Análise dos métodos para consenso distribuído aplicados à tecnologia Blockchain

João Henrique Faes Battisti[1], **Charles Christian Miers**[1]

[1]Departamento de Ciência da Computação
Universidade do Estado de Santa Catarina (UDESC)

joaobattisti@gmail.com, charles.miers@udesc.br

Resumo. *A adesão massiva a sistemas de comércio eletrônico implicou em um aumento da dependência das instituições financeiras para realização do processamento de pagamentos eletrônicos. Como uma solução alternativa, destaca-se a tecnologia Blockchain que foi elaborada sem a necessidade desta confiança centralizada, mas sim dependente de tecnologias seguramente encadeadas nas quais clientes e vendedores possam realizar negociações seguras. A tecnologia Blockchain utiliza um conjunto de diversas tecnologias conhecidas como: criptografia, matemática, algoritmos, redes Peer-to-peer (P2P), métodos de consenso distribuído e um padrão econômico. Entretanto, para todo aumento de eficiência e controle há um contra-ponto, neste caso há um custo computacional elevado realizado pelos mineradores que são recompensados pelo seu trabalho. O objetivo deste artigo é realizar uma revisão sobre a tecnologia Blockchain, analisando os diferentes modelos de métodos de consenso distribuído.*

1. Introdução

A dependência por pagamentos eletrônicos tem crescido e aos poucos vem superando o comércio local. Com este crescimento a problemática dos comércios eletrônicos ampliase, que é a dependência quase exclusiva de instituições financeiras para processar estas transações. A partir deste contexto surgiu o Bitcoin como uma nova proposta de pagamento digital que utiliza criptografia no lugar das instituições financeiras clássicas. Assim, o Bitcoin, que é uma solução baseada na tecnologia Blockchain, permite que de modo seguro duas ou mais pessoas realizem processos de negócios sem a necessidade de uma parte de confiança [Nakamoto 2008].

A tecnologia Blockchain é basicamente um *livro-razão* com todas as transações realizada e executadas pela tecnologia. A tecnologia tem crescido constantemente através de *mineradores* que incluem novos blocos[1]. O Blockchain surgiu como solução pra problemas de segurança e desempenho dos sistemas distribuídos.

O Blockchain desde seu desenvolvimento apresentou versatilidade, permitindo que seja utilizado em diversos setores como: industrial, governamental, financeiro, saúde e *etc* [Swan 2015]. A questão da utilização do Blockchain é seu custo computacional, que é considerado alto por utilizar criptografia e mecanismos que geram provas de confiabilidade. A partir desta questão foram desenvolvidos outros métodos de consenso que

[1]Um bloco é uma estrutura que faz parte do Blockchain, ele é composto com cabeçalho com as principais informações e o corpo com as transações já realizadas

realizam o processo de confiabilidade, estes métodos possuem custos computacionais inferiores que o *Proof of Work* (PoW)[2].

Com esta problemática e com métodos que viabilizam o uso do Blockchain, o presente trabalho visa realizar uma análise dos principais métodos de consenso, suas características e a relação de cada um deles no uso em paralelo com diferentes tecnologias. Assim, tem-se o objetivo de propor a classificação de métodos de consenso conforme a necessidade do usuário, avaliando o seu desempenho, consumo de energia e de recursos computacionais.

2. Conceitos básicos sobre Blockchain

O Blockchain é um conjunto de tecnologias, como: criptografia, algoritmo, P2P, consenso distribuído na solução de problemas e também um padrão econômico de segmento [Lin and Liao 2017]. A tecnologia Blockchain é basicamente um *livro-razão* com todas as transações realizadas e executadas usando Blockchain. Seu crescimento é constante através dos mineradores[3] que incluem novos blocos com sucesso, o sucesso destes blocos é adquirido através do consenso distribuído[4].

O mecanismo de consenso distribuído permite construir um ambiente praticamente inviolável, no qual as transações de qualquer ativo digital são verificadas por uma gama de participantes/colaboradores autênticos [Swan 2015]. Através do uso de criptografia, blocos de transações são encadeados conjuntamente para possibilitar a imutabilidade dos registros. Assim, o Blockchain opera como um livro de razões no qual os registros são facilmente verificáveis, mas as abordagens criptográficas empregadas tornam difícil de ser explorada por um atacante.

Segundo [Lin and Liao 2017] o Blockchain possui seis aspectos básicos: Descentralização, transparência, Verificação e desenvolvimento abertos, autonomia, imutabilidade e anonimato. Além disso, tem como base de criação quatro fundamentos: (i) registro compartilhado das transações, (ii) consenso para verificação das transações, (iii) um contrato que determina as regras de funcionamento das transações e (iv) emprego de criptografia. [Corporation 2018]. Sendo que para realizar qualquer forma de alteração do que foi acordado e registrado no bloco, há a necessidade de um novo consenso, tornando-o desta forma a tecnologia mais segura e confiável.

3. Consenso Distribuído

Em sistemas distribuídos um dos problemas mais conhecidos é o do consenso, em que há garantias de acordos de maneira ”democrática”, acordos estes que garantem a confiabilidade do que é acordado e distribuído. O consenso tem a função de garantir que os participantes concordem, através de provas, que alcancem decisões em comum e consigam a veracidade do sistema.

Há vários processos para obter o consenso Blockchain, que são eles: *Proof of Work*(PoW) [Nakamoto 2008], *Proof of Stake*(PoS) [Kostarev 2017], *Delegate Proof*

[2]É um mecanismo de consenso , que trabalha para solucionar uma função de *Hash*.

[3]Mineradores são grupos de pessoas que recebem taxas e subsídios a partir da geração de novos blocos.

[4]Consenso Distribuído é o alcance da confiabilidade do sistema de acordo com uma maioria, mesmo que haja presentes processos criminosos.

of Stake(DPoS) [Kostarev 2017], *Leased Proof of Stake*(LPoS) [Kostarev 2017], *Practical Byzantine Fault Tolerance*(PBFT) [Castro and Liskov 1999], *Proof of Importance*(POI) [Kostarev 2017], *Ripple* [Schwartz et al. 2014] e *Tendermint* [Kwon 2014]. A Tabela 1 lista os diferentes métodos de consenso, comparando-os com base em duas funcionalidades: Gerenciamento do nó e Economia de Energia.

Funcionalidades	Gerenciamento do Nó	Economia de Energia
PoW	Aberto	Não
PoS	Aberto	Parcial
DPoS	Aberto	Parcial
LPoS	Aberto	Parcial
PBFT	Permissão	Sim
PoI	Aberto	Sim
Ripple	Aberto	Sim
Tendermint	Permissão	Sim

Tabela 1. Tabela de Comparação entre Algoritmos de Consenso do Blockchain.

Para cada modelo do Blockchain existe uma situação que é mais benéfica determinado algoritmo de consenso, como por exemplo o *Bitshares*, plataforma de *SmartContracts*, que adota o algoritmo DPoS enquanto o *Bitcoin* utiliza PoW. Diferenças estas que ressaltam a necessidade de análises e estudos para compreensão, de forma específica, sobre o modelo aplicado em determinadas situações e recursos requeridos.

4. Problema

A tecnologia Blockchain tem mostrado uma considerável versatilidade, versatilidade esta quem tem atraído interesse de diversos setores, como os industriais, finanças, saúde, serviços públicos e agências governamentais. Porém, a tecnologia possui algumas adversidades principalmente pelo seu alto custo computacional e questões ligadas a segurança variando pelo propósito que a tecnologia será aplicada. Desta forma, torna necessário o estudo de viabilidade de quais tecnologias devem ser aplicadas com o Blockchain, levando em conta análise de modelo aplicado, versão e algoritmo de consenso que proporcionam benefícios a custos computacionais reduzidos.

4.1. Definição do problema

Atualmente, há uma considerável demanda por aplicações da tecnologia Blockchain em diferentes contextos e realidades de usuários. Quanto a estas aplicações do Blockchain, busca-se melhorar a eficiência da tecnologia e também qualidade, mas há uma preocupação ligada ao alto custo computacional que é necessário para aplicação do Blockchain. Neste sentido, percebe-se que, há diversas metodologias de consenso que realizam o processo de validação do Blockchain, mas não foi encontrado estudos que definem exatamente quais as características que tornam determinada metodologia a melhor escolha para determinadas aplicações.

O problema, então, consiste em desenvolver uma análise que apresente os diferentes métodos que existem para o consenso e suas principais características que tornam o método atrativo para aplicação. Por exemplo, a viabilidade de aplicar o método *DPOS* ou o método *POW*, sendo que implica também a utilização de um modelo público ou privado e também o grau de confiabilidades existentes em seus pares. A escolha de qual tecnologia aplicada pode produzir resultados satisfatórios em ambos os casos e com variabilidade no seu custo computacional. A partir disto, torna-se necessário que haja esta análise junto com as variáveis de aplicação.

4.2. Proposta

A tecnologia Blockchain tem apresentado considerável versatilidade no contexto de possíveis aplicações, tornando-se benéfica para diferentes contextos, *e.g.*, contratos inteligentes, nuvens computacionais, internet das coisas e *etc*. A utilização do Blockchain de forma paralela a estas tecnologias tem proporcionado um ambiente íntegro, seguro, descentralizado e transparente.

A proposta consiste em analisar os métodos para obtenção de consenso, definidos na Seção 3. A realização desta análise será baseada nos possíveis usos da tecnologia Blockchain em paralelo com outras aplicações, no intuito de identificar as melhores alternativas para aplicação de cada metodologia em diferentes contextos do uso do Blockchain. As diretrizes seguidas por esta proposta contém considerações sobre questões de desempenho, custo computacional, custo monetário, segurança e viabilidade da aplicação. Quanto aos critérios de análise, os seguintes foram elencados: Finalidade da Tecnologia; Versão do Blockchain; Modelo Blockchain; Gerenciamento do Nó; Controle do Nó; Economia de Energia; e Possíveis Vulnerabilidades e Ataques.

5. Considerações & Trabalhos futuros

Este presente trabalho tem como objetivo propor o desenvolvimento de análise como solução para a questão da problemática. A proposta visa analisar diferentes métodos de consenso existentes, suas características e as soluções tecnológicas que podem ser aplicadas. Desta forma, este aprofundamento traz benefícios de maior compreensão para seus usuários e seus pares, garantindo maior eficiência, confiabilidade e satisfatoriedade para os mesmos.

A proposta será aplicada em um trabalho de conclusão de curso, permitindo que pessoas interessadas em aplicar a tecnologia Blockchain possam seguir métricas para a escolha da metodologia mais adequada para seu projeto.

Agradecimentos: Os autores agradecem o apoio do LabP2D/UDESC e a FAPESC.

Referências

Castro, M. and Liskov, B. (1999). Practical Byzantine Fault Tolerance.

Corporation, I. B. M. (2018). Blockchain.

Kostarev, G. (2017). Review of blockchain consensus mechanisms.

Kwon, J. (2014). Tendermint: Consensus without Mining.

Lin, I.-C. and Liao, T.-C. (2017). Survey of blockchain security issues and challenges.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Schwartz, D., Youngs, N., and Britto, A. (2014). The Ripple Protocol Consensus Algorithm.

Swan, M. (2015). Blockchain: Blueprint for a new economy.