IEEE Open Journal of the Computer Society

Recebido em 10 de janeiro de 2023; aceito em 23 de fevereiro de 2023. Data de publicação em 13 de março de 2023;
data da versão atual 22 de maio de 2023. A revisão deste artigo foi organizada pelo Editor Associado Deze Zeng.

Identificador de objeto digital 10.1109/OJCS.2023.3251854

Aplicativo descentralizado baseado em blockchain:

Um questionário

PEILIN ZHENG[1], ZIGUI JIANG[1](Membro, IEEE), JIAJING WU[2], E ZIBIN ZHENG[1](Fellow, IEEE)

[1]Escola de Engenharia de Software, Universidade Sun Yat-sen, Zhuhai, Guangdong 519000, China
[2]Escola de Ciência da Computação e Engenharia, Universidade Sun Yat-sen, Guangzhou, Guangdong 510006, China

AUTOR CORRESPONDENTE: Zigui Jiang (e-mail: jiangzg3@mail.sysu.edu.cn)

Este trabalho é financiado em parte pela National Natural Science Foundation of China sob Grants 62032025 e 62002393, em parte pela Guangdong Basic and Applied Basic Research Foundation sob Grant 2023A1515011336, e em parte pelo Technology Program of Guangzhou, China sob Grant 202103050004.

ABSTRATOAplicativos descentralizados baseados em blockchain (DApp) chamam mais atenção com o crescente desenvolvimento e ampla aplicação de tecnologias blockchain. Uma riqueza de fundos é investida no financiamento coletivo de vários tipos de DApp. Conforme relatado em agosto de 2022, existem mais de 5.000 DApps com mais de 1,67 milhão de carteiras ativas únicas diárias (usuários). No entanto, a definição, arquiteturas e classificações dos DApps ainda não foram esclarecidas até agora. Esta pesquisa tem como objetivo fornecer uma visão abrangente dos DApps para pesquisas futuras. Primeiramente, são apresentadas as definições e arquiteturas típicas de DApps. Em seguida, coletamos 3.118 DApps populares e os categorizamos em diferentes tipos e resumimos suas vantagens e desafios típicos. Finalmente,

TERMOS DO ÍNDICE Blockchain, aplicativo descentralizado.

I. INTRODUÇÃO

A ideia de blockchain foi proposta pela primeira vez como a tecnologia subjacente do Bitcoin[1]. Uma blockchain geralmente é mantida por pares em uma rede de transações P2P, onde os pares registram transações em um período de tempo e as agrupam em um bloco para ingressar na blockchain. A tecnologia Blockchain é descentralizada, inviolável e rastreável[2]. Em um blockchain, um contrato inteligente[3]é uma promessa orientada a eventos definida pela linguagem de programação. Um contrato inteligente na blockchain pode ser invocado enviando uma transação para os pares da blockchain, com a execução independente de cada par. Por fim, a execução do contrato é finalizada, com o resultado retornado ao blockchain. O protocolo chamado protocolo de consenso mantém todos os pares com o mesmo blockchain. Como tal execução é independente de todos os pares, o resultado é controlado por todos os participantes e, portanto, pode ser confiável para todos.

Aplicativos descentralizados foram propostos muito antes da tecnologia blockchain. Como os aplicativos descentralizados baseados em blockchain (DApp) podem aumentar a confiabilidade, diminuir o custo da autoridade confiável central e ter ampla aplicações (por exemplo, finanças, IoT, proveniência de dados, etc.), eles ganharam muita atenção da indústria e da academia nos últimos anos[4]. Em[5], os aplicativos descentralizados são classificados em duas classes: aplicativos descentralizados totalmente anônimos e aplicativos descentralizados baseados em reputação. No entanto, há uma área cinzenta substancial entre esses dois tipos. Portanto, a definição de aplicativos descentralizados baseados em blockchain ainda está indefinida.

Embora existam algumas pesquisas[4],[6],[7]sobre tecnologias blockchain, a definição, arquiteturas e categorias de DApps ainda não estão claras. Portanto, uma visão sistemática do DApp é urgentemente necessária para melhor compreensão e trabalho de pesquisa adicional em diferentes aspectos.

Este artigo considera o aplicativo descentralizado baseado em blockchain como sendo o aplicativo que usa blockchain como sua tecnologia subjacente para garantir características descentralizadas. Neste artigo, as arquiteturas de aplicativos descentralizados baseados em blockchain são resumidas em quatro tipos, que são Native Client como DApp, Smart Contract como DApp, Web & Contract como DApp e DApp totalmente descentralizado, com base em suas diferentes arquiteturas .

Em sentido estrito, os chamados DApps hoje em dia comumente se referem ao terceiro tipo, ou seja, o Web & Contract como um DApp. Como reportado[8], existem mais de 5.000 DApps pertencentes a esse tipo, dos quais o número de carteiras ativas únicas diárias foi de 1,67 milhão em agosto de 2022. Portanto, este artigo investiga ainda mais o Web & Contract como um DApp. Uma quantia crescente de dinheiro tem sido dedicada ao financiamento coletivo de tais tipos de DApps como investimentos[9]. Portanto, vários DApps precisam ser classificados para melhorar a compreensão dos DApps. Neste artigo, 3.118 DApps são coletados e categorizados em diferentes tipos, incluindo os populares DApps DeFi (Finanças Descentralizadas), NFT (Token Não Fungível) e GameFi (Jogo+DeFi) nos últimos anos. Essas categorias são propostas com vantagens sobre soluções centralizadas.

Além disso, este artigo também discute as pesquisas recentes sobre DApps nos aspectos de economia, segurança e desempenho. Quanto à economia, resumimos o problema econômico dos DApps em política de incentivo, avaliação de risco e efeito minerador. Quanto à segurança do DApp, dividimos a vulnerabilidade em três camadas: web, blockchain e contrato inteligente. Quanto ao desempenho, comparamos ferramentas com métricas. Nesses aspectos, apresentamos avanços recentes e oportunidades de pesquisa.

As principais contribuições deste artigo estão resumidas a seguir:

- Damos uma pesquisa abrangente sobre a definição e arquiteturas típicas de aplicativos descentralizados baseados em blockchain.
- Coletamos e categorizamos aplicativos descentralizados baseados em blockchain. Enquanto isso, resumimos suas vantagens típicas sobre soluções centralizadas.
- Conduzimos uma visão geral dos problemas de pesquisa em DApps sob os aspectos de economia, segurança e desempenho para fornecer oportunidades de pesquisa para pesquisadores interessados neste campo.

Esta pesquisa fornece uma visão abrangente da pesquisa sobre aplicativos descentralizados baseados em blockchain. O restante da pesquisa está organizado da seguinte forma. SeçãoII dá uma introdução aos conceitos básicos. SeçãoIIImostra a definição e as arquiteturas típicas de aplicativos descentralizados baseados em blockchain. Seção4categoriza os aplicativos descentralizados e os compara com os aplicativos centralizados tradicionais. SeçãoVpropor os problemas econômicos, de segurança, de desempenho e soluções correspondentes de DApps. SeçãoVIconclui o artigo.

II. CONCEITOS BÁSICOS

Esta seção apresenta os princípios e conceitos básicos de blockchain, protocolo de consenso e contratos inteligentes.

A. BLOCKCHAIN

Em um sentido restrito, blockchain é um tipo de estrutura de dados. O conceito de blockchain foi proposto pela primeira vez como o armazenamento subjacente para pagamentos ponto a ponto em Bitcoin [10]. Em um blockchain, cada bloco contém transações por um período de tempo. Em seguida, cada bloco é unido a uma estrutura de dados em cadeia chamada blockchain. Cada ponto na rede ponto a ponto mantém um blockchain por si só. E o par mantém o mesmo com o outro por meio de protocolos de consenso. Uma vez que cada bloco tem um valor de hash próprio e o valor de hash está contido no próximo bloco, o conteúdo (por exemplo, timestamps, transações) é resistente a adulterações e rastreável. Deve-se notar que o blockchain pode ser descrito como uma tecnologia abrangente que inclui a estrutura de dados subjacente, protocolos de consenso[10], e aplicações superiores[11]Num amplo sentido[6]. Mas neste artigo, o blockchain é considerado um tipo de estrutura de dados. E o aplicativo descentralizado baseado em blockchain é o aplicativo que usa essa estrutura de dados subjacente.

B. PROTOCOLO DE CONSENSO

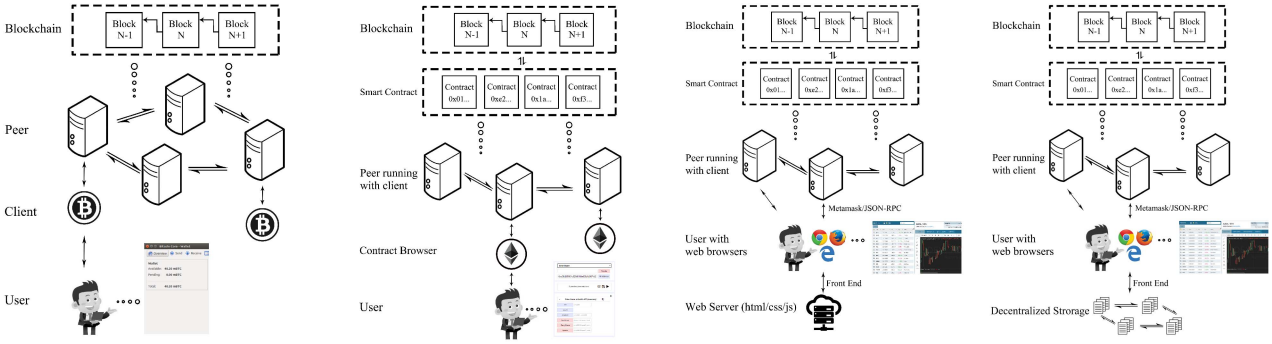
O protocolo de consenso[10]é um protocolo implementado em todos os nós de um sistema blockchain para mantê-los com o mesmo registro. Algoritmos de consenso foram desenvolvidos em sistemas distribuídos tradicionais por anos. Mas em sistemas blockchain, especialmente blockchain público, os pares têm mais motivação para a desonestidade, então há mais problemas, como o problema do gasto duplo. Assim, os sistemas blockchain precisam de diferentes protocolos de consenso para equilibrar as motivações técnicas e econômicas. Diferentes DApps (ou seus blockchains subjacentes) usam diferentes protocolos de consenso. Nesse caso, alguns dos problemas com DApps em economia, segurança e desempenho resultam dos protocolos de consenso, que serão mostrados na SeçãoV.

C. CONTRATO INTELIGENTE

O contrato inteligente é uma promessa definida pela forma digital[13] . Um contrato inteligente baseado em blockchain é uma promessa orientada a eventos definida pela linguagem de programação. Um contrato inteligente pode ser invocado enviando uma transação (incluindo o endereço do contrato, a função de chamada e os parâmetros) para os pares de validação. Depois disso, o contrato inteligente será executado de forma independente por cada par[12]. Finalmente, diferentes pares chegam a um consenso e salvam o resultado de volta no blockchain. Em alguns cenários, um contrato inteligente em blockchain pode ser considerado um aplicativo descentralizado. No entanto, ainda é controverso. As diferentes definições e arquiteturas de aplicativos descentralizados baseados em blockchain serão descritas na SeçãoIII.

D. CRESCIMENTO

Nos estágios iniciais do desenvolvimento do DApp, a maioria dos DApps são construídos no Ethereum[13]. No entanto, com o desenvolvimento de DApps, o desempenho do Ethereum não pode permitir o rápido crescimento de usuários. Portanto, existem cada vez mais plataformas (blockchains) desenvolvidas e utilizadas pelos usuários. Atualmente, as outras plataformas populares de contratos inteligentes são: BinanceSmartChain[14], EÓSIO[15], TRON[16], Fantástico[17], Polígono[18], Solana[19], Avalanche[20], e assim por diante. Não há evidências simples e intuitivas para comparar toda a ecologia DApp de cada plataforma. No entanto, nós iremos



(a) Native Client as a DApp (b) Smart Contract as a DApp (c) Web & Contract as a DApp (d) Fully-decentralized DApp

FIGURA 1.Arquiteturas de aplicações descentralizadas.

introduza a métrica de Total Value Locked (TVL) em Decentralized Finance (DeFi) para comparar os DApps financeiros nessas blockchains.

III. DEFINIÇÃO E ARQUITETURA

Um aplicativo descentralizado é um aplicativo que não é controlado por uma organização centralizada. A motivação para aplicativos descentralizados é que o aplicativo/estrutura centralizada tradicional é muito vulnerável a ataques e gera corrupção. O conceito de aplicativo descentralizado foi proposto muito antes do blockchain. Por exemplo, BitTorrent[21]é um aplicativo descentralizado, assim como muitos softwares ponto a ponto. Para representação rigorosa e conveniente, o "DApp" ou "aplicativo descentralizado" mencionado abaixo refere-se a aplicativos descentralizados baseados em blockchain.

Diferentes arquiteturas de DApps são propostas na subseção a seguir.

A. CLIENTE NATIVO COMO DAPP

Bitcoin pode ser considerado como um dos aplicativos descentralizados baseados em blockchain em pagamento. Cada usuário executa um cliente em um ponto e, em seguida, ingressa na rede ponto a ponto. Como o registro de pagamento é descentralizado, as pessoas podem usar seu próprio cliente (por exemplo, Bitcoin Wallet) para transferir Bitcoin para outras pessoas. Como o usuário só usa o cliente para interagir com a rede, o cliente é um DApp. Nesta pesquisa, essa arquitetura é denominada Native Client as a DApp.

Figo.1(a)mostra a arquitetura do Native Client como um DApp. É usado pela maioria das primeiras criptomoedas semelhantes ao Bitcoin, como o Litecoin[22], PPcoin[23], e assim por diante. A deficiência dessa arquitetura é que o blockchain é personalizado para o aplicativo (por exemplo, pagamento).

B. CONTRATO INTELIGENTE COMO DAPP

No "Cliente Nativo como um DApp", modificar o blockchain para novos aplicativos é difícil. E os desenvolvedores de cada novo DApp precisam desenvolver um novo blockchain e cliente, o que reduz a eficiência. Isso pode ser resolvido por contratos inteligentes.

Os desenvolvedores podem usar contratos inteligentes no blockchain (por exemplo, Ethereum) para registrar qualquer informação que desejarem. Assim, os desenvolvedores do DApp podem optar por escrever um contrato inteligente como um DApp para os usuários. Tomando o Ethereum como exemplo, se os desenvolvedores quiserem desenvolver um DApp para transferir tokens, eles podem escrever um contrato de token em 100 linhas de código no Ethereum. Em seguida, os usuários podem usar um navegador de contrato inteligente (por exemplo, Remix, Mist, etc.) para carregar um contrato na rede Ethereum e chamar as funções escritas pelos desenvolvedores. Em alguns casos, o cliente também é o navegador do contrato. Como mostrado na Fig.1(b), essa arquitetura é chamada de Smart Contract as a DApp.

No entanto, o gargalo dessa arquitetura é que ela exige que os usuários tenham algum conhecimento básico de programação. Enquanto isso, os navegadores de contrato de muitas plataformas não são tão fáceis para os usuários porque poucos deles possuem interfaces gráficas de usuário.

C. WEB E CONTRATO COMO DAPP

Para melhorar os gargalos do Contrato como um DApp e facilitar o uso do DApp pelos usuários, a maioria dos desenvolvedores de DApp cria um front-end da Web para os contratos inteligentes. Como mostrado na Fig.1(c), o front-end é fornecido como páginas da web, incluindo a interface gráfica do usuário escrita no código html/css/js. E os navegadores da web executam o JavaScript (ou instalam o Metamask[24]) para se conectar aos pares de blockchain. Existem também alguns clientes leves (por exemplo, imToken[25]) que definem navegadores da web e carteiras juntos para que seja mais fácil para os usuários usar DApps. Observe que o cliente Web nesta arquitetura é diferente do cliente nativo anterior. Os pares podem ser remotos ou locais. Por fim, os navegadores podem obter as informações importantes (por exemplo, saldo, token) do blockchain e apresentá-las ao front-end.

Este Web & Contract como um DApp é amplamente utilizado pela maioria dos DApps. A ideia principal é armazenar a GUI (Graphic User Interface) no site e as informações importantes (por exemplo, saldo) no blockchain. Isso parece ser mais familiar para os usuários. No entanto, causa outro problema centralizado: embora alguns DApps (por exemplo, Compound[26], Uniswap[27],

TABELA 1.Pesquisa sobre quatro arquiteturas usadas pelo DApp

Architecture	DApp
Native Client as a DApp	Bitcoin [10], Zcash [36], Monero [37]
Smart Contract as a DApp	DanKu [38], EurocupBet [39], The DAO [40]
Web & Contract as a DApp	MakderDAO [41], Uniswap [29], Curve [42], Compound [28], Aave [43], Kyber [44], CryptoPunk [45], OpenSea [46], Augur [47], CryptoKitties [48], ForkDelta [30], ENS [49], EosBet [50], AxieInfinity [51]
Fully-decentralized DApp	TornadoCash [34]

ForkDelta[28], etc.) são de código aberto tanto na web quanto no código de contrato, muitos desenvolvedores de DApp não abrem seu código-fonte de front-end.

D. DAPP TOTALMENTE DESCENTRALIZADO

Taylor Gerring propõe uma arquitetura[29], o que pode eliminar a noção de separar o conteúdo da apresentação, eliminando a necessidade de servidores. Consiste em três módulos: Ethereum para lógica descentralizada, Swarm [30]para armazenamento descentralizado, e Whisper[31]para mensagens descentralizadas. Nesta pesquisa, essa arquitetura é denominada DApp totalmente descentralizada. Se esse conceito puder ser totalmente implementado, os desenvolvedores e usuários usarão o DApp totalmente descentralizado. A principal diferença entre DApp totalmente descentralizado e Web & Contrato como DApp está no armazenamento do front-end. O armazenamento do DApp totalmente descentralizado não depende do serviço centralizado, mas dos sistemas de arquivos descentralizados, conforme mostrado na Fig.1(d). TornadoCash[32]é restrita por alguns países para regulamentação econômica, que será descrita na SeçãoV. Existem poucos serviços centralizados que fornecem armazenamento para ele. Portanto, o TornadoCash precisa mover seus arquivos front-end (html/css/js) para sistemas de arquivos descentralizados (por exemplo, IPFS[33])

Em resumo, quatro arquiteturas de DApp são listadas nesta pesquisa. e mesa1mostra os DApps que são conduzidos por essas arquiteturas.

4. TIPO DE APLICAÇÕES

Nesta seção, primeiro coletaremos e forneceremos uma visão geral de 3.118 DApps do StateOfTheDApps. Em seguida, categorizamos os aplicativos descentralizados baseados em blockchain e resumimos suas vantagens típicas sobre soluções centralizadas.

A. VISÃO GERAL

Existem muitas plataformas de DApps, como Ethereum, EOS e assim por diante. Diferente dos aplicativos tradicionais, não existe uma loja de aplicativos centralizada como a AppStore para distribuir aplicativos. Porém, ainda existem alguns sites orientadores que registram as informações dos DApps. Os mercados de DApp já cresceram. Existem vários sites do mercado DApp, como StateOfTheDApps[50], DAppReview[51], DApp.com [52], DAAppRadar[53], e assim por diante.

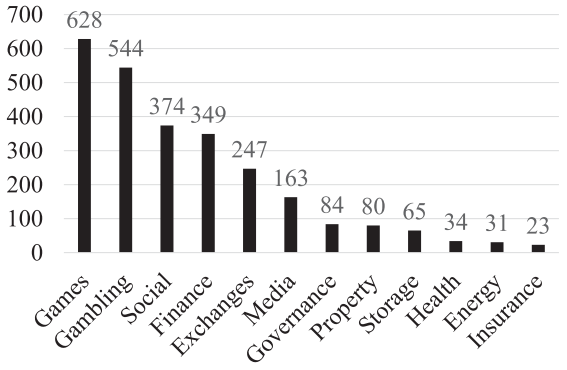


FIGURA 2.Estatísticas de DApp em diferentes categorias de State Of The DApps (outubro de 2022).

3.118 DApps do StateOfTheDApps são coletados e categorizados nesta pesquisa. As estatísticas do DApp em diferentes categorias são mostradas na Fig.2. A maioria dos DApps publicados no StateOfTheDApps são jogos. E a segunda são as trocas por criptomoeda. Os seguintes são finanças, comunidade, jogos de azar, mídia, propriedade, governança, armazenamento, energia, saúde e seguros. Deve-se notar que os DApps de troca têm DAU (Daily Active Users) mais altos, pois a troca de criptomoedas é realmente ativa e quente no mercado. Algumas categorias de DApps serão descritas em detalhes.

B. FINANÇAS (DeFi)

Os serviços financeiros tradicionais dependem de uma parte confiável para assumir algum risco e obter o benefício (por exemplo, investimento financeiro, seguro, etc.). Mas, de alguma forma, os DApps podem remover terceiros confiáveis. Portanto, os DApps têm amplas aplicações em finanças. Nesta subseção, serão apresentados três campos típicos de DApps em finanças. Um conceito geral desse tipo de DApps é o Financiamento Descentralizado (o chamado DeFi).

*Financiamento colaborativo:*Os mercados de capitais tradicionais tornam difícil para as pessoas levantar dinheiro ou fazer investimentos. O tempo de liquidação pode ser superior a um mês devido à revisão financeira. Mas hoje em dia, muitos desenvolvedores levantam o financiamento coletivo no contrato inteligente. Então eles podem obter um grande número de criptomoedas em um período muito curto de tempo. Chama-se Oferta Inicial de Moedas (ICO)[9]. Como os DApps da ICO registram todas as contribuições financeiras, eles podem recompensar as contribuições financeiras das pessoas para um projeto com ações reais do projeto. Tapscott et ai.[54]propor uma revisão da OIC. A escala de crowdfunding em DApps está crescendo rapidamente. No entanto, muitas fraudes aparecem nesse meio tempo.

*Troca de tokens:*No Ethereum e em outras plataformas, após o envio de criptomoedas para um contrato de Crowd-Funding, os usuários seriam recompensados com tokens, que são a prova de seu investimento. O protocolo ERC20 no Ethereum permite que os detentores de token enviem os tokens para outros. Portanto, muitos DApps para troca descentralizada (DEX) de tokens aparecem. IDEX[55] é uma bolsa descentralizada para negociar Ethereum

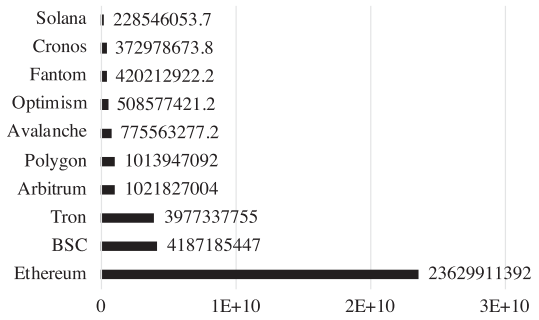


FIGURA 3.Valor total bloqueado (USD) em DeFi DApps em diferentes blockchains (Top10) de DefiLlama (janeiro de 2023).

tokens, combinando a velocidade da centralização com a segurança da liquidação em blockchain. E ForkDelta[28]também é uma troca semelhante à IDEX. Kyber Network[42]é um serviço de troca que permite a conversão instantânea de tokens com liquidez garantida. 0x[56]é proposto como um protocolo sem permissão para negociar tokens ERC20 no Ethereum. Com o desenvolvimento do DEX, um novo tipo de protocolo chamado Automated Market Maker (AMM) é introduzido aos DApps. Ele permite que ativos digitais sejam negociados sem permissão e automaticamente usando pools de liquidez em vez de um mercado tradicional de compradores e vendedores[57]. Os DApps típicos que usam AMM são Uniswap[27]e curva[40].

*Empréstimo de tokens:*O empréstimo, ou o chamado "empréstimo", é um dos casos mais utilizados no mercado financeiro tradicional. No blockchain, também existem essas necessidades de tomar emprestado/emprestar os tokens e pagar com juros. Portanto, existem alguns DApps que se concentram no suporte ao empréstimo de tokens. Composto[26]é um DApp para fornecer ou emprestar ativos. As contas no blockchain fornecem capital para receber ou emprestar ativos do protocolo. Seus contratos inteligentes rastreiam esses saldos e definem taxas de juros algoritmicamente para os mutuários. Aave[41]é semelhante ao Compound, mas fornece mais padrões de empréstimo. MakerDAO[39]foi projetado para emprestar tokens estáveis (vinculados a dólares americanos) para usuários e se tornou um dos DeFi DApps mais populares[58].

*Seguro:*Mainelli et ai.[59]explore o potencial da tecnologia blockchain para transformar o seguro pessoal. Os aplicativos descentralizados no setor de seguros podem melhorar a eficiência, economizar custos e reduzir as despesas gerais de processamento no tratamento de sinistros[60]. E os prêmios mais baixos são pagos pelos consumidores.

Conforme mencionado na SeçãoII, a métrica de Total Value Locked (TVL) pode ser usada para avaliar a popularidade dos DeFi DApps em diferentes blockchains. Coletamos os dados TVL do DefiLlama[58]em dólares americanos e mostre as estatísticas na Fig.3. Como mostrado nesta Fig.3, Ethereum é agora um dos blockchains mais populares para DeFi DApps. E ocupa mais de 50% do TVL em todos os 10 principais blockchains. As outras blockchains (BinanceSmartChain[14], TRON[16], Fantástico[17], Polígono[18], Solana[19], Avalanche[20], etc.) também atrai alguns usuários DeFi para bloquear suas criptomoedas em seus DeFi DApps.

Os DApps financeiros podem realmente melhorar a eficiência, reduzir custos de tempo e tornar a execução automática. E os desafios são listados a seguir:**(1) Evasão fiscal:**Transações financeiras tradicionais são fáceis de auditar. Mas os DApps financeiros são difíceis de auditar, pois os usuários podem ser anônimos. Um usuário pode ser dividido em várias contas para reduzir o imposto. Assim, o imposto poderia ser sonegado pelos usuários do DApps.**(2) Operação difícil:**Tomando como exemplo os seguros DApps, não é fácil relatar um acidente na blockchain. São necessárias muitas operações complexas e difíceis para confirmar o acidente.

C. JOGO (GameFi)

O jogo construído em blockchain é um dos campos mais quentes dos DApps. Como mostrado na Fig.2, o jogo também é o mais tipo de DApps. Além disso, nos últimos meses, GameFi tem sido um tema quente em DApps. Ele combina jogo e DeFi, e os usuários podem vender ou comprar os itens do jogo por meio de protocolos DeFi.

Axie Infinity[49]é o GameFi DApps mais popular atualmente. Os jogadores podem obter lucros jogando o jogo e vendendo os tokens nos mercados descentralizados. No entanto, também custa dinheiro para iniciar o jogo. Observe que a GUI do Axie não é totalmente baseada na Web. As GUIs parciais dele são baseadas em um único cliente em computadores pessoais.

CryptoKitties[46]é um jogo famoso construído na blockchain Ethereum. CryptoKitties são gatos colecionáveis digitais construídos na blockchain Ethereum. Eles podem ser comprados e vendidos usando Ether e criados para criar novos gatos com características emocionantes e níveis variados de fofura. A mecânica principal está ligada a ações associadas a criptomoedas e contratos inteligentes. Em resumo, os Cryptokitties são a prova de que você pode criar algo no Ethereum, e os usuários podem comprar, vender e negociar CryptoKitties. A razão para o uso do blockchain é que ele garante que cada gato seja verdadeiramente único e persistente.

A ideia principal dos jogos é usar o blockchain como uma estrutura de dados para armazenar a jogabilidade e os elementos executáveis do programa do jogo. Mas também causa alguns problemas:**(1) Rendimento:**A taxa de transferência de um blockchain público é limitada agora. E é relatado que os Crypto-Kitties interromperam a rede Ethereum para ficar muito lotada em alguns dias. Ref.[61]**(2) Código não aberto (controle centralizado):**Alguns códigos DApp são totalmente controlados e atualizados apenas pelos desenvolvedores.**(3) Dependência de Pedido de Transação:**Este é um tipo de vulnerabilidade que pode afetar os usuários para obter lucro no jogo.

D. ARMAZENAMENTO DE DADOS E PROVENIÊNCIA (NFT)

A blockchain pública fornece armazenamento permanente para os dados armazenados nela e também é útil para proveniência.

CriptoPunks[43]é um DApp que fornece 10.000 caracteres gerados exclusivamente armazenados no Ethereum. Neste DApp, os personagens podem ser comprados de alguém por meio de seu mercado, que também está embutido no blockchain. O protocolo subjacente a essa compra e venda é o Non-Fungible Token (NFT). Dessa forma, os rastros e proveniências dos tokens (no DApp) podem ser resistentes à temperatura no blockchain, pois todos os dados principais são armazenados no blockchain. o site de

CryptoPunks mostra que o preço mais baixo atual de um personagem é de mais de 300.000 dólares americanos.

Além disso, como os CryptoPunks (e NFTs) são populares entre os usuários do DApp, muitos DApps que o imitam foram produzidos. Mar aberto[44]fornece outro mercado independente para NFTs, itens digitais raros e colecionáveis criptográficos. Os usuários podem comprar, vender, leiloar e descobrir os NFTs de outros DApps, como os mencionados CryptoKitties, CryptoPunks e assim por diante.

Observe que nem todos os DApps nesta subseção são NFTs. NFT DApps é apenas um subconjunto. Existem também outros DApps que utilizam blockchain para armazenamento e proveniência de dados. EtherShare[62] é um DApp para os usuários compartilharem informações com armazenamento permanente e acesso aberto. EthereumNameService[47] toma um nome de domínio descentralizado como um NFT e, em seguida, o resolve para um endereço específico, a fim de facilitar o uso do endereço.

No entanto, alguns desafios são listados a seguir:**(1) Resíduos de armazenamento:**Os DApps geralmente armazenam os dados em cada par blockchain. É necessário, mas também causa desperdício de armazenamento, principalmente alguns tipos de Big Data.**(2) Autenticação de identidade:**Um usuário DApp é representado como "endereço" no blockchain. Assim, é difícil vincular o endereço à identidade do mundo real em uma situação descentralizada.**(3) Problema de pirataria:**Alguns DApps fornecem apenas a solução para armazenar os dados para que os dados sejam fáceis de serem copiados. O problema da pirataria é urgente para os DApps de armazenamento de dados.

E. PROTEÇÃO DE PRIVACIDADE

Os DApps podem ser considerados nativamente anônimos porque a tecnologia blockchain é nativamente anônima. Então, de alguma forma, o DApp pode proteger a privacidade dos usuários. Zyskind et ai.[63] propor um DApp como um sistema descentralizado de gerenciamento de dados pessoais, garantindo que os usuários assumam o controle total de seus dados privados. E Lin. e outros[64]também descrevem um gerenciador de controle de acesso baseado em blockchain no ecossistema de TI de saúde, chamado Health Care Blockchain. Zyskind et ai.[65]propõe Engima, uma plataforma de computação descentralizada para permitir que os usuários compartilhem seus dados com garantias criptográficas de privacidade.

No entanto, em alguns sistemas públicos de blockchain, todas as transações são visíveis e expostas em todo o mundo. Zerocash, proposto por Ben-Sasson et al.[66], é conduzido com fortes garantias de privacidade do Bitcoin, com os avanços em argumentos de conhecimento sucintos e não interativos de conhecimento zero. Em outra criptomoeda chamada Monero, um método de anel confidencial é proposto por Noether et al.[67] para ocultar os valores das transações, o que aumenta a privacidade do Monero. Outra melhoria de ofuscação do Monero é proposta por Mackenzie et al.[68]para fornecer resistência de longo prazo da criptomoeda contra análise de blockchain.

Quanto a este tipo de DApps, também existem algumas desvantagens e desafios:**(1) Violação da lei:**Por exemplo, o Monero permite que as pessoas transfiram dinheiro contra a censura do governo. Em alguns casos, é a chamada "liberdade" e "privacidade". No entanto, isso também ajudará os criminosos a receber dinheiro. É difícil fazer um equilíbrio entre lei e privacidade em DApps.**(2) Consumo de recursos computacionais:** Os algoritmos para gerar a transação protegida por privacidade sempre consomem muitos recursos de computação. Por exemplo, o Zerocash leva alguns minutos para o usuário gerar uma transação. Assim, um algoritmo mais rápido é necessário.

F. COMPARTILHAMENTO

Uma das principais vantagens do DApp é permitir o compartilhamento ponto a ponto sem um terceiro confiável. Os usuários podem usar DApps para compartilhar as coisas que desejam gratuitamente ou por uma taxa. Xu et al.[69] propõem o Prc, uma plataforma de economia de compartilhamento baseada em blockchain para manter os recursos desejáveis que o blockchain público oferece para compartilhar aplicativos de economia sem sacrificar a privacidade do usuário. Bogner e outros.[70]demonstrar um DApp para compartilhar objetos do cotidiano com base no contrato inteligente no Ethereum. Kang e outros.[71]projetar um sistema de comércio de eletricidade P2P localizado com blockchain de consórcio para ilustrar operações detalhadas de comércio de eletricidade P2P localizado. Luu et al.[72]implementar e implantar o SMARTPOOL, um DApp para o pool de mineração descentralizado, permitindo que os mineradores Ethereum contribuam com sua taxa de hash e compartilhem as recompensas.

No campo da computação em nuvem, os DApps podem ser usados para compartilhar os recursos de computação dos usuários. IExec[73]depende de contratos inteligentes da Ethereum e permite a construção de uma infraestrutura de nuvem virtual que fornece serviços de computação de alto desempenho sob demanda. Semelhante a IExec, Golem[74], e SOMM[75] também são os DApps para compartilhar recursos de computação. As diferenças são: Golem monta uma rede para atrair usuários regulares de renderização 3D primeiro, e SONM visa computação de névoa e borda. Em computação em nuvem e borda de veículos elétricos, Liu et al.[76]propõe moedas de dados e moedas de energia inspiradas em blockchain, nas quais a frequência de contribuição de dados e a quantidade de contribuição de energia são aplicadas para obter a prova de trabalho.

Existem alguns problemas com o compartilhamento de DApps.**(1) Supervisão insuficiente:**Compartilhamento descentralizado significa que qualquer pessoa pode compartilhar na rede P2P. No entanto, uma vez que a controvérsia sobre o compartilhamento aparece, falta a supervisão. É necessária uma forma de supervisão ou arbitragem de compartilhamento. **(2) Baixo rendimento:**Semelhante aos DApps IoT, os DApps de compartilhamento precisam de alto rendimento para garantir a experiência do usuário. Assim, esse tipo de DApps também sofre com o baixo throughput do blockchain.

G. MERCADO DE PREVISÃO E JOGOS DE AZO

Embora existam algumas diferenças entre jogo e mercado de previsão[89], esta pesquisa junta esses dois tipos, já que a ação dos usuários do DApp é quase a mesma: Aposte em uma previsão com algum dinheiro e receba as recompensas se for verdade. O jogo tradicional e o mercado de previsões custam aos usuários algumas taxas para terceiros confiáveis (por exemplo, cassinos), e é fácil ser injusto com os usuários. Hoje em dia, existem muitos DApps para mercados de apostas ou previsões. Por exemplo, Etheroll[85] é um DApp para fazer apostas em nosso provavelmente sem depósitos ou inscrições. Cada lançamento de dados é comprovadamente aleatório e criptograficamente seguro. Miller e outros. [86]apresentar um protocolo de loteria com garantia zero em Bitcoin e Ethereum. Cryptocup[87]é um DApp como um jogo de previsão da Copa do Mundo com tokens ERC 721.

MESA 2.Comparação de diferentes tipos de DApps

Types of DApps	Advantages	Challenges
Finance (DeFi) [9], [44], [57], [61], [62], [80]	(1)Improving efficiency (2)Reducing the time costs (3)Automatic execution	(1)Tax evasion (2)Difficult operations
Game (GameFi) [48], [81], [82]	(1)Permanent game assets (2)Improving asset mobility (3)Ensuring role uniqueness	(1)Vulnerabilities of randomness (2)Non open-source (2)Transaction-Ordering Dependence
Data Storage and Provence (NFT) [64], [65], [83], [84]	(1)Permanent storage (2)Preserving privacy (3)Improving reliability	(1)Waste of storage (2)Identity authentication (3)Piracy problem
Privacy Protection [66], [67], [69]–[71], [85], [86]	(1)Preserving privacy (2)Improving user ownership of data	(1)Violation of law (2)Computing resources consumption
Sharing [72], [73], [75]–[79]	(1)Improving efficiency (2)Removing trusted third party (3)Promoting resource sharing	(1)Insufficient supervision (2)Low throughput
Gambling and Prediction Market [47], [87]–[90]	(1)Removing trusted third party (2)Less fees (3)Automatic execution	(1)Centralized oracle (2)Not absolute truth (3)Higher delay

Os usuários irão prever as partidas da Copa do Mundo para ganhar recompensas em potencial. Quanto ao mercado de previsão, Peterson et al.[45] propõem um oráculo descentralizado e uma plataforma de previsão de mercado chamada Augur.

Um problema-chave do mercado de apostas e previsões é como inserir o resultado do mundo real (por exemplo, campeão da Copa do Mundo) nos contratos inteligentes. Adler e outros.[88]propõe o AS-TRAEA, um oráculo descentralizado baseado em um jogo de votação, para resolver o problema. oraclize[90]e Chaves da Realidade[91]também são as soluções oracle.

Existem também alguns desafios deste tipo de DApps:**(1) Oráculo centralizado:**Embora Oraclize e ASTRAEA tentem ajudar a inserir dados do mundo real no contrato inteligente, eles ainda não são descentralizados. Uma nova solução oracle é uma oportunidade.**(2) Não é verdade absoluta:**No mercado de previsão, o resultado da previsão pode ser afetado pelos usuários. Por exemplo. O campeão da Copa do Mundo é informado pelos usuários. Se a maioria dos usuários optar por mentir, o resultado pode ser falso.**(3) Maior atraso:** Os mercados tradicionais de apostas e previsões podem garantir atrasos muito baixos. Mas os DApps exigem um atraso maior na confirmação do bloco ou na votação do resultado.

Em resumo, os DApps apresentam grandes vantagens em muitos campos de aplicação. Mesa2mostra as vantagens e desafios resumidos de diferentes tipos de DApps.

V. PROBLEMAS DE DAPPS

Nesta seção, discutiremos os problemas dos DApps. Resumiremos os problemas dos DApps em três campos: economia, segurança e desempenho.

A. POLÍTICA ECONÔMICA E RISCO

Nesta pesquisa, os problemas econômicos dos DApps se dividem em três vertentes: Política de Incentivos, Avaliação de Riscos e Efeitos do Minerador, conforme mostrado na Tabela3.

TABELA 3.Problemas econômicos em DApps

Economic Problem	Related Studies
Incentive Policy	Design [29], [46]
	Measurement [94]
Risk Evaluation	Scam [95], [96]
	Measurement [94]
	Management [97]
Miner Effect	Definition [98]
	Quantifying [99], [100]
	Explorer [101]
Economic Regulation	Censorship [102]

Política de Incentivos:Nos DApps citados, incluindo os DeFi, GameFi e NFTs, há um problema: como atrair usuários para usar o DApp? A resposta resulta na economia da política de incentivos. Em outras palavras, na maioria dos DApps, a forma comum de motivar os usuários é fazê-los ganhar dinheiro, o que é um problema econômico. Por exemplo, Uniswap[27] recompensa os usuários com taxas e tokens de governança como incentivos. Mar aberto[44]retorna as taxas personalizadas aos criadores de NFTs como incentivos. Qin e outros.[92]propõem um estudo empírico sobre a medição do incentivo dos DApps de empréstimo, processando os dados da blockchain on-chain. A pesquisa sobre políticas de incentivo pode ser uma oportunidade.

Avaliação de risco:Quanto ao usuário, ao usar um DApp, o risco vem de várias áreas. Pesquisadores encontraram alguns DApps que podem ser golpes[93],[94]. Além disso, o risco também vem da volatilidade do mercado. Qin e outros.[92]medir vários riscos aos quais os participantes da liquidação estão expostos e quantificar as instabilidades dos DApps de empréstimo existentes. Com mais DApps sendo desenvolvidos, medindo e gerenciando o risco[95]para os usuários pode ser útil e desafiador.

*Efeitos mineiros:*Os mineradores Blockchain têm grandes efeitos nos DApps. O valor extraível do minerador (MEV) é uma medida do lucro que um minerador (ou validador, sequenciador, etc.) pode obter por meio de sua capacidade de incluir, excluir ou reordenar transações arbitrariamente nos blocos que produzem[96]. E muitos estudos são propostos para MEV. FlashBots[97]fornece um estudo sobre as transações front-running nos DEX DApps. Eles também fornecem uma ferramenta para os mineradores Ethereum na última versão, que foi aplicada a muitos mineradores para obter lucros extras. Qin e outros.[98]quantificar o MEV em outra perspectiva chamada valor extraível de blockchain. O site do explorador MEV[99] mostra que mais de 24 milhões de dólares americanos foram extraídos por mineradores em novembro de 2021. Portanto, investigar os efeitos mineiros de DApps pode ser uma oportunidade de pesquisa.

*Regulamento Econômico:*A descentralização dos DApps dificulta a regulação econômica. Por exemplo, Tornado-Cash[32]é um projeto desenvolvido para misturar criptomoedas de forma descentralizada. Este projeto aumenta a privacidade dos usuários, mas também ativos ilegais. Portanto, alguns países, incluindo os Estados Unidos, restringiram este projeto. Por exemplo, os americanos estão proibidos de se envolver em transações envolvendo TornadoCash, inclusive por meio de endereços de carteira de moeda virtual que o governo identificou[101]. Conforme mencionado anteriormente, embora o TornadoCash tenha sido migrado para os sistemas de arquivos descentralizados, suas transações são relatadas como rejeitadas[100]. Mais soluções para o equilíbrio entre privacidade e regulamentação podem ser oportunidades de pesquisa.

B. RISCO DE SEGURANÇA

Como a maioria dos DApps são conduzidos com criptomoedas, a segurança é muito importante. Uma vez que os DApps fossem atacados, bilhões de criptomoedas poderiam ser roubadas, não havendo como reaver o dinheiro devido às características do blockchain. Nesta seção serão apresentadas vulnerabilidades e ataques típicos, com as soluções de segurança.

*Vulnerabilidades e Ataques:*SeçãoIIImostra diferentes arquiteturas de DApps. Web & Contract como DApp é a arquitetura mais utilizada até agora. Essa arquitetura pode ser abstraída em três camadas: web, contrato inteligente e blockchain. Então essas três camadas podem ser atacadas por diferentes vulnerabilidades, conforme mostrado na Tabela4. Mesa4mostra as vulnerabilidades e ataques em casos do mundo real. A centralização em DApps resultou da centralização da Web GUI. Como mostrado na Tabela4, a camada da Web é uma das camadas vulneráveis mais importantes. Em dezembro de 2021, o front-end do BadgerDAO foi controlado por hackers[102]. Neste ataque, vários tokens no valor de cerca de 120 milhões de dólares americanos são roubados. Áugure[45]e outros DApps são relatados com bug de sincronização inconsistente[103]. MyEtherWallet é um famoso DApp amplamente utilizado como carteira para transferência de tokens. é relatado[104]para ser atacado, e mais de $ 152.000 são roubados pelos hackers por meio do sequestro de DNS. Em novembro de 2020, foi relatado que o Infura.io ficou fora do ar por horas[105]. Naquela época, vários navegadores DApp foram relatados para exceções de saldos dos usuários e operações DApp, o que pode causar operações erradas dos usuários[106]. Quanto às vulnerabilidades do DApp

TABELA 4.Vulnerabilidades e Ataques em DApps

Layer	Vulnerability	DApps
Web	Front-end Tampering	BadgerDAO [104]
	Inconsistent Synchronization	Augur [105]
	DNS Server Hijacking	Myetherwallet [106]
	Centralized Down	Infura [107], [108]
Blockchain	51% Vulnerability	Bitcoin Gold [109]
	Balance Attack	R3 [110]
	Double Spending	Bitcoin [111]
	Transaction-Ordering Dependence	Rock-ps [112]
	Timestamp Dependence	TheRun [113]
Contract	Mishandled Exception	KoET [114]
	Reentrancy Vulnerability	TheDAO [40]
	Immutable Bugs	Rubixi [115]
	Blockhash	EtherPot [116]

resultante de blockchain e contratos inteligentes, detalhes podem ser encontrados em pesquisas anteriores[115].

*Avanços recentes:*Como existem muitas vulnerabilidades e ataques em DApps, as ferramentas e soluções para DApps são necessárias com urgência. E a maioria das ferramentas é baseada na resolução de vulnerabilidades de blockchain e contratos inteligentes. A verificação formal funciona como uma das soluções. OYENTE[112]é construído como uma ferramenta de execução simbólica para encontrar possíveis bugs de segurança. A ferramenta pode verificar o bytecode dos contratos e então ajudar os desenvolvedores a evitar vulnerabilidades. Bhargavan1 et al. [116] propõem uma estrutura para segurança em tempo de execução e correção funcional de contratos inteligentes, traduzindo os contratos para uma linguagem de programação funcional chamada F*. KEVM[117]é proposto como uma semântica executável completa do ambiente de execução de contratos inteligentes. Outra estrutura semântica é apresentada em asemantic como uma semântica completa de pequenos passos de bytecode de contratos inteligentes. DappGuardGenericName [118]é desenvolvido como uma ferramenta para classificar ataques conhecidos de dados de transação, proteger os DApps de ataques e determinar atores maliciosos para aprender novos ataques. DArcher[103]é uma ferramenta para detectar bugs de sincronização onchain-off-Chain para DApps. Pettersson e outros.[119]implemente um compilador de prova de conceito para contratos inteligentes para reduzir o risco de erros e a necessidade de testes. CertiK[120]é uma estrutura de verificação formal para ajudar a provar matematicamente se um DApp é resistente a hackers. Outra maneira de manter a segurança é gerar contratos inteligentes automaticamente. FSolidM[121],[122]é uma estrutura enraizada em semântica rigorosa para projetar contratos como máquinas de estado finito, com uma ferramenta para criar os contratos em uma interface gráfica. Frantz e outros.[123]propor uma abordagem de modelagem para apoiar a tradução automática de representações de contrato legíveis por humanos para contratos inteligentes executáveis. Wohrer et ai.[124]também encontrar padrões de design para contratos inteligentes são encontrados em detalhes e fornecem o código para melhor ilustração. Modificar o mecanismo do blockchain também é a solução. Karame et al.[109]propor uma modificação na implementação Bitcoin existente para garantir a detecção de ataques de gasto duplo. Chen et ai.[125]propor um gás adaptativo

mecanismo de custo para se defender contra ataques DoS conhecidos e desconhecidos com configurações de parâmetros flexíveis no Ethereum. Marinho et ai.[126]definir os padrões para alterar e desfazer os contratos inteligentes para que os usuários possam evitar perder dinheiro nos contratos inseguros. E os desenvolvedores também podem tentar usar linguagens seguras de programação de contratos inteligentes, como Pact e Liquidity, nas quais menos vulnerabilidades são encontradas[127].

*Oportunidades de pesquisa:*As ferramentas e soluções de segurança são grandes oportunidades tanto na academia quanto na indústria. As oportunidades de pesquisa são resumidas a seguir:**(1) Web confiável para DApps**É necessário desenvolver uma camada confiável de DApps na web. Existem duas maneiras opcionais. Uma delas é desenvolver sistemas de arquivos descentralizados. A outra é desenvolver as ferramentas que defendem a página web centralizada de ataques, como o Darcher[103].**(2) Verificação formal:**Embora já exista alguma pesquisa sobre a verificação formal de contratos inteligentes, o código de contratos inteligentes está se desenvolvendo rapidamente. Assim, a verificação formal do código do contrato ainda é um bom tópico para pesquisa.**(3) Modelos Padrão:**Para novos desenvolvedores de DApp, é difícil escrever um código que garanta a ausência de bugs ou vulnerabilidades. Uma solução possível é fornecer modelos DApp padrão para os desenvolvedores. Isso pode ser semelhante à pesquisa do FSolidM[121],[122]. Mas este campo ainda está em branco.**(4) Mais vulnerabilidades e ferramentas:** DApps ainda estão em um momento muito inicial. Mais plataformas e tipos de DApps estão em processo de trabalho. Assim, mais e mais vulnerabilidades e ferramentas correspondentes devem ser encontradas para evitar perdas econômicas.**(5) Detecção de Similaridade:**Para o novo desenvolvedor DApp, não é fácil usar ferramentas formais de verificação e outras ferramentas de detecção de vulnerabilidade. No entanto, pode ser uma boa ideia realizar uma detecção de similaridade dos DApps. Dessa forma, os desenvolvedores podem descobrir se existem algumas vulnerabilidades semelhantes em seus DApps.

C. BAIXO DESEMPENHO

Esta subseção discute os desafios dos DApps em desempenho e também apresenta os avanços recentes com uma comparação.

*Desafios:*Os DApps ainda não foram usados tão amplamente quanto os aplicativos para PC e móveis porque os DApps não atendem ao uso diário tão facilmente quanto os aplicativos móveis. Um dos problemas mais urgentes é o desempenho. Existem tantos DApps que sofrem com o baixo rendimento dos sistemas blockchain. É relatado que o Ethereum foi interrompido por DApps. Conseqüentemente, muitos DApps podem não funcionar bem, pois as transações não podem ser totalmente confirmadas. E existem milhares de pares em um sistema blockchain, então é necessário saber o que está acontecendo no sistema. Dessa forma, as pessoas que executam os pares podem fazer algumas análises ou corrigir erros se o sistema blockchain se tornar anormal. Mas os pares pertencem a partidos diferentes. Assim, surgem os desafios de como monitorar todo o status, incluindo as transações do blockchain e o desempenho geral. Por exemplo, EO[15]é declarado para atingir um rendimento extremamente alto de centenas de milhares. Mas a Bitmex Research mostra que a taxa de transferência do mundo real no EOS não é muito melhor do que a do Ethereum[139]. Em sistemas distribuídos tradicionais, existem alguns estudos de caixa preta, como Project5[140], WAP5[141], e o sistema Sherlock [142]. Portanto, os benchmarks universais ou padrão de diferentes sistemas blockchain são necessários. Por fim, alguns estudos demonstraram que a disponibilidade de DApps não consegue atender a exigência de aplicações diárias. Então como otimizar o desempenho dos DApps se torna um desafio.

*Avanços recentes:*Os avanços recentes dos DApps baseados em blockchain são resumidos na camada de blockchain e armazenamento descentralizado.**(1)**Quanto à camada blockchain, Zheng et al.[128] propõem uma estrutura escalável para monitoramento detalhado e em tempo real de sistemas blockchain, que tem sobrecarga muito menor e mais detalhes sobre os sistemas blockchain em comparação com abordagens anteriores. Uma das principais ideias é dividir as métricas em métricas gerais para usuários e métricas detalhadas para desenvolvedores. Weber et ai.[129]um método para identificar as limitações de disponibilidade de Bitcoin e Ethereum, mostrando que a disponibilidade de leitura é alta enquanto a disponibilidade de gravação é baixa. Kalodner et ai.[130]propõem uma plataforma de software de código aberto para sistemas blockchain, que analisa os dados dos nós p2p e os dados brutos do blockchain para que os usuários monitorem e analisem o sistema. Dinh et al.[131]descrever estruturas para analisar blockchains privados em cargas de trabalho variadas. Gupta et al.[132]também propõem um método para analisar o desempenho. Gervais et ai.[133] apresentam uma nova estrutura quantitativa para a segurança e desempenho de blockchains PoW. Em alguns casos, os DApps apresentam baixo desempenho graças ao suporte limitado de consultas dos sistemas blockchain. Assim, Li et al.[134] propor EtherQL como uma camada de consulta para Ethereum. Ele também fornece dois níveis de interfaces para recuperação de dados ou para servir como um provedor de dados RESTful. **(2)**Quanto à camada de armazenamento descentralizado, Abdullah et al. [135]registrar e analisar as métricas de desempenho do IPFS[143]e FTP. Ismael et ai.[136] avaliar os custos e a latência dos sistemas de arquivos descentralizados existentes. Shen e outros.[137]use os servidores Amazon EC2 para avaliar o desempenho das operações de E/S de dados da perspectiva dos clientes IPFS. Trautwein e outros.[138]avaliar o desempenho do IPFS e descobrir as características dos pares IPFS.

*Oportunidades de pesquisa:*Mesa5mostra a comparação das métricas utilizadas no desempenho dos DApps. Assim, a taxa de transferência e a latência são as duas métricas nas quais muitos pesquisadores se concentram. O principal motivo é que há uma grande lacuna entre a taxa de transferência e a latência dos DApps agora e o requisito em aplicativos do mundo real. E algumas outras métricas, como consumo de hardware e tolerância a falhas, também devem ser avaliadas em diferentes plataformas blockchain de DApps. Existem muitos pares executando os clientes blockchain hoje em dia. Assim, essas métricas também são as principais métricas para a avaliação de plataformas DApp. As demais métricas da tabela, como execução de contrato e custo de consenso, parecem receber menos atenção. No entanto, essas métricas também refletem os gargalos dos sistemas blockchain. Se a taxa de transferência for alta o suficiente e o consumo de hardware for baixo o suficiente, essas métricas se tornarão a chave para a próxima otimização dos DApps. Algumas oportunidades de pesquisa estão listadas a seguir:**(1) Execução da Execução do Contrato:**O contrato inteligente é um dos mais

TABELA 5.Comparação de métricas usadas na pesquisa de desempenho do DApp

Layer	Studies	Throughput	Latency	Hardware Consumption	Contract Execution	Fault Tolerance	Read Availability	Consensus Cost
Blockchain	Zheng et.al [130]	√	√	√	√		√	√
	Weber et al. [131]		√					
	Kalodner et al. [132]	√						
	Dinh et al. [133]	√	√	√		√		
	Gupta et al. [134]	√	√	√		√		√
	Gervais et al. [135]	√						
	Li et al. [136]						√	
Decentralized Storage	Abdullah et.al [137]		√	√			√	
	Ismail et.al [138]		√					
	Shen et.al [139]	√	√					
	Trautwein et.al [140]		√					

partes importantes do DApp. Já existem muitas pesquisas sobre o desempenho do sistema blockchain subjacente. No entanto, a pesquisa sobre o desempenho de contratos inteligentes está em branco.**(2) Referência padrão:**Embora existam alguns artigos que se concentram no benchmark dos sistemas blockchain. No entanto, quanto ao DApp, não há benchmark. É necessário um conjunto padrão de fluxos de trabalho ou operações para o benchmark do DApp.**(3) Testes automatizados:**Existem muitas ferramentas de teste automatizadas para aplicativos de computador tradicionais ou aplicativos móveis. Isso ajudará os desenvolvedores a conhecer a confiabilidade do aplicativo. As ferramentas de teste para DApp estão faltando. Portanto, é também uma oportunidade.

VI. CONCLUSÃO

Esta pesquisa fornece uma visão abrangente da pesquisa sobre aplicativos descentralizados baseados em blockchain. A definição e arquiteturas típicas de DApps são resumidas com seus pontos fortes e fracos. Além disso, coletamos e categorizamos os DApps em diferentes tipos com os detalhes, dos quais são apresentadas as vantagens sobre as soluções centralizadas. Quanto aos aspectos de pesquisa recentes de economia, segurança e desempenho em DApp, este artigo também fornece uma visão geral e as oportunidades de pesquisa nesses aspectos.

REFERÊNCIAS

[1] S. Nakamoto,*Bitcoin: um sistema de dinheiro eletrônico ponto a ponto*, 2008, acessado em: 15 de abril de 2023. [Online]. Disponível: https://bitcoin.org/bitcoin.pdf

[2] Z. Zheng, S. Xie, H. Dai, X. Chen e H. Wang, "Uma visão geral da tecnologia blockchain: arquitetura, consenso e tendências futuras", em *Proc. IEEE Int. Congr. Big Data*, 2017, pp. 557–564.

[3] N. Szabo, "A ideia de contratos inteligentes", 1997, acessado em: 15 de abril de 2023. [Online]. Disponível: https://nakamotoinstitute.org/the-idea-ofsmart-contracts/

[4] Z. Zheng et al., "Uma visão geral da tecnologia blockchain: arquitetura, consenso e tendências futuras", em*Proc. IEEE Int. Congr. Big Data*, 2017, pp. 557–564.

[5] V. Buterin e D. DAOs, "DAs e mais: um guia de terminologia incompleto,"*BLOG ETHEREUM*, 2014. [On-line]. Disponível: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-morean-incomplete-terminology-guide/

[6] Z. Zheng et al., "Desafios e oportunidades de blockchain: uma pesquisa," *Int. J. Web Grid Serv.*, vol. 14, pp. 352–375, 2016.

[7] X. Li et al., "Uma pesquisa sobre a segurança dos sistemas blockchain,"*Futuro Gerador. Comput. Sist.*, vol. 107, pp. 841–853 2017.

[8] DAppRadar, DApp Industry Report, agosto de 2022. [Online]. Disponível: https://dappradar.com/blog/dappradar-blockchain-industry-reportaugust-2022

[9] Wikipedia, "Initial Coin Offers," Acessado em: 15 de abril de 2023. [Online]. Disponível: https://en.wikipedia.org/wiki/Initial_coin_offering

[10] D. Mingxiao et al., "Uma revisão sobre o algoritmo de consenso da blockchain," em*Proc. IEEE Int. conf. Syst., Homem, Cybern.*, 2017, pp. 2567–2572.

[11] G. Foroglou e AL Tsilidou, "Further applications of the blockchain", 2015, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.researchgate.net/publication/276304492_ Further_applications_of_the_blockchain

[12] C. Sillaber e B. Waltl, "Ciclo de vida de contratos inteligentes em ecossistemas blockchain,"*Datenschutz und Datensicherheit-DuD*, vol. 41, nº. 8, pp. 497–500, 2017.

[13] V. Buterin, "Ethereum white paper," 2013. [Online]. Disponível: https://ethereum.org/whitepaper/

[14] Binance Smart Chain, "Binance Smart Chain". Acesso: 15 de abril de 2023. [Online]. Disponível: https://github.com/binance-chain/bsc

[15] EOSIO, "Technical White Paper v2," Acessado em: 15 de abril de 2023. [Online]. Disponível: https://github.com/EOSIO/Documentation/blob/master/Technical

[16] TRON, site TRON, acessado em: 15 de abril de 2023. [Online]. Disponível: https://tron.network/

[17] Fantom, Fantom Website, acessado em: 15 de abril de 2023. [Online]. Disponível: https://fantom.foundation/

[18] Polygon, Polygon Website, acessado em: 15 de abril de 2023. [Online]. Disponível: https://polygon.technology/

[19] Solana, Solana Website, acessado em: 15 de abril de 2023. [Online]. Disponível: https://Solana.com/

[20] AVAX, Avalanche Website, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.avax.network/

[21] B. Cohen, "A especificação do protocolo BitTorrent", 2008, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.bittorrent.org/beps/bep_0003.html

[22] C. Lee, "Litecoin White Paper", 2011, acessado em: 15 de abril de 2023. [Online]. Disponível: https://whitepaper.io/coin/litecoin

[23] S. King e S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with 851 proof-of-stake," 2012, Acessado em: 15 de abril de 2023. [Online]. Disponível: https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf

[24] MetaMask, "MetaMask browser extension," Acesso em: 15 de abril de 2023. [Online]. Disponível: https://github.com/MetaMask/metamaskextension

[25] ImToken, "ImToken Medium", acessado em: 15 de abril de 2023. [Online]. Disponível: https://medium.com/imtoken/imtoken-1-2-0-fullysupports-the-offline-signing-of-transactions-d385899d3350

[26] R. Leshner e G. Hayes, "Compound: The money market protocol," White Paper, 2019, acessado em: 15 de abril de 2023. [Online]. Disponível: https://compound.finance/documents/Compound.Whitepaper.pdf

[27] G. Angeris, H.-T. Kao, R. Chiang, C. Noyes e T. Chitra, "Uma análise dos mercados uniswap", 2019, acessado em: 15 de abril de 2023. [Online]. Disponível: https://arxiv.org/abs/1911.03380

[28] ForkDelta, "ForkDelta," Acessado em: 15 de abril de 2023. [Online]. Disponível: https://forkdelta.github.io/about/
[29] T. Gerring, "Building the descentralized web3," 2014, Acesso: 15 de abril de 2023. [Online]. Disponível: https://blog.ethereum.org/2014/08/18/building-decentralized-web
[30] Swarm Team, ETH Swarm, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.ethswarm.org/
[31] Equipe Whisper, Whisper, acessado em: 15 de abril de 2023. [Online]. Disponível: https://github.com/ethereum/whisper
[32] A. Pertsev, R. Semenov e R. Storm, "Tornado cash privacy solution versão 1.4", 2019, acessado em: 15 de abril de 2023. [Online]. Disponível: https://berkeley-defi.github.io/assets/material/Tornado% 20Cash%20Whitepaper.pdf
[33] J. Benet, "IPFS-conteúdo endereçado, versionado, P2P," *Sistema de arquivo*, 2014, acessado em: 15 de abril de 2023. [Online]. Disponível: https://arxiv.org/abs/1407.3561
[34] A. Greenberg, "Zcash, uma alternativa de bitcoin não rastreável, lançada em alfa", 2016, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.wired.com/2016/01/zcash-an-untraceable-bitcoinalternative-launches-in-alpha/
[35] NT Courtois, "Stealth address, ring signatures, monero", 2016, acessado em: 15 de abril de 2023. [Online]. Disponível: http: // www.nicolascourtois.com/bitcoin/paycoin_privacy_monero_6.pdf
[36] AB Kurtulmus e K. Daniel, "Contratos de aprendizado de máquina sem confiança; Avaliando e trocando modelos de aprendizado de máquina no blockchain ethereum", 2018, acessado em: 15 de abril de 2023. [Online]. Disponível: https://arxiv.org/abs/1802.10185
[37] "EurocupBet", Acessado em: 15 de abril de 2023. [Online]. Disponível: https://forum.ethereum.org/discussion/7425/dapp-lets-bet-on-theeuro-cup-2016-winner
[38] Wikipedia, "The Dao," Acessado em: 15 de abril de 2023. [Online]. Disponível: https://en.wikipedia.org/wiki/The_DAO_(organização)
[39] G. Bogoni, "Sistemas de estabilização de criptomoedas: um foco no caso MakerDAO", 2019, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.politesi.polimi.it/handle/10589/152447
[40] CurveFinance, site da Curve, acessado em: 15 de abril de 2023. [Online]. Disponível: https://curve.fi/
[41] AAVE, site da AAVE, acessado em: 15 de abril de 2023. [Online]. Disponível: https://aave.com
[42] A YVL Luu, "Kybernetwork: serviço de troca e pagamento descentralizado sem confiança", 2017.
[43] CryptoPunks, site CryptoPunks, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.larvalabs.com/cryptopunks
[44] OpenSea, OpenSea Website, acessado em: 15 de abril de 2023. [Online]. Disponível: https://opensea.io/
[45] J. Peterson et al., "Augur: um oráculo descentralizado e plataforma de mercado de previsão", 2018, acessado em: 15 de abril de 2023. [Online]. Disponível: https://arxiv.org/abs/1501.01042
[46] CryptoKitties, "Gatos colecionáveis e procriáveis fortalecidos pela tecnologia blockchain," White Paper, 2017. [Online]. Disponível: http: // cryptokitties.co/
[47] N. Johnson, "ENS Documentation Release 0.1," 2019.
[48] "EosBet," Whitepaper. [On-line]. Disponível: https://github.com/EOSBetCasino
[49] AxieInfinity, site da AxieInfinity, acessado em: 15 de abril de 2023. [Online]. Disponível: https://axieinfinity.com/
[50] StateOfTheDApps, site StateOfTheDApps, acessado em: 15 de abril de 2023. [Online]. Disponível: https://stateofthedapps.com
[51] DAppReview, site DAppReview, acessado em: 15 de abril de 2023. [Online]. Disponível: https://dapp.review
[52] DApp.com, site DApp.com, acessado em: 15 de abril de 2023. [Online]. Disponível: https://stateofthedapps.com
[53] DAppRadar, site DAppRadar, acessado em: 15 de abril de 2023. [Online]. Disponível: https://dappradar.com
[54] A. Tapscott e D. Tapscott, "Como a blockchain está mudando as finanças," *Ônibus Harvard. Rev.*, vol. 1, pp. 2–5, 2017.
[55] AuroraLab, "Uma troca inteligente de con912 ethereum em tempo real e de alto rendimento," Acessado em: 15 de abril de 2023. [Online]. Disponível: https:// idex.market/static/IDEX-Whitepaper-V0.7.5.pdf
[56] W. Warren e A. Bandeali, "0x: Um protocolo aberto para troca descentralizada na blockchain Ethereum," pp. 4–18, 2017. [Online]. Disponível: https://github.com/0xProject/whitepaper
[57] Cryptopedia, "O que são criadores de mercado automatizados?", Acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.gemini.com/cryptopedia/amm-what-are-automated-marketmakers#section-liquidity-pools-and-liquidity-providers
[58] Defillama, "MakerDAO on Defillama", acessado em: 15 de abril de 2023. [Online]. Disponível: https://defillama.com/protocol/makerdao
[59] M. Mainelli e B. Manson, "Como a tecnologia blockchain pode transformar o seguro por atacado," Acesso: 15 de abril de 2023. [Online]. Disponível: https://www.pwc.lu/en/fintech/docs/pwc-how-blockchaintechnology-might-transform-insurance.pdf
[60] B. Cant et al., "Smart Contracts in Financial Services: Getting from Hype to Reality," *Consultoria Capgemini*, 2016, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.capgemini.com/consulting-de/ wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0. pdf
[61] Open Trading Networ, "How crypto-kitties disrupted the ethereum network," Acessado em: 15 de abril de 2023. [Online]. Disponível: https:// hackernoon.com/how-crypto-kitties-disrupted-the-ethereumnetwork-845c22aa1e6e
[62] EtherShare, "Compartilhar informações com armazenamento permanente e acesso aberto, Acessado em: 15 de abril de 2023. [Online]. Disponível: http://etherShare. organização
[63] G. Zyskind e O. Nathan, "Usando blockchain para proteger dados pessoais," em *Proc. IEEE Segur. Oficinas de privacidade*, 2015, pp. 180–184.
[64] LA Linn e MB Koo, "Blockchain for health data and its potencial use in health it and health care related research", em *Proc. ONC/NIST usa Blockchain Healthcare Res. Oficina*, 2016, pp. 1–10.
[65] G. Zyskind, O. Nathan e Pentland A. Enigma, "Plataforma de computação descentralizada com privacidade garantida", 2015, acessado em: 15 de abril de 2023. [Online]. Disponível: https://arxiv.org/abs/1506.03471
[66] EB Sasson et al., "Zerocash: pagamentos anônimos descentralizados de bitcoin," em *Proc. IEEE Simp. Seguro. Privacidade*, 2014, pp. 459–474.
[67] S. Noether e A. Mackenzie, "Anel de transações confidenciais," *Razão* vol. 1, pp. 1–18, 2016.
[68] A. Mackenzie, S. Noether e MC Team, "Improving ofuscation in the cryptonote protocol," Monero Research Lab Rep. MRL-0004, 2015.
[69] L. Xu et al., "Habilitando a economia compartilhada: privacidade respeitando contrato baseado em blockchain público," em *Proc. ACM Workshop Blockchain, Contratos de Criptomoedas*, 2017, pp. 15–21.
[70] A. Bogner, M. Chanson e AA Meeuw, "aplicativo de compartilhamento descentralizado executando um contrato inteligente na blockchain ethereum," em *Proc. 6ª Int. conf. Coisas da Internet*, 2016, pp. 177–178.
[71] J. Kang et al., "Permitindo o comércio de eletricidade ponto a ponto localizado entre veículos elétricos híbridos plug-in usando blockchains de consórcio," *IEEE Trans. Ind. Informar.*, vol. 13, não. 6, pp. 3154–3164, dezembro de 2017.
[72] L. Luu, Y. Velner e J. Teutsch, "SMARTPOOL: Mineração prática descentralizada em pool", em *Proc. USENIX Segur. Simp.*, 2017, pp. 1909–1426.
[73] "IEXEC", white paper IEXEC, acessado em: 15 de abril de 2023. [Online]. Disponível: https://iex.ec/whitepaper/iExec-WPv3.0-English.pdf
[74] Golem, "The golem project crowdfunding whitepaper," 2016, Acesso: 15 de abril de 2023. [Online]. Disponível: https://whitepaper.io/coin/ golem
[75] SONM, "About SONM," 2022. Acesso: 15 de abril de 2023. [Online]. Disponível: https://docs.sonm.com/home
[76] H. Liu, Y. Zhang e T. Yang, "Segurança habilitada para blockchain em veículos elétricos em nuvem e computação de ponta," *Rede IEEE*, vol. 32, nº. 3, pp. 78–83, maio/junho de 2018.
[77] P. De Filippi, "Crowdfunding baseado em Blockchain: Qual o impacto na produção artística e no consumo de arte?", Observatorio Itaú Cultural, no. 19 de 2015.
[78] PetChain, site da Petchain, acessado em: 15 de abril de 2023. [Online]. Disponível: https://pet-chain.duxiaoman.com/
[79] "HyperDragons", HyperDragons-WhitePaper, acessado em: 15 de abril de 2023. [Online]. Disponível: https://storage.googleapis.com/hyperdragons-imgs/file/HyperDragons-WhitePaper(ch).pdf
[80] A. Ramachandran e D. Kantarcioglu, "Using blockchain and smart contracts for secure data provenance management", 2017, acessado em: 15 de abril de 2023. [Online]. Disponível: https://arxiv.org/abs/1709.10000
[81] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat e L. Njilla, "ProvChain: Uma arquitetura de proveniência de dados baseada em blockchain em ambiente de nuvem com privacidade e disponibilidade aprimoradas", em *Proc. 17º IEEE/ACM Int. Simp. Computação em Cluster, Nuvem e Grade.*, 2017, pp. 468–477.

[82] Etherscan, “SaveData,” [Online]. Disponível: https://etherscan.io/address/0xf34cd2fd11233df8f90646ab658b03bfea98aa92#code

[83] D. Ron e A. Shamir, “Análise quantitativa do gráfico completo da transação bitcoin,” em *Proc. Segurança de Dados de Criptografia Financeira: 17th Int. conf.*, 2013, pp. 6–24.

[84] A. Kosba, A. Miller, E. Shi, Z. Wen e C. Papamanthou, “Hawk: O modelo blockchain de criptografia e contratos inteligentes de preservação da privacidade”, em *Proc. IEEE Simp. Seguro. Privacidade*, 2016, pp. 839–858.

[85] EthRoll, site da EthRoll, acessado em: 15 de abril de 2023. [Online]. Disponível: https://etheroll.com/

[86] A. Miller e I. Bentov, “Loterias com garantia zero em bitcoin e ethereum”, em *Proc. IEEE Eur. Simp. Seguro. Oficinas de privacidade*, 2017, pp. 4–13.

[87] Cryptocup Whitepaper, “A primeira aposta na copa do mundo alimentada por blockchan,” Acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.cryptocup.io/assets/pdf/Cryptocup/whitepaper.pdf

[88] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira e A. Kastania, "Astraea: A decentralized blockchain oracle", em *Proc. IEEE Int. conf. Internet Things, IEEE Green Comput. Comun., IEEE Cyber, Phys. Social Comput., IEEE Smart Data*, 2018, pp. 1145–1152.

[89] J. Wolfers e E. Zitzewitz, “Mercados de previsão,” *J. Econ. Perspectivas*, vol. 18, não. 2, pp. 107–126, 2004.

[90] Oraclize, site da Oraclize, acessado em: 15 de abril de 2023. [Online]. Disponível: http://www.oraclize.it

[91] R. Keys, “Fatos sobre a futura prova criptográfica quando eles se tornarem realidade,” Acesso: 15 de abril de 2023. [Online]. Disponível: https://www.realitykeys.com/

[92] K. Qin, L. Zhou, P. Gamito, P. Jovanovic e A. Gervais, "Um estudo empírico de liquidações DEFI: Incentivos, riscos e instabilidades", em *Proc. 21º ACM Internet Meas. conf.*, 2021, pp. 336–350.

[93] W. Chen et al., “Detectando esquemas Ponzi no Ethereum: Rumo a uma tecnologia blockchain mais saudável”, em *Proc. 2018 World Wide Web Conf.*, 2018, pp. 1409–1418.

[94] M. Bartoletti et al., “Dissecting Ponzi schemas on Ethereum: Identification, analysis, and impact,” *Futuro Gerador. Comput. Sist.*, vol. 102, pp. 259–277, 2017.

[95] JR Jensen e O. Ross, “Managing risk in DEFI”, 2020, acessado em: 15 de abril de 2023. [Online]. Disponível: https://ceur-ws.org/Vol-2749/short3.pdf

[96] CoinMarketCap, “Valor extraível do minerador (MEV),” Acessado em: 15 de abril de 2023. [Online]. Disponível: https://coinmarketcap.com/alexandria/glossary/miner-extractable-value-mev

[97] P. Daian et al., "Flash boys 2.0: Frontrunning in descentralized exchanges, miner extractable value, and consensoinstability", em *Proc. IEEE Simp. Seguro. Privacidade*, 2020, pp. 910–927.

[98] K. Qin, L. Zhou e A. Gervais, “Quantificando o valor extraível da blockchain: Quão escura é a floresta?”, em *Proc. IEEE Simp. Seguro. Privacidade*, 2022, pp. 198–214.

[99] FlashBots, “MEV explorer,” Acesso: 15 de abril de 2023. [Online]. Disponível: https://explore.flashbots.net/

[100] Labrys, “MEV watch,” Acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.mevwatch.info/

[101] Departamento do Tesouro dos EUA, “Perguntas frequentes sobre o dinheiro do tornado”, acessado em: 15 de abril de 2023. [Online]. Disponível: https://home.treasury.gov/policy-issues/financial-sanctions/faqs/added/2022-09-13

[102] R. Lawler, “Alguém roubou 120 milhões em criptografia hackeando um site DeFi”, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.theverge.com/2021/12/2/22814849/badgerdao-defi-120- Million-hack-bitcoin-ethereum

[103] W. Zhang, L. Wei, S. Li, Y. Liu e S.-C. Cheung, “Darcher: Detectando bugs de sincronização on-chain-off-chain em aplicativos descentralizados”, em *Proc. 29ª Reunião Conjunta da ACM Eur. Softw. Eng. conf. Simp. Fundações Softw. Eng.*, 2021, pp. 553–565.

[104] D. Floyd, “150 K roubados de usuários myetherwallet em sequestro de servidor DNS”, 2018, acessado em: 15 de abril de 2023. [Online]. Disponível: https://www.coindesk.com/markets/2018/04/24/150kstolen-from-myetherwallet-users-in-dns-server-hijacking/

[105] Y. Khatri, “O provedor de infraestrutura Ethereum Infura está inoperante, as trocas de criptografia começam a desabilitar as retiradas de Eth, 2020, Acessado: 15 de abril de 2023. [Online]. Disponível: https://www.theblock.co/post/84232/ethereum-infrastructure-provider-infura-is-down

[106] S. Chipolina, “Serviço Crucial Ethereum Infura sofre grande interrupção, 2020, Acesso: 15 de abril de 2023. [Online]. Disponível: https://decrypt.co/47846/ethereum-backbone-infura-suffers-major-damage/

[107] J. John Roberts, “O ouro do Bitcoin sofre o raro 'ataque de 51%'”, 2018, acessado em: 15 de abril de 2023. [Online]. Disponível: https://fortune.com/crypto/2018/05/29/bitcoin-gold-hack/

[108] C. Natoli e V. Gramoli, “The balance attack against proof-of-work blockchains: The R3 testbed as a example,” 2016, Accessed: April 15, 2023. [Online]. Disponível: https://arxiv.org/abs/1612.09426

[109] GO Karame, E. Androulaki e S. Capkun, “Double-spending fast Payments in bitcoin,” em *Proc. ACM Conf. Comput. Comum. Seguro.*, 2012, pp. 906–917.

[110] Etherscan, “RockPaperScissors Contract,” Acessado em: 15 de abril de 2023. [Online]. Disponível: https://etherscan.io/address/0x1d77340D3819007BbfD7fdD37C22BD3b5c311350

[111] Etherscan, “TheRun Contract,” Acessado em: 15 de abril de 2023. [Online]. Disponível: https://etherscan.io/address/0xcac337492149bdb66b088bf5914bedfbf78ccc18

[112] L. Luu et al., "Tornando contratos inteligentes mais inteligentes", em *Proc. ACM SIGSAC Conf. Comput. Comum. Seguro.*, 2016, pp. 254–269.

[113] Etherscan, “Rubixi Contract,” Acessado em: 15 de abril de 2023. [Online]. Disponível: https://etherscan.io/address/0xf34cd2fd11233df8f90646ab658b03bfea98aa92

[114] EtherPot, “EtherPot,” [Online]. Disponível: http://etherpot.github.io/

[115] T. Hewa, M. Ylianttila e M. Liyanage, “Pesquisa sobre contratos inteligentes baseados em blockchain: aplicações, oportunidades e desafios,” *J. Netw. Comput. Appl.*, vol. 177, 2021, art. não. 102857.

[116] K. Bhargavan et al., "Verificação formal de contratos inteligentes: documento curto", em *Proc. Programa de Workshop ACM. Lang. Anal. Seguro.*, 2016, pp. 91–96.

[117] E. Hildenbrandt et al., “KEVM: A Complete Semantics of the Ethereum Virtual Machine,” *Proc. IEEE 31ª Computação. Seguro. Fundações Simp.*, 2018, pp. 204–217.

[118] T. Cook, A. Latham e JH Lee, “DappGuard: Active Monitoring and Defense for Solidity Smart Contracts,” 2017, Acessado em: 15 de abril de 2023. [Online]. Disponível: https://courses.csail.mit.edu/6.857/2017/project/23.pdf

[119] J. Pettersson e R. Edstrom, "Contratos inteligentes mais seguros por meio do desenvolvimento orientado a tipos", tese de mestrado, Depart. Comput. ciência Eng. Chalmers Univ. Tecnol. Univ. Gotemburgo, Gotemburgo, Suécia, 2016.

[120] CertiK, “Rumo à construção de contratos inteligentes totalmente confiáveis e ecossistema blockchain,” [Online]. Disponível: https://certik.org/whitepaper.html

[121] A. Mavridou e A. Laszka, “Projetando contratos inteligentes Ethereum seguros: uma abordagem baseada em máquina de estado finito”, 2017, *arXiv:1711.09327*.

[122] A. Mavridou e A. Laszka, “Demonstração de ferramenta: FSolidM para projetar contratos inteligentes Ethereum seguros,” em *Proc. Príncipe Seguro. Confiança: 7º Int. Conf., Post, Realizada Parte Eur. Conferência Conjunta Teoria Prática. Softw.*, 2018, 270–277.

[123] CK Frantz e M. Nowostawski, “Das instituições ao código: rumo à geração automatizada de contratos inteligentes”, em *Proc. IEEE Int. Workshops Fundamentos Appl. Auto Sist.*, 2016, pp. 210–215.

[124] M. Wohrer e U. Zdun, “Padrões de design para contratos inteligentes no ecossistema Ethereum,” em *Proc. IEEE Int. conf. Internet Things, IEEE Green Comput. Comun., IEEE Cyber, Phys. Social Comput., IEEE Smart Data*, 2018, pp. 1513–1520.

[125] T. Chen et al., “Um mecanismo adaptativo de custo de gás para Ethereum se defender contra ataques DoS subestimados”, em *Proc. Inf. Seguro. Praticar. Experiência: 13º Int. conf.*, 2017, pp. 3–24.

[126] B. Marino e A. Juels, “Definindo padrões para alterar e desfazer contratos inteligentes,” em *Proc. Regra Technol. Res., Ferramentas, Appl.: 10º Int. Simp.*, 2016, pp. 151–166.

[127] RM Parizi e A. Dehghantanha, “Linguagens de programação de contratos inteligentes em blockchains: uma avaliação empírica de usabilidade e segurança”, em *Proc. 1ª Int. Conf., Realizada Parte Serv. conf. Federação*, 2018, pp. 75–91.

[128] P. Zheng et al., “Uma estrutura de monitoramento de desempenho detalhada e em tempo real para sistemas blockchain,” em *Proc. 40º Int. conf. Softw. Eng.: Softw. Eng. Praticar.*, 2018, pp. 134–143.

[129] I. Weber et al., “Sobre a disponibilidade para sistemas baseados em blockchain,” *Proc. IEEE 36º Simp. Distribuição confiável Sist.*, 2017, pp. 64–73.

[130] H. Kalodner et al., “BlockSci: Design and applications of a blockchain analysis platform”, em*Proc. USENIX Segur. Simp.*, 2020, pp. 2721–2738.

[131] TTA Dinh et al., “Blockbench: uma estrutura para analisar blockchains privados”, em*Proc. ACM Int. conf. Gerenciar. Dados*, 2017, pp. 1085–1100.

[132] Anuj Das Gupta e A. Dickson, “Analyzing performance in blockchain-based systems”, Acesso em: 15 de abril de 2021. [Online]. Disponível: https://github.com/stratumn/performance/

[133] A. Gervais et al., “On the security and performance of proof of work blockchains”, em*Proc. ACM SIGSAC Conf. Comput. Comum. Seguro.*, 2016, pp. 3–16.

[134] Y. Li et al., “EtherQL: Uma camada de consulta para o sistema blockchain,” em*Proc. Sistema de banco de dados Adv. Ap.: 22º Int. conf.*, 2017, pp. 556–567.

[135] OA Lajam e TA Helmy, “Avaliação de desempenho de IPFS em redes privadas”, em*Proc. 4ª Int. conf. Armazenamento de dados Eng. de dados*, 2021, pp. 77–84.

[136] A. Ismail, M. Toohey, YC Lee, Z. Dong e AY Zomaya, "Análise de custo e desempenho em sistemas de arquivos descentralizados para aplicativos baseados em blockchain: relatório de última geração", em*Proc. IEEE Int. conf. Blockchain*, 2022, pp. 230–237.

[137] J. Shen, Y. Li, Y. Zhou e X. Wang, "Compreendendo o desempenho de E/S do armazenamento IPFS: a perspectiva de um cliente", em*Proc. IEEE/ACM 27ª Int. Simp. Qual. Serviço*, 2019, pp. 1–10.

[138] D. Trautwein et al., "Design e avaliação do IPFS: uma camada de armazenamento para a web descentralizada", em*Proc. ACM SIGCOMM Conf.*, 2022, pp. 739–752.

[139] Bitcoin.com, “Relatório: EOS propenso à censura precisa re-arquitetar sua infraestrutura,” [Online]. Disponível: https://news.bitcoin.com/reportcensorship-prone-eos-needs-to-re-architect-its-infrastructure/

[140] Marcos K. Aguilera, Jeffrey C. Mogul, Janet L. Wiener, P. Reynolds e A. Muthitacharoen, “Depuração de desempenho para sistemas distribuídos de caixas pretas,”*Sistema Operacional ACM SIGOPS. Rev.*, vol. 37, nº. 5, pp. 74–89, 2003.

[141] P. Reynolds, Janet L. Wiener, Jeffrey C. Mogul, Marcos K. Aguilera e A. Vahdat, “WAP5: depuração de desempenho de caixa preta para sistemas de área ampla”, em*Proc. 15ª Int. conf. Rede mundial de computadores*, 2006, pp. 347–356.

[142] P. Bahl, R. Chandra, A. Greenberg, S. Kandula, DA Maltz e M. Zhang, “Rumo a serviços de rede corporativa altamente confiáveis por meio da inferência de dependências de vários níveis”, em “*Proc. Computação ACM SIGCOMM. Comum. Rev.*, 2007, vol. 37, pp. 13–24.

[143] E. Daniel e F. Tschorsch, “IPFS e amigos: uma comparação qualitativa da próxima geração de redes de dados ponto a ponto,”*IEEE Comun. Sobreviver Tut.*, vol. 24, não. 1, pp. 31–52, jan.–mar. 2022.