

Escalabilidade na Rede Ethereum: Vantagens e Desvantagens das Principais Técnicas Utilizadas

João Vitor Franco Lorenz¹, Igor Machado Coelho²

¹Instituto de Computação – Universidade Federal Fluminense (UFF)
24.210-346 – Niterói – RJ – Brasil

jfrancolorenz@gmail.com, imcoelho@ic.uff.br

Abstract. *This article employs the Kitchenham approach to carry out a systematic mapping of the scaling techniques present in the Ethereum blockchain. The study focused on analyzing the advantages and disadvantages of seven of the most popular solutions, including: sharding, state channel, sidechains, plasma, validium, rollup zk and optimistic. The results indicate that the mapped techniques offer benefits, such as increasing transaction capacity and reducing costs. Finally, the study also present limitations and risks that affect network security.*

Resumo. *O presente artigo emprega a abordagem Kitchenham para realizar um mapeamento sistemático das técnicas de escalonamento presentes na blockchain Ethereum. O estudo focou em analisar as vantagens e desvantagens de sete das soluções mais populares, incluindo: sharding, state channel, sidechains, plasma, validium, rollup zk e otimista. Os resultados indicam que as técnicas mapeadas oferecem benefícios, como aumento da capacidade de transações e redução dos custos. No entanto, também apresentam limitações e riscos que afetam a segurança da rede.*

1. Introdução

O desafio da escalabilidade está presente em diferentes blockchains públicas e descentralizadas de primeira camada. Em síntese, esse problema surge como resultado do trilema enfrentado entre segurança, descentralização e escalabilidade. De maneira simplista, o trilema infere que é necessário reduzir a ênfase em uma dessas características para aprimorar as demais (Parashar et al., 2022). Nesse sentido, um dos sistemas mais afetados é a rede Ethereum (Wood, 2014), onde a falta de escalabilidade resulta em outros problemas, como o aumento dos custos das taxas de transações (Neiheiser et al., 2023).

Visando solucionar o problema da escalabilidade, soluções de escalonamento foram propostas. Dito isso, parte das soluções desenvolvidas foram projetadas para atuarem diretamente na rede principal (Li et al., 2023). No entanto, a maioria das técnicas elaboradas operam de maneira híbrida ou off-chain, isto é, são sistemas adjacentes responsáveis por processar as transações fora da cadeia original. Embora as técnicas de escalabilidade desenvolvidas sejam benéficas para a rede Ethereum, elas também apresentam limitações e vulnerabilidades que podem prejudicar a segurança e a eficiência da rede (Thibault et al., 2022).

Com base nessa perspectiva, no presente trabalho realizamos um mapeamento sistemático da literatura a fim de identificar e descrever as principais técnicas de escalabilidade atualmente empregadas na blockchain Ethereum. Dessa forma, apesar da existência

de mais soluções de escalabilidade (Hafid et al., 2020), concentramos o escopo deste artigo em sete das técnicas mais populares, visando explorar suas vantagens e apresentar de maneira clara suas principais desvantagens e limitações. Além disso, buscamos como contribuição fortalecer a base de conhecimentos científicos no tema em idioma português, dado que a grande maioria dos materiais existentes ainda são *literatura cinzenta*, do inglês, *gray literature*, como *posts* em blogs, vídeos e pequenas notas técnicas.

As próximas seções do artigo estão organizadas da seguinte maneira: A Seção 2 contextualiza a tecnologia blockchain. A Seção 3 apresenta a blockchain Ethereum. A Seção 4 dedica-se à metodologia do trabalho. A Seção 5 aborda os principais trabalhos relacionados. A Seção 6 apresenta as técnicas de escalabilidade mapeadas e, finalmente, a Seção 7 aborda as considerações finais da pesquisa.

2. Blockchain

A tecnologia blockchain foi desenvolvida pelo pseudônimo de Satoshi Nakamoto em 2008, com o objetivo de criar a criptomoeda Bitcoin (Nakamoto, 2008). Desde então, ganhou notoriedade por seu potencial de revolucionar transações financeiras, consenso distribuído e propriedades de anonimato (Alemany et al., 2022). Nesse contexto, a tecnologia atua como um sistema de registro distribuído, seguro e transparente que não requer a necessidade de entidades centralizadas para efetuar o armazenamento de informações. Portanto, a blockchain atua como um livro-razão, possibilitando que o registro de transações seja distribuído por vários computadores (Treiblmaier and Clohessy, 2020).

De modo geral, sua estrutura é composta por uma rede de computadores responsáveis por registrar e validar um conjunto de transações. Logo, as transações em blockchain representam uma transferência de valor ou informação entre dois endereços alfanuméricos. Cada endereço é gerado a partir de um par de chaves criptográficas, composto por uma chave pública e outra privada, comumente gerados através de algoritmos de criptografia de curvas elípticas (Böhme et al., 2014). Para garantir a segurança e integridade das informações, as transações são reunidas e armazenadas em blocos. Os blocos são processados pelos nós da rede por meio de um mecanismo de consenso. Após o processamento, um hash é gerado para o bloco minerado e adicionado no cabeçalho do bloco seguinte, formando uma cadeia de blocos (Treiblmaier and Clohessy, 2020).

3. Ethereum

A blockchain Ethereum é uma plataforma de computação de contrato inteligente, cujo objetivo é expandir as funcionalidades da tecnologia blockchain além de transações financeiras (Wood, 2014). Em síntese, esses contratos são programas que funcionam como acordos digitais executados sem a necessidade de intermediários (Kemmo et al., 2020). Na atualidade, a Ethereum é uma das blockchains mais populares do mundo, sendo que sua tecnologia é utilizada em várias aplicações descentralizadas, incluindo finanças, jogos e outros (AAVE, 2023; Besançon et al., 2022).

Uma das características mais notáveis da plataforma Ethereum é o uso da *Ethereum Virtual Machine* (EVM), uma máquina virtual responsável por executar contratos inteligentes. A EVM consegue interpretar instruções permitindo que os desenvolvedores programem aplicativos descentralizados em diferentes linguagens de programação (Ethereum, 2024). Dentre as linguagens suportadas pela EVM, destaca-se a Solidity,

que foi desenvolvida especificamente para a plataforma Ethereum e possui alta compatibilidade com a mesma (Solidity, 2023). A escalabilidade é um dos principais desafios da Ethereum, pois a rede atual suporta cerca de 20 Transações Processadas por Segundo (TPS) (Thibault et al., 2022). Para enfrentar esse desafio, a Ethereum está trabalhando em soluções de escalabilidade. Dito isso, uma das soluções foi a mudança de seu mecanismo de consenso, passando de *Proof of Work* (PoW) para *Proof of Stake* (PoS). No entanto, essa não é a única solução para a escalabilidade, e outras técnicas também estão sendo desenvolvidas.

4. Metodologia

A pesquisa desenvolvida neste estudo consiste em uma pesquisa de natureza qualitativa, onde seu foco é de caráter exploratório. Dessa forma, para efetuarmos o mapeamento sistemático da literatura, utilizamos o método de Kitchenham (Kitchenham, 2004), portanto, definimos as seguintes perguntas de pesquisa:

- 1) Quais são as técnicas de escalabilidade utilizadas na rede Ethereum?
- 2) Quais são as vantagens e desvantagens dessas técnicas?

4.1. Ferramenta de pesquisa

O mapeamento sistemático da literatura ocorreu com o auxílio da ferramenta Parsifal (Parsifal, 2024), uma ferramenta baseada na diretriz de Kitchenham que auxilia os pesquisadores no desenvolvimento de revisões e mapeamentos no contexto da Engenharia de Software. A ferramenta pode ser encontrada no site do Parsifal¹.

4.2. Base de dados

Optamos por bibliotecas acadêmicas que oferecem integração com o sistema Parsifal. Nesse sentido, foram incluídos os seguintes repositórios: IEEE Xplore e Scopus. Diante disso, a string de busca foi derivada das perguntas de pesquisa. Como consequência, obtivemos a seguinte expressão:

```
("Ethereum" OR "Blockchain") AND ("scalability techniques"  
OR "Plasma" OR "Rollup" OR "Sharding" OR "Sidechain" OR  
"layer 2" OR "scalability approaches" OR "scalability  
methods" OR "second layer solutions" OR "state channel"  
OR "validium") AND ("advantages" OR "benefits" OR "  
disadvantages" OR "limitations" OR "risks")
```

Após a definição da string de busca, efetuamos a pesquisa nas diferentes bases de dados. Como resultado, foram identificados 87 estudos na base IEEE Xplore e 236 na Scopus. Além disso, também foram adicionados 2 artigos manualmente.

4.3. Critérios de inclusão e exclusão

Para reduzir o número de artigos selecionados, definimos uma série de critérios de inclusão e exclusão. Nesse contexto, foram estabelecidos os seguintes critérios de inclusão:

¹<https://parsif.al/>

1) O artigo deve estar diretamente relacionado a escalabilidade; 2) Deve abranger ao menos uma das técnicas contidas na string de busca. Em contrapartida, definimos os seguintes parâmetros de exclusão: 1) Artigos duplicados; 2) Texto não acessível pela CAPES; 3) Livros ou capítulos; 4) Resumo de Conferência; 5) Artigos anteriores a 2020 (concentramos o escopo do artigo em pesquisas mais recentes); 6) Artigos que não estejam na língua inglesa (nenhum artigo em Português foi obtido através da string de busca); 7) Artigos que não possuem relação direta ao tema e 8) Artigos com foco principal em outras blockchains.

4.4. Avaliação da Qualidade

A avaliação de qualidade realizada para elaborar o filtro secundário da pesquisa foi conduzida por meio de 6 perguntas. Em síntese, cada estudo coletado foi submetido às perguntas com o intuito de avaliá-los perante o tema proposto. Dessa forma, os estudos foram classificados por meio de notas. Cada questão recebeu um peso de 0 a 1, onde 0 representa a não satisfação do critério, 0,5 indica uma satisfação parcial e 1 representa uma satisfação total. Diante disso, a nota de corte dos estudos foi estabelecida em 3,0, sendo que as seguintes perguntas foram realizadas:

- 1) O artigo possui relação explícita com o Ethereum?
- 2) O artigo aborda detalhadamente pelo menos uma técnica de escalabilidade?
- 3) Ocorrem comparações entre as técnicas de escalabilidade?
- 4) Os autores apresentam as vantagens das técnicas de escalabilidade discutidas?
- 5) Os autores apresentam as desvantagens das técnicas de escalabilidade?
- 6) Os autores apresentam possíveis soluções para as desvantagens?

4.5. Parâmetros extraídos

Dentre as informações obtidas dos artigos encontram-se: nome dos autores, data de publicação, técnicas de escalabilidade avaliadas, objetivo do estudo, estudo de caso e seus resultados e conclusões. Com base nessa perspectiva, a Figura 1 apresenta todo o processo realizado na triagem dos artigos, contendo quantos estudos permaneceram em cada etapa.

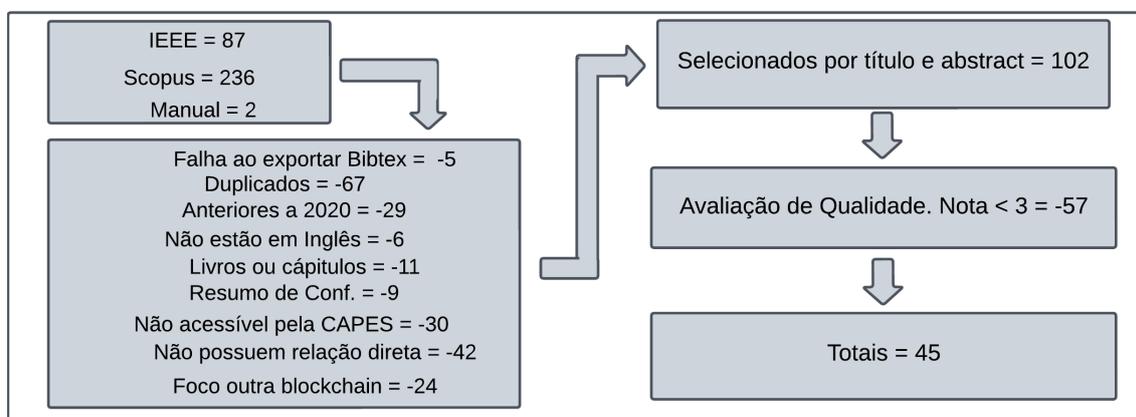


Figura 1. Diagrama da triagem dos artigos

5. Trabalhos relacionados

Com base na pesquisa realizada, diversos estudos possuem relação com o tema proposto. Nesta seção, apresentaremos de forma sucinta oito pesquisas relevantes. No entanto, é importante mencionar que não encontramos nenhuma pesquisa específica dedicada à técnica Validium. Diante disso, Hafid et al. (2020) realizam uma pesquisa abrangente sobre escalabilidade em blockchains, concentrando-se principalmente na solução de Sharding. O trabalho propõe uma taxonomia com base na formação de comitês e no consenso intracomitê, além de avaliar as vantagens e desvantagens das soluções existentes. Em contrapartida, Singh et al. (2020) fornecem uma revisão sobre as Sidechains, identificando os avanços atuais da tecnologia e analisando suas principais desvantagens. Além disso, Dziembowski et al. (2020) exploram as limitações existentes em protocolos Plasma, com foco principal nas soluções Plasma Cash e Fungible Plasma.

Negka e Spathoulas (2021) apresentam uma pesquisa dedicada ao estado da arte das soluções de State Channels. Neste estudo, eles oferecem uma visão abrangente da tecnologia, incluindo uma análise de suas principais limitações. Por outro lado, Thibault et al. (2022) analisam as principais vantagens e desvantagens das soluções de escalonamento de blockchain de primeira e segunda camada. No entanto, o foco principal do trabalho está direcionado para as técnicas de rollups. Da mesma forma, Lavaur et al. (2023) discutem os benefícios dos zk-rollups como soluções de segunda camada.

Li et al. (2023) abordam o problema da escalabilidade na tecnologia blockchain e discutem suas diversas soluções; no entanto, o foco principal do trabalho também está direcionado à técnica de Sharding. Além disso, ao longo do artigo, os autores conduzem uma análise sobre diferentes blockchains de fragmentação de última geração. Por fim, Neiheiser et al. (2023) apresentam um estudo voltado para as limitações existentes em protocolos de segunda camada da rede Ethereum, analisando seus designs, segurança, desempenho e impacto na cadeia principal.

6. Resultados

Conforme apresentado na Figura 1, após a aplicação dos filtros, foram obtidos 45 estudos. Diante disso, sintetizamos as informações e organizamos esta seção em tópicos a fim de explicar cada técnica mapeada, juntamente com suas principais vantagens e desvantagens.

6.1. Sharding

A técnica de Sharding, ilustrada na Figura 2, visa aprimorar a escalabilidade por meio da fragmentação dos nós da rede. Nesse sentido, cada grupo fragmentado (Shard) é designado para executar parte das transações em paralelo, possibilitando o processamento simultâneo em diferentes sub-redes (Li et al., 2023). Diante disso, conforme apresentado por Liu et al. (2023), a técnica demonstra benefícios relacionados à melhora na quantidade de TPS, velocidade de execução e na redução da latência presente na confirmação das transações. No entanto, de acordo com Zhang et al. (2023), a técnica de Sharding também apresenta limitações, que vão desde a possibilidade de inconsistência de dados entre diferentes shards, até uma possível sobrecarga na comunicação devido ao excesso de transações entre os fragmentos. Dito isso, segundo Honari et al. (2022), outra desvantagem consiste no aumento da complexidade do sistema, uma vez que dividir a rede em múltiplas sub-redes pode tornar mais complexa a coordenação do mecanismo. Além disso,

conforme indicado por Hafid et al. (2020), a técnica também pode apresentar vulnerabilidades em relação a ataques de sincronização e controle de execução de transações, o que permite que nós maliciosos controlem um fragmento. Contudo, medidas como sistemas de reputação e alocação aleatória de nós, podem dificultar que agentes mal-intencionados explorem essa vulnerabilidade. Diante disso, conforme apresentado por Breslin and Keel (2023), embora a técnica de Sharding tenha sido proposta para escalar a rede Ethereum, ela ainda requer mais investigação para efetivamente entrar em vigor. Dessa forma, soluções alternativas como Danksharding estão sendo desenvolvidas. De maneira simplista, Danksharding simplifica o processo de validação usando referências a grandes conjuntos de dados verificáveis probabilisticamente, sem a necessidade de fragmentação completa dos validadores.

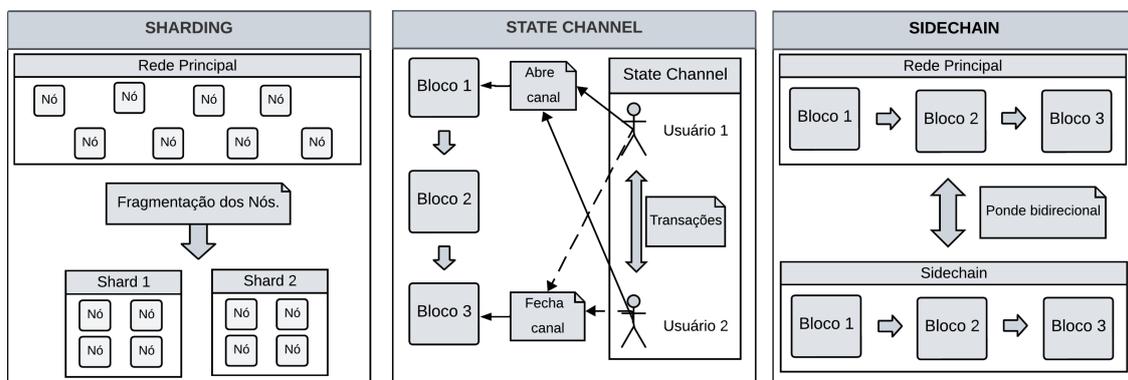


Figura 2. Estrutura de Sharding, State Channel e Sidechain

6.2. State Channel

Os State Channels consistem em um método off-chain de escalabilidade. Em síntese, conforme apresentado na Figura 2, os usuários estabelecem a abertura de um canal de comunicação com a blockchain e realizam transações fora da cadeia principal. Após o término das negociações, eles atualizam seus respectivos fundos e fecham o canal (Thibault et al., 2022). O principal benefício dessa estratégia consiste em permitir que os usuários realizem diversas transações com baixo custo e privacidade, uma vez que as transações realizadas off-chain não são processadas diretamente pelos validadores e nem registradas no livro razão (Ajorlou and Abbasfar, 2020). No entanto, segundo Negka and Spathoulas (2021), os State Channels apresentam barreiras relacionadas às restrições de aplicações, ou seja, não são adequados para todos os tipos de aplicativos que requerem interações mais abertas ou dinâmicas com um grande número de participantes. Outro ponto presente nos State Channels é a necessidade de participantes pré-definidos, para que haja confiança entre os usuários. Além disso, outros requisitos técnicos como segurança e gestão do tempo em sistema blockchain também são apontados como desafios dessa tecnologia.

6.3. Sidechain

As sidechains, ilustradas na Figura 2, utilizam a interoperabilidade como ponto fundamental para escalar uma rede blockchain. Em suma, esse tipo de tecnologia funciona como uma rede autônoma e paralela que se conecta via pontes com a rede principal. De

maneira simplista, as sidechains permitem que os usuários migrem tokens entre as redes, beneficiando-se dos custos das taxas de transações na rede secundária e dos protocolos não existentes na camada um (Li et al., 2020). No entanto, de acordo com Singh et al. (2020), as sidechains podem apresentar lentidão ao realizar a transferência de ativos. Outro ponto destacado é que, por serem redes autônomas, uma das principais desvantagens dessa tecnologia é que a segurança do seu protocolo não é garantida pela rede principal, portanto, alguns tipos de sidechains podem introduzir centralização política, o que significa que a transferência de ativos entre blockchains pode depender de uma entidade centralizada. Além disso, segundo Mao et al. (2023), a introdução de várias sidechains pode causar ataques de replay cruzado, onde uma transação é transmitida para várias cadeias, resultando na perda de ativos.

6.4. Plasma

Os sistemas Plasma podem ser considerados uma evolução das sidechains. Portanto, também são constituídos por uma cadeia separada da rede principal. No entanto, submetem informações de estado e são gerenciadas por contratos inteligentes implementados na camada um. Como consequência, esse tipo de tecnologia é considerada mais segura que sidechains tradicionais e podem reduzir os custos das transações. Em contrapartida, conforme ressaltado por Dziembowski et al. (2020), os sistemas Plasma apresentam vulnerabilidades relacionadas a ataques que forcem partes honestas a se comunicarem excessivamente com a blockchain principal. Outra limitação é que as vantagens de dois dos tipos mais proeminentes de Plasma, chamados Plasma Cash (proteção individual de moedas) e Fungible Plasma (fungibilidade de moedas), não podem ser alcançadas simultaneamente. Além disso, conforme apresentado por Thibault et al. (2022), os sistemas plasma também necessitam de um período para efetuar a resolução de disputas relacionadas à verificação de transações fraudulentas, o que resulta em períodos de espera para os usuários, aumentando o tempo necessário para a conclusão das transações. Por fim, de acordo com Neiheiser et al. (2023), os sistemas Plasma demonstram incompatibilidade com grande parte das operações de contratos inteligentes na cadeia lateral, suportando apenas um conjunto restrito de aplicações.

6.5. Rollup Otimista

Rollup otimista, ilustrado na Figura 3, consiste em uma técnica de escalabilidade híbrida que visa sequenciar e agregar as transações em lotes fora da rede principal, publicando os dados de forma resumida na camada um (Lavaur et al., 2023). Portanto, conforme apresentado por Thibault et al. (2022), além de reduzir os custos das transações, uma de suas principais vantagens reside no fato de que as transações processadas na camada dois estão disponíveis na camada um, oferecendo a possibilidade de executar novamente todas as transações do sistema. Contudo, outro benefício da técnica é a capacidade de execução de contratos inteligentes sem a necessidade de modificação fora da camada um, proporcionando flexibilidade e compatibilidade com contratos já existentes (Lavaur et al., 2022). No entanto, seu principal problema reside no fato de que não há prova de validade incluída, e os nós da camada um supõem com otimismo que a computação executada pelo agregador é válida. Além disso, como indicado por Gorzny et al. (2022), as versões iniciais de rollups otimistas trouxeram modificações na semântica da computação e na representação de criptomoedas nativas, o que pode apresentar riscos para os usuários.

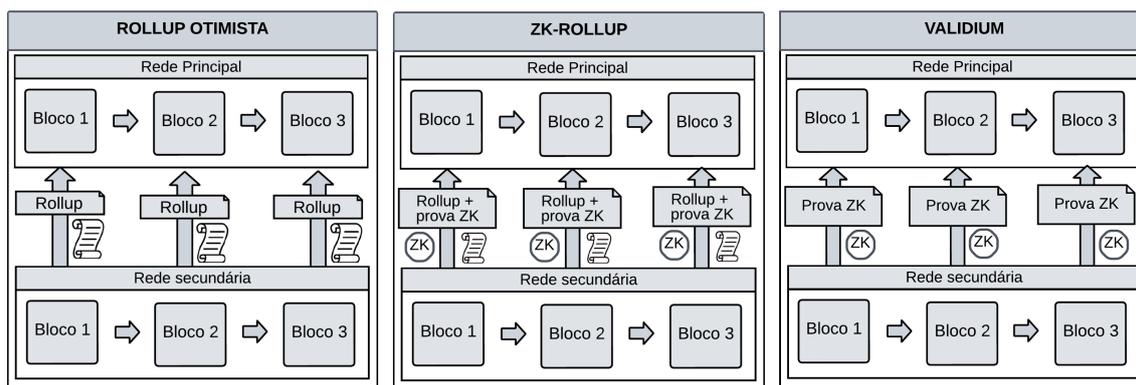


Figura 3. Estrutura Rollup Otimista, ZK-Rollup e Validium

6.6. ZK-Rollup

Assim como os Rollups Otimistas, os ZK-rollups agregam as transações fora da camada um e publicam os dados de forma resumida na rede principal. No entanto, conforme ilustrado na Figura 3, esse tipo de tecnologia também submete provas de conhecimento zero para garantir a veracidade das transações. Diante disso, segundo Lavour et al. (2022), a utilização dos zk-rollups permite o aumento no número de TPS e a redução dos custos das taxas de transações. Além disso, a integridade das transações é garantida por meio de provas criptográficas, o que reduz o tempo necessário para efetuar sua confirmação. No entanto, apesar de serem as soluções mais seguras, os zk-rollups possuem uma alta complexidade técnica e necessitam de um grande poder computacional, o que pode prejudicar o desenvolvimento da tecnologia (Lavour et al., 2022). Dessa forma, conforme apresentado por Neiheiser et al. (2023), os zk-rollups possuem uma sobrecarga computacional maior do que os rollups otimistas, o que resulta em custos de retirada mais altos para os usuários. Portanto, os saques são geralmente executados em lotes, o que reduz o custo, mas acarreta latência adicional para o cliente.

6.7. Validium

As soluções Validium, ilustradas na Figura 3, também são redes secundárias gerenciadas por contratos inteligentes implantados na camada um. Diante disso, da mesma forma que os ZK-Rollups, as redes Validium submetem provas de conhecimento zero referentes às transações realizadas. No entanto, as transações não são armazenadas na camada um, portanto, o armazenamento de dados é delegado a terceiros confiáveis, como um grupo autorizado ou até mesmo uma blockchain externa. Essa característica viabiliza que o processamento das transações seja mais rápido que os ZK-Rollup (Lavour et al., 2022). No entanto, conforme apresentado por Thibault et al. (2022), o principal problema dessa tecnologia é a disponibilidade de dados, pois, caso a entidade externa responsável por armazenar as informações se recuse a fornecê-las, não é possível efetuar a prova criptográfica que garante a veracidade das transações. Uma comparação do Validium com as demais tecnologias pode ser vista na Tabela 1.

Tabela 1. Comparativo de Técnicas de Escalabilidade

| Técnica | Vantagens | Desvantagens |
|----------------|--|---|
| Sharding | <ul style="list-style-type: none">• Aumento de TPS.• Redução da latência.• Redução de custo.• Escalabilidade Horizontal• Melhor Utilização de Recursos | <ul style="list-style-type: none">• Inconsistência de dados.• Sobrecarga na comunicação.• Aumento da complexidade do sistema.• Ataques sincronizados. |
| State Channel | <ul style="list-style-type: none">• Aumento Indireto de TPS.• Redução da latência.• Redução de custo.• Privacidade nas transações. | <ul style="list-style-type: none">• Restrições de aplicações.• Participantes presentes ao longo de todo o processo.• Necessidade de confiança entre participantes.• Sem segurança compartilhada. |
| Sidechain | <ul style="list-style-type: none">• Aumento Indireto de TPS.• Redução de custo.• Interoperabilidade. | <ul style="list-style-type: none">• Lentidão na transferência de ativos.• Sem segurança compartilhada.• Possibilidade de centralização.• Vulnerabilidade a ataques. |
| Plasma | <ul style="list-style-type: none">• Aumento Indireto de TPS.• Redução de custo.• Interoperabilidade.• Segurança compartilhada. | <ul style="list-style-type: none">• Vulnerabilidade a ataques.• Possibilidade de centralização.• Período para resolução de disputas.• Incompatibilidade com alguns contratos inteligentes. |

Continua na próxima página

Tabela 1 – continuação da página anterior

| Técnica | Vantagens | Desvantagens |
|--------------------|--|--|
| Rollup Otimista | <ul style="list-style-type: none">• Aumento Indireto de TPS.• Redução de custo.• Interoperabilidade.• Segurança compartilhada.• Transações disponíveis na camada principal. | <ul style="list-style-type: none">• Sem prova de validade.• Possibilidade de centralização.• Período para resolução de disputas. |
| ZK-Rollup | <ul style="list-style-type: none">• Aumento Indireto de TPS.• Redução de custo.• Interoperabilidade.• Segurança compartilhada.• Transações disponíveis na camada principal.• Prova de validade. | <ul style="list-style-type: none">• Possibilidade de centralização.• Aumento da complexidade do sistema.• Aumento na necessidade de poder computacional. |
| Validium | <ul style="list-style-type: none">• Aumento Indireto de TPS.• Redução de custo.• Interoperabilidade.• Segurança compartilhada.• Prova de validade. | <ul style="list-style-type: none">• Possibilidade de centralização.• Aumento da complexidade do sistema.• Aumento na necessidade de poder computacional.• Negação de dados.• Transações não disponíveis na camada principal. |

7. Considerações finais

No decorrer desta pesquisa foi realizado um mapeamento sistemático seguindo a abordagem de Kitchenham, abrangendo sete das principais técnicas de escalabilidade empregadas na rede Ethereum. Ao longo do artigo, foram apresentadas as vantagens e desvantagens das seguintes soluções: sharding, state channel, sidechains, plasma, validium, rollup zk e otimista. Foi possível observar que grande parte das soluções apresentadas implicam no aumento da quantidade de TPS suportada pela rede Ethereum e na redução dos custos das taxas de transações. No entanto, todas as abordagens também apresentam limitações. Diante disso, considerando as técnicas off-chain ou híbridas, as soluções como Validium, Rollup Otimistas e ZK-Rollup aparentam ser mais seguras, porém, necessitam de uma maior complexidade técnica. Por outro lado, soluções como State Channel e Sidechains, possuem um grau menor de segurança compartilhada com a rede principal. Outro ponto importante é que as soluções Plasma estão gradualmente sendo migradas para alternati-

vas mais eficientes e seguras, um exemplo disso é o ecossistema da rede Polygon (Polygon, 2024). Contudo, apesar da técnica Validium apresentar um avanço significativo nas soluções de escalabilidade, no mapeamento efetuado não foi encontrada nenhuma pesquisa dedicada a essa tecnologia. Portanto, na perspectiva dos autores, ainda há muito espaço para pesquisa na área de escalabilidade em blockchain, em especial, abordando tecnologias mais recentes, como Sharding, Rollups e Validium. Como trabalhos futuros, propomos a construção de uma plataforma web para catalogar conteúdo na área, no formato de um observatório de tecnologias de escalabilidade em blockchain, de forma a facilitar que desenvolvedores e a comunidade em geral tenha acesso mais fácil e direto ao conteúdo acadêmico explorado nesse trabalho, bem como demais conteúdos publicados como *gray literature* na Internet.

Referências

- AAVE (2023). Introduction to aave. Disponível em: <https://docs.aave.com/faq/>, Acesso em: 22/03/2024.
- Ajorlou, A. and Abbasfar, A. (2020). An optimized structure of state channel network to improve scalability of blockchain algorithms. In *2020 17th International ISC Conference on Information Security and Cryptology (ISCISC)*, pages 73–76.
- Aleman, P., Vilalta, R., Munoz, R., Casellas, R., and Martinez, R. (2022). Evaluation of the abstraction of optical topology models in blockchain-based data center interconnection. *Journal of Optical Communications and Networking*, 14(4):211–221.
- Besançon, L. et al. (2022). A blockchain ontology for dapps development. *IEEE Access*, 10:49905–49933.
- Breslin, A. and Keel, T. (2023). Ethereum evolved: Dencun upgrade part 5, eip-4844. Disponível em: <https://consensys.io/blog/ethereum-evolved-dencun-upgrade-part-5-eip-4844>, Acesso em: 16/01/2024.
- Böhme, R. et al. (2014). Bitcoin: Economics, technology, and governance. *Economics of Innovation eJournal*.
- Dziembowski, S., Fabiański, G., Faust, S., and Riahi, S. (2020). Lower bounds for off-chain protocols: Exploring the limits of plasma. Cryptology ePrint Archive, Paper 2020/175.
- Ethereum (2024). Máquina virtual do ethereum (evm). Disponível em: <https://ethereum.org/pt-br/developers/docs/evm/>, Acesso em: 22/03/2024.
- Gorzny, J., Po-An, L., and Derka, M. (2022). Ideal properties of rollup escape hatches. In *Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good, DICG '22*, page 7–12, New York, NY, USA. Association for Computing Machinery.
- Hafid, A., Hafid, A. S., and Samih, M. (2020). Scaling blockchains: A comprehensive survey. *IEEE Access*, 8:125244–125262.
- Honari, K., Zhou, X., Rouhani, S., Dick, S., Liang, H., Li, Y., and Miller, J. (2022). A scalable blockchain-based smart contract model for decentralized voltage stability using sharding technique. In *2022 IEEE International Conference on Blockchain (Blockchain)*, pages 124–131.
- Kemmo, V. Y. et al. (2020). Recent advances in smart contracts: A technical overview and state of the art. *IEEE Access*, 8:117782–117801.
- Kitchenham, B. A. (2004). Procedures for performing systematic reviews.

- Lavour, T., Detchart, J., Lacan, J., and Chanel, C. P. (2023). Modular zk-rollup on-demand. *Journal of Network and Computer Applications*, 217:103678.
- Lavour, T., Lacan, J., and Chanel, C. P. C. (2022). Enabling blockchain services for ioe with zk-rollups. *Sensors*, 22(17):6493.
- Li, M., Tang, H., Hussein, A. R., and Wang, X. (2020). A sidechain-based decentralized authentication scheme via optimized two-way peg protocol for smart community. *IEEE Open Journal of the Communications Society*, 1:282–292.
- Li, Y., Wang, J., and Zhang, H. (2023). A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces. *Journal of Network and Computer Applications*, 217:103686.
- Liu, X., Xie, H., Yan, Z., and Liang, X. (2023). A survey on blockchain sharding. *ISA Transactions*, 141:30–43.
- Mao, H., Nie, T., Sun, H., Shen, D., and Yu, G. (2023). A survey on cross-chain technology: Challenges, development, and prospect. *IEEE Access*, 11:45527–45546.
- Nakamoto, S. (2008). A peer-to-peer electronic cash system. Disponível em: <https://bitcoin.org/bitcoin.pdf>, Acesso em: 22/03/2024.
- Negka, L. D. and Spathoulas, G. P. (2021). Blockchain state channels: A state of the art. *IEEE Access*, 9:160277–160298.
- Neiheiser, R., Inácio, G., Rech, L., Montez, C., Matos, M., and Rodrigues, L. (2023). Practical limitations of ethereum’s layer-2. *IEEE Access*, 11:8651–8662.
- Parashar, D., Sharma, M., Sharma, V., and Nand, P. (2022). Approaching solutions to blockchain security trilemma and consensus mechanisms. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pages 2030–2036.
- Parsifal (2024). Perform systematic literature reviews. Disponível em: <https://parsif.al/>, Acesso em: 14/01/2024.
- Polygon (2024). Polygon 2.0: Polygon pos to zk l2. Disponível em: <https://polygon.technology/blog/polygon-2-0-polygon-pos-zk-layer-2>, Acesso em: 10/01/2024.
- Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., and Choo, K.-K. R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, 149:102471.
- Solidity (2023). Introdução aos smart contracts. Disponível em: <https://solidity-portuguese.readthedocs.io/pt/latest/introduction-to-smart-contracts.html#a-maquina-virtual-ethereum-evm>, Acesso em: 22/03/2024.
- Thibault, L. T., Sarry, T., and Hafid, A. S. (2022). Blockchain scaling using rollups: A comprehensive survey. *IEEE Access*, 10:93039–93054.
- Treiblmaier, H. and Clohessy, T. (2020). *Blockchain and Distributed Ledger Technology Use Cases: Applications and Lessons Learned*. Springer.
- Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151:1–32.
- Zhang, M., Li, J., Chen, Z., Chen, H., and Deng, X. (2023). An efficient and robust committee structure for sharding blockchain. *IEEE Transactions on Cloud Computing*, 11(3):2562–2574.