarem as transações, minerarem blocos e participarem de consenso. Já em cadeias permissionadas, os nós possuem papéis distintos, dependendo de sua identificação. Um grupo de nós é responsável por realizar o consenso e apenas um subgrupo é autorizado a minerar novos blocos.

Em **redes públicas não permissionadas** de cadeias de blocos é exigido rigidez aos mecanismos de consenso, devido à desconfiança mútua entre os usuários da rede. Isso é justificável pela característica principal de uma rede pública, a igualdade entre os nós. Todo nó pode ingressar e sair da rede. Uma vez participante da rede, o nó recebe um par de chaves criptográficas para assinar e realizar transações. Além disso, qualquer nó pode ser um minerador e fazer parte do mecanismo de consenso da rede. Os problemas associados às cadeias de blocos públicas são as taxas que devem ser pagas para incentivar os nós a participarem da rede e minerarem os blocos, a preocupação com a escalabilidade da rede e com o tempo de confirmação das transações. Tais problemas relacionam-se ao fato de as redes públicas não permissionadas serem ambientes colaborativos e, portanto, dependem do comportamento benigno dos nós. Ademais, para redes

de dados sensíveis, a disponibilidade de todas as informações para todos os usuários representa um desafio à privacidade. As **redes públicas permissionadas** foram desenvolvidas para aplicação de mecanismos de consenso menos custosos em redes públicas não permissionadas. A diferença entre as redes públicas não permissionadas e as permissionadas é a desigualdade de atuação dos nós na rede. Em redes públicas permissionadas, o nó só participa da rede após a verificação adequada de sua identidade e, assim, aloca-se as permissões que determinam quais atividades o nó pode executar na rede[Armknecht et al., 2015].

As **redes privadas não permissionadas** se diferenciam das redes púbicas por restringirem a entrada de participantes. Isto é, a rede privada é geralmente governada por uma única instituição ou um conjunto de instituições, que determinam quem são os nós autorizados a participarem da rede. Os nós que participantes têm funções iguais e exercem a mesma importância na rede. Uma vez autorizado a participar da rede, o nó pode gerar transações, gerar blocos e participar do consenso. As **redes privadas permissionadas** permitem apenas que alguns nós façam parte do consenso e apenas um subconjunto desses nós possam gerar o próximo bloco.

Em redes públicas tais como *Bitcoin* e *Ethereum* [Wood, 2014], o mecanismo de consenso empregado é a Prova de Trabalho (*Proof of Work - PoW*). Nakamoto sugere que a prova seja realizar um cálculo computacional não trivial. Assim, a acessibilidade a mais recursos computacionais determina o nó vencedor, pois este realizará o cálculo em menos tempo. Nesse mecanismo de consenso, o nó minerador é aquele capaz de provar que realizou o cálculo não trivial, apresentado a resolução do desafio computacional. Após minerar o bloco, todos os outros nós respeitam a capacidade do vencedor e alcançam o consenso, encadeando este bloco à cadeia [Nakamoto, 2008]. No entanto, por se tratar de um mecanismo de consenso probabilístico, já que depende da probabilidade de um nó concluir o cálculo não trivial antes dos demais, é possível que vários nós possam reivindicar o próximo bloco a ser adicionado à cadeia. Com base na disseminação do novo bloco, isso pode levar à ramificação da cadeia. Esses ramos são frequentemente de curta duração, pois todos os nós tendem a se alinhar à cadeia mais longa, o que, por sua vez, leva à poda dos ramos. Ressalta-se que um nó recebe recompensa quando consegue minerar um bloco e anexá-lo à cadeia mais longa. Portanto, é vantajoso alinhar os blocos minerados sempre à cadeia mais longa, para que os recursos computacionais empregados para a mineração não sejam desperdiçados com um bloco que será descartado. Apesar do mecanismo tender probabilisticamente à convergência, a Prova de trabalho apresenta desvantagens como a crítica à sustentabilidade do processo de mineração, em que há um gasto exacerbado de energia para criação de um bloco. É observada uma alta latência para alcançar o consenso na rede. Como consequência, há uma baixa vazão na quantidade de transações validadas no tempo. Além disso, o mecanismo de prova de trabalho pode ser comprometido teoricamente por um usuário que controle mais de 50% dos recursos computacionais da rede. Essa possibilidade teórica tem implicações práticas, pois um grupo de mineradores pode compartilhar recursos para gerar blocos mais rapidamente, distorcendo a natureza descentralizada da rede.

Uma alternativa ao alto custo computacional da Prova de Trabalho é a Prova de Posse (*Proof of Stake* - PoS). O mecanismo PoS visa preservar a natureza descentralizada da rede pública. No mecanismo PoS, um nó com n recursos, recebe n oportunidades em tempo para gerar um bloco. Portanto, o princípio subjacente ao PoS é que o nó com maior participação reivindica a geração do próximo bloco. Para determinar a participação de um nó, uma combinação de um ou mais fatores, como riqueza, recursos e assim por diante, pode ser utilizada. O mecanismo PoS requer um conjunto de nós para atuar como mineradores. Qualquer nó que queira atuar como um minerador precisa bloquear seus recursos como prova de sua participação [King e Nadal, 2012]. Para criar um novo bloco, um conjunto de validadores par-

ticipa do mecanismo de consenso. O mecanismo PoS usa um algoritmo pseudoaleatório para selecionar um minerador, que cria um novo bloco e o adiciona à cadeia de blocos existente. A frequência de seleção do minerador é determinada por um intervalo de tempo predefinido.

No contexto das redes privadas, em vez da prova de trabalho ou de posse, se propõe o uso da Prova de Autoridade (*Proof of Authority* - PoA). Nessas redes, existe uma entidade responsável pela rede que pode predeterminar o papel de alguns nós. Assim, na Prova de Autoridade, a ideia é designar um conjunto de nós com autoridade para participar do consenso. Esses nós são encarregados da tarefa de gerar novos blocos e validar as transações. A PoA endossa um bloco como parte da cadeia se ele for assinado por pelo menos um nó com autoridade. O modelo de incentivo na PoA destaca que é do interesse de um nó manter sua reputação para permanecer como nó de autoridade. Sendo assim, existe um mecanismo de confiança que avalia o comportamento dos nós de autoridade na rede. Vale ressaltar que PoA mantém a natureza distribuída da rede pelo fato de que todos devem concordar sobre o estado global da cadeia.

Os mecanismos de consenso anteriormente apresentados consideram que o comportamento probabilístico dos nós da rede é bem-intencionado. Em ambientes hostis, os nós podem apresentar comportamento maliciosos, levando a falhas bizantinas, ou seja, comportamentos arbitrariamente maliciosos ou falhas que fogem do protocolo predefinido. O modelo prático de tolerância a falhas bizantinas (*Practical Bizantine Fault Tolerance* – PBFT) é a referência para protocolos Bizantinos de Tolerância a Falha que vem sendo adaptado para cadeia de blocos [Bessani et al., 2014, Castro e Liskov, 2002, Alvarenga et al., 2018]. Os protocolos baseados no PBFT garantem o consenso apesar da participação de nós maliciosos. O PBFT resiste a um número limite de nós maliciosos, chamados de bizantinos, f, em que $f \leq \frac{n+1}{3}$ e n representa o número total de nós da rede. Protocolos baseados em PBFT reduzem o custo de processamento comparado com a Prova de Trabalho, ao custo de grande complexidade de mensagens, $O(n^2)$. Consequentemente, esses protocolos são adequados para redes de cadeia de blocos com poucos nós, devido à sobrecarga de mensagem.

4. Plataformas de Cadeia de Blocos Analisadas

Este artigo foca em redes de cadeias de blocos privadas permissionadas. O objetivo é avaliar o comportamento de duas plataformas de cadeia de blocos que permitem a implementação de redes privadas permissionadas, a plataforma *Parity* e a *Multichain*. A *Parity* é uma plataforma de desenvolvimento de cadeia de blocos baseada na rede *Ethereum*. Inicialmente, seu objetivo é fornecer uma interface de interação dos usuários com a rede *Ethereum*. No entanto, a *Parity* também possibilita a configuração de rede privada permissionada, adotando o modelos de dados de contratos inteligentes utilizados na *Ethereum*. A *Parity* implementa uma versão do mecanismo de consenso de Prova de Autoridade, com um conjunto de nós de autoridade predeterminados que podem gerar novos blocos.

Uma das principais diferenças da *Parity* para a rede *Ethereum* original é que a *Parity* armazena todo o conteúdo do bloco em memória, ao contrário da *Ethereum* que utiliza banco de dados não relacionais para armazenar dados referenciados na cadeia de blocos. Com isso, a organização dos dados nos blocos ocorre através de uma árvore de Merkle-Patricia modificada, que suporta atualizações e operações de busca. Para a obtenção de blocos e transações com base em seus identificadores (IDs), a *Parity* expõe um conjunto abrangente de interfaces de programação de aplicação (*Application Programming Interface* – API) via chamada remota de procedimentos representadas em codificação JSON (*JSON-RPC*), suportando consultas de estados por blocos específicos e de outras estatísticas sobre os blocos[1]. A *Parity* adota a linguagem

[1]Disponível em https://parity.io/

de máquina (*bytecode*) e uma máquina virtual, chamada EVM (*Ethereum Virtual Machine*), para executar o código desenvolvido pela *Ethereum*. A EVM é otimizada para operações específicas da *Ethereum*. Por exemplo, toda instrução de código executada na *Ethereum* custa uma certa quantidade de *gas* e o custo total deve ser adequadamente rastreado e cobrado ao remetente da transação. Além disso, o código deve manter o controle dos estados intermediários e revertê-los se o *gas* disponível for insuficiente para a execução.

A *Multichain* é uma plataforma de criação e desenvolvimento de cadeias de blocos privadas permissionadas [Greenspan, 2015] baseada em uma ramificação do *Bitcoin Core*, o cliente oficial da rede *Bitcoin*[2]. A *Multichain* usa a arquitetura de transação da *Bitcoin*, com alterações apenas no processo inicial de conexão entre os nós (*handshaking*), visto que na *Multichain*, o usuário administrador fornece as permissões iniciais aos novos nós da rede, como leitura, escrita e mineração. As permissões podem ser mudadas posteriormente, caso seja necessário. Outros recursos da cadeia são implementados usando metadados ou através de modificações dos parâmetros de validação de transações e blocos. A interface de programação de aplicação é compatível com a do *Bitcoin Core*. Os dados são armazenados dentro da estrutura de dados da cadeia, na qual as transações são armazenadas em ordem cronológica, agrupadas por número de bloco, sem quaisquer índices adicionais [Greenspan, 2015]. Dentro dos blocos, a organização dos dados emprega a versão simplificada da árvore de Merkle. A *Multichain* usa um protocolo de consenso PoA, empregando um algoritmo rotativo (*round-robin*) para determinar o nó responsável pelo consenso [Greenspan, 2015]. Assim, nós com autoridade de minerador participam do grupo que irá alternar a tarefa de gerar blocos. Na prática, o parâmetro de diversidade de minerador, *minediversity*, dita qual porcentagem do grupo de mineradores está ativa para a mineração, deixando alguns nós como reserva, para substituir algum nó ativo em caso de falha. Tal comportamento aumenta a resiliência do protocolo a falhas de nó [Greenspan, 2015].

5. Avaliação Experimental de Plataformas de Cadeia de Blocos

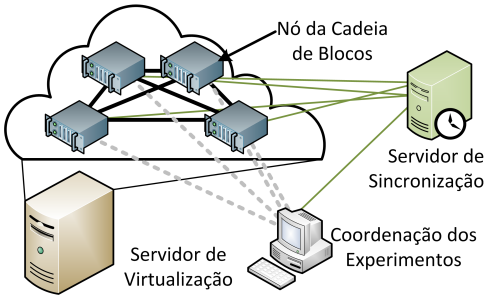
A avaliação de desempenho das plataformas é realizada aplicando uma carga de trabalho realística para a rede implantada. As redes de cadeia de bloco foram implantadas em um ambiente virtualizado, com 10 nós virtuais criados sobre a plataforma de virtualização VMWare ESXi 5[3], em um servidor com dois processadores Xeon E5-2650, em que cada nó da rede da cadeia de blocos foi configurado com 4 GB de RAM e 1 núcleo de processamento virtual, mostrados na Figura 4(a). O cenário de testes conta ainda com um computador usado para monitorar e coordenar os experimentos e um servidor de sincronização de tempo NTP (*Network Time Protocol*) para garantir que todos os nós das redes implantadas e o computador de coordenação estejam com a mesma referência de tempo. A carga de trabalho é obtida a partir da distribuição de probabilidade do tempo entre chegadas de transações da rede *Bitcoin* no período entre junho de 2017 e junho de 2018[4]. A Figura 4(b) mostra que o tempo de ocorrência entre transações segue uma distribuição normal generalizada, com $\mu = 0.371$, $\alpha = 0.143$ e $\beta = 2.786$. Em todos os experimentos as distribuições de probabilidade que melhor definem os dados foram calculadas pelo método dos mínimos quadrados e o ajuste da distribuição aos dados foi realizado pela biblioteca `Stats` do pacote `Scipy` da linguagem `Python`.

Os experimentos consistem na geração e envio de transações para as cadeias seguindo a carga de trabalho da *Bitcoin* durante o período de uma hora. Neste cenário as cargas de trabalho representam clientes da rede enviando transações uns para os outros através dos nós da

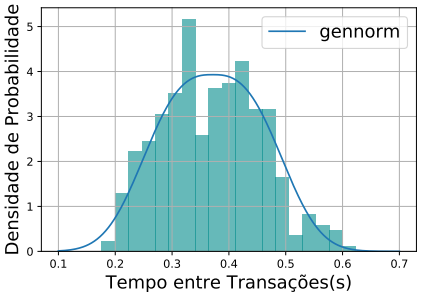
[2]Disponível em https://multichain.com/

[3]Disponível em https://www.vmware.com/ .

[4]Disponível em https://blockchain.info/



(a) Cenário de execução das redes.



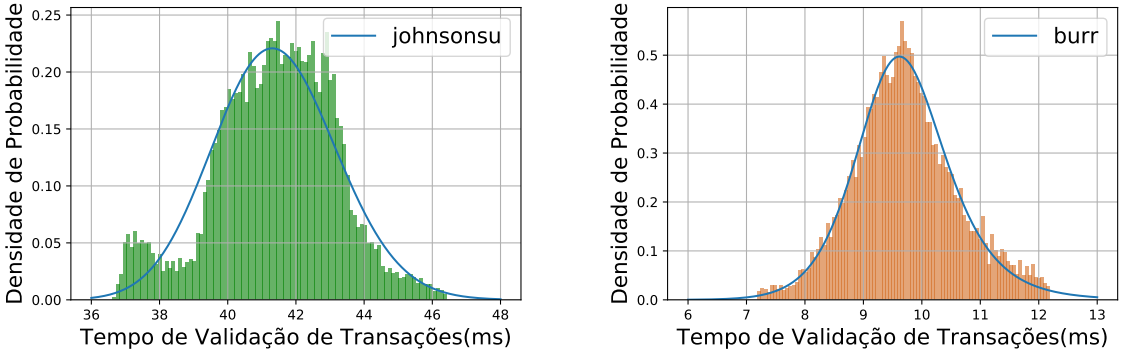
(b) Intervalo entre transações na *Bitcoin*.

Figura 4: Avaliação das redes de cadeia de blocos. a) Cenário de avaliação com cadeia executando em ambiente virtual. b) Distribuição do tempo entre chegadas de transações na rede *Biticoin* estimado no período entre junho de 2017 e junho de 2018. Os valores seguem uma distribuição normal generalizada com $\mu = 0.371$, $\alpha = 0.143$ e $\beta = 2.786$.

rede. A carga é configurada para que cada nó aguarde um intervalo de tempo definido pela variável aleatória que segue a distribuição observada na Figura 4(b). As execuções das redes foram realizadas usando configurações padrões recomendadas para a criação de redes privadas permissionadas pelos desenvolvedores da *Parity*[5] e da *Multichain*[6]. Os parâmetros que determinam o funcionamento do mecanismo de consenso são determinados no momento da construção das redes de cadeia de blocos. Os parâmetros foram definidos para que as redes apresentassem o comportamento mais similar possível a mérito de justiça na comparação. Cada execução de cada rede é iniciada com os nós conectados, porém sem qualquer transação sendo submetida. Em seguida as cargas de trabalho são aplicadas e cada nó submete transações enviando uma unidade da moeda corrente de sua posse para outros nós vizinhos. Esse processo é executado durante uma hora. Durante essa etapa são armazenados os registros de tempo de envio das transações e o tempo decorrido para que uma submissão seja aceita. Além disso, também são armazenados os identificadores de cada transação submetida para realizar posteriormente o experimento de tempo de busca das transações na cadeia de blocos. Durante a execução das buscas são obtidos os valores de tempo de busca por transações, tempo de busca por blocos e o instante da geração do bloco, a partir do qual é possível obter o tempo de mineração.

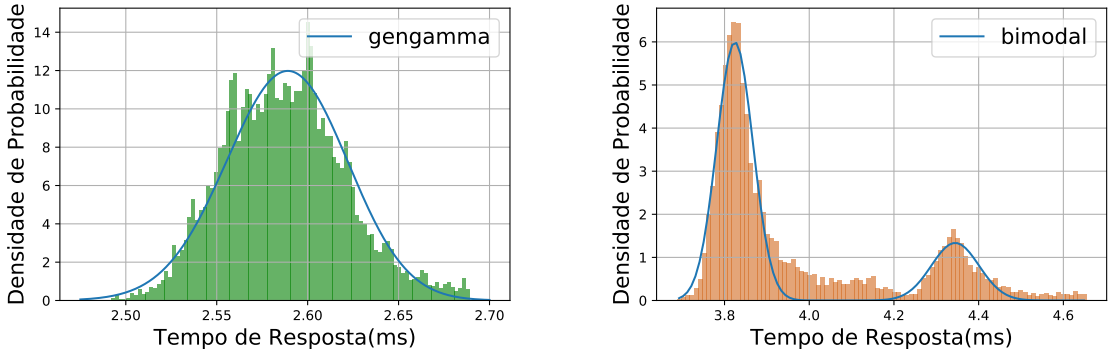
O tempo de validação da transação representa o tempo desde que um usuário envia uma transação, já assinada, para um nó e este realiza o processo de validação, verificando se a transação está devidamente formada. Registrando-se o momento em que a transação foi submetida e o tempo em que a confirmação de que a transação é válida é recebido, é possível calcular o tempo gasto para que uma transação seja validada. A Figura 5 apresenta os resultados para o tempo de validação de transações das duas plataformas. Ressalta-se que o comportamento do tempo de validação das transações na *Parity* segue uma distribuição S_u de Johnson, uma variação da distribuição normal, enquanto na *Multichain*, o tempo de validação segue uma distribuição de Burr, distribuição log-logística generalizada. Na Figura 5(a), observa-se que o tempo de validação na plataforma *Parity* variou entre os 37 ms e 46 ms, com a maior concentração de validações acontecendo em um intervalo em torno de 42 ms. A Figura 5(b) apresenta os resultados observados para os tempos de validação de transações na plataforma *Multichain*, que variaram entre 7 ms e 12 ms, tendo maior concentração de acontecimentos entre 9 ms e 10 ms. Portanto, é possível afirmar que a *Multichain* é, em média, 4 vezes mais rápida para validar uma transação.

[5]Disponível em https://parity.io/
[6]Disponível em https://multichain.com/



(a) *Parity* (b) *Multichain*

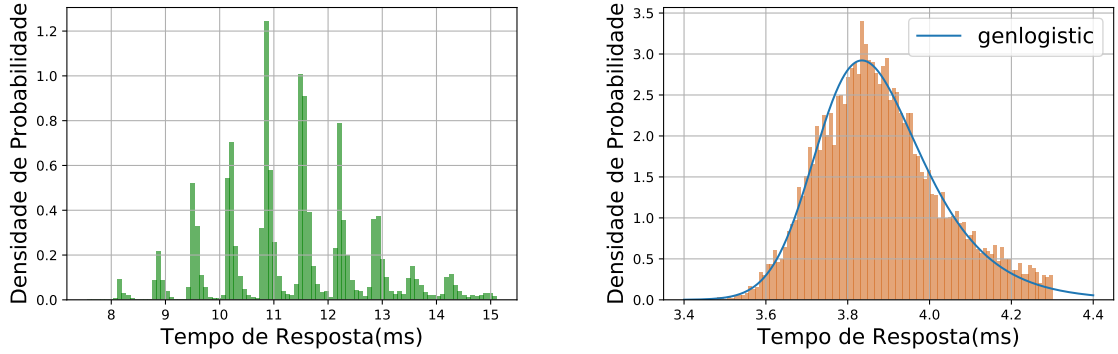
Figura 5: Desempenho medido em tempo de validação de transações. A *Multichain* é até 4 vezes mais rápida para validar uma transação. a) O tempo de validação segue uma distribuição S_u de Johnson. b) O tempo de validação segue uma distribuição de Burr, log-logística generalizada.



(a) *Parity* (b) *Multichain*

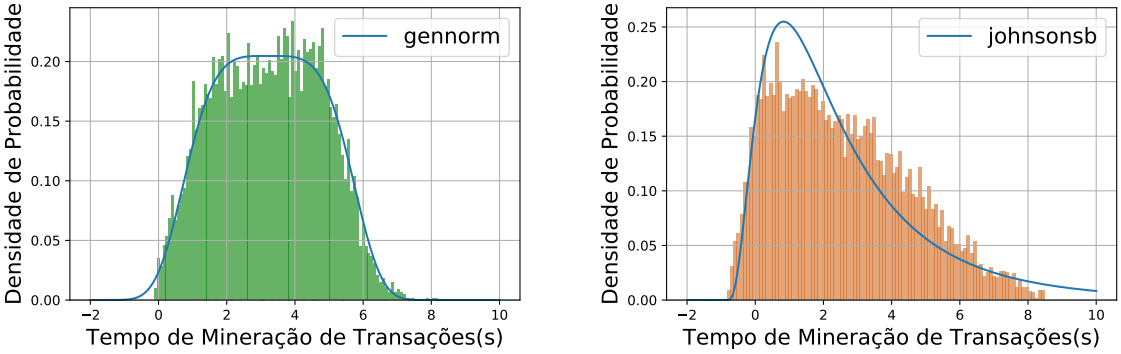
Figura 6: O tempo de resposta para a busca por transações é, em média, duas vezes menor na *Parity* que na *Multichain*. a) O tempo de busca de transações segue a distribuição Gamma generalizada. b) A*Multichain* apresenta uma distribuição de tempo para busca de transações bimodal, indicando a presença de diferentes níveis de armazenamento dos dados.

O tempo de busca por uma transação representa o tempo que a requisição de busca por uma determinada transação leva para retornar uma resposta válida. A busca é feita utilizando como parâmetro o identificador da transação. O tempo de busca é obtido registrando o instante que a requisição é enviada e o instante em que a resposta da requisição é recebida. Em seguida, o tempo de busca é a diferença entre o instante de submissão e o de resposta. A Figura 6(a) mostra o tempo de respostas das buscas por transações na *Parity*, que variam entre 2,5 ms e 2,7 ms, seguindo a função de distribuição de probabilidade Gamma generalizada. A Figura 6(b) apresenta os resultados da *Multichain* para as buscas por transação, observando que os resultados têm dois picos de concentração no histograma, o primeiro e maior em torno de 3,8 ms, e o segundo em 4,8 ms, com uma distribuição bimodal, formada por duas gaussianas com as médias nos dois picos de concentração. De forma semelhante à busca por transação, o tempo de busca por um bloco é calculado utilizando o registro do instante da submissão da busca e o instante em que a reposta é recebida. Para realizar a busca é utilizado o identificador do bloco que se deseja buscar.



(a) *Parity* (b) *Multichain*

Figura 7: O tempo de resposta para a busca por bloco é no mínimo duas vezes mais rápido na *Multichain*. a) Comportamento periódico para busca por blocos indica o armazenamento em memória volátil de blocos recentemente acessados. b) Tempo de acesso a blocos segue uma distribuição logística generalizada.



(a) *Parity* (b) *Multichain*

Figura 8: A latência entre a submissão de uma transação e a efetivação da transação na cadeia é estatisticamente a mesma em ambas as plataformas. a) O tempo de mineração de um bloco segue uma distribuição normal generalizada. b) O tempo de mineração segue a distribuição S_b de Johnson.

O tempo de busca de um bloco é a diferença entre os instantes de tempo de submissão da operação de busca e o retorno da resposta. A Figura 7(a) apresenta os resultados de buscas por blocos na cadeia *Parity*. A distribuição de probabilidades apresenta um comportamento periódico entre 8 ms e 15 ms, que não se adéqua a uma distribuição de probabilidades predefinida. Esse comportamento periódico pode ser justificado pelo fato de a *Parity* armazenar os últimos blocos acessados em memória volátil em detrimento de blocos mais antigos que são armazenados em disco. Isto faz com que buscas por transações que foram armazenadas no mesmo bloco de uma transação pesquisada recentemente não sejam feitas novamente em toda a cadeia, mas somente na memória volátil. A Figura 7(b) apresenta os resultados das buscas por blocos na *Multichain*. O tempo de busca por blocos é modelado por uma distribuição logística generalizada, tendo sua maior concentração de resposta por busca em torno de 3,9 ms. As buscas por blocos na cadeia *Multichian* têm a vantagem de serem indexas na cadeia de duas maneira. Convencionalmente, o bloco contêm o *hash* do bloco anterior em seu cabeçalho. Contudo a *Multichain* armazena também no cabeçalho do bloco o *hash* do bloco seguinte ao adicioná-lo na cadeia. Esta busca bidirecional faz com que o *Multichain* apresente respostas mais rápidas.

Para calcular o tempo de mineração de transações em cada uma das plataformas é necessário conhecer o registro de tempo do bloco e o registro de tempo da transação. O registro de

tempo do bloco pode ser obtido através da resposta da busca por um bloco e o registro de tempo da transação é armazenado durante a execução da carga de trabalho na etapa inicial da execução da rede de cadeia de blocos. Por fim o tempo de mineração é obtido através da diferença entre o tempo de submissão de uma transação e o registro de tempo de o bloco ter sido inserido na cadeia. A Figura 8 mostra os resultados dos tempos de mineração de transações para as duas plataformas. A Figura 8(a) apresenta o histograma dos resultados da cadeia *Parity*, que seguem distribuição de probabilidades normal generalizada, com os tempo de mineração variando entre 0 s e 7 s, com a média em 3,5 s. A Figura 8(b) apresenta os resultados da cadeia *Multichain* para o tempo de mineração das transações. Os resultados variam entre 0 s e 8 s[7], seguindo uma distribuição S_b de Johnson, em que o pico de ocorrências é em 1 s. Vale ressaltar, que quanto aos resultados de tempo de mineração, as duas plataformas levam estatisticamente o mesmo tempo para minerar os blocos.

6. Conclusão

Esse artigo realizou uma avaliação de desempenho de duas plataformas de cadeia de blocos privadas permissionadas, *Parity* e *Multichain*. As transações geradas para avaliar as plataformas seguiram a distribuição do intervalo entre chegadas de transações real da *Bitcoin*. Através das cargas de trabalho realísticas foi possível verificar o funcionamento das plataformas e analisar o tempo necessário para a validação de transações, as buscas por transações e por blocos da cadeia e o tempo efetivo de uma transação emitida ser adicionada a um bloco minerado e efetivado na cadeia. Os resultados demostraram que a plataforma *Multichain* apresenta melhores resultados para as quatro métricas de avaliação de desempenho ao custo de apresentar transações simples. A simplicidade da plataforma consiste em permitir somente transações de troca de ativos entre pares, enquanto a *Parity* suporta transações complexas como a execução de contratos inteligentes e, consequentemente, implica maior tempo para realizar as mesmas funções. Como trabalhos futuros, deseja-se comparar as plataformas apresentadas aplicando outras cargas de trabalho para avaliar critérios de escalabilidade e tolerância a falhas, além de expandir os experimentos a outras plataformas que permitam a utilização de cadeia privadas permissionadas.

Referências

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

Armknecht, F., Karame, G. O., Mandal, A., Youssef, F. e Zenner, E. (2015). Ripple: Overview and outlook. Em *Proc. of International Conference on Trust and Trustworthy Computing*, p. 163–180.

Bach, L. M., Mihaljevic, B. e Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. Em *Proc. of International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, p. 1545–1550.

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

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

[7]Os valores abaixo de 0 s são erros de precisão devido à sincronização ao se utilizar o servidor NTP e, portanto, não são relevantes para a análise de desempenho.

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

Dai, M., Zhang, S., Wang, H. e Jin, S. (2018). A low storage room requirement framework for distributed ledger in blockchain. *IEEE Access*.

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

Greenspan, G. (2015). Multichain private blockchain – white paper. Relatório técnico.

Guo, R., Shi, H., Zhao, Q. e Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access*, 776(99):1–12.

Gupta, S. e Sadoghi, M. (2018). *Blockchain Transaction Processing*, p. 1–11. Springer International Publishing.

Han, R., Gramoli, V. e Xu, X. (2018). Evaluating blockchains for iot. Em *Proc. of IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, p. 1–5.

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

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

Macdonald, M., Liu-Thorrold, L. e Julien, R. (2017). The blockchain: A comparison of platforms and their uses beyond bitcoin. Relatório técnico.

Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D. e Weinhardt, C. (2018). A blockchain-based smart grid: towards sustainable local energy markets. *Computer Science-Research and Development*, 33(1-2):207–214.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. Em *Proc. of International Conference on e-Health Networking, Applications and Services (Healthcom)*, p. 1–3.

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

Pahl, C., Ioini, N. E. e Helmer, S. (2018). A decision framework for blockchain platforms for iot and edge computing. Em *Proc. of International Conference on Internet of Things, Big Data and Security - Volume 1: IoTBDS*, p. 105–113.

Pilkington, M. (2016). *Blockchain technology: principles and applications*, p. 225–251. Edward Elgar Publishing.

Rebello, G. A. F., Alvarenga, I. D., Sanz, I. J. e Duarte, O. C. M. B. (2018). Sinfonia: Gerenciamento seguro de funções virtualizadas de rede através de corrente de blocos. Em *Anais do WBlockchain - SBRC*, volume 1.

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

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Relatório técnico.

Zheng, Z., Xie, S., Dai, H., Chen, X. e Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. Em *Proc. of International Congress on Big Data*, p. 557–564.

Zyskind, G., Nathan, O. et al. (2015). Decentralizing privacy: Using blockchain to protect personal data. Em *Proc. of Security and Privacy Workshops (SPW)*, p. 180–184.