Perspectivas em BLS e DKG para Consenso Anti-MEV na Blockchain Neo

Igor M. Coelho[4], Shili Hu[2],Mengyu Liu[2], Wang Yong Qiang[2], Hongfei Da[3], Vitor N. Coelho[1]

[1]Pesquisador Independente – Comunidade NeoResearch
Ouro Preto - MG, Brasil

vncoelho@gmail.com

[2]Research & Development Department – Neo Global Development
Shanghai, China

{hushili, liumengyu, wangyongqiang}@ngd.neo.org

[3]NEO Founder – Neo Global Development
Shanghai, China

dahongfei@neo.org

[4]Instituto de Computação – Universidade Federal Fluminense (UFF)
Niterói, RJ – Brasil

imcoelho@ic.uff.br

Abstract. *This research communication paper introduces recent advances in a Maximal Extractable Value (MEV) resistant consensus inspired by the Neo dBFT, improved with Boneh-Lynn-Shacham (BLS) and Distributed Key Generation (DKG) cryptography primitives, also requiring an extra phase on the dBFT. This combination of shared secrets with encryption techniques provides unique properties from the well-known threshold signatures, that are used for the decryption of anonymous blockchain transactions. This is an improvement upon existing consensus for the public blockchain Neo, also contributing for the introduction of a decentralized mechanism capable of generating verifiable and deterministic random numbers in smart contracts, another important feature for blockchain DApps.*

Resumo. *Este artigo de comunicação de pesquisa apresenta os avanços recentes em um consenso resistente ao Valor Extraível Máximo (MEV) inspirado no Neo dBFT, aprimorado com as primitivas de criptografia Boneh-Lynn-Shacham (BLS) e Geração Distribuída de Chaves (DKG), também exigindo uma fase extra no dBFT. Esta combinação de segredos compartilhados com técnicas de criptografia fornece propriedades únicas em relação às conhecidas assinaturas de limiar, que são usadas para a descriptografia de transações de blockchain anônimas. Isso representa uma melhoria em relação ao consenso existente para o blockchain público Neo, contribuindo também para a introdução de um mecanismo descentralizado capaz de gerar números aleatórios verificáveis e determinísticos em contratos inteligentes, outra característica importante para aplicativos descentralizados de blockchain (DApps).*

1. Introdução

A busca por aprimoramentos no ecossistema de blockchain continua em amplo crescimento desde a criação do Bitcoin [Nakamoto 2008] com seu consenso de prova de trabalho (PoW). À medida que novas aplicações descentralizadas (DApps) e modelos de negócio surgem, como a Finança Descentralizada (DeFi), consequentemente surgem novas formas de ataques. Nessa expansão, diversos projetos começam a migrar para consensos bizantinos [Lamport et al. 1982], explorando alternativas de governança em redes públicas, seja em camada 1 ou 2 [Sguanci et al. 2021], e também para redes permissionadas. O clássico algoritmo de Tolerância a Falhas Bizantinas Prática (PBFT, do inglês *Practical Byzantine Fault Tolerance*) [Castro and Liskov 1999] é considerado o primeiro algoritmo na família de consenso BFT (Tolerância a Falhas Bizantinas) resistente a falhas a resolver eficientemente o problema na prática. Ele é capaz de resistir a até f nós bizantinos de um total de $N = 3f + 1$ nós. Outras variantes são bem conhecidas na literatura, como o *Spinning BFT* e o *Redundant BFT* [Aublin et al. 2013].

Neo Smart Economy é um projeto de blockchain que estendeu o PBFT em 2014 para a gestão de um livro-razão público, focado na economia inteligente [Hongfei, Da and Zhang, Erik 2015]. O mecanismo de consenso proposto foi denominado *Tolerância a Falhas Bizantinas Delegadas* (dBFT), capaz de agregar transações de uma *mempool* ponto a ponto (P2P) em blocos e fornecer uma ordem total [Coelho et al. 2020]. Ele também permite que um conjunto de N nós independentes seja eleito em uma rede descentralizada por meio de um processo de votação *permissionless* baseado em tokens. Sua implementação de consenso atual em produção (Main Net) é o dBFT 2.0, e ela conta com o clássico Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA, do inglês *Elliptic Curve Digital Signature Algorithm*) denominado NIST-P256 para garantir comunicação segura, tomada de decisões e consolidação de estado. O formato atual de transação é baseado em texto simples, portanto está sujeito a ser sobreposto por agentes maliciosos e ataques de *Maximal Extractable Value* (MEV).

O principal objetivo deste trabalho é introduzir um consenso resistente ao MEV [Malkhi and Szalachowski 2022] que é adaptado do Neo dBFT. A motivação para desenvolver algoritmos anti-MEV pode ser vista como uma comparação entre os protocolos http e https, principalmente para melhorar a privacidade, da mesma forma que os padrões modernos proíbem o uso de http devido à sua forma insegura de texto simples de habilitar a comunicação entre provedores. No cenário de blockchain, uma transação pode ser vista como o pacote de comunicação essencial no qual os usuários registram, requerem e extraem informações de um livro-razão distribuído. Atualmente, quase todas as transações que existem em blockchains públicos amplamente utilizados são legíveis e seus resultados podem ser previstos antes da inserção final no livro-razão. Ao conhecer o resultado esperado, agentes MEV podem manipular a ordem das transações, buscando definir a posição mais lucrativa desta transação no registro do blockchain, conhecida como ataques MEV.

Neste trabalho em colaboração a equipe de desenvolvimento do Neo, o mecanismo de consenso Neo dBFT 2.0 é aprimorado com o uso de um esquema de limiar clássico [Das and Ren 2023], combinando o uso da Geração Distribuída de Chaves (DKG) [Frankel et al. 1998] e primitivas Boneh-Lynn-Shacham(BLS) [Boneh et al. 2001]. Levando em consideração a disponibilidade desses novos mecanismos pelo consenso, este artigo também introduz uma melhoria na geração do campo de número aleatório do bloco

de maneira verificável, o que é amplamente utilizado por DApps.

Dois conceitos-chave neste trabalho são DKG e BLS. A criptografia DKG pode ser vista como um procedimento que permite que múltiplas partes gerem colaborativamente um par de chaves público/privado compartilhado de forma descentralizada [Kate and Goldberg 2009]. Este processo é fundamental para a criação de sistemas nos quais a confiança é distribuída entre os participantes, como em computação segura multi-party e sistemas de criptografia de limiar. As aplicações de DKG podem melhorar a segurança de sistemas distribuídos. Ao permitir uma maneira de distribuir responsabilidades entre múltiplas entidades, o DKG ajuda na criação de infraestruturas mais resilientes contra pontos únicos de falha ou ataques. Historicamente, a maioria dos casos de uso de DKG foi realizada em condições síncronas. No entanto, a necessidade recente de sistemas blockchain, em particular aqueles inspirados em protocolos BFT, requer atenção extra para o Asynchronous DKG seguro (ADKG) [Abraham et al. 2021]. Para simplificar, mantemos o termo como DKG ao longo deste artigo. Outra técnica fundamental é a criptografia BLS, que foi introduzida por Dan Boneh, Ben Lynn e Hovav Shacham, e refere-se a um esquema de assinatura digital que permite a verificação da autenticidade de um signatário. As assinaturas BLS têm propriedades particulares para agregação de assinaturas de forma que múltiplas assinaturas possam ser combinadas [Boneh et al. 2004].

As principais contribuições alcançadas durante este trabalho são: (i) o projeto de um mecanismo anti-MEV para uma rede blockchain pública; (ii) a combinação de DKG e BLS no processo de decisão realizado pelos agentes BFT; (iii) a extensão de um algoritmo de consenso consolidado ao introduzir uma nova fase; (iv) o projeto de uma função aleatória verificável para fornecer entropia para DApps.

2. Conceitos gerais

2.1. Estado atual dos algoritmos de MEV

O *Maximal Extractable Value* (ou *Miner* [Judmayer et al. 2023]) refere-se ao lucro que pode ser obtido por um minerador ou validador quando ele usa sua influência para reordenar ou filtrar transações. Normalmente, vários bots automáticos monitoram o fluxo da rede para detectar oportunidades de extrair valor de transações de blockchain em andamento que ainda não foram finalizadas, por meio de *frontrunning* ou até mesmo *backrunning* de uma transação específica antes que ela seja incluída definitivamente no livro-razão. O *frontrunning* é às vezes alcançado ao enviar transações com taxas mais altas ou até mesmo subornando as partes interessadas responsáveis pela tomada de decisões. Na literatura, também há referências ao Valor Extraível do Blockchain como um conjunto de oportunidades que não são exploradas apenas por mineradores, mas também por usuários, e não se limitam apenas ao uso de *frontrunning* [Qin et al. 2022]. O MEV aumentou em atividade, trazendo desafios para o crescimento das DeFi e dos mecanismos de consenso inspirados em BFT.

2.2. BLS e DKG para Blockchain

A criptografia BLS encontrou aplicações generalizadas em vários projetos de blockchain [Tanwar 2022]. Assinaturas independentes produzidas a partir de curvas BLS podem ser agregadas a partir de múltiplas mensagens em uma única assinatura, melhorando a escalabilidade e eficiência. A natureza determinística das assinaturas BLS garante que

elas sejam não maleáveis [Bowe et al. 2020]. As assinaturas BLS também podem atender à importante necessidade de sistemas blockchain capazes de gerar números aleatórios descentralizados e confiáveis. Por meio de primitivas criptográficas conhecidas como Funções Aleatórias Verificáveis (VRFs) [Micali et al. 1999], as assinaturas BLS podem garantir a aleatoriedade em diferentes casos de uso (especialmente, em DeFi).

DKG facilita funcionalidades como assinaturas de limiar, onde um subconjunto de participantes pode assinar em nome de todo o grupo, adicionando assim flexibilidade e eficiência às operações seguras [Pedersen 1991]. Nesse sentido, desempenha um papel fundamental em aprimorar a segurança e a descentralização dos ecossistemas de blockchain e DLT. Usando tais esquemas de limiar, uma transação ou ação no blockchain requer um número mínimo de assinaturas de um grupo pré-definido de participantes antes que possa ser executada.

3. Proposta de consenso dBFT anti-MEV com criptografia BLS DKG

O consenso atual do Neo dBFT 2.0 possui três fases, nas quais a primeira rodada contém uma proposta (feita pelo Orador) para os dados que serão incluídos no próximo bloco. As duas fases restantes são usadas para garantir um acordo global entre os validadores dos nós de consenso, respeitando a *liveness* e a *safety* da rede diante de um número máximo de f Nós de Consenso (CNs) maliciosos. A melhor compreensão de detalhes da adaptação do consenso baseado em BFT pode exigir conceitos de [Coelho et al. 2020].

Estas são as modificações principais propostas:

(M.1) modificar a confirmação da proposta do nó *Speaker* de uma curva ECDSA tradicional para um BLS DKG (também usado como um VRF);
(M.2) descriptografar o conjunto de transações encriptadas (utilizando criptografia AES) enviando um fragmento para essa descriptografia em vez da assinatura do bloco na Fase 3, conhecida como fase de *commit* no dBFT2.0
(M.3) introdução de uma Fase informativa adicional, definida como Fase de Agregação (*Aggregation Phase*), na qual um bloco final determinístico é calculado com base no resultado da Fase 3, assim, enviando uma assinatura final para um bloco compatível com o padrão de rede Ethereum.

Experimentos conduzidos no repositório `https://github.com/txhsl/tpke` verificaram a viabilidade prática da criptografia para a implementação existente do Neo em linguagem Go. Esse experimento foca na estrutura básica de decodificação de transações do protocolo e respectivo uso de assinaturas digitais com DKG.

O conjunto de experimentos foi executado em um AMD Ryzen 9 7945HX 2.50GHz, 64GB DDr5, WIN11. As implementações foram feitas na linguagem Go, para preservar a compatibilidade com os clientes de nós existentes do Neo e Ethereum. O tempo médio para configurar o DKG foi de 115 milissegundos. O tamanho do fragmento de descriptografia das chaves AES é definido como 48 bytes, enquanto a assinatura no pré-cabeçalho é de 96 bytes. Transações criptografadas grandes, com um tamanho total de 1MB, são consideradas. Ao considerar uma lista de 1000 transações, o tempo médio para gerar uma parcela de descriptografia é de 68 milissegundos, enquanto o tempo para agregá-las e resolver a descriptografia de limiar é de 116 milissegundos. Finalmente, o tempo médio para assinar um determinado pré-cabeçalho com tamanho de 5MB é de 2

milissegundos, e o tempo médio para obter uma assinatura com M assinaturas é de 5 milissegundos. As chaves AES são resolvidas em um tempo médio de 112 milissegundos. De acordo com esses valores, não há gargalos substanciais relacionados a essas operações criptográficas. É considerado que o tempo relatado é rápido em relação a outras operações que os nós de consenso precisam realizar ao participar do processo de decisão descentralizado (atualmente, o dBFT 2.0 está configurado para produzir blocos a cada $15s$). A Figura 1 apresenta o funcionamento proposto da quarta fase, com notação de [Coelho et al. 2020]. O pedido é inicialmente enviado pela réplica 1, respostas dada pelas 0 e 2, com *timeouts* nas 0 e 1, e posterior recuperação (em azul) com a conclusão do bloco parcial $pBlock$. A replica 3 se encontra falha. Finalmente, as amarelas decriptam o bloco final $Block$ na quarta e última fase.

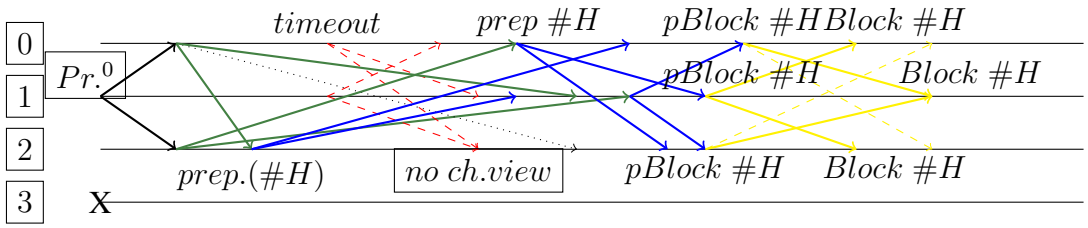

Figura 1. Processo básico de consenso, onde linhas mostram mensagens trocadas, sendo as amarelas da última fase proposta

4. Considerações Finais

Este artigo de comunicação de pesquisa aborda um problema desafiador das tecnologias blockchain, relacionado à capacidade que validadores de blocos e partes interessadas têm de selecionar a ordem das transações em favor de interesses econômicos, conhecido como MEV. Sua solução requer o design de mecanismos para fornecer privacidade às transações até que sua ordem e inclusão no livro-razão estejam completamente definidas. Para resolver esse problema, este artigo apresenta um mecanismo inovador para o consenso Neo dBFT 2.0, adicionando uma fase extra a ele com o uso de primitivas criptográficas bem estabelecidas (DKG baseado em BLS). Finalmente, buscamos trazer à comunidade brasileira avanços recentes no projeto de código-aberto Neo Blockchain, detalhando os desafios do MEV e estratégias em desenvolvimento como o proposto mecanismo anti-MEV.

Referências

Abraham, I., Jovanovic, P., Maller, M., Meiklejohn, S., Stern, G., and Tomescu, A. (2021). Reaching consensus for asynchronous distributed key generation. In *Proceedings of the 2021 ACM Symposium on Principles of Distributed Computing*, pages 363–373.

Aublin, P., Mokhtar, S. B., and Quéma, V. (2013). Rbft: Redundant byzantine fault tolerance. In *2013 IEEE 33rd International Conference on Distributed Computing Systems*, pages 297–306.

Boneh, D., Lynn, B., and Shacham, H. (2001). Short signatures from the weil pairing. In Boyd, C., editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 514–532, Berlin, Heidelberg. Springer Berlin Heidelberg.

Boneh, D., Lynn, B., and Shacham, H. (2004). Short signatures from the weil pairing. *Journal of Cryptology*, 17(4):297–319.

Bowe, S., Chiesa, A., Green, M., Jain, A., Miers, I., and Tromer, E. (2020). Scalable multi-signatures for blockchain applications. In *Proceedings of the ACM Conf. on Computer and Communications Security*.

Castro, M. and Liskov, B. (1999). Practical byzantine fault tolerance. In *OSDI*, volume 99, pages 173–186.

Coelho, I. M., Coelho, V. N., Araujo, R. P., Yong Qiang, W., and Rhodes, B. D. (2020). Challenges of pbft-inspired consensus for blockchain and enhancements over neo dbft. *Future Internet*, 12(8).

Das, S. and Ren, L. (2023). Adaptively secure bls threshold signatures from ddh and co-cdh. Cryptology ePrint Archive, Paper 2023/1553. `https://eprint.iacr.org/2023/1553`.

Frankel, Y., MacKenzie, P. D., and Yung, M. (1998). Robust efficient distributed rsa-key generation. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 663–672.

Hongfei, Da and Zhang, Erik (2015). Neo: A distributed network for the smart economy. Technical report, NEO Foundation.

Judmayer, A., Stifter, N., Schindler, P., and Weippl, E. (2023). Estimating (miner) extractable value is hard, let's go shopping! In Matsuo, S., Gudgeon, L., Klages-Mundt, A., Perez Hernandez, D., Werner, S., Haines, T., Essex, A., Bracciali, A., and Sala, M., editors, *Financial Cryptography and Data Security. FC 2022 International Workshops*, pages 74–92, Cham. Springer International Publishing.

Kate, A. and Goldberg, I. (2009). Distributed key generation for the internet. In *2009 29th IEEE International Conference on Distributed Computing Systems*, pages 119–128.

Lamport, L., Shostak, R., and Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401.

Malkhi, D. and Szalachowski, P. (2022). Maximal extractable value (mev) protection on a dag. *arXiv preprint arXiv:2208.00940*.

Micali, S., Rabin, M., and Vadhan, S. (1999). Verifiable random functions. In *40th annual symposium on foundations of computer science (cat. No. 99CB37039)*, pages 120–130. IEEE.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Accessed on February 06, 2024.

Pedersen, T. P. (1991). A threshold cryptosystem without a trusted party. In *Proceedings of the EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science*.

Qin, K., Zhou, L., and Gervais, A. (2022). Quantifying blockchain extractable value: How dark is the forest? In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 198–214. IEEE.

Sguanci, C., Spatafora, R., and Vergani, A. M. (2021). Layer 2 blockchain scaling: A survey. *arXiv preprint arXiv:2107.10881*.

Tanwar, S. (2022). Basics of cryptographic primitives for blockchain development. In *Blockchain Technology: Theory to Practice*. Springer.