**Nome:** Arthur Siwerski Stachowski

**Nome:** João Victor Bezerra de Lima

**Data:** quarta-feira, 2 de outubro de 2024 (02/10/2024)

**Atividade de Segurança da Informação – 3ºF**

**Fichamento sobre Blockchain**

# **1 FICHAMENTO**

Pode-se definir o conceito de “blockchain” como uma tecnologia de estrutura de dados que envolve criptografia e que permite realizar transações de moeda virtual de modo relativamente seguro e sem a necessidade de uma parte mediadora a que se centraliza a responsabilidade de garantir a segurança. Todos os processos envolvendo bitcoins são fundamentados no mecanismo blockchain.

Embora a ideia de uma moeda virtual remeta à década de 1980, havia muitas dificuldades para implementar um sistema assim. Por exemplo, precisaria se fazer algo para evitar que o mesmo dinheiro fosse usado duas vezes. Uma inovação importante ocorreu em 1997, quando Adam Back sugeriu o uso do conceito de hashcash. Mas foi em 2009 que, pela primeira vez, a bitcoin foi implementada, resolvendo a maioria dessas questões com o uso de blockchain.

De forma resumida, o conceito de blockchain se baseia no mecanismo de consenso, em que todas as partes devem concordar uma única vez e funcionar apesar dos chamados “nodes maliciosos” que podem surgir. Os benefícios incluem a confiança decentralizada, o aspecto econômico, a transparência e a eficiência.

Contudo, há também desafios a serem solucionados, por exemplo, na questão da privacidade. Isso se dá porque não é possível obter transparência e privacidade ao mesmo tempo, e o blockchain opta pela transparência.

**2 COMO FUNCIONA O BLOCKCHAIN**

O mecanismo blockchain se baseia em blocos, como indica o nome. Blocos são transações empacotadas e organizadas de forma lógica, contendo referências a blocos anteriores (exceto no caso do chamado “genesis block”, que é o primeiro). Portanto, trata-se de uma corrente de blocos.

A transação de bitcoin em blockchain ocorre da seguinte maneira: 1) um node começa a transação usando a private key; 2) ocorre a validação com o protocolo Gossip; 3) a transação é incluída em um bloco, sendo assim já considerada confirmada; 4) então é confirmada pela segunda vez (a primeira no bloco); 5) depois, a transação é reconfirmada a cada bloco criado, sendo considerada finalizada após a sexta confirmação.

**3 ANÁLISE DO GRUPO**

O blockchain abre o caminho para a negociação com moedas virtuais (bitcoin), o que garante mais liberdade e acompanha o passo das tecnologias modernas, da tendência de se fazer as coisas virtualmente, e portanto deve ganhar mais espaço no futuro, com a expectativa de ser popularizada a ponto de substituir o dinheiro físico um dia.