Análise das soluções de escalabilidade do Bitcoin: Tecnologias Atuais e Perspetivas Futuras

Resumo

O Bitcoin, limitado a cerca de 7 transações por segundo (TPS) devido à sua ênfase na segurança e descentralização, enfrenta desafios significativos de escalabilidade perante a sua adoção crescente. Este artigo examina seis categorias de soluções propostas para ultrapassar essa limitação, com base em literatura académica e fontes atualizadas até 30 de março de 2025: atualizações de protocolo (ex.: SegWit, aumento do tamanho do bloco), soluções de camada 2 (ex.: Lightning Network, side-chains, rollups), técnicas de compressão e abordagens inovadoras (ex.: machine learning, sharding). A análise, suportada por artigos obtidos em bases de dados como ScienceDirect, ResearchGate e Scielo, revela que o SegWit melhora a segurança, mas não a escalabilidade em massa, enquanto o aumento do tamanho do bloco compromete a descentralização. A Lightning Network destaca-se com um potencial de 1 milhão de TPS e uma adoção em alta (16,6% em 2024), apesar de problemas de liquidez. Rollups e side-chains proporcionam eficiência, mas requerem alterações protocolares ou confiança em validadores. As técnicas de compressão reduzem o tamanho da blockchain em 78% e aumentam a capacidade dos blocos até 60 vezes, mantendo a descentralização. Abordagens como machine learning e sharding prometem menor latência e maior throughput, mas enfrentam obstáculos técnicos e de consenso. Conclui-se que nenhuma solução resolve isoladamente o trilema da blockchain, sugerindo combinações híbridas como via viável, embora dependam de progressos técnicos e aceitação da comunidade para garantir a escalabilidade do Bitcoin.

Palavras-chave: Bitcoin, scalability, Lightning Network, SegWit, rollups, blockchain, layer 2.

1. Introdução

Bitcoin, a criptomoeda pioneira, enfrenta desafios significativos de escalabilidade que limitam a sua capacidade de processar transações em larga escala e em tempo útil. A escalabilidade refere-se à capacidade de um sistema de suportar um aumento no volume de transações sem comprometer o desempenho ou a eficiência. No caso do Bitcoin, a rede processa atualmente cerca de 7 transações por segundo (TPS), um valor substancialmente inferior ao dos sistemas de pagamento tradicionais, como o Visa, que processa milhares de TPS.

Esta limitação decorre do design da blockchain do Bitcoin, que prioriza a segurança e a descentralização em detrimento da capacidade de processamento, são estas três componentes que constituem o Trilema das Blockchains. O facto da adoção do Bitcoin apresentar uma

tendência crescente implica o desenvolvimento, criação e aplicação de soluções de escalabilidade, para suprir uma necessidade que se torna-se mais premente. Este artigo, com base em literatura académica e fontes atualizadas até 30 de março de 2025, explora seis categorias de soluções propostas para melhorar a escalabilidade do Bitcoin, com o objetivo de fornecer uma visão abrangente das tecnologias disponíveis e soluções atuais emergentes, comparando-as e discutindo os seus potenciais benefícios e desafios.

2. Metodologia

Esta análise baseia-se numa revisão de vários artigos académicos principais e fontes adicionais de informação disponíveis na internet.
Os artigos analisados foram obtidos nas bases de dados sciencedirect, researchgate e scielo e as soluções de escalabilidade identificadas foram classificadas em quatro grupos:

- atualizações de protocolo,
- soluções de 2ª camada,
- técnicas de compressão e
- abordagens inovadoras.

3. Resultados

3.1. Atualizações de Protocolo

As atualizações de protocolo alteram o núcleo do Bitcoin para melhorar a capacidade de processamento, dentro desta classe existem:

SegWit: Implementado em 2017, separa os dados de testemunho, aumentando a capacidade efetiva dos blocos para 4 MB. Lincopinis e Llantos (2024) indicam que o limite permanece em 7 TPS, insuficiente para uso massivo. Nasir et al. (2022) destacam que o SegWit também melhora a segurança contra ataques de maleabilidade, mas o impacto na escalabilidade é incremental.

Aumento do Tamanho do Bloco e redução do tempo de criação: Propostas como o Bitcoin Cash que seguiram o caminho de blocos maiores (8 e 32Mb) ou da redução do tempo de criação o bloco como a Litecoin (2,5 min), porém Kaur et al. (2024) argumentam que estas opções podem aumentar a latência de propagação e os requisitos de largura de banda, favorecendo nós mais poderosos e comprometendo a descentralização.

3.2. Soluções de 2ª Camada

Estas soluções processam transações fora da cadeia, reduzindo a carga na blockchain principal.

Lightning Network: Lançada em 2018, permite transações instantâneas com um potencial de 1 milhão de TPS. Barbaravičius (2024) reporta um crescimento de adoção de 6,5% (Q2 2022) para 16,6% (Q2 2024), impulsionado por melhorias como AMP (Atomic Multi-path Payments) e os Wumbo Channels. Kaur, et al., (2020) assinalam que a Lightning enfrenta desafios de liquidez e roteamento, mas as atualizações de super nós mitigam essas questões (Alshahrani et al., 2023).

Side-chains: Rootstock (RSK) integra contratos inteligentes ao Bitcoin, enquanto a Liquid Network acelera transações entre exchanges (Qi, 2024). Nasir et al. (2022) sublinham que as cadeias laterais oferecem flexibilidade, mas exigem um alto nível de confiança nos validadores da 2ª camada.

Rollups: Tradicionalmente usados no Ethereum, os rollups estão a ser adaptados para o Bitcoin. O artigo publicado em Bitcoinrollups.com indica que os rollups potenciam o Bitcoin para além das suas limitações atuais, oferecendo escalabilidade, eficiência de custos e novas funcionalidades, tudo enquanto preservam a sua segurança e descentralização. Neste âmbito encontram-se possibilidades, nomeadamente:

Escalabilidade Melhorada: Os rollups permitem processar um grande volume de transações fora da cadeia principal (off-chain), reduzindo a sobrecarga na

blockchain do Bitcoin, que está limitada a cerca de 7 transações por segundo, permitindo aumentar significativamente a capacidade da rede;

Custos Reduzidos: Ao agregar múltiplas transações numa única submissão à blockchain principal, os rollups diminuem as taxas por transação, tornando a utilização do Bitcoin mais económica, especialmente em períodos de alta procura;

Manutenção da Segurança: Os rollups utilizam a blockchain do Bitcoin para disponibilidade de dados e liquidação final, aproveitando a sua robusta segurança e descentralização, sem comprometer os princípios fundamentais do protocolo;

Funcionalidades Avançadas: Permitem a introdução de capacidades como contratos inteligentes e maior privacidade através de ambientes de execução alternativos (ex.: validity rollups), mantendo a compatibilidade com o Bitcoin nativo;

Flexibilidade sem Riscos Adicionais: Soluções como os sovereign rollups usam o Bitcoin apenas para armazenar dados de transações (semelhante aos Ordinals), não introduzindo riscos de segurança, enquanto os validity rollups, embora requeiram um soft fork, já foram amplamente pesquisados e aplicados em outras blockchains como o Ethereum.

Porém, Qi et al (2024) sugerem que os rollups exigem funcionalidades avançadas que o Bitcoin não suporta nativamente, como gestão de estado e provas de validade, necessitando de alterações no protocolo (ex.: covenants) e consenso comunitário, difícil de alcançar devido à resistência a mudanças. A falta de contratos inteligentes nativos também dificulta sua adoção.

3.3. Técnicas de Compressão

Estas abordagens diminuem o tamanho da blockchain, facilitando a participação de nós. Alshahrani et al. (2023) demonstram que a sumarização e compressão (deflate) economizam 78,104% de espaço no Bitcoin, reduzindo requisitos de armazenamento de 500 GB para cerca de 110 GB. Zhang, et al., (2023) referem que os protocolos de compressão diminuem o tamanho das transações na propagação, permitindo que os blocos do Bitcoin suportem até 60 vezes mais transações, mantendo a descentralização intacta.

3.4. Abordagens Inovadoras

Métodos emergentes exploram tecnologias avançadas para otimizar o consenso e o desempenho.

Pawar e Patil (2023) propõem **regressão logística** para selecionar mineradores eficientes, reduzindo a latência para 0,1407 ms com 91,49% de precisão em testes no Ethereum.

Baniata et al. (2022) sugerem que **algoritmos de machine learning** poderiam adaptar o consenso Proof of Work (PoW) do Bitcoin. No artigo, os autores apresentam uma abordagem híbrida de mineração para blockchains PoW, combinando métodos clássicos e modelos de aprendizagem automática (SGDRegressor e PolynomialFeatures). A proposta foi testada com 780 mil blocos do Bitcoin, alcançando taxas de sucesso de 64,3% e 70,5%, superando os 50% dos mineradores tradicionais e reduzindo o tempo de resolução. Através dos resultados obtidos é sugerido que a machine learning pode acelerar a mineração e potencialmente controlar a rede com apenas 35,5% do poder computacional, abrindo caminho para futuras pesquisas e aplicações, incluindo em IoT.

Bulgakov et al. (2024) investigam a escalabilidade e segurança em redes blockchain, destacando o **sharding** como uma solução promissora para o Bitcoin, que enfrenta limitações de throughput em virtude do protocolo de consenso Proof of Work (PoW). Analisaram protocolos como Elastico, OmniLedger, Pyramid, RepChain e SSchain, que dividem a rede em shards para processamento paralelo de transações, aumentando a capacidade, mas introduzindo desafios como gestão de nós e consistência de dados entre shards. Apesar de o PoW do Bitcoin ser quase incompatível com sharding tradicional, o estudo propõe um modelo conceptual com sharding de

transações, estados e redes, testado numa rede Ethereum privada.
Para o Bitcoin, isso sugere que ajustes no protocolo base (ex.: covenants) e soluções híbridas poderiam melhorar a escalabilidade, mantendo a descentralização, embora sejam necessários avanços para superar a latência e vulnerabilidades. Lincopinis e Llantos (2024) abordam o KSI Cash, o sharding processa ordens de pagamento com blocos fragmentados e autenticação específica, oferecendo escalabilidade ilimitada, o Ostraka que melhora o throughput significativamente ao paralelizar nós, mas não fragmentando a largura de banda ou recursos computacionais e o RapidChain, resiliente a falhas bizantinas, otimiza latência e fragmenta comunicação, computação e armazenamento, embora seja vulnerável a ataques de particionamento.

4. Discussão

Os resultados apresentados refletem uma multiplicidade de perspetivas sobre como abordar o desafio de escalabilidade do Bitcoin, com os autores a convergirem na identificação do limite TPS como uma barreira crítica, mas divergindo nas soluções propostas e nas suas implicações para o trilema da blockchain (escalabilidade, segurança e descentralização).

Nas atualizações de protocolo, Lincopinis e Llantos (2024) e Nasir et al. (2022) concordam que o SegWit melhora a segurança contra ataques de maleabilidade, mas ambos sublinham a sua insuficiência para escalabilidade massiva, mantendo o throughput em 7 TPS. Já Kaur et al. (2024) divergem ao criticar alternativas como o aumento do tamanho do bloco (ex.: Bitcoin Cash) ou a redução do tempo de criação (ex.: Litecoin), argumentando que estas opções sacrificam a descentralização ao favorecer nós mais poderosos, uma preocupação que Nasir et al. (2022) não enfatizam tanto, focando mais nos benefícios incrementais.

Nas soluções de camada 2, Barbaravičius (2024) e Kaur et al. (2020) partilham otimismo sobre a Lightning Network, destacando o seu potencial de 1 milhão de TPS e o crescimento de adoção (6,5% em 2022 para 16,6% em 2024), impulsionado por melhorias como AMP e Wumbo Channels. Contudo, Kaur et al. (2020) apontam desafios de liquidez e roteamento, parcialmente mitigados por super nós (Alshahrani et al., 2023), enquanto Barbaravičius (2024) foca mais no progresso prático sem aprofundar essas limitações.

Nasir et al. (2022) complementam esta visão com as side-chains (ex.: Rootstock e Liquid Network), valorizando a flexibilidade, mas alertando para a dependência de validadores, um ponto de divergência com a ênfase na descentralização da Lightning. Sobre os rollups, o síio web Bitcoinrollups.io destaca a capacidade de melhorar escalabilidade e custos sem comprometer a segurança, uma visão otimista contrastada por Qi et al. (2024), que sublinham a necessidade de ajustes no protocolo (ex.: *covenants*) e a resistência da comunidade, evidenciando um obstáculo comum às soluções mais inovadoras.

Nas técnicas de compressão, Alshahrani et al. (2023) e Zhang et al. (2023) convergem na eficácia da redução do tamanho da blockchain (78% de economia de espaço e blocos até 60 vezes mais transações), preservando a descentralização. Não há divergências significativas entre eles, mas a abordagem é vista como complementar às outras soluções, não como uma resposta direta ao throughput.

Já nas abordagens inovadoras, Pawar e Patil (2023) e Baniata et al. (2022) propõem o uso de machine learning, com Pawar focando na eficiência (latência de 0,1407 ms) e Baniata testando uma abordagem híbrida no Bitcoin, sugerindo um potencial disruptivo ao reduzir o poder computacional necessário

para controlo da rede. Apesar da similaridade no uso de tecnologias avançadas, Baniata et al. (2022) exploram implicações mais amplas, como aplicações em IoT, enquanto Pawar se limita a melhorias de desempenho.

Sobre o *sharding*, Lincopinis e Llantos (2024) e Bulgakov et al. (2024) partilham a visão de que dividir a rede em *shards* aumenta o throughput via processamento paralelo, analisando protocolos. Ambos reconhecem a incompatibilidade do PoW do Bitcoin com *sharding* tradicional, mas Bulgakov et al. (2024) avançam com um modelo conceptual, enquanto Lincopinis e Llantos (2024) destacam implementações específicas como KSI Cash (escalabilidade ilimitada) e Ostraka (melhoria de throughput). Divergem, porém, nas limitações: Bulgakov foca em desafios de consistência e latência, enquanto Lincopinis enfatiza vulnerabilidades como ataques de particionamento no RapidChain.

Estas abordagens inovadoras, embora promissoras, enfrentam resistências técnicas e comunitárias semelhantes às dos rollups (Qi et al., 2024), sugerindo que o sucesso depende de superar barreiras estruturais do Bitcoin.

5. Conclusões

Esta investigação conclui que o Bitcoin, limitado a 7 TPS devido ao seu design centrado em segurança e descentralização, pode beneficiar de uma variedade de soluções de escalabilidade, cada uma com pontos fortes e desafios distintos.

As atualizações de protocolo, como o SegWit, oferecem ganhos incrementais e segurança adicional (Lincopinis & Llantos, 2024; Nasir et al., 2022), mas não resolvem a escalabilidade massiva, enquanto o aumento do tamanho do bloco compromete a descentralização (Kaur et al., 2024).

A Lightning Network destaca-se como a solução mais avançada e de adoção crescente (Barbaravičius, 2024), embora enfrente questões de liquidez (Kaur et al., 2020).

Side-chains e rollups ampliam funcionalidades e eficiência (Nasir et al., 2022; Bitcoinrollups.io), mas exigem confiança em validadores ou mudanças protocolares complexas (Qi et al., 2024). As técnicas de compressão reduzem significativamente o tamanho da blockchain (78%) e aumentam a capacidade dos blocos (60 vezes), mantendo a descentralização (Alshahrani et al., 2023; Zhang et al., 2023). Abordagens inovadoras como machine learning (Pawar & Patil, 2023; Baniata et al., 2022) e *sharding* (Lincopinis & Llantos, 2024; Bulgakov et al., 2024) mostram potencial disruptivo, com melhorias em latência e throughput, mas enfrentam barreiras técnicas e de consenso.

Os resultados revelam que nenhuma solução resolve, isoladamente, o trilema da blockchain, sugerindo que combinações — como Lightning com compressão ou *sharding* com rollups — podem ser o caminho mais viável. Contudo, a implementação enfrenta resistências devido à rigidez do protocolo Bitcoin e à aceitação da comunidade.

Desta forma, há uma clara necessidade de maior investigação para validar estas soluções em cenários práticos, desenvolver mecanismos de consenso compatíveis com o PoW, e simplificar a adoção para utilizadores finais. Trabalhos futuros devem incluir testes de larga escala, na integração de *covenants* para suportar rollups e *sharding*, e na exploração de modelos híbridos que equilibrem escalabilidade, segurança e descentralização, assegurando a relevância do Bitcoin face à sua crescente.

6. Referências

1. Alshahrani, H., Islam, N., Syed, D., Sulaiman, A., Al Reshan, M. S., Rajab, K., … Soomro, A. (2023). Sustainability in blockchain: A systematic literature review on scalability and power consumption issues. *Energies*, *16*(3), 1510. doi:10.3390/en16031510
2. Baniata, H., Prodan, R., & Kertesz, A. (2022). *Machine Learning for alternative mining in PoW-based blockchains: Theory, implications and applications*. doi:10.36227/techrxiv.21383184.v1
3. Barbaravičius, V. (2024, October 22). *Year-over-year data shows rising Lightning Network adoption*. CoinGate Blog. https://coingate.com/blog/post/lightning-network-year-over-year-data
4. Bulgakov, A. L., Aleshina, A. V., Smirnov, S. D., Demidov, A. D., Milyutin, M. A., & Xin, Y. (2024). Scalability and security in blockchain networks: Evaluation of sharding algorithms and prospects for decentralized data storage. *Mathematics*, *12*(23), 3860. doi:10.3390/math12233860
5. Fujihara, A. (2023, September 29). Theoretical considerations on bitcoin scalability problem and block size distribution. *Proceedings of Blockchain Kaigi 2022 (BCK22)*. Presented at the Proceedings of Blockchain Kaigi 2022 (BCK22), Sendai, Japan. doi:10.7566/jpscp.40.011007
6. Jain, A. K., Gupta, N., & Gupta, B. B. (2025). A survey on scalable consensus algorithms for blockchain technology. *Cyber Security and Applications*, *3*(100065), 100065. doi:10.1016/j.csa.2024.100065
7. Kaur, G., & Gandhi, C. (2020). Scalability in Blockchain: Challenges and Solutions. In *Handbook of Research on Blockchain Technology* (pp. 373–406). doi:10.1016/b978-0-12-819816-2.00015-0
8. Lincopinis, D. R., & Llantos, O. E. (2024). The current research status of solving blockchain scalability issue. *Procedia Computer Science*, *239*, 314–321. doi:10.1016/j.procs.2024.06.177
9. Nasir, M. H., Arshad, J., Khan, M. M., Fatima, M., Salah, K., & Jayaraman, R. (2022). Scalable blockchains — A systematic review. *Future Generations Computer Systems: FGCS*, *126*, 136–162. doi:10.1016/j.future.2021.07.035
10. Pawar, M. K., & Patil, P. (2025). Logistic regression for enhancing scalability of blockchain system. *Procedia Computer Science*, *252*, 146–153. doi:10.1016/j.procs.2024.12.016
11. Qi, M., Wang, Q., Wang, Z., Schneider, M., Zhu, T., Chen, S., … Hardjono, T. (2024). SoK: Bitcoin Layer Two (L2). doi:10.48550/ARXIV.2409.02650