BLOCKCHAIN E SEGURANÇA DA INFORMAÇÃO - FORTRESS OF SECURITY

Carlos Eduardo da Silva Soares
Edgar Yukio Ishibashi
Silvio Cesar Bogsan
Vagner Gonçalves Martins
Victor Hugo Fernandes Rodrigues

RESUMO

Este trabalho tem como finalidade, explanar o seguimento da Segurança da Informação, com foco em *cibersecurity* (segurança cibernética) numa abordagem dentro da tecnologia Blockchain e suas transações, com o intuito de mostrar um panorama do mercado atual e como a proteção a dados e informações têm sido algo crucial nas culturas organizacionais e requisitos de regulamentações.

Palavras-chave: Blockchains, Cibersegurança, Segurança, Criptomoeda, Bitcoin**.**

ABSTRACT:

This work aims to explain the follow-up of Information Security, focusing on cybersecurity in an approach within the Blockchain technology and its transactions, in order to show an overview of the current market and how data protection and information has been crucial in organizational cultures and regulatory requirements.

Keywords: Blockchains, cybersecurity, Cryptography, Bitcoin**.**

INTRODUÇÃO

Nunca se tem falado tanto em Segurança da Informação como atualmente, na chamada Era dos dados digitais, em que através da *Internet* ocorrem milhares de transações de dados e informações por minuto, tudo está cada vez mais rápido. No entanto, a pergunta que surge é: O quão seguro estão os dados e as informações? Sensíveis ou não, esses dados e essas informações precisam ser protegidos, e o seu vazamento ou dano pode gerar prejuízos enormes a organizações, mercados, serviços e principalmente aos usuários a quem pertence.

Para fomentar ainda mais esse segmento, surgiu em 2008 uma nova tecnologia chamada *Blockchain* que era palco das transações da então criada criptomoeda *Biticoin* (BTC). Se tornou comum aliar essa tecnologia apenas ao mundo das criptomoedas, mas o que faz a *Blockchain* ser tão seguro? E esta tecnologia está limitada somente ao *Biticoin*?

A resposta é não! O *Blockchain* é uma tecnologia que está muito além das moedas digitais e hoje tem sido usada para diversas finalidades, sua transparência e segurança tem a tornado uma plataforma muito útil para validações e autenticação de dados em sistemas e organizações.

Este documento, tem como objetivo, trazer uma abordagem sobre o que estar por trás do *BlockChain* e como sua segurança tem sido vista no mercado atual, e de que forma vem sendo aplicada.

1 O QUE É BLOCKCHAIN?

O *Blockchain* é uma tecnologia em crescimento e atualmente tem uma força muito significativa no mercado, principalmente quando falamos em criptomoedas. Mas o que é *Blockchain*? Também chamado de “Cadeia de blocos” em sua tradução literal, o *Blockchain* é um livro-razão imutável e compartilhado que facilita o processo de registro de transações e rastreamento de ativos em redes corporativas, ou seja, é uma rede descentralizada que permite transações de ativos de valor de forma rastreável, imutável e segura.

Esses ativos podem ser tangíveis (casas, carros, dinheiro, terrenos) ou intangíveis (direitos de propriedade intelectual, patentes, direitos autorais e marcas). Além disso, quase todos os itens valiosos podem ser rastreados e negociados na rede *Blockchain*, o que reduz os riscos e custos para pessoas que desejam realizar negociações. Ainda, a segurança do *Blockchain* através da sua

ISSN 2965-5285

imutabilidade e transparência permite sua disseminação de forma positiva e hoje está além do mundo das moedas digitais.

2 *BLOCKCHAIN* É SEGURO?

A segurança do *Blockchain* é baseada em criptografia, tecnologia de *Hash*, imutabilidade e transparência, e isso tem o tornado um sistema cada vez mais seguro e confiável para usuários e empresas *Entreprise*.

Dentro do *Blockchain* todos os membros da rede precisam chegar a um consenso sobre a precisão dos dados, e todas as transações verificadas são imutáveis porque são registradas permanentemente através de um registro chamado *timestamp*, e ninguém, nem mesmo os administradores do sistema, pode excluir transações.

Aliados a outros fatores isso se torna um dos principais motivos pelos quais o *Blockchain* não precisa de órgãos intermediários para validação (como um banco, por exemplo), pois sua imutabilidade garante o registro do início ao fim das transações realizadas.

As transações são bloqueadas em conjunto em uma cadeia irreversível: a partir do início de uma transação vão se criando nós (blocos) que validam a autenticidade da transação, cada bloco adicional fortalece a verificação do bloco anterior utilizando tecnologia de *hash*, fortalecendo assim a verificação e criando uma cadeia de blocos, o que torna o *Blockchain* inviolável. Qualquer usuário da rede pode fazer essa validação, que seria diversos cálculos matemáticos que exigem uma quantidade mínima de poder computacional para serem realizados, a partir de cada validação a cadeia de blocos vai se formando até chegar ao destino da transação.

Além disso é possível verificar todas as transações, pois o *Blockchain* possui um livro de registros onde de forma transparente, todos os usuários da rede podem acessá-lo.

3 DE QUE MANEIRA SÃO FEITAS AS TRANSAÇÕES?

Transações são a forma de negociação dos ativos no *Blockchain*, essas transações são protegidas por meio de criptografia e são realizadas no modelo *peer-to-peer* (ponto a ponto). A partir do início de uma transação, cada validação se torna um bloco, vale ressaltar que, por ser uma

ISSN 2965-5285

tecnologia descentralizada, as validações podem ser feitas por quaisquer usuários que estejam na rede.

Nesse aspecto, cada bloco é composto por várias informações sobre várias transações e tem uma assinatura digital exclusiva chamada *hash* ou prova de trabalho. Essa assinatura é usada como impressão digital para o bloco e ajuda a tornar o processo mais seguro, pois tudo é criptografado. Esse *hash* é usado como um *link* entre os blocos, porque um bloco carrega seu próprio *hash* e o *hash* do bloco anterior. Desse modo, é formada uma cadeia ou cadeia que liga várias informações.

Por exemplo, vamos considerar o envio de uma criptomoeda pela rede *Blockchain*, para que isso ocorra, são necessárias várias etapas, como:

- **Possuir a chave:** Primeiramente, o usuário precisa da chave pública do destinatário (empresa ou pessoa física) da transação, que pode ser criptomoeda ou *tokens*.
- **Fazer um pedido pela Internet:** O usuário informa ao sistema que deseja fazer uma transação através do *software* utilizado na *Internet*. A maneira mais fácil é usar uma carteira digital criptografada.
- **Verificar registros:** para garantir que os usuários tenham saldo suficiente para novas transações, os nós do sistema verificam os registros de transferência do remetente na rede *blockchain*.
- **Realizar registro:** Assim que a transação for confirmada pelo *blockchain*, ela será registrada no bloco de transmissão e verificada pelo nó.
- **Garanta a segurança:** Quando uma transação é enviada, ela não pode ser revogada ou alterada, pois se isso acontecer, todas as transferências de bloqueio devem ser concluídas novamente, o que exigiria um poder computacional absurdo.

4 CRIPTOMOEDAS E BLOCKCHAIN

Sempre ouvimos falar do *Blockchain* ligado ao mundo das criptomoedas e suas possibilidades, mas o que seria as criptomoedas e de onde vieram? Criptomoedas em geral é o nome genérico para moedas digitais descentralizadas, criadas em uma rede *blockchain*, a partir de sistemas avançados de criptografia que protegem as transações, suas informações e os dados de

ISSN 2965-5285

quem transaciona. Além disso, essas moedas digitais não podem ser transformadas em cédulas reais, ainda que possuam valor real.

A primeira e mais famosa criptomoeda criada foi o *Bitcoin* que surgiu em 31 de outubro de 2008, criada por Satoshi Nakamoto (pseudônimo). Além disso, por ser uma criptomoeda o *BTC* (*Bitcoin*) pode ser transferida sem o intermédio de instituições financeiras, o que abre diversas possibilidades para transações do mundo financeiro longe de burocracias e processos demorados, pois até mesmo duas pessoas mesmo morando em países diferentes, podem enviar *BTC* um para o outro sem precisar de um banco ou de uma empresa de remessa internacional.

O *Blockchain* é o que torna as transações das criptomoedas possíveis, por ser um sistema descentralizado em que a validação dessas transações pode ser feita por qualquer pessoa dentro da rede, as transações podem ser feitas a qualquer momento. Além disso, o *Blockchain*. funciona como uma espécie de banco de dados que armazena todas as informações sobre as transações *Bitcoin*, que ficam disponíveis para todos os usuários da rede.

5 OUTROS TIPOS DE TRANSAÇÕES BLOCKCHAIN

O *Blockchain* não se restringe apenas ao mundo das moedas digitais, por mais importante que seja sua ligação a isso. Além das criptomoedas, o *Blockchain* também pode ser usada para validação de documentos – como contratos e troca de ações –, transações financeiras, comercialização de músicas ou filmes, rastreamento de remessas e até votos.

Pela sua capacidade de descentralização, criptografia e principalmente imutabilidade, foi possível através do *Blockchain* facilitar modelos transacionais, não mais precisando de intermediadores. Em um sistema de troca de ativos, dinheiro por exemplo, precisa de um intermediador como um órgão bancário para validar a transação desse valor, no *blockchain* isso não se torna necessário uma vez que ao realizar a transação gera-se um *timestamp* (funciona como um registro da transação).

Antes de falarmos de outros tipos de transações, vamos entender como funciona uma transação básica na Blockchain (LEITE, 2019):

1. Maria quer enviar um ativo digital (uma criptomoeda, um contrato ou um arquivo digital) para João;

ISSN 2965-5285

2. O ativo é representado online como um bloco onde os detalhes estão armazenados;

3. O bloco é distribuído pela rede e cada máquina fica com uma cópia da transação em tempo real;

4. A rede verifica se o ativo é válido em questão de minutos;

5. Se aprovado, o bloco é adicionado a uma corrente de blocos e ganha um registro permanente na rede. Isso significa que ele não pode ser alterado;

6. A propriedade do ativo, que era de Maria, agora fica registrada na rede como sendo de João.

Ao observamos como funciona uma simples transação na *Blockchain*, é possível perceber que não há intervenção de nenhum órgão intermediário para que seja válida a transação. Isso porque quando Maria envia seu ativo digital num bloco, qualquer um no mundo que esteja conectado à rede pode fazer essa validação, essa distribuição é o que garante que a *Blockchain* seja um sistema imutável, pois cada máquina possui uma cópia exata da transação, ou seja, se algo estiver fora do lugar ou algum dado for alterado, será facilmente descoberto por toda a rede.

Nesse aspecto, o *Blockchain* hoje tem sido visto como uma tecnologia eficiente para a validação de outros ativos, como documentos. Com essa tecnologia, é possível criar redes que conectam participantes como escolas, universidades, empregadores e órgãos públicos de educação (MANCINI, 2020). A segurança da rede *blockchain* garante que os dados não sejam corrompidos, além de ser possível para qualquer usuário da rede ver as transações realizadas “assim, quando um estudante tenta inserir uma informação acadêmica na rede, é possível verificar sua veracidade e, então, fazer um registro imutável e bem criptografado nos blocos.”

Dessa forma, é possível aplicar o *Blockchain* para muito além do mundo das criptomoedas, sua segurança e transparência permite que isso aconteça. Portanto, pode-se esperar muito ainda dessa tecnologia para o futuro, com impactos relevantes para todo o mundo.

ISSN 2965-5285

6 BLOCKCHAIN PARA EMPRESAS E OUTROS MERCADOS

A *Blockchain* no início se tornou famosa através da criptomoeda *Biticoin*, é importante destacar que o setor financeiro é o que representa de certa forma uma maior preocupação com validação em transações. Isso se dá pelas inúmeras possibilidades de corrupção e violação de dados, no mundo digital isso se torna ainda mais perigoso. Dessa forma, o *blockchain* foi usado para garantir que não haja violação de segurança permitindo uma liberdade maior para transação de valores.

Atualmente, entretanto, outros mercados têm se aproveitado dessa tecnologia, um exemplo claro tem acontecido no mercado de varejo. A tecnologia é adequada ao varejo pela multiplicidade de participantes e dados envolvidos: parceiros, bancos, empresas de logística, contadores e auditorias, e inúmeros documentos tais como as Notas Fiscais associadas a cada ordem de compra, numa rede *blockchain* as validações ao mesmo tempo que estariam seguras seriam mais ágeis, tornando todo o processo de logística mais produtivo. Além disso, o artigo cita pontos atrativos para o uso dessa tecnologia, como (KAUFMAN, 2019):

(a) o compartilhamento da base de dados, informação única e acessível à todos os participantes, que não podem alterá-la (somente acrescentar informação/itens);

(b) a privacidade dos dados, acesso exclusivo aos participantes da rede (autorizados previamente, e criptografado);

(c) a obrigatoriedade de consenso, com a transação só se concretizando se todas as partes estiverem de acordo;

(d) os “contratos inteligentes” que podem ser rastreados em tempo real.

Além disso, essa cadeia de blocos simplifica os mecanismos de verificação de autenticidade dos participantes da cadeia de suprimentos (confere “certificado de autenticidade”), dessa forma, é possível trazer um equilíbrio entre segurança e agilidade de forma transparente.

Entretanto, é importante destacar que por ser uma tecnologia ainda considerada recente, nem todas as empresas estão preparadas para aderirem a *Blockchain*, há um legado a considerar e implementar novos processos na logística de gerenciamento de compra e vendas podem gerar grandes empecilhos. Nesse sentido, por mais rentável e eficiente possa ser, uma nova tecnologia como a *Blockchain* poderá representar um risco para algumas empresas, o que limita sua consolidação no mercado.

7 SEGURANÇA DA INFORMAÇÃO E BLOCKCHAIN

A *Blockchain* hoje está muito além do mercado financeiro e do mundo das moedas digitais, ela pode ser usada como ferramenta de segurança da informação. Entretanto, vale ressaltar que essa tecnologia que é contra a corrupção pela sua transparência e integridade, pode servir de escape para crimes cibernéticos como compartilhamento de pornografia infantil e compra e venda ilegal de armas. Por isso, é importante analisarmos os pontos positivos e negativos que a *Blockchain* produz.

7.1 Impactos Positivos da Blockchain

O *Blockchain* atende a todos os 3 pilares da segurança da informação: Integridade, Disponibilidade e Confidencialidade. Em todas as transações através da criptografia dos dados e tecnologia de *hash*, a integridade dos dados nas transações, além da validação delas através da própria rede. Vale ressaltar que, um usuário dentro de uma rede *blockchain* tem seu anonimato o que garante a confidencialidade tanto do usuário quanto dos dados da transação em si. Além disso, dentre outros aspectos positivos do *blockchain* se destacam:

- Transparência
- Rastreamento das transações:
- Aumentar segurança e a confiabilidade
- Descentralização

7.2 Impactos Negativos da *Blockchain*

ISSN 2965-5285

É importante ressaltar que, os impactos negativos do *blockchain* estão ligados a sua existência e a como os usuários o utilizam, isso porque como dito anteriormente, o *blockchain* é uma das tecnologias mais seguras atualmente existentes e por isso não há registros de ataques a rede em que o hacker obteve sucesso, ou até mesmo registros de alteração de informações depois que uma transação foi feita, para que isso ocorresse exigiria um poder computacional absurdo, e até hoje vem seguindo irrefutável. Portanto, dentre alguns dos impactos negativos da cadeia de blocos, destacam-se:

- Impacto ambiental
- Pornografia infantil
- Drogas, armas e crimes
- Falta de conhecimento.

8 CONCLUSÃO

O *Blockchain* é considerado hoje uma das tecnologias mais promissoras para a atualidade e para o futuro, ainda que pouco dissolvida por ser emergente, promete trazer soluções que irão impactar o mercado e as organizações. Nesse aspecto, tanto a segurança de uma solução *Blockchain*, quanto a transparência, pode levar muitas organizações a desenvolverem projetos e planos utilizando essa tecnologia.

No entanto, é considerável que o fato de ainda estar em crescimento, o *Blockchain* pode enfrentar desafios como implementação, mão de obra qualificada e credibilidade, isso porque, como é o caso de outras tecnologias emergentes como a Computação em Nuvem, ainda existem sistemas legados que não são tão simples de serem deixados de lado pois carregam consigo dados e informações que põe em risco as organizações.

Além disso, ainda que uma rede *Blockchain* seja uma arma contra a corrupção, fraudes e crimes envolvendo falsificação, por ser descentralizada e assim não necessitar de órgãos fiscais intermediários, pode gerar certas rejeições com relação a utilização desse tipo de sistema. Entretanto, isso não impede de que empresas disruptivas possam surgir e inovar padrões no mercado, como muitas vêm fazendo atualmente.

Segundo a *International Data Corporation (IDC*), estima-se que até 2024 companhias de todo o mundo invistam mais de 20 bilhões de dólares no *Blockchain*, o que representa um grande

passo na disseminação da tecnologia por todo o mundo e na usabilidade de soluções baseadas nela por empresas do globo. O que podemos esperar? Depois de mais de 10 anos de existência o *Blockchain* ainda segue firme e com grande potencial de crescimento. Além disso, segurança da informação é uma preocupação e uma necessidade para todos.

Sendo assim, as estimativas são positivas com relação a essa tecnologia, e hoje o *Blockchain* está sendo usado para fins além das transações de moedas digitais. Dessa forma, ele tem se configurado como uma ferramenta eficaz de segurança e um modelo de negócio promissor para facilitação de processos e logísticas, favorecendo o rastreamento e transparência nas negociações, além de contribuir para a validação de ciclos de vida de produtos.

REFERÊNCIAS

INFOMONEY, REVISTA. O QUE é Bitcoin?. *In*: **Guia sobre Bitcoin: conheça a origem da primeira criptomoeda do mundo**. InfoMoney, 2020. Disponível em: https://www.infomoney.com.br/guias/o-que-e-bitcoin/. Acesso em: 21 nov. 2021.

LEITE, Vitor. O que é blockchain – uma explicação simples. *In*: **O que é blockchain – uma explicação simples**. [*S. l.*], 18 ago. 2019. Atualizado em 05 nov 21. Disponível em: https://blog.nubank.com.br/o-que-e-blockchain/. Acesso em: 21 nov. 2021.

LEITE, Vitor. O que é criptomoeda? Entenda de uma vez. **O que é criptomoeda? Entenda de uma vez**. [*S. l.*], 23 abr. 2020. Atualizado em 02 ago 21. Disponível em: https://blog.nubank.com.br/o-que-e-criptomoeda/. Acesso em: 17 nov. 2021.

SHIMABUKURO, Igor. Investimentos em blockchain podem chegar a US$ 19 bilhões em 2024, diz levantamento. In: Olhar Digital. [S. l.], 26 maio 2021. Disponível em: https://olhardigital.com.br/2021/05/26/pro/investimentos-em-blockchain-podem-crescer-188-por-cento-ate-2024/. Acesso em: 4 nov. 2021.