

# **BLOCKCHAIN A DISRUPÇÃO TECNOLÓGICA NOS NEGÓCIOS**

Carlos Gustavo Lopes da Silva<sup>1</sup>  
Geisse Martins<sup>2</sup>  
William Pacheco Machado<sup>3</sup>  
Hugo Silva Ferreira<sup>4</sup>

## **RESUMO**

Com o advento dos computadores e da internet ter revolucionado o mundo, ela apresenta três importantes desafios no dia a dia da população: privacidade, segurança e inclusão, e que há muito tempo os inventores buscam soluções para esses problemas usando a criptografia. No entanto, é em 2008 que surge o *Bitcoin*, que com o seu protocolo da confiança, o *blockchain*, tem possibilitado grandes avanços com relação a solução desses problemas e promete gerar uma grande revolução. O *blockchain* é uma estrutura de dados que regista as transações a serem incluídas em um livro-razão público em blocos. Ainda focado na estrutura de segurança do *blockchain*, a segurança e a privacidade em uma rede são implementadas por meio da utilização de camadas: consenso, mineração, propagação e imutabilidade. O sistema de segurança do *blockchain* estão relacionadas aos processos de distribuição e replicação, à impossibilidade de monopólio de mineiros e de gasto duplo e ao sistema de consenso. São muitos os agentes interessados no avanço da *blockchain* e seus usos potenciais, contudo concordam que uma das grandes fragilidades é a ausência de governança que possa definir padrões, conferir segurança e credibilidade ao processo como um todo. Enquanto grandes empresas e governos estiverem interessadas em algo o ciclo de prosperidade tenderá a ser crescente.

**Palavras-chave:** *Blockchain; Bitcoin; Privacidade, Segurança; Inclusão; Moeda Virtual.*

## **ABSTRACT**

With the advent of computers and the internet having revolutionized the world, it presents three important challenges in the daily life of the population: privacy, security and inclusion, and that inventors have long sought solutions to these problems using cryptography. However, it is in 2008 that Bitcoin appears, which with its trust protocol, the blockchain, has enabled great advances in relation to the solution of these problems and promises to generate a great revolution. Blockchain is a data structure that records transactions to be included in a public ledger in blocks. Still focused on the blockchain security framework, security and privacy in a network are implemented through the use of layers: consensus, mining, propagation and immutability. The blockchain security system is

<sup>1</sup> Doutorando em Gestão e Negócios (UNISINOS). Mestre em Tecnologias Educacionais em Rede (UFSM). Especialização em Desenvolvimento de Jogos Digitais (ESTÁCIO). Pós-Graduação (MBA) em Administração Estratégica (ESTÁCIO). e-mail: cgsilva33@gmail.com

<sup>2</sup> Doutorando em Educação (Yvy Enber). Mestre em Administração de empresas pela Must University. e-mail: geisse@geisse.com.br

<sup>3</sup> Graduação em Administração de Empresas pela Universidade Castelo Branco (UCB). Especialização em Logística Empresarial pela Faculdade Internacional Signorelli. Mestrando em Administração de Empresas pela Miami University of Science and Technology (MUST UNIVERSITY). E-mail: <willianpmachado@gmail.com>

<sup>4</sup> Graduação em Administração pela UNIFAEEL. Especialização em Docência do Ensino Superior e MBA em Educação Corporativa. Mestre em Administração pela Must University. E-mail: prof.hugosferreira@gmail.com

related to the distribution and replication processes, the possibility of miners monopoly and double spending and the consensus system. There are many agents interested in the advancement of Blockchain and its potential uses, however they agree that one of the major weaknesses is the absence of governance that can define standards, provide security and credibility to the process as a whole. As long as big companies and governments are interested in something, the cycle of prosperity will tend to be growing.

**Keywords:** Blockchain; Bitcoin; Privacy, Security; Inclusion; Virtual Currency.

## Introdução

Com o advento dos computadores e da internet ter revolucionado nossas vidas, ela apresenta três importantes desafios no dia a dia da população: privacidade, segurança e inclusão e que há muito tempo os inventores buscam soluções para esses problemas usando a criptografia.

Segundo Nakamoto (2008), “*Bitcoin: A Peer-to-Peer Electronic Cash System*”, lançado em 2008 pelo autor pseudônimo Satoshi Nakamoto. Blockchain é uma tecnologia para armazenamento descentralizado de informações. Essas informações se referem a transações geradas por clientes de aplicações de arquitetura peer-to-peer (P2P).

No entanto, é em 2008 que surge o *Bitcoin*, que com o seu protocolo da confiança, o *blockchain*, tem possibilitado grandes avanços com relação a solução desses problemas e promete gerar uma grande revolução.

Podemos definir o *blockchain* como um livro razão distribuído que representa um consenso de rede de todas as transações que já ocorreram. A nova plataforma permite a reconciliação de registros digitais referentes a quase tudo em tempo real.

O princípio da integridade da rede *blockchain* considera a confiança intrínseca, não extrínseca. Assim, a integridade é codificada em cada etapa do processo e distribuída, portanto não é uma responsabilidade atribuída a um membro individual.

Para o problema levantado neste artigo, apoiado na classificação de Gil (2002), e observados os objetivos explicitados, o modelo adequado para a investigação é o da pesquisa exploratória, pois se pretende aprofundar conhecimentos a respeito da o *Blockchain* a Disrupção Tecnológica nos Negócios Geração de Empregos, Renda, Educação e Aceitação Institucional por Governos e Empresas.

## ***Blockchain: Privacidade, Segurança e Inclusão***

Com o advento dos computadores e da internet ter revolucionado nossas vidas, ela apresenta três importantes desafios no dia a dia da população: **privacidade, segurança e inclusão** e que há muito tempo os inventores buscam soluções para esses problemas usando a criptografia.

Para Braga (2017), *blockchain* é uma lista crescente de registros, também chamados de blocos ou nodes, os quais são vinculados e protegidos com criptografia. Cada bloco contém um *hash* criptográfico do bloco anterior, um *timestamp* e dados de transação. O *blockchain* está relacionado ao fato de que o sistema distribui energia por uma rede ponto a ponto sem um único ponto de controle, de modo que nenhuma parte pode desconectar o sistema. Se uma autoridade central conseguir esconder ou isolar um indivíduo ou grupo, o sistema ainda sobreviverá. Se mais da metade da rede tentar sobrepor tudo, todos verão o que está acontecendo.

O valor como incentivo visa alinhar os incentivos de todas as partes interessadas. Desse modo, no *blockchain* de *Bitcoin* o software recompensa quem trabalha nele, assim, ele pertence a quem possui e usa seus *tokens*, isso estimula que todos cuidem dele. A segurança visa incorporar medidas à rede sem nenhum ponto único de falha, de modo que fornecam não apenas confidencialidade, mas também autenticidade e não-repúdio (garantia de que o autor não pode negar alguma informação ou documento que tenha criado na rede) a todas as atividades. Qualquer pessoa que quiser participar deve usar criptografia - recusar não é uma opção - e as consequências do comportamento imprudente são exclusivas da pessoa que se comportou de maneira imprudente.

Nakamoto (2008), “O *timestamp* prova que os dados devem ter existido no tempo, obviamente, para entrar no *hash*. Cada registro de data e hora inclui o registro de data e hora anterior em seu *hash*, formando uma cadeia, com cada *timestamp* adicional reforçando os anteriores”. Os três princípios da economia *blockchain*: **privacidade, direitos preservados e inclusão**. O princípio da privacidade considera que as pessoas devem controlar seus próprios dados. Elas têm o direito de decidir o que, quando, como e quanto compartilhar sobre suas identidades com outras pessoas.

Cada bloco é validado pelo minerador (hardware utilizado para validação) por meio de um processo matemático de alta complexidade, envolvendo *hash* criptográfico (NAKAMOTO, 2008). Os direitos preservados consideram que os direitos de propriedade são transparentes e aplicáveis e as liberdades individuais são reconhecidas e respeitadas. Por fim, o princípio da inclusão considera que a economia funciona melhor quando funciona para todos. Isso significa diminuir as barreiras à participação. Significa criar plataformas para o capitalismo distribuído, não apenas um capitalismo redistribuído.

## **Blockchain: Livro Razão**

No entanto, é em 2008 que surge o *Bitcoin*, que com o seu protocolo da confiança, o *blockchain*, tem possibilitado grandes avanços com relação a solução desses problemas e promete gerar uma grande revolução. Podemos definir o *blockchain* como um livro razão distribuído que representa um consenso de rede de todas as transações que já ocorreram. A nova plataforma permite a reconciliação de registros digitais referentes a quase tudo em tempo real.

Conforme Slaughter e May (2016), o *blockchain* original do *Bitcoin* foi projetado como um livro-razão distribuído e relativamente simples, para registrar transferências de *tokens* de moeda entre participantes da rede em um ambiente semi anônimo. A distribuição de dados em um sistema *blockchain* é feita usando uma arquitetura ponto a ponto. Nesse tipo de arquitetura, cada ponto tem uma versão completa dos dados e os dados são replicados muitas vezes, um por par. Um bloco é uma estrutura de dados que registra as transações a serem incluídas em um livro-razão público. Ainda focado na estrutura de segurança do *blockchain*, a segurança e a privacidade em uma rede são implementadas por meio da utilização de camadas: consenso, mineração, propagação e imutabilidade. O sistema de segurança do *blockchain* estão relacionadas aos processos de distribuição e replicação, à possibilidade de monopólio de mineiros e de gasto duplo e ao sistema de consenso.

O valor correto descoberto pelo minerador, ou seja, o *nonce* correto ou *golden nonce*, é a prova de trabalho, ou *proof-of-work*, que o cálculo iterativo (por tentativas) foi realizado e que o bloco pode ser adicionado ao *blockchain* (AUMASSON, 2009). A aplicação do *blockchain* nos serviços financeiros têm o potencial de reduzir custos, possibilitar a utilização de contratos inteligentes, melhorar a gestão de ricos e o *compliance* (atendimento a legislação e regulamentos). A tecnologia tem o potencial de beneficiar a área da saúde, com novos modelos de gestão e de compartilhamento de registros médicos; a área da pesquisa científica, garantindo a confiabilidade dos dados; e diversas outras áreas, como o governo.

Muitas organizações já perceberam as vantagens de utilização da tecnologia *Blockchain* e já estão utilizando a tecnologia, dentre elas, podemos mencionar a *IBM*, *JPMorgan Chase*, *ANZ Bank*, *Cisco*, *Accenture*, *Intel* e *London Stock Exchange Group*. A adoção bem-sucedida do *blockchain* se torna importante nos seguintes pontos: as provas de conceito devem ser confiáveis e convincentes, é preciso entender o status atual e o impacto futuro, a nova tecnologia precisa de mais

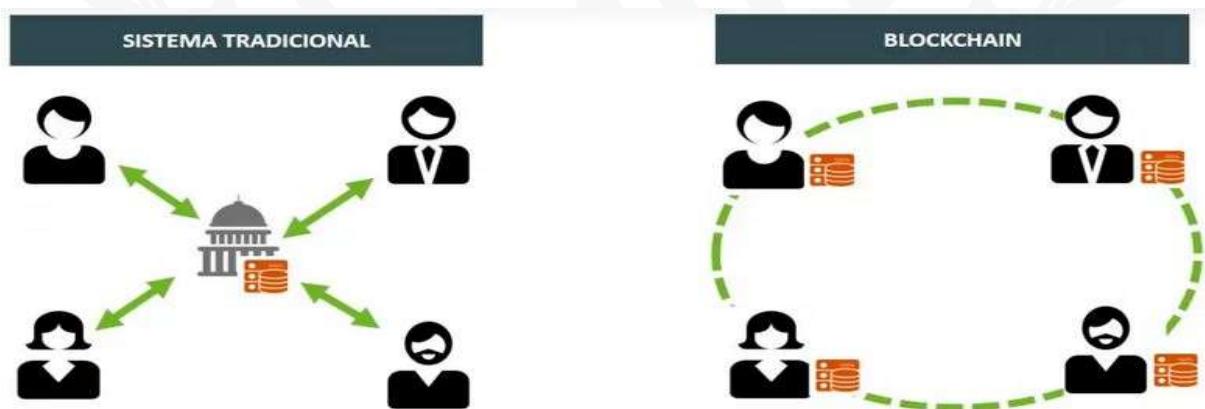
tempo para o sucesso, é preciso preencher a lacuna entre tecnologia e indústria, é necessária a atuação dos reguladores, é preciso considerar a escalabilidade e realizar acordos sobre padrões comuns.

### **Blockchain: Mercado Financeiro**

O *Blockchain* oferece um meio confiável e eficaz não apenas de eliminar intermediários, mas também de reduzir radicalmente os custos de transação, transformando empresas em redes, distribuindo poder econômico e permitindo a criação de riqueza e um futuro mais próspero. Isso ocorre porque essa tecnologia reduz os custos de pesquisa, custos de contratação, custos de coordenação e custos de construção/reconstrução da confiança.

Segundo Diniz (2017), bancos são instituições que há muito tempo investem no desenvolvimento de sistemas e tecnologia da informação, exatamente por ser a informação seu grande ativo. A segurança é um desafio a ser enfrentado diante dos ataques e tentativas de fraudes constantes aos sistemas. O blockchain irá contribuir para a inovação dos modelos de negócios permitindo modelos baseados em contratos inteligentes, empresas em rede abertas, agentes autônomos e empreendimento autônomo distribuído. Pode ser utilizada em: Educação; Armazenamento em nuvem; Sistemas de pagamentos; Moedas digitais; Contratos inteligentes; Saúde; *Supply Chain Management*; entre outros.

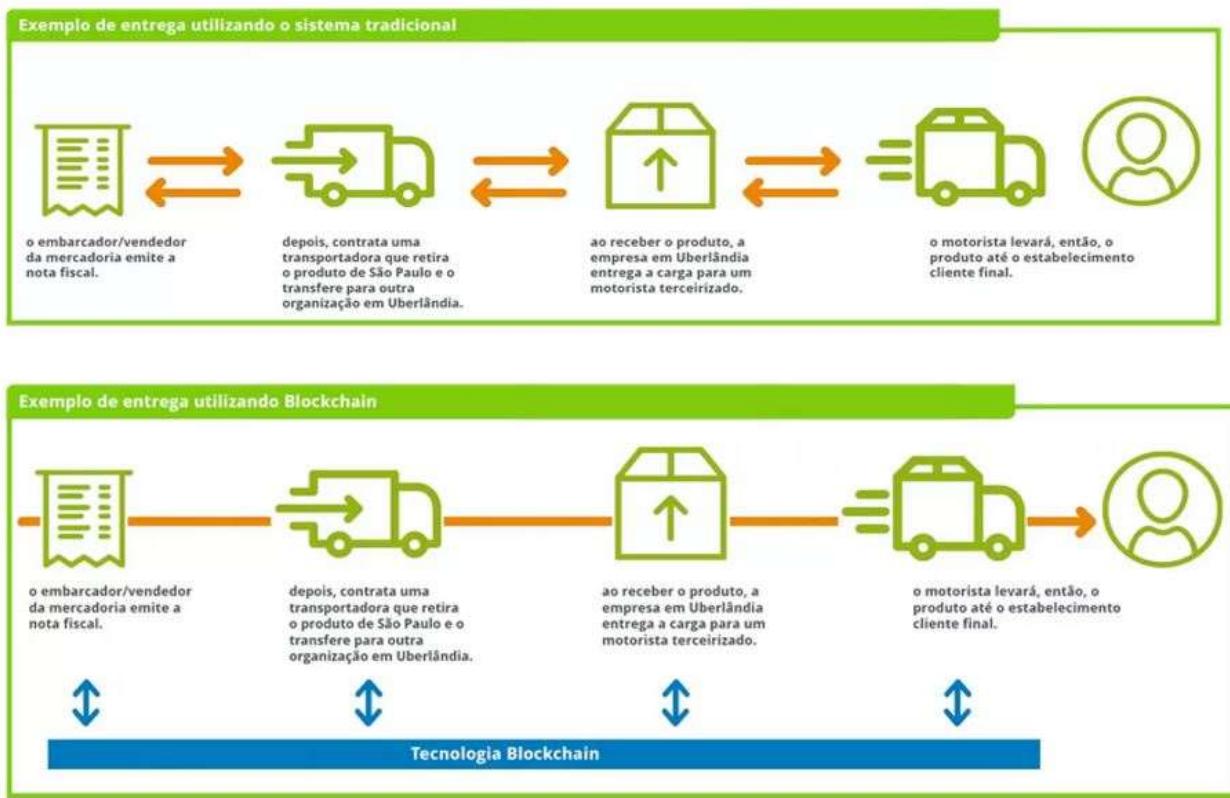
Veja a imagem 1 abaixo representando o Sistema Tradicional e o Sistema *Blockchain*.



Fonte: Site Interlispot (adaptado). Pesquisado em 07 de dez. 2021.

O *Blockchain* não está transformando apenas o setor econômico. Demais setores da economia vêm se beneficiando da tecnologia, como o de *Supply Chain Management*.

Veja na imagem 2 abaixo a diferença entre as entregas.



Fonte: Site Interlispot (adaptado). Pesquisado em 07 de dez. 2021.

O design do blockchain tem potencial para conduzir a grandes transformações no governo, pois oferece suporte e permite níveis mais elevados de integridade, poder, valor, preservação de direitos, segurança e inclusão. A nova tecnologia permite a utilização de ferramentas democráticas como: brainstorming digital, pesquisa deliberativa e a realização de desafios, juris e painéis de cidadãos.

Para Ulrich (2014), originalmente, Satoshi Nakamoto idealizou a tecnologia blockchain como solução para o problema do “gasto duplo”, considerado situação fática em uma transação online a qual necessita da presença de um terceiro para efetivação, funcionando como intermediador. Sua aplicação inicial foi nas criptomoedas virtuais, tais como o Bitcoin. O blockchain está modificando o mercado financeiro porque essa tecnologia permite a atestação, redução de custo, maior velocidade, melhor gestão de risco, maior inovação de valor, além de utilizar código aberto. Com essas características, as principais áreas que serão transformadas são: autenticação de identidade e valor, movimentação de valor, armazenamento de valor, empréstimos, troca de valor, financiamento e investimento, garantia de valor e gerenciamento de risco, contabilização de valor.

## **Blockchain: Moedas Virtuais**

As moedas digitais são aquelas que não utilizam o papel-moeda, ou seja, são utilizadas em transações de forma virtual, em que os valores são eletronicamente creditados ou debitados. Como o Bitcoin, existem outras moedas digitais, como por exemplo, a *Ethereum*, a *Cardano*, a *Rennimbi*; *Polkadot*; etc.

Segundo Christensen (2012), o advento das Tecnologias da Informação e da Comunicação (TICs) foi de grande relevância para o estabelecimento do cenário atual, no qual se verifica evolução na prestação de serviços e oferta de produtos bancários. As principais vantagens relacionadas à utilização das moedas virtuais desenvolvidas com a tecnologia *blockchain* são: **alternativa de pagamento mais rápida, independência, escopo global, custo-benefício, facilidade de uso e privacidade de dados**. Por outro lado, as limitações e riscos, relacionados a essas moedas são: vulnerabilidade, volatilidade, anonimato e falta de medidas.

Os fatores que geram bolhas de preços são a especulação excessiva; mas além da especulação, outros fatores afetaram o preço da moeda ao longo de sua existência, como roubos e crimes que envolvem a apreensão da moeda.

Acerca desse argumento, White (2014, p.12) faz outro comentário sobre isso:

Ao contrário de um Cometimento de Preço, ele [o Cometimento de Quantidade] deixa o preço do mercado da moeda variar de acordo com a demanda. Isso explica como é possível os preços do Bitcoin e de outras criptomoedas serem voláteis como recentemente.

Nakamoto (2008, pg. 1). “O que se precisa é um sistema de pagamento eletrônico baseado em prova criptográfica em vez de prova de confiança”.

Os fatores de sucesso relacionados ao desenvolvimento das moedas digitais estão relacionados tanto ao lado da demanda, incluindo fatores como custo, facilidade de uso, segurança, irrevogabilidade, volatilidade, velocidade de transação e privacidade de dados; quanto do lado da oferta, envolvendo fatores com fator técnico, anonimato, fragmentação e eficiência.

Para Charitou e Markides (2003), as inovações disruptivas, diferente das formas tradicionais, encaminham ou evidenciam características não exploradas do produto ou serviços.

As ofertas iniciais de moedas podem ser uma forma de captação financeira para as organizações, assim como o *IPO* é para as organizações tradicionais. A *ICO* não é considerada uma forma regulamentada de financiamento e normalmente utiliza formas de *crowdfunding*. Você aprendeu também, que existem vários critérios para qualificar uma *ICO*, dentre eles podemos destacar a

análise da equipe, da divulgação e marketing, dos produtos e da viabilidade. O resultado de vendas de *tokens* é altamente influenciado pela forma como é estruturada sua venda, que pode ser pré-vendas privadas, limites fixos, limite flexível, ilimitado e preço fixo e leilão holandês; cada um desses modelos apresenta pontos positivos e negativos e os melhores resultados irão depender dos objetivos do projeto.

Alguns obstáculos que precisam ser superados para a implementação plena do blockchain e alguns riscos observados até o momento pelos experimentos disponíveis. Outros elementos que precisam ser superados para a utilização adequada da tecnologia *Blockchain* e seu subproduto mais conhecido, a *criptomoeda* exemplificada aqui exclusivamente pela *Bitcoin* (moedas virtuais).

De acordo com Christensen (2012), é possível explicar o fracasso de grandes organizações a partir da ocorrência de inovações disruptivas em seu mercado de atuação. Os impactos da utilização do *blockchain* são inúmeros e permite a implementação de política de incentivo à produção científica, o reconhecimento do mérito dos autores e suas obras, além de oportunizar o acesso ao financiamento estudantil de maneiras nunca antes possíveis, com base no mérito e na evolução acadêmica do estudante, contribuindo inclusive para o maior reconhecimento da instituição de ensino, pois quanto maior for o engajamento da instituição no desenvolvimento dos estudantes, maiores serão as quantidades de financiamento direcionadas a ela.

## Considerações Finais

São muitos aos agentes interessados no avanço da *Blockchain* e seus usos potenciais, contudo concordam que uma das grandes fragilidades é a ausência de governança que possa definir padrões, conferir segurança e credibilidade ao processo como um todo. A comunidade de desenvolvedores, que é a base desse avanço tecnológico, resiste a implantação de governança, pois o excesso pode limitar a liberdade oferecida por um código aberto.

Encontrar o equilíbrio entre controle e liberdade, a medida exata que a governança deve apresentar para garantir a segurança desejada pelo mercado e governos, sem restringir a liberdade criativa dos desenvolvedores é o ponto chave.

Há muito o que se pensar e as oportunidades são imensas. Todavia, outras grandes revoluções tecnológicas que criaram negócios bilionários há poucas décadas já não existem mais. Por exemplo, quem se lembra quando foi a última vez que você foi buscar uma fita *VHS* na *Blockbuster* ou precisou comprar um filme *Kodak* de 24 poses?

Muitas fortunas são criadas e outras são perdidas e o ciclo evolutivo continua. Por isso é preciso estar atento para aproveitar os momentos de construção de riqueza, principalmente quando grandes players decidem investir em algo e divulgam para os pequenos investidores, e aceitar que em algum momento essa onda pode mudar. Enquanto grandes empresas e governos estiverem interessadas em algo o ciclo de prosperidade tenderá a ser crescente.

### **Referências Bibliográficas**

- Aumasson, Jean-Phillipe *et al.* *Cryptanalysis of Dynamic SHA* (2). 2009. Disponível em: <<https://eprint.iacr.org/2009/184.pdf>>. Acesso em: 21 de janeiro de 2022.
- Braga, Alexandre. TECNOLOGIA BLOCKCHAIN: Fundamentos, Tecnologias de Segurança e Desenvolvimento de Software 2017. Disponível em: <[https://www.cpqd.com.br/wp-content/uploads/2017/09/whitepaper\\_blockchain\\_fundamentos\\_tecnologias\\_de\\_seguranca\\_e\\_desenvolvimento\\_de\\_softwar\\_FINAL.pdf](https://www.cpqd.com.br/wp-content/uploads/2017/09/whitepaper_blockchain_fundamentos_tecnologias_de_seguranca_e_desenvolvimento_de_softwar_FINAL.pdf)>. Acesso em: 22 de janeiro de 2022.
- Charitou, C. D., & Markides, C. C. (2003). *Responses to disruptive strategic innovation*. *MIT Sloan Management Review*, 44 (2), 55-63.
- Christensen, C. (2012). O Dilema da Inovação. São Paulo: M. Books do Brasil Editora.
- Diniz, E. H. (2017). Emerge uma nova tecnologia disruptiva. *GV Executivo*, 16 (2), 47-50.
- Gil, Antônio Carlos. Como elaborar projetos de Pesquisa (4<sup>a</sup> ed). São Paulo: Atlas. (2002).
- Nakamoto, Satoshi. *Bitcoin: a peer-to-peer electronic cash system*. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 22 de janeiro de 2022.
- Site Intelipost. *Blockchain*. Disponível em: <<https://www.intelipost.com.br/blockchain/>>. Pesquisado em 07 dez 2021.

Slaughter and May (2016). *Blockchain Settlement: Regulation, Innovation and Application.* Disponível em <file:///C:/Users/William/Downloads/swift\_news\_pdf\_blockchain\_settlement\_regulation\_paper.pdf>. Acesso em: 22 de janeiro de 2022.

Ulrich, F (2014). *Bitcoin: A moeda na era Digital.* São Paulo: Instituto Ludwig Von Mises Brasil.  
WHITE, L. H. *The market of cryptocurrencies.* Virginia: George Mason University, 2014. 12-26p.