Análise de Segurança dos Mecanismos de Consenso no PBFT usando Multichain e PoW usando Ethereum Aplicados em Redes Blockchain Privadas/Consórcio

João H.F. Battisti
Universidade do Estado de Santa Catarina (UDESC) - Programa de Pós-Graduação em Computação Aplicada (PPGCA)
joao.battisti@edu.udesc.br

Maurício A. Pillon
Universidade do Estado de Santa Catarina (UDESC) - Programa de Pós-Graduação em Computação Aplicada (PPGCA)
mauricio.pillon@udesc.br

Guilherme P. Koslovski
Universidade do Estado de Santa Catarina (UDESC) - Programa de Pós-Graduação em Computação Aplicada (PPGCA)
guilherme.koslovski@udesc.br

Charles C. Miers
Universidade do Estado de Santa Catarina (UDESC) - Programa de Pós-Graduação em Computação Aplicada (PPGCA)
charles.miers@udesc.br

ABSTRACT

A considerable number of electronic transaction systems employ classic approaches based on centralized trust mechanisms, not exploiting the latest technological advances. Alternatively, the concept of blockchain stands out, elaborated without the need for this centralized trust, but rather dependent on securely chained technologies in which the elements involved can conduct secure negotiations. Blockchain is designed to address security and distributed system issues through the use of encryption, algorithms, P2P networks, and consensus mechanisms. This paper presents a Denial of Service (DoS) security analysis of the more traditional Practical Byzantine Fault Tolerance (PBFT) and Proof of Work (PoW) consensus mechanisms available on Multichain and Ethereum solutions based on a private / consortium blockchain scenario. We present our results of a controlled DoS attack, revealing the importance and need for security-related analysis of blockchain implementations of private / consortium blockchains.

1 INTRODUÇÃO

O grande volume de transações eletrônicas realizadas é essencial para a execução das relações comerciais. Manter e/ou ampliar a oferta de tecnologias que forneçam maior eficiência e segurança nessas transações é um desafio constante. Soluções sustentadas por paradigmas centralizados são questionadas tanto para ponto único de falhas quanto limitações de escalabilidade, integridade e/ou confiabilidade. A partir destas preocupações e com desenvolvimento de tecnologias descentralizadas, ocorre um crescente movimento que tem como objetivo elaborar novos conceitos e soluções com abordagens não-centralizadas.

Um banco de dados tradicional utiliza uma arquitetura cliente-servidor, em contraste surgiu a tecnologia blockchain com uma abordagem descentralizada, na qual os participantes, estes confiáveis ou não, calculam, atualizam e mantém novas entradas de dados, que são replicadas em todos os nós do sistema. Estas entradas de dados são chamadas de transações que formam uma espécie de livro razão distribuído, que pode ser acessado por qualquer usuário com objetivo de verificar as validações das transações realizadas [19]. Como forma de garantir estes recursos, o blockchain emprega um conjunto de tecnologias que são conhecidas como: criptografia, al-goritmos, redes Peer-to-Peer (P2P) e mecanismos de consenso [12].

A tecnologia surgiu como solução para problemas de segurança e desempenho dos sistemas distribuídos, utilizando a tecnologia P2P com *timestamp* e aplicando o mecanismo de consenso *Proof of Work* (PoW) para comprovar a ordem cronológica das transações. Embora o blockchain tenha sido criado para permitir transações financeiras, e seja comumente associado a esse domínio, outras áreas de aplicação e uso de blockchain estão surgindo com o crescimento da atenção do público em torno da tecnologia [18]. A primeira implementação Bitcoin, aplicando a tecnologia blockchain, foi introduzida em 2008 [15]. Desde então, vários sistemas blockchain, como Ethereum [22], Hyperledger [23] e Multichain [7] emergiram com propostas fora do setor financeiro [1]. Com a versatilidade de utilização do blockchain, uma das questões geradoras de discussões na utilização da tecnologia é o seu custo computacional, que é considerado alto por utilizar criptografia e mecanismos que geram provas de confiabilidade. A partir desta questão foram desenvolvidos outros mecanismos de consenso (*Practical Byzantine Fault Tolerance* (pBFT), *Proof of Stake* (PoS), *Delegated Proof of Stake* (DPoS), *Leased Proof of Stake* (LPoS), *Proof of Importance* (PoI), *Proof of Authority* (PoA), *Proof of Burn* (PoB), *Proof of Capacity* (PoC) *etc.*) visando custos computacionais menores ao PoW [8].

Com estas novas possibilidades de aplicações do blockchain, é necessário compreender e identificar como estes mecanismos de consenso atuam. Outro ponto importante é que a grande maioria dos estudos realizados são direcionados para aplicações do blockchain, mas ainda são escassas as pesquisas sobre ameaças e vulnerabilidades da tecnologia associada, assim como o impacto na rede em que o blockchain encontra-se inserido. Com esta problemática e com plataformas e mecanismos que viabilizam o uso do blockchain, o presente trabalho visa realizar uma análise com foco na segurança dos mecanismos de consenso PoW e pBFT bem como suas características e relação destes no uso em instâncias virtuais. Sobretudo, o trabalho aborda a ocorrência de ataques do tipo DoS.

O artigo está organizado da seguinte forma. Na Seção 2 é realizada uma breve revisão sobre o blockchain, assim como os seus modelos, versões e mecanismos de consenso. Na Seção 3, são elencadas as principais ameaças de segurança associadas ao uso de

blockchain e apresentada uma classificação para as vulnerabilidades. Na Seção 4 é introduzida a problemática deste trabalho. Na Seção 5, são discutidos os trabalhos relacionados. A proposta de análise é descrita na Seção 6. A partir da definição de proposta, o ambiente de testes e os experimentos são descritos na Seção 7. A Seção 8 contém a análise dos resultados. As considerações finais e trabalhos futuros são apresentados na Seção 9.

2 BLOCKCHAIN & MECANISMOS DE CONSENSO

Um banco de dados tradicional, geralmente, utiliza uma arquitetura cliente-servidor, em que as entradas feitas pelos usuários são armazenadas em um servidor central e, eventualmente, replicadas. O blockchain, diferentemente, opera em um modelo descentralizado, em que cada participante mantém, calcula e atualiza novas entradas que são replicadas em todos os nós do sistema. Este sistema de registros cria um *livro-razão* distribuído, que contêm todas as transações realizadas.

Os sistemas que implementam o conceito de blockchain podem ser classificados em três modelos principais quanto ao seu acesso [2, 12]:Público, Consórcio e Privado. A Tabela 1 lista alguns critérios para comparação entre estes modelos [24].

Tabela 1: Comparação modelos de acesso do blockchain.

	blockchain Público	**blockchain Consórcio**	**blockchain Privado**
Consenso Distribuído	Todos Mineradores	Mineradores Selecionados	Mineradores Selecionados
Permissão de Verificação	Pública	Restrita	Restrita
Imutabilidade	Sim	Adulterável	Adulterável
Centralização	Descentralizado	Parcial	Centralizado
Processo de Consenso	Todos Mineradores	Mineradores Selecionados	Mineradores Selecionados

A partir da Tabela 1, pode-se inferir que o modelo público é atrativo por possuir uma quantidade superior de adeptos e pelo fato de ser aberto a todos que possuem interesse, possibilitando a entrada de novos mineradores de uma forma simples e branda. Ainda, é possível observar a similaridade entre os modelos de consórcio e privado, ambos são executados e controlados de acordo com as necessidades dos pares envolvidos. No caso do privado se torna mais atrativo para segurança da informação, pois possui um modelo mais tradicional utilizando computação distribuída.

Os algoritmos aplicados aos mecanismos de consenso do blockchain existem há bastante tempo na literatura, mas pode-se afirmar que a tecnologia blockchain aplicada da maneira atual é razoavelmente recente. Esse curto período de existência não impediu, entretanto, que os conceitos que suportam a tecnologia evoluíssem. De fato, alguns autores identificam diferentes eras ou estágios de evolução do blockchain, que, embora nem sempre tenham sido formalmente definidos, apresentam características marcantes que os diferenciam [21]. Na Tabela 2 é apresentado um comparativo entre mecanismos de consenso e as três versões aplicáveis do blockchain. A mesma é apresentada com os seguintes critérios: funcionalidades, abrangência de consenso e suas principais aplicações.

A partir da Tabela 2 observa-se o processo de desenvolvimento da tecnologia blockchain através de suas versões. A tecnologia iniciou-se com a vinda da era do Bitcoin e surgimento das criptomoedas, nos anos seguintes um novo potencial da tecnologia foi descoberto, a aplicação como contratos inteligentes, possibilitando a independência de uma terceira parte para questões contratuais [15].

Tabela 2: Comparativo básico entre as versões do blockchain

	blockchain 1.0	**blockchain 2.0**	**blockchain 3.0**
Funcionalidades	Criptomoedas	*Smart Contracts*	Aplicativos Descentralizados
PoW	Sim	Sim	Sim
DPoS	Não	Sim	Sim
PoS	Sim	Sim	Sim
pBFT	Não	Sim	Sim
LPoS	Não	Sim	Sim
PoI	Não	Sim	Sim
PoA	Não	Sim	Sim
PoB	Sim	Sim	Sim
PoC	Não	Sim	Sim
Ripple	Não	Sim	Sim
Tendermint	Não	Sim	Sim
Aplicações	Bitcoin	Ethereum,MasterCoin, *Open assets, Colored Coins*	Computação Descentralizada, Armazenamento Descentralizado

Como o recente desenvolvimento de aplicações diversas, evoluiu para computação e armazenamento descentralizados, envolvendo desta forma diferentes setores industriais e governamentais.

3 SEGURANÇA & BLOCKCHAIN

Com a necessidade de investigar as principais vulnerabilidades conhecidas da tecnologia blockchain, é realizado uma revisão bibliográfica que identifica as principais vulnerabilidade em relação a tecnologia. Na Tabela 3, são apresentadas as principais vulnerabilidades conhecidas no blockchain e as versões do blockchain que sofrem influências destas vulnerabilidades. A partir desta apresentação foi elaborada uma classificação inicial associando-as a três categorias principais: Redes, Poder Computacional e Usuário.

(1) **Redes:**
Aspectos relacionados ao controle dos nós, forma das transações ou até mesmo incapacitação operacional da rede.

(a) DDoS: O objetivo do atacante é tornar o serviço indisponível durante o processo de ataque. Os sistemas de defesa contra (DDoS) normalmente não são capazes de resistir sozinhos contra ataques em larga escala [17]. É importante notar que devido a natureza totalmente distribuída/replicada de blockchains, estes se tornam naturalmente resilientes a ataques de negação de serviço distribuídos. Além disto, o modelo de custo associado a blockchains públicos (impondo taxas para as transações), evita que usuários maliciosos realizem o envio em massa de transações impondo um alto custo a este tipo de ataque. *Distributed Ledger*s (DLTs) que não possuem um modelo de custo associado a cada transação estão suscetíveis a ataques de negação de serviço por parte de nos maliciosos dentro de um consorciou ou organização. Porém, entidades com permissões de escrita em uma DLT possuem um certo grau de confiança dentro da organização/consórcio.

(b) Ataque Eclipse: O Ataque Eclipse tem como intenção ganhar controle sobre os nós, desta forma controlando grande maioria do tráfego da rede. Quando um ataque Eclipse é bem sucedido, permite que o invasor controle todo tráfego de sobreposição, permitindo negação arbitrária de serviço ou de censura [20].

(c) Gasto Duplo: Esta vulnerabilidade está diretamente atribuída às criptomoedas, nas quais atacantes fazem múltiplas transações com a mesma moeda. Para este ataque ser realizado é necessário que o atacante minere privativamente, tentando estender ao máximo o tempo do bloco minerado sem publicar o cálculo, então é transmitida a transação para a organização

Tabela 3: Principais ataques e vulnerabilidades identificadas relacionadas a blockchain classificadas em categorias.

Ataque/Vulnerabilidade	Versão blockchain	Categoria	Relação
"Vulnerabilidade 51%"	1.0, 2.0, 3.0	Redes	Imutabilidade/Procedência
Chave Privada de Segurança	1.0	Usuário	Cifragem
DDoS	1.0, 2.0, 3.0	Redes	Transações/Procedência
Gasto Duplo	1.0, 2.0, 3.0	Redes	Arquitetura
Ataque Eclipse	1.0, 2.0, 3.0	Redes	Arquitetura/Transação/Procedência
Ataque de Vivacidade (*Liveness*)	1.0	Poder Computacional	Transações/Procedência
Mineração Egoísta	1.0, 2.0, 3.0	Poder Computacional	Procedência
Otimização *Smart Contract*	1.0, 2.0, 3.0	Usuário	Transparência/Transação
Privacidade de Transação	1.0, 2.0	Redes	Arquitetura
Retenção de Blocos	1.0, 2.0, 3.0	Poder Computacional	Transparência
Smart Contract Malicioso	2.0	Usuário	Procedência/Transações

de interesse e esperar para que a transação seja registrada, e então minerado até que este bloco seja maior do que o bloco público, assim é publicado o cálculo apagando a transação feita com a organização [**?**]. O problema do gasto duplo ocorre de maneira diferente para os diferentes tipos de mecanismos de consenso. Por exemplo, em um blockchain baseada em PoW, o gasto duplo exige que o atacante tenha controle sobre 51% do poder computacional da rede, decidindo, deste modo, priorizar uma cadeia de blocos em detrimento a outra. No entanto, em um blockchain baseada em em PoS, na qual não se exige um gasto de recursos como prova de trabalho, a rede fica mais suscetível a criação de cadeias paralelas (uma vez que estas cadeias podem ser geradas sem esforço computacional). Neste caso, a alternativa para blockchains baseados em PoS é um mecanismo de consenso híbrido entre PoS e PoW no qual introduz-se um esforço computacional para a geração de blocos, mas mantendo a determinação dos mineradores baseando-se em seus recursos ("*stake*").

(d) Privacidade de Transação: Esta vulnerabilidade está relacionada com a possibilidade de rastreabilidade do blockchain, conforme o modo de programação o destinatário pode ser detectado através da transação da rede [11]. A maioria das criptomoedas públicas utilizam um esquema de pseudo-anonimidade, na qual usuários são identificados por endereços (*hash* gerado criptograficamente) não revelando, deste modo, sua identidade. Neste sentido, é possível observar todas as transações financeiras de contas mas não a identidade do usuário que gerencia a conta. No entanto, a conversão de uma criptomoeda para um dinheiro final requer a utilização de uma casa de cambio, que por sua vez exige a identificação do usuário, e assim estabelecer uma relação entre usuário-conta. No entanto, existem criptomoedas como Monero [10] que utiliza um protocolo (CryptoNote) que ofusca por meio de uma primitiva baseada em *ring signatures* as três partes essenciais de uma transação: remetente, valor e destinatário. Mas questões quanto a privacidade de transações variam de acordo com as necessidades que a aplicação exige, pois ao relacionar quanto a blockchain para auditoria é interessante estas abordagens que permitem maior transparência.

(e) "Vulnerabilidade 51%": Este ataque é realizado a partir do mecanismo de consenso do blockchain, em que se o invasor obter 51% do *hashing* do *pool* ele tem o controle sobre o bloco. A partir disto, existe a possibilidade de realizar mudanças entre outras questões [11].

(2) **Poder Computacional:**
Ataques relacionados ao aumento de *hashing* com o intuito de obter benefícios sobre mineradores honestos ou simplesmente reduzir a recompensa que um grupo de mineradores tem direito.

(a) Retenção dos Blocos: Objetiva sabotar mineradores honestos, fazendo com que desistam do *pool*. O minerador inicia o processo como um minerador honesto, mas o atacante envia apenas uma parcial da prova de trabalho. Se encontrar uma solução completa que constitua uma prova de trabalho descarta a solução, reduzindo o rendimento total [5].

(b) Mineração Egoísta: Este ataque tem como finalidade obter recompensa ou perda de poder computacional de mineradores honestos. Especificamente, a mineração egoísta força os mineradores honestos a gastar seus ciclos computacionais em blocos destinados a não fazer parte do blockchain. Mineradores egoístas atingem esse objetivo revelando seletivamente seus blocos minados para invalidar o trabalho dos mineradores honestos [6].

(c) Ataque de Vivacidade(*Liveness*): Este ataque é realizado para atrasar o máximo possível o tempo de confirmação de uma transação alvo [9]. Este ataque passa por três fases: a primeira que é quando o minerador malicioso cria vantagem sobre os mineradores honestos, a segunda é de *Denial-of-Service* (DoS) e a terceira que é a retardadora do blockchain.

(3) **Usuário**:
Ataques relacionados a categoria usuários são relacionados a programação, intenções maliciosas e até mesmo falta de conhecimento.

(a) Chave Privada de Segurança: Este ataque é relacionado a chave de segurança privada de cada usuário. Caso a chave for roubada ou perdida o usuário dificilmente conseguirá recupera-lá.

(b) *Smart Contract* Criminoso: Este contrato pode facilitar o vazamento de informações confidenciais, roubo de chaves criptográficas e vários tipos de comportamentos do usuário [11].

(c) Otimização *Smart Contract*: Relacionado a programação do contrato, em que este é pouco otimizado causando grandes perdas para quem o utiliza. Segundo [4] foram detectados alguns padrões em códigos que demonstram funções inúteis, que não são utilizadas, e também códigos em *loop*.

4 DEFINIÇÃO DO PROBLEMA

Há um crescimento considerável de aplicações blockchain, mas estas aplicações possuem diferentes contextos e realidades de usuários.

No contexto destas aplicações, busca-se a melhoria da eficiência e qualidade da tecnologias, mas também há preocupações ligadas ao seu alto custo computacional que é necessário para manter seu desempenho e segurança. Em um contexto que uma aplicação que utiliza PoW exige que diversos pares da rede disputem entre si para resolver um problema matemático no qual somente um destes competidores recebe os incentivos do bloco.

Percebe-se que há diversos mecanismos de consenso, responsáveis em realizar várias operações entre estas o processo de validação do blockchain. Entretanto, não foram encontrados estudos que tenham como finalidade realizar análises destes diferentes mecanismos de consenso em contexto com nenhuma outra tecnologia. Com base no escopo definido até o momento, percebe-se a dificuldade na escolha do método de consenso que deve ser aplicado, levando em consideração as necessidades dos usuários, a versão e o modelo blockchain, com preocupação nos pilares da segurança: Confidencialidade, Integridade e Disponibilidade.

A decisão de qual tecnologia aplicar é bastante complexa, pois impacta diretamente nas questões de segurança e desempenho dos sistemas. Com o levantamento da Tabela 3, torna-se fundamental analisar as tecnologias de consenso do blockchain com as possíveis vulnerabilidades e as definições de segurança definidos por organizações, como por exemplo *National Institute of Standards and Technology* (NIST) e *Cloud Security Alliance* (CSA) que são voltadas para questões de computação em nuvens, máquinas virtuais, etc.

Quanto a questão uma exemplificação é uma aplicação blockchain que permite que sejam utilizados dois mecanismos de consenso conhecidos, o pBFT e o PoW. Torna-se necessário a compreensão das características do seu sistema e os aspectos dos mecanismos de consenso para realizar a melhor escolha. A partir desta necessidade é necessário a realização da análise para entender e auxiliar na decisão de qual destes mecanismos de consenso possuem os melhores aspectos para serem aplicados, os riscos dos mesmos e se atendem as necessidades que a instituição necessita.

No atual cenário do uso da tecnologia blockchain, há incertezas quanto a viabilidade da aplicação da tecnologia, principalmente pelo fato de sua popularidade, de qual melhor modelo e mecanismo deve-se aplicar com outras tecnologias, principalmente pela diversidade de opções existentes. O problema em questão é a falta de critérios para comparar os mecanismos de consenso do blockchain e sua relação com vulnerabilidades, ameaças e riscos existentes que são intrínsecos às tecnologias e arquiteturas empregadas.

5 TRABALHOS RELACIONADOS

Alguns trabalhos como de [25] são voltados ao problemas de privacidade dos dados, em que verificam ameaças à privacidade dos dados em serviços *online*, seja por áreas industriais, da saúde, redes sociais entre outras. Os autores [25] afirmam o quão frágil é a privacidade do usuário quando dependem de uma terceira entidade, pois os usuários não tem controle sobre quais dados estão sendo coletados, armazenados e também utilizados. [13] realiza comparações entre as plataformas Ethereum, IBM *Open blockchain*, Intel *Sawtooth Lake*, BlockStream *Sidechain Elements* e Eris relacionadas a usabilidade, desenvolvimento, flexibilidade, escalabilidade, mecanismos de consenso e segurança. O trabalho de [3] também exploram algumas plataformas de blockchain e que possuem mecanismos de consenso relacionados ao pBFTs. [3] apresentam questões relacionadas ao algoritmo de consenso, quanto a validação e sua resistência, destacando que é interessante a realização de uma comparação destes algoritmos de consenso em um ambiente real com a realização de ataques. Outro trabalho interessante, [19] relaciona o blockchain como uma tecnologia futura na área de *cybersecurity*. [19] apresentam uma estruturação da tecnologia blockchain na sua aplicação voltada a segurança da informação, mas abrem pontos sobre o encorajamento ou não, dependendo de sua aplicação, no uso do blockchain na área de segurança. Pois, as plataformas de tecnologia blockchain apresentam cada vez mais agentes maliciosos que buscam vulnerabilidades da rede.

Quanto a questão da segurança dos mecanismos de consenso aplicados à tecnologia blockchain, não foram encontrados trabalhos relacionados, informação desta falta de conteúdo sobre as questões de segurança do blockchain são apontadas também por [19]. A Tabela 4 apresenta um comparativo dos trabalhos relacionados.

Tabela 4: Comparativo dos trabalhos relacionados.

Trabalhos	Plataformas blockchain	Mecanismos de Consenso	Ameaças, Riscos e Vulnerabilidades	Possíveis Soluções
[25]	Não Aborda	Não Aborda	Aborda	Não Aborda
[13]	Aborda	Aborda	Não Aborda	Não Aborda
[19]	Não Aborda	Não Aborda	Aborda	Aborda
[3]	Aborda	Não Aborda	Aborda	Não Aborda

A partir da Tabela 4 é possível identificar que nenhum dos trabalhos aqui relacionados aborda por completo os aspectos determinados neste artigo. Entre estes, o trabalho que revela-se mais interessante e preocupado com as questões de segurança é o de [19], por levantar questões do uso de blockchain como mecanismo de segurança, questionando sobre as próprias vulnerabilidades que a tecnologia possui. Um dos principais pontos é sobre a atual necessidade de trabalhos que co-relacionem as questões de vulnerabilidade do blockchain com resultados reais e testados.

6 PROPOSTA

As configurações de uma instância no blockchain representam a disponibilidade de recursos para utilização do nó da blockchain. Estes recursos são relacionados as transações que um nó pode realizar para operacionalizar a aplicação, mas também podem ser alterados conforme as configurações do mecanismo de consenso aplicado. As configurações padrões podem ser suficientes para operacionalização da aplicação, contudo é necessário averiguar as questões de vulnerabilidades, quanto a ataques como o DoS.

A proposta para este trabalho consiste na realização de um experimento com uma breve análise de segurança dos mecanismos de consenso pBFT e PoW em um ambiente com blockchain privado quando submetidos há ataques simples de DoS. No atual cenário as organizações buscam o blockchain como solução com o objetivo de empregar aspectos como: auditoria, procedência dos dados, proteção e gerenciamento dos dados e segurança no gerenciamento do ciclo de vida das informações.

Atualmente, há pesquisas que indicam que os principais responsáveis pelas violações de dados que ocorrem em ambientes de nuvens computacionais são funcionários das empresas [16, 25]. Este fato demonstra a necessidade da realização de análises voltados para soluções com ambientes privados e consórcios. Outro motivo que apresenta esta necessidade são as vulnerabilidades apresentadas na Tabela 3, que delimitam em grupos estas análises.

A escolha pelo ataque DoS pertence ao grupo de redes que envolvem outros ataques como: Ataque Eclipse, Gasto Duplo, Privacidade das Transações e a Vulnerabilidade "51%". As questões relacionadas a este grupo impactam no desempenho, funcionalidade, custo computacional e podem atingir não somente a rede blockchain, mas todo o sistema em si [19].

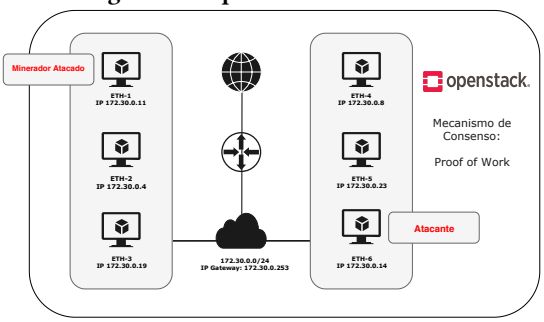
Desta forma, o intuito desta análise é responder questões e amenizar dúvidas relacionadas aos mecanismos de consenso, apresentando possíveis boas práticas para as questões. Facilitando que usuários e novos usuários da tecnologia realizem integrações ao seu sistema com uma tecnologia segura, eficiente, viável, melhor custo benefício, desempenho e funcionalidade para seu cenário.

7 AMBIENTE DE TESTES & EXPERIMENTOS

Os experimentos e cenários baseiam-se nos critérios levantados na Seção 4. Dois cenários de blockchain de Modelo Privado foram definidos em uma nuvem computacional utilizando a solução OpenStack, sendo a distinção dos cenários é dada pelo mecanismo de consenso do blockchain. As configurações do ambiente de testes são as necessárias exigidas pelas plataformas, Ethereum e Multichain. A topologia dos dois cenários possuem seis instâncias com imagens padrão da distribuição GNU/Linux Ubuntu Server 16.04 LTS.

7.0.1 Cenário I - Plataforma Ethereum com PoW. Utiliza uma rede privada blockchain com mecanismo de consenso PoW. Possui seis instâncias que tem como finalidade a realização dos processos de validação e mineração de blocos/transações da rede blockchain, estas instâncias podem ser observadas na Figura 1.

Figura 1: Arquitetura do Cenário I.



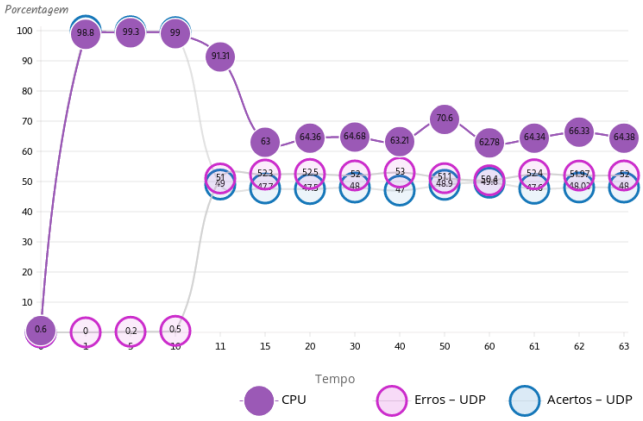
O cenário, apresentado na Figura 1, tem como objetivo a investigação do comportamento do ambiente apresentado blockchain com o mecanismo de consenso PoW. O experimento tem como intuito averiguar a garantia de procedência de dados [14], controle e gerenciamentos dos nós [14] e também a estabilidade da rede, a partir de ataques DoS. Para este experimentos, o teste realizado foi utilizado a plataforma Ethereum, que é uma plataforma de código aberto e aplicada para ambientes públicos, privados e consórcios.

O Ethereum é uma plataforma descentralizada que aplica o mecanismo de consenso PoW. A plataforma Ethereum quando aplicada à um modelo blockchain privado ou consórcio não tem a necessidade de utilização de *Unidade de Processamento Gráfico* (GPU) para realizar processos de mineração e validação de transações, que é um requisitos de modelos públicos. Como complementação, o Ethereum utiliza os protocolos TCP e UDP para troca de informações.

Com a identificação dos protocolos utilizados pela plataforma, foram selecionados dois experimentos de ataques à plataforma o *UDP Flood* e *Transactions Flood*, ambos algoritmos foram desenvolvidos pelos autores na linguagem Python. O ataque *Transaction Flood*, foi realizado a partir da instância ETH-6 contra a instância ETH-1 (Figura 1). A partir da realização deste ataque é observado que não houve nenhum dano nos quesitos de estabilidade, controle e gerenciamento dos nós e a procedência dos dados. Não foram identificados alterações ao processamento e memória que causassem impactos negativos para a instância ou para rede em si, é observado apenas que há *buffer* que é a limitação de velocidade de transações.

Com os testes realizados com o ataque *UDP Flood*, novamente foram realizados ataques a partir da instância ETH-6 contra a instância ETH-1. Na Figura 2 observa-se três linhas de marcações, representando o consumo do processador, pacotes UDP recebidos e uma representando os pacotes UDP que apresentaram erro.

Figura 2: Consumo de processador no ataque *UDP Flood*.



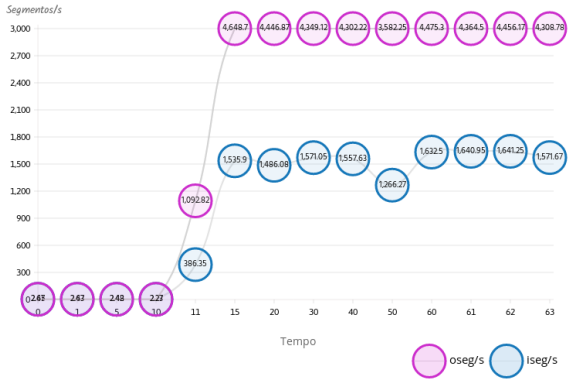
Na Figura 2 e Tabela 5 é possível observar que nos dez primeiros minutos a mineração é realizada de forma padrão, sem uso de GPU. O ataque é iniciado, a partir, do momento onze minutos, em que se observa o início de uma queda do uso do processamento e aumento na quantidade de erros-*User Datagram Protocol* (UDP). Observa-se, como efeito do ataque *UDP Flood*, a ocorrência de uma diminuição significativa de mineração e validações dos blocos/transações, que por vezes a troca de informações da rede blockchain é interrompida temporariamente.

Tabela 5: Consumo de processador no ataque *UDP Flood*.

Tempo/Min	Processamento	Acertos-UDP	Erros-UDP
0	0.60%	100%	0.00%
1	98.80%	100%	0.00%
5	99.30%	98.80%	0.20%
10	99.00%	98.50%	0.50%
11	91.31%	49.02%	50.98%
15	63.00%	47.70%	52.30%
20	64.36%	47.50%	52.50%
30	64.68%	48.00%	52.00%
40	63.21%	47.00%	53.00%
50	70.60%	48.90%	51.10%
60	62.78%	49.60%	50.40%
61	64.34%	47.60%	52.40%
62	66.33%	48.03%	51.97%
63	64.38%	48.00%	52.00%

O comportamento do Tráfego TCP durante a execução do ataque é apresentado na Figura 3.

Figura 3: Tráfego TCP no ataque *UDP Flood.*



É possível identificar (Tabela 6) que a partir do tempo dez, em que o ataque é inicializado, um fluxo mais intenso do tráfego de rede, crescimento de entradas e saídas de dados. Este aumento do fluxo da rede, permite a identificação de atrasos durante a troca de informações entre os nós da rede blockchain, causando atrasos e até mesmo possibilidade de exploração de outras vulnerabilidades.

Tabela 6: Tráfego TCP durante o ataque *UDP Flood.*

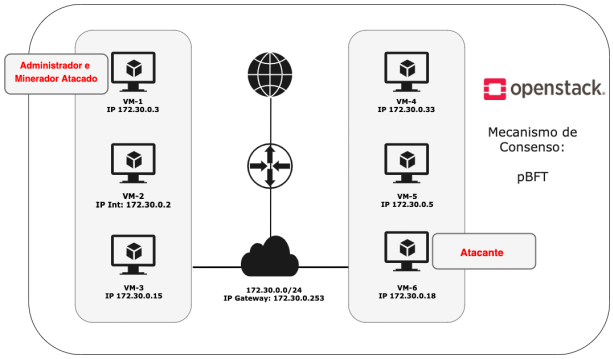
Tempo/Min	Entrada/Segundo	Saída/Segundo
0	2.65	2.47
1	2.67	2.43
5	2.42	2.48
10	2.23	2.27
11	386.35	1092.82
15	1535.90	4648.70
20	1486.08	4446.87
30	1571.05	4349.12
40	1557.63	4302.22
50	1266.27	3582.25
60	1632.50	4475.30
61	1640.95	4364.50
62	1641.25	4456.17
63	1571.67	4308.78

Com os experimentos do Cenário I realizados, é perceptível as implicações do ataque *UDP Flood* perante o desempenho do nó perante os outros nós da rede blockchain. Desta forma, empregando um ataque simples e conhecido como o DoS é possível detectar atrasos na troca de informações, prejudicando desta forma a participação do nó no mecanismo de consenso e também reduções nas taxas de mineração de novos blocos. A partir dos análises dos resultados obtidos, é importante a realização de monitoramentos do fluxo da rede como boas práticas de segurança para evitar ou mitigar impactos de ataques à rede blockchain.

7.0.2 Cenário II - Plataforma Multichain com pBFT. O segundo cenário apresenta uma rede privada blockchain com o mecanismo de consenso pBFT. Este ambiente possui seis instâncias que tem como finalidade a realização dos processos de validação e mineração de blocos/transações da rede blockchain, estas instâncias podem ser observadas na Figura 4.

Este cenário (Figura 4) possui como objetivo a investigação do comportamento do ambiente apresentado blockchain com o mecanismo de consenso pBFT. O intuito deste experimento é averiguar a garantia de procedência de dados, controle e gerenciamento dos nós e também a estabilidade da rede, a partir da aplicação de ataques DoS. Nste experimento foi utilizada a plataforma Multichain 1.0.5,

Figura 4: Arquitetura do Cenário II.



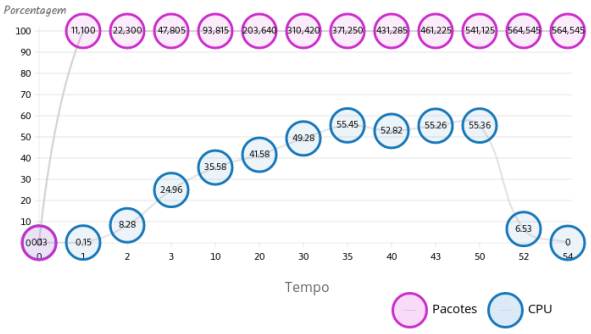
que é uma plataforma de código aberto e aplicada somente para uso de blockchains privados e consórcios.

A plataforma Multichain utiliza uma rede centralizada ou parcialmente descentralizada, possuindo a existência de um administrador, este administrador é responsável pelo gerenciamento da rede e também a criação do bloco Genesis. Entre as responsabilidades deste gerenciamento de redes está a permissão de todos nós que participam da rede, dando a estes a responsabilidade de participação no processo de consenso, do envio e recebimento de transações entre outras funções. Como complementação, as redes Multichain utilizam como método de comunicação o *Remote Procedure Call* (RPC).

Com a identificação do uso de RPC, foi selecionado dois experimentos de ataques o *SSH Flood* e *Transactions Flood*, ambos algoritmos foram desenvolvidos pelos autores na linguagem python. O primeiro ataque aplicado foi o *SSH Flood*, que é realizado a partir da instância VM-6 endereçado para a instância VM-1. A partir da realização deste ataque é observado que não houve nenhum dano nos quesitos de estabilidade, controle e gerenciamento dos nós e a procedência dos dados. Não foram identificados alterações ao processamento e memória que causassem impactos negativos para a instância ou para a rede em si.

Já com os testes realizados com o ataque *Transaction Flood*, novamente foram realizados ataques a partir da carteira da instância VM-6 endereçados para a carteira da VM-1, que é o administrador da rede. O mecanismo de consenso pBFT é um mecanismo com baixo consumo de CPU, basicamente não necessita altas taxas de processamento para criação e validação de novos blocos ou transações. Este comportamento pode ser observado na Figura 5.

Figura 5: Consumo de processador: *Transactions Flood.*



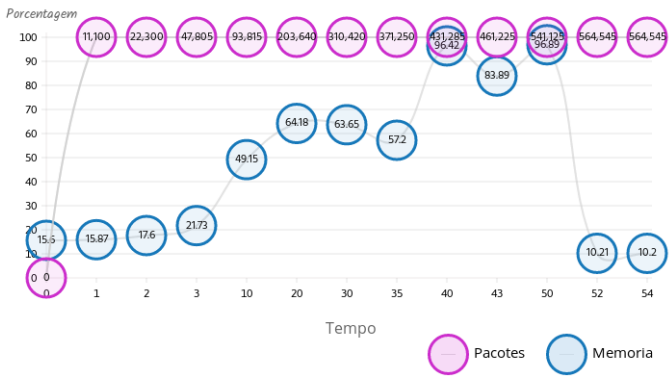
Na Tabela 7 é perceptível que após um período de tempo há uma estabilização de crescimento da memória, acredita-se que deve-se ao fato da ocorrência de retransmissões TCP e também ao estouro de memória.

Tabela 7: Consumo de processador, *Transaction Flood.*

Tempo/Min	Processamento	Pacotes/Transações
0	0.13%	0
1	0.15%	11100
2	8.28%	22300
3	24.96%	47805
10	35.58%	93815
20	41.58%	203640
30	49.28%	310420
35	55.45%	371250
40	52.82%	431285
43	55.26%	461225
50	55.36%	541125
52	6.53%	564545
54	0,09%	564545

Observando a Figura 6 percebe-se que o impacto mais expressivo durante o ataque ocorre justamente nos parâmetros de consumo de memória. A partir da análise da Tabela 8 que com o envio de novas transações a partir da VM-6, há um aumento significativo na quantidade de memória consumida pela aplicação da rede blockchain.

Figura 6: Consumo de Memória: Ataque *Transactions Flood.*



Na Figura 6 é possível observar que há alguns pontos em que a memória reduz momentaneamente sua taxa de uso, existe a necessidade de um maior aprofundamento para compreender o motivo desta redução, uma hipótese é a ocorrência de descartes de blocos realizados pela plataforma.

Tabela 8: Consumo de memória, *Transaction Flood.*

Tempo/Min	Processamento	Pacotes/Transações
0	15.60%	0
1	15.87%	11100
2	07.60%	22300
3	21.73%	47805
10	49.15%	93815
20	64.18%	203640
30	63.65%	310420
35	57.20%	371250
40	96.42%	431285
43	83.89%	461225
50	96.89%	541125
52	10.21%	564545
54	10.20%	564545

Quanto aos experimentos realizados com o ataque DoS *Transaction Flood* observa-se na Figura 6 que a partir dos cinquenta minutos (Tabela 8) há a ocorrência de estouro de memória. O estouro de memória implica no encerramento abrupto da aplicação, ou seja, o nó responsável pela administração da rede foi perdido temporariamente causando diversos erros e instabilidades para a rede blockchain.

O experimento aplicado ao Cenário II foi possível observar o desempenho da rede blockchain modelo privado e mecanismo pBFT. Este cenário revelou a fragilidade de uma rede blockchain centralizada ou semi-descentralizada. Pois, com apenas um atacante, instância VM-6, foi possível realizar estouro de memória ao nó administrador da rede, causando instabilidade de modo generalizado à rede blockchain. Tornando-se necessário o monitoramento dos fluxos da rede interna, atreladas com boas práticas de segurança e a dependência da necessidade de confiança entre os nós da rede.

8 ANÁLISE DE RESULTADOS

Os resultados apresentados nesta análise são condizentes com as necessidades que foram abordadas por [19]. Os autores apresentam as questões de ataques, em destaque para este trabalho, o DoS como uma questão de segurança, ataques como este além de causarem danos para a rede do blockchain, também tem influência sobre outras questões do sistemas. Contudo, para as vulnerabilidades apresentadas na Tabela 3 há a possibilidade de mitigação dos impactos dos ataques através de mecanismos de segurança e flexibilização na configuração dos sistemas.

Com o Cenário I foi possível verificar o funcionamento da rede blockchain Ethereum e seu mecanismo de consenso PoW. O Ethereum é uma plataforma descentralizada e demonstrou considerável segurança no recebimento de diversas transações. O fato da plataforma não possuir um nó centralizador, administrador em comparação com o Multichain, permite uma maior garantia no quesito segurança.

No teste realizado com o ataque *UDP Flood*, no Cenário I, o mecanismo de consenso não apresentou falhas, apenas teve seu tempo de validação blocos e transações aumentado. O mecanismo PoW exige uma quantidade significativa de demanda de poder computacional e com o ataque o tempo de resposta foi aumentado.

A partir do Cenário II foi possível verificar o funcionamento da rede blockchain Multichain com seu mecanismo de consenso pBFT. No teste com o ataque *Transactions Flood* ocorreram resultados interessantes, pois apresentou estouro de memória, que indica a perda significativa de transações enviadas e também do controle que a instância VM-1 tem perante a rede blockchain. Revelando que redes privadas centralizadas ou semi-descentralizadas necessitam de maior segurança e cuidado com os pares que estão na mesma rede. O processo de consenso pBFT não apresentou falhas durante o ataque e tolerância a possíveis erros, outro ponto interessante em relação ao consenso é a questão de vulnerabilidade de violação, pois necessita que dois terços dos nós aprovem a validação de um bloco e que realizem diversas confirmações durante o período de atividade do sistema.

Como consolidação dos resultados obtidos, a Tabela 9 apresenta a relação entre os critérios de procedência dos dados [14] e controle e gerenciamento dos nós [14], os problemas encontrados durante os testes e o relacionamento destes com os critérios.

Tabela 9: Visão geral dos resultados da análise do trabalho.

Critérios	Consenso	Problemas	Boas práticas
Procedência dos dados	PoW	Não apresentou problemas em relação a segurança dos dados	Realizar verificações de transações e blocos para garantia contínua da procedência
	PBFT	Problemas com validação de Transações, Possibilidade de alteração do conteúdo das transações	Monitoramento CPU/Memória
Controle e Gerenciamento do Nó	PoW	Problemas com Mineração, Tráfego intenso em seus protocolos	Monitoramento de tráfego interno, Monitoramento de processamento
	PBFT	Problemas com administração da rede Blockchain	Monitoramento de transações

Para o critério de Procedência dos Dados foram encontrados problemas relacionados a validação de transações/blocos, que foram geradas por atrasos na mineração ou queda do sistema. Neste critério há uma outra questão que fica em aberto, que é a do anonimato, pois em modelos privados a rede não consegue assegurar esta garantia. Como solução para estes casos, torna-se necessário a realização de uma ampla investigação sobre o sistema para fins de mitigar, a realização de monitoramento constante nas redes internas e pré-definidas aos participantes.

Quanto ao critério de Controle e Gerenciamento do Nó, os principais problemas encontrados são relacionados as questões de mineração, tráfego intenso na rede e no cenário 7.0.2, particularmente, a questão de um nó administrador da rede blockchain. As questões relacionadas à este critério permitem a abertura para outras vulnerabilidades, principalmente as que são vinculadas a rede e poder computacional. Sendo que, alguns atacantes podem utilizar combinações de ataques para explorar de formas mais agressivas vulnerabilidades como Mineração Egoísta, Ataque Eclipse, Retenção de Blocos e o Ataque "51%". Como solução ou possíveis boas práticas para evitar a exploração destas vulnerabilidades é interessante que seja realizado monitoramento do tráfego, transações e de processamento.

9 CONSIDERAÇÕES

São diversos os benefícios que o uso de Blockchain traz às organizações em termos de economia, gerenciamento de dados, auditoria e segurança que são descritos em diversos trabalhos relacionados. Ficou contundente neste trabalho a necessidade determinar a melhor forma de aplicação do Blockchain e seus mecanismos de consenso, levando em consideração as características da aplicação e sua linha de segmento.

Os experimentos realizados neste trabalho indicam que blockchains do tipo Privado ou Consórcio demandam de atenção quando inseridos nas organizações. Tipicamente um nó de uma rede blockchain é alocado em um máquina virtual padrão, de configuração similar a usada nos experimentos deste trabalho, revelando que usuários maliciosos podem de uma maneira simples comprometer/prejudicar a operação da blockchain. Assim, a adoção de soluções blockchain tipo Privado ou Consórcio necessita de atenção especial em sua inserção nas redes das organizações de modo a diminuir a superfície de ataque. De um modo geral, quanto ao uso dos mecanismos de consenso, é perceptível que há possibilidade, através das boas práticas, destes problemas serem minimizados.

Quanto a trabalhos futuros, está sendo desenvolvido um método que correlaciona a quantidade de transações na blockchain em função do consumo de recursos computacionais (processador, memória e rede) usando mecanismos de consenso PoW e pBFT. Este estudo permite dimensionar a configuração da máquinas virtuais bem como identificar limites de operação normal de possíveis ataques de DoS.

Agradecimentos: Os autores agradecem ao LabP2D, UDESC e FAPESC.

REFERÊNCIAS

[1] Karan Bharadwaj. 2016. The Blockchain 1.0: Currency. (2016). "http://www.linkdapps.com/Blockchain1.0-Currency.pdf"
[2] Vitalik Buterin. 2015. On Public and Private Blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
[3] Christian Cachin and Marko Vukolić. 2017. Blockchain Consensus Protocols in the Wild. arXiv:cs.DC/1707.01873
[4] Ting Chen, Xiaoqi Li, Xiapu Luo, and Xiaosong Zhang. 2017. Under-Optimized Smart Contracts Devour Your Money. *arXiv:1703.03994 [cs]* (March 2017). http://arxiv.org/abs/1703.03994 arXiv: 1703.03994.
[5] I. Eyal. 2015. The Miner's Dilemma. 89–103. https://doi.org/10.1109/SP.2015.13
[6] Ittay Eyal and Emin Gun Sirer. 2013. Majority is not Enough: Bitcoin Mining is Vulnerable. *CoRR* abs/1311.0243 (2013). arXiv:1311.0243 http://arxiv.org/abs/1311.0243
[7] Gideon Greenspan. 2015. MultiChain Private Blockchain — White Paper. (2015), 17. https://www.multichain.com/download/MultiChain-White-Paper.pdf
[8] Fabíola Greve, Leobino Sampaio, Jauberth Abijaude, Antonio Coutinho, Ítalo Valcy, and Sílvio Queiroz. 2018. Blockchain e a Revolução do Consenso sob Demanda. (2018), 52.
[9] Aggelos Kiayias and Giorgos Panagiotakos. 2016. On Trees, Chains and Fast Transactions in the BlockChain. (2016), 25.
[10] Emilien Le Jamtel. 2018. Swimming in the Monero pools. In *2018 11th International Conference on IT Security Incident Management & IT Forensics (IMF)*. IEEE.
[11] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2017. A survey on the security of blockchain systems. *Future Generation Computer Systems* (Aug. 2017). https://doi.org/10.1016/j.future.2017.08.020
[12] Iuon-Chang Lin and Tzu-Chun Liao. 2017. Survey of Blockchain Security Issues and Challenges. (2017).
[13] M Macdonald, Lisa Liu-Thorrold, and R Julien. 2017. The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin. (02 2017). https://doi.org/10.13140/RG.2.2.23274.52164
[14] Charles Miers, Guilherme Koslovski, Mauricio Aronne Pillon, Marcos Simplicio Jr, Tereza Carvalho, Bruno Rodrigues, and Joao Battisti. 2019. Análise dos métodos para consenso distribuído aplicados à tecnologia Blockchain. In *SBSeg 2019 - Minicursos*. USP - São Paulo, Chapter 3, 1–49. https://sbseg2019.ime.usp.br/minicursos.pdf
[15] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. (2008). "https://bitcoin.org/bitcoin.pdf"
[16] Security Report. 2019. Funcionários são responsáveis por nove em cada dez violações de dados na nuvem. http://www.securityreport.com.br/overview/funcionarios-sao-responsaveis-por-nove-em-cada-dez-violacoes-de-dados-na-nuvem/
[17] Bruno Rodrigues, Thomas Bocek, and Burkhard Stiller. 2017. Enabling a Cooperative , Multi-domain DDoS Defense by a Blockchain Signaling System (BloSS).
[18] Bruno Rodrigues, Eder John Scheid, Roman Blum, Thomas Bocek, and Burkhard Stiler. 2019. Blockchain and Smart Contracts – From Theory to Practice. (2019).
[19] Artur Rot and Bartosz Blaicke. 2019. Blockchain's future role in cybersecurity. Analysis of defensive and offensive potential leveraging blockchain-based platforms. (2019).
[20] A. Singh, T. Ngan, P. Druschel, and D. S. Wallach. 2006. Eclipse Attacks on Overlay Networks: Threats and Defenses. In *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*. 1–12. https://doi.org/10.1109/INFOCOM.2006.231
[21] Melanie Swan. 2015. Blockchain: Blueprint for a new economy. (2015).
[22] The Blockchain Review. 2018. Ethereum White Paper Made Simple. (2018), 29. https://blockchainreview.io/wp-content/uploads/2018/03/02.01._final_Ethereum-White-Paper-Made-Simple.pdf
[23] The Linux Foundation. 2018. An Introduction to Hyperledger. (2018), 33. https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf
[24] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. 2017. Blockchain Challenges and Opportunities: A Survey. (2017), 25.
[25] G. Zyskind, O. Nathan, and A. '. Pentland. 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *2015 IEEE Security and Privacy Workshops*. 180–184. https://doi.org/10.1109/SPW.2015.27