Análise comparativa dos protocolos de consenso IBFT 2.0, QBFT e smartBFT em blockchains

Carlos Daniel Schmitt Bunn, Charles Christian Miers
ANÁLISE DE SEGURANÇA DE CREDENCIAIS SPIFFE/SPIRE E INTEGRAÇÃO COM FERRAMENTAS DE SEGURANÇA.

INTRODUÇÃO

A pesquisa foi concentrada no desempenho de arquiteturas blockchains, ambas da *hyperledger fundation*, utilizado dois modelos diferentes para comparar três consensos*: quorum byzantine fault tolerance (QBFT), istanbul byzantine fault tolerance (IBFT) e smart byzantine fault tolerant (smartBFT).* traçando as semelhanças e diferenças, a fim de desenvolver quais aspectos de cada arquitetura possui melhor qualidade de serviço dentro do aspecto esperado, elencando *throughput, payload* e latência para análise de desempenho.

DESENVOLVIMENTO

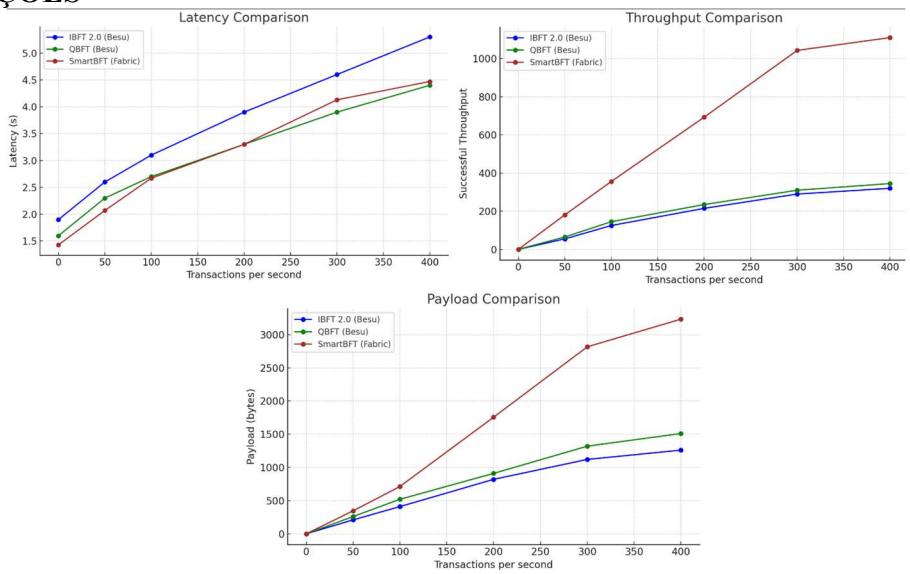
Tendo como arquitetura para a realização dos testes a máquina Babitonga, (LabP2D), as redes blockchain implementadas buscam se apresentar o mais semelhante possível, embora sejam de duas arquiteturas diferentes: *Hyperledger Besu* e *Hyperledger Fabric*. Foi adotado o uso de redes blockchain privadas, nas quais todos os participantes devem apresentar sua opinião e informações a cada nova necessidade de alteração nos dados fixos. Assim, todos os nós partem do princípio de possuírem o mesmo poder de voto na rede. Na rede *Fabric*, utilizada para executar apenas o *smartBFT*, há a possibilidade de habilitar personalizações. O *Besu*, utilizado para *IBFT 2.0* e *QBFT*, o processamento de novas alterações ocorre por meio da emulação do ambiente do Ethereum. Todas as redes exigem que pelo menos três quartos dos nós estejam de acordo sobre as informações, visando dificultar a intervenção de nós maliciosos em redes *on-chain*. A pesquisa realizada tem como objetivo analisar a diferença de desempenho quando a rede é submetida a diferentes perfis de transações. Ao correlacionar *throughput*, *payload* e latência com transações por segundo (TPS), é possível avaliar como a rede se comporta diante do aumento no número de transações e se mantém a qualidade do serviço. Essa métrica permite a comparação entre diferentes classes de serviço dentro de um mesmo contexto de análise. A observação experimental se baseou na produção e implementação destas redes sob uma carga de 400 TPS, tendo como gatilho de processamento o TPS e analisando o tempo de processamento quando um novo bloco ou informação era registrado. Em média, cada rodada demandou 5 minutos, embora esse tempo variasse de acordo com a configuração dos arquivos de rede. Cada rede foi projetada para simular requisições entre duas entidades, necessitando da aprovação dos demais nós, e todas as infraestruturas contavam com quatro nós para consenso. Embora as redes possuam pequenas diferenças de configuração, esses detalhes se devem ao fato de pertencerem a projetos distinto. O *throughput* em redes blockchain refere-se ao número de transações concluídas com sucesso por segundo, representando a capacidade do sistema em lidar com altos volumes de requisições de forma eficiente e sem gerar filas ou atrasos. Um *throughput* elevado indica maior robustez do algoritmo em processar rapidamente transações mesmo sob carga crescente, enquanto valores baixos revelam limitações na estrutura de comunicação ou no modelo de execução da rede.

CONSIDERAÇÕES

A análise comparativa dos três consensos: *IBFT 2.0, QBFT e smarBFT* evidenciou diferenças marcantes nos três principais indicadores: *throughput*, latência e *payload*. O *smartBFT* destacou-se como o mais eficiente, alcançando maior *throughput* e menor latência mesmo sob altas cargas, embora com *payloads* mais robustos devido a sua arquitetura modular. O *QBFT* mostrou desempenho intermediário, com latência reduzida e capacidade de suportar mais transações por bloco, graças à sua estratégia de manutenção de liderança, equilibrando escalabilidade e eficiência. Por fim, o *IBFT 2.0*, embora simples e confiável, apresentou maior latência, *throughput* limitado e escalabilidade restrita, mostrando-se mais adequado para cenários de baixa demanda.

Palavras-chave:
blockchain; hyperledger Besu; hyperledger Fabric; consenso permissionado; IBFT 2.0; QBFT; smartbft; desempenho; *performance*; *throughput*; latência; *payload*; protocolos bizantinos; *byzantine fault tolerance*.

ILUSTRAÇÕES



REFERÊNCIAS BIBLIOGRÁFICAS

GITHUB. Hyperledger-SmartBFT-IBFT-2.0-and-QBFT. Disponível em: https://github.com/carlossbunn/Hyperledger-SmartBFT-IBFT-2.0-and-QBFT

Aaron, A.; Kartikasari, D. P.; Shaffan, N. H. Pengaruh algoritma konsensus raft dan smartBFT dalam teknologi blockchain dengan platform hyperledger Fabric pada lingkungan multi-vm. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, v. 9, n. 13, 2025.

Junior, Byzantine Fault Tolerant Consensus for Hyperledger Fabric. 2024. Tese (Doutorado) – University of North Carolina at Charlotte, Charlotte, 2024.

Tkachuk, R.-V.; Ilie, D.; Robert, R.; Kebande, V.; Tutschku, K. On the performance and scalability of consensus mechanisms in privacy-enabled decentralized renewable energy marketplace. *Annals of Telecommunications*, v. 79, n. 3, p. 271–288, 2024.

Zaghdoudi, B.; Butucaru, M. P. Public vs Private Blockchains lineage storage. *Cryptology ePrint Archive*, 2025. Disponível em: https://eprint.iacr.org/2024/1115

DADOS CADASTRAIS

BOLSISTA: Carlos Daniel Schmitt Bunn
MODALIDADE DE BOLSA: PIBIC-AF/CNPq (IC)
VIGÊNCIA: 09/2024 a 08/2025 – Total: 12 meses
ORIENTADOR(A): Charles Christian Miers
CENTRO DE ENSINO: CCT
DEPARTAMENTO: Departamento de Ciência da Computação
ÁREAS DE CONHECIMENTO: Ciências Exatas e da Terra / Ciência da Computação
TÍTULO DO PROJETO DE PESQUISA: Expadindo a expressividade das credenciais SPIFFE para gerenciamento de identidades em nuvem (SVID-NG)
Nº PROTOCOLO DO PROJETO DE PESQUISA: NPP3231-2023