BLOCKCHAIN: APORTE TEÓRICO E SUGESTÕES DE APLICAÇÕES EM DIFERENTES SETORES

Amanda de Caires Ferreira, Fatec Antônio Russo - São Caetano do Sul. E-mail:amanda.ferreira24@fatec.sp.gov.br

Estefânia Angélico Pianoski Arata, Fatec Antônio Russo - São Caetano do Sul. E-mail:estefania.arata@fatec.sp.gov.br

Resumo

Alguns especialistas colocam a blockchain como o próximo passo evolutivo da internet. Sua arquitetura tem como base quatro pilares fundamentais: segurança das operações, a descentralização do armazenamento ou computação, a integridade de dados e a imutabilidade das transações. Este artigo tem como objetivo apresentar um estudo teórico da tecnologia *blockchain*, além de apontar suas funcionalidades e as formas em que pode ser empregada em diferentes setores. Caracteriza-se por uma pesquisa bibliográfica, que utiliza artigos, capítulos de livros e documentos da área de segurança da informação. Por fim, concluiu-se que a tecnologia *blockchain* está em constante ascensão, possui grande potencial de mudar completamente a relação dos usuários com a internet, a proteção de dados e que há grandes expectativas quanto ao seu futuro.

Palavras-chave: *blockchain*, criptografia, segurança digital.

Abstract

Some experts put the blockchain as the next evolutionary step for the internet. Its architecture is based on four fundamental pillars: security of operations, decentralization of storage or computing, data integrity and transaction immutability. This article aims to present a theoretical study of blockchain technology, in addition to pointing out the tools it employs and and the ways in which it can be used in different sectors. It is characterized by a bibliographical research, which uses articles, book chapters and documents in the information security area. Finally, it was concluded that blockchain technology is constantly on the rise, has great potential to completely change the relationship of users with the internet, the data protection and that there are high expectations for its future.

Keywords: blockchain, cryptography, digital security.

1. Introdução

Segundo Formigoni (2017), alguns especialistas colocam a plataforma *blockchain*, ou *Distributed Ledger Technology* (DTL), como o próximo passo evolutivo da internet, sendo denominada Internet do Valor. De acordo com esses especialistas, a tecnologia permitirá que o dinheiro flua na rede de internet tão livremente como os dados fluem atualmente. Desta forma, é esperado que a tecnologia possa afetar as aplicações relacionadas com transações da mesma forma que os aplicativos de navegação GPS (em inglês *global positioning system*) mudaram o transporte pessoal.

Com base nessa visão, este artigo tem como objetivo apresentar um estudo teórico da tecnologia *blockchain*, além de apontar suas funcionalidades e as formas em que pode ser empregada em diferentes setores. Caracteriza-se por uma pesquisa bibliográfica, que utiliza artigos, capítulos de livros e documentos da área de segurança da informação.

Para melhor entendimento, o texto foi dividido nas seguintes seções: na seção 2 são apresentados as origens e conceitos da plataforma *blockchain*; na seção 3 descreve-se as principais ferramentas que compõem a plataforma e é explicado o funcionamento da *blockchain*; na seção 4 são abordadas as vantagens e desvantagem de sua implementação; na seção 5 são mostradas outras áreas de aplicação, além das criptomoedas e, por fim, na seção 6 são apresentadas as considerações e comentários finais.

2. Origens e conceitos da *blockchain*

A essência do que é a tecnologia *blockchain* existente hoje está na palavra "*ledger*", um termo contábil que traduzido do inglês significa livro-razão. Por sua vez, um livro-razão "é um conceito datado do século XV e que envolve, tipicamente, um balanço inicial de ativos, tangíveis ou não tangíveis, diversas operações de débito e crédito detalhados em colunas separadas e um balanço final". (CERQUEIRA, 2017)

A motivação que envolve o surgimento da tecnologia *blockchain* está na tentativa de solucionar as deficiências do sistema de transações atuais. Pois ainda que o mercado atual seja complexo quanto aos métodos de comercialização, comunicação e acordos financeiros, basicamente a sociedade ainda troca dinheiro por algo ao qual dá mais valor. (CERQUEIRA, 2017)

Para Gupta (2017), ao longo da história surgiram vários instrumentos de confiança, como o papel moeda, as moedas cunhadas, as cartas de crédito e vários sistemas bancários, cuja finalidade era facilitar transações e proteger compradores e vendedores. Porém, o que se verifica hoje é que esses instrumentos custam caro, porque envolvem mediadores que cobram taxas pelos serviços prestados, ou se mostram ineficientes, devido a atrasos na execução de contratos e ao duplo esforço necessário à manutenção de vários livros-razão. Verifica-se também que são vulneráveis, pois havendo um comprometimento ou indisponibilidade do sistema central, como em um banco, seja por fraude, ataque cibernético ou um erro qualquer, toda a rede comercial será afetada.

Ainda segundo Gupta (2017), paralelamente surgiram também inovações importantes como as linhas telefônicas, sistemas de cartão de crédito, internet e tecnologias móveis que melhoraram significativamente as convenções, a velocidade e eficiência das trocas enquanto virtualmente eliminaram a distância geográfica entre compradores e vendedores. Com isso, o volume de transações ocorrendo em todo o mundo está crescendo exponencialmente e certamente aumentará as complexidades, vulnerabilidades, ineficiências, e custos dos sistemas de transação atuais. É dessa preocupação que surge a tecnologia *blockchain*.

De acordo com Tapscott (2016), desde 1981 os cientistas de dados tentavam usar a criptografia para resolver problemas de privacidade, segurança e invasão da internet. Porém, foi apenas em 1993 que surgiu um sistema que tornava possível fazer pagamentos na *web* de maneira segura e anônima, por meio do envio de moedas eletrônicas, o *eCash*, lançada pelo matemático David Chaum. Porém, apesar do projeto ser considerado promissor e atrair o interesse de grandes empresas de tecnologia, o consumidor final não estava interessado em privacidade e segurança *on-line*. Então, a empresa de Chaum, *DigiCash*, faliu em 1998.

Nessa época, um dos sócios de Chaum, Nick Szabo, escreveu um pequeno artigo intitulado "*O protocolo de Deus*". Ainda de acordo com Tapscott (2016, p.35):

> Em seu artigo, Szabo se concentrou na criação de um protocolo de tecnologia "todo-poderoso" que designou "Deus" a terceira parte de confiança no meio de todas as transações: "Todas as partes iriam enviar suas entradas a Deus que, de maneira confiável, determinaria e retornaria os resultados. Deus, sendo a última palavra em discrição confessional, faria que nenhuma das partes soubesse algo

> a mais sobre as entradas dos outros envolvidos além de suas próprias entradas e saídas".

Dez anos depois, em 2008, um artigo intitulado "*Bitcoin: A peer-to-peer Electronic Cash System*", contendo os princípios de funcionamento de uma criptomoeda denominada *bitcoin*, foi publicado anonimamente no grupo de discussão "*The Cryptography Mailing*", usando o pseudônimo Satoshi Nakamoto. Em seu texto Formigoni (2017) explica que a proposta desse artigo era "a criação de uma moeda digital mundial que funcionasse em uma rede *peer-to-peer* e que permitisse o envio de pagamentos *on-line* de forma totalmente segura, sem o envolvimento de instituições financeiras para todos os participantes da rede". A plataforma tecnológica utilizada para funcionamento dessa rede é a *blockchain*.

> Após a implantação das primeiras criptomoedas, vários especialistas observaram que propriedades intrínsecas à tecnologia *blockchain* (tais como segurança, resiliência, inviolabilidade e imutabilidade) poderiam ser usadas em vários outros tipos de aplicações. Neste sentido, as plataformas de desenvolvimento *blockchain* evoluíram e permitiram a inserção de transações mais complexas através dos contratos inteligentes (*smart contracts*) (FORMIGONI, 2017, p. 03).

A moeda *bitcoin* é a primeira e a mais conhecida aplicação da tecnologia *blockchain*. Por isso é comum que as pessoas não saibam distinguir *blockchain* da *bitcoin*, já que a tecnologia é a plataforma digital que oferece suporte para o funcionamento da rede de criptomoedas idealizada por Satoshi Nakamoto. Mas o alcance do *blockchain* vai muito além da *bitcoin*. Para Gupta (2017, p.03):

> *Blockchain* é um livro-razão compartilhado e distribuído que facilita o processo de registro de transações e rastreamento de ativos em uma rede de negócios. Um ativo pode ser tangível - uma casa, um carro, dinheiro, terrenos - ou intangíveis como propriedade intelectual, como patentes, direitos autorais ou *branding*. Praticamente qualquer coisa de valor pode ser rastreada e negociada em uma rede *blockchain*, reduzindo o risco e corte de custos para todos os envolvidos.

Como todas as informações introduzidas e armazenadas na ferramenta são compartilhadas entre vários usuários, chamados de nós, torna-se desnecessário confiar em uma terceira pessoa para que os dados sejam registrados de maneira adequada e não haja perigo de fraudes.

E para Maçoli (2020), o processamento em blocos dessa base de dados é feita da seguinte maneira: para cada novo bloco processado é criado um código de verificação, sempre baseado nos blocos processados anteriormente a ele. Isso faz com que *blockchain*

seja uma solução de alta confiabilidade, pois havendo a adulteração de um bloco, ela impactará em todos os demais blocos processados.

3. Funcionalidade da plataforma *blockchain*

A *blockchain* é uma plataforma que usa um tipo específico de criptografia para proteger as transações entre os usuários, a função *hash*. Após submeter um documento elaborado a uma função *hash*, um número hexadecimal é gerado. Segundo Maçoli (2020, p.11), "esse número é único e, se porventura qualquer caractere do documento original for modificado ao ser submetido à função *hash*, o número será diferente, garantindo a integridade do documento".

Na *blockchain*, cada novo bloco processado é submetido a função *hash* e esse *hash* está diretamente ligado ao *hash* do bloco anterior. Isso faz com que haja uma interligação entre todos os blocos da cadeia, garantindo desta forma a total integridade de todas as transações ocorridas via *blockchain*. Ainda segundo Maçoli (2020), isso significa que caso haja qualquer adulteração nas informações contidas em um bloco, haverá o conflito com o *hash* do próprio bloco, assim como do bloco anterior e do bloco que o sucede. É todo esse processamento em blocos que garante a confiabilidade do *blockchain*. A figura 01 mostra o funcionamento do *hash* conforme descrito.

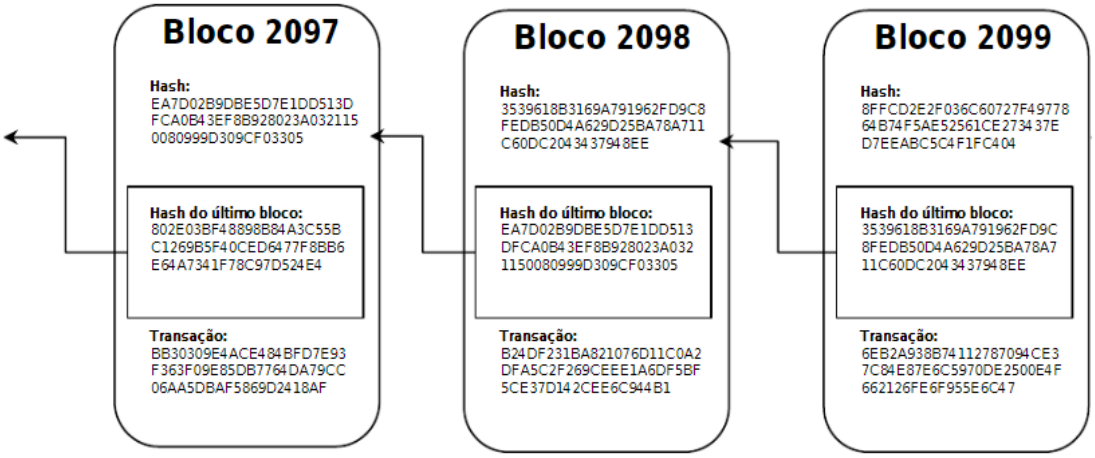

Figura 01 – Criptografia *hash*. Fonte: https://www.gta.ufrj.br

Outra ferramenta importante utilizada na plataforma *blockchain* é a assinatura digital. Trata-se de uma tecnologia que também utiliza a criptografia e vincula um certificado digital a um documento eletrônico que está sendo assinado, dando garantias de "autenticidade, confidencialidade, integridade, irretratabilidade e possui validade jurídica". (CERTISIGN, 2021)

A rede *peer-to-peer* ou rede ponto a ponto, é outra tecnologia usada pela *blockchain*. Diz respeito a maneira como estão dispostos os computadores interligados à uma rede específica. "É uma rede onde cada computador conectado, realiza as funções de cliente e servidor ao mesmo tempo, dessa forma, tudo é descentralizado". (MEYER, 2015)

No caso específico da arquitetura *blockchain*, o emprego da rede *peer-to-peer* é muito importante por se tratar de uma tecnologia que, segundo Maçoli (2020, p.16), é "descentralizada, compartilhada, com vários nós participando do processamento, distribuída e segura". A figura 2 apresenta as diferenças de organização entre as topologias de rede.

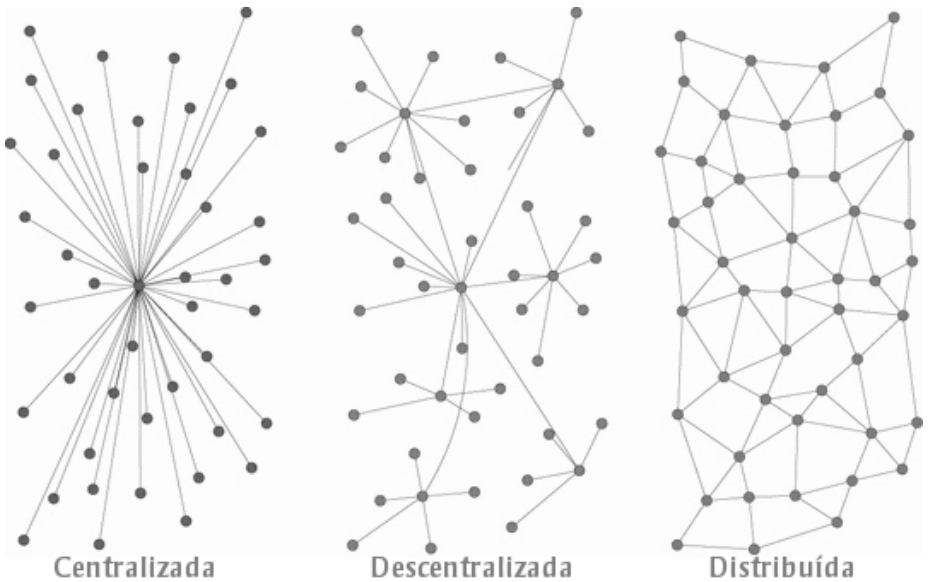

Figura 02 – Topologias de rede. Fonte: https://outraspalavras.net

Para Formigoni (2017, p.06), a arquitetura da tecnologia *blockchain* foi construída em cima de quatro pilares estruturais fundamentais: "a segurança das operações, a descentralização do armazenamento ou computação, a integridade de dados e a imutabilidade das transações". Ainda segundo o autor:

> *Blockchain* é uma *"ledger of facts*" replicada em computadores que participam de uma rede *peer-to-peer*, onde:
>
> - O *ledger* é um livro de registros digital, no qual uma vez validado um registro, este nunca mais poderá ser apagado;
>
> - Um fato (*fact*) pode significar várias coisas, desde uma transação monetária, a um conteúdo de determinado documento, ou até mesmo um programa de computador, contendo, em algumas plataformas, até uma base de dados pequena;
>
> - Os membros participantes da rede podem, ou não ser anônimos e são chamados *peers* ou "nós";
>
> - Toda operação ou transação dentro da *ledger* é protegida por tecnologias criptográficas de assinatura digital, inclusive para identificar os nós emissores e receptores das transações;
>
> - Quando um nó deseja adicionar ao *ledger* um fato novo, é necessário um consenso entre todos ou alguns nós previamente determinados da rede, para decidir se um fato pode ser registrado no *ledger*;
>
> - Havendo consenso, o fato será escrito e nunca mais poderá ser apagado, em tese, um processo levemente semelhante à escritura e registro de um imóvel no Brasil. (FORMIGONI, 2017, p. 06).

Com base nos itens acima, Maçoli (2020) conclui que toda transação, ou operação, que ocorre dentro da *blockchain* é protegida pelas tecnologias que compõem a plataforma, a saber: *hash*, assinatura digital, certificado digital, e redes *peer-to-peer*.

4. *Blockchain*: Vantagens e desvantagens

Quando se fala da plataforma *blockchain* frequentemente se pergunta quais seriam as vantagens que o emprego dessa tecnologia possui em relação as outras tecnologias ditas convencionais, respondendo os mesmos problemas. Segundo Formigoni (2017), as principais vantagens são:

- Economia de tempo, pois as operações digitais realizadas via *blockchain* podem ser processadas em minutos, ao contrário do que pode ocorrer em sistemas convencionais onde a mesma operação levaria dias até ser processada;

- Redução dos custos a proporções mínimas, já que ao garantir acesso confiável a uma base de dados consistente e distribuída, se elimina custos com operações desnecessárias bem como a necessidade de uma terceira parte para intermediar negociações;
- Redução de riscos, pois ao oferecer transparência e garantir acesso a uma base dados que são imutáveis e íntegros, a plataforma *blockchain* facilita a adoção de medidas que visam reduzir fraudes, adulterações e outros crimes cibernéticos;
- Construção de uma relação de confiança, tendo em vista que na *blockchain* os processos e registros são compartilhados de maneira mais segura e transparente, quando necessário. Essa medida facilita a verificação, a auditoria e o rastreamento da base de dados, o que garante para os parceiros de negócio o bom funcionamento do suporte tecnológico do qual são dependentes.

Cabe também ressaltar as principais desvantagens para adoção da plataforma *blockchain*. Para o site Binance Academy (2020), são elas:

- A possibilidade de ataques de 51%, que pode acontecer se uma organização conseguir controlar mais que 50% do poder computacional da rede. Essa organização poderia interferir no funcionamento da rede excluindo ou modificando a ordenação das transações. Porém este seria um problema maior para rede menores e não para redes consolidadas como a *blockchain* da *bitcoin*.
- A dificuldade para modificação de informações depois que os dados são inseridos à rede, o que não deixa margem para erros ou alterações no sistema. Uma característica que é contraditória, pois é ela que confere estabilidade a rede.
- Caso o usuário perca suas chaves de criptografia privadas, que são necessárias para acessar documentos e validar as transações, os dados são perdidos e não há possibilidade de recuperação.
- Os livros das *blockchains* podem crescer muito ao longo do tempo, as vezes crescendo mais rápido do que a capacidade de armazenamento dos discos rígidos (HDs). Com isso a rede corre o risco de perder *nodes* e de que seus usuários sejam impedidos de baixar e armazenar os livros.

Ainda que desafios de implementação e desvantagens existam, as vantagens da *blockchain* são promissoras. E segundo Maçoli (2020), embora seu uso como moeda e

sistema financeiro que dispense intermediários seja o mais famoso, há várias outras possibilidades de aplicações por meio dos *smart contracts* ou contratos inteligentes.

5. Contratos inteligentes e as aplicações da *blockchain*

Maçoli (2020) define os contratos inteligentes como o próximo passo evolutivo na prevenção de fraudes. Trata-se de um acordo entre duas partes cuja execução é automática, realizada por algoritmos que traduzem "um discurso legal em um programa executável". Esse algoritmo é responsável por identificar se as condições acordadas foram atendidas e, em caso afirmativo, ele automaticamente executa os termos estipulados, sem a necessidade de determinar uma autoridade central ou um sistema judicial para isso.

De acordo com Formigoni (2017), com a possibilidade de utilização dos contratos inteligentes disponíveis, as chances de aplicação da plataforma *blockchain* crescem significativamente permitindo controle de imóveis, cadeias de produção, gestão de identidade de coisas e pessoas entre outras atividades. Ainda de acordo com Formigoni (2017), há a possibilidade de sua aplicação em diferentes setores:

- Para os governos a tecnologia traria benefícios como: gestão mais transparente, diminuição de fraudes e a possibilidade de compartilhamento de dados de maneira segura. Isso permitiria que importantes medidas fossem colocadas em prática, como: realização de votação eletrônica mais segura; gerência da identidade digital das pessoas para implementação confiável de programas sociais e políticas públicas, e para controle, digital ou físico, daqueles que acessarem os vários serviços e órgãos públicos; possibilitaria o rastreamento do pagamento de programas sociais e monitoração de ativos do governo, para melhor controle dos recursos públicos.
- No setor de telecomunicações a tecnologia poderia ajudar as operadoras a cortar custos com operações e assim ofertar serviços digitais por um preço melhor. Serviços como: autenticação de usuários quando estiverem fora da área de cobertura contratada (em *roaming*); providenciar conexão mais segura em *Wi-Fi* públicos para que pagamentos e autenticações possam ser feitos em segurança; melhor gerência de identidade dos usuários e possibilidade de projetos de cidades inteligentes mais transparentes e auditáveis.

- Para o setor financeiro, que é o que mais tem investido no desenvolvimento da tecnologia *blockchain*, os principais benefícios esperados seriam: a simplificação e diminuição dos custos com operações, redução da quantidade de intermediários, redução de fraudes e possibilidade de ofertar novos serviços. Além disso, seria possível aplicar a *blockchain* na gerência de identidade digital, de empréstimos e cartas de crédito, na implantação de criptomoedas, para facilitação de pagamentos no mundo todo e fornecimento de seguros.
- Na era da *internet of things* ou internet das coisas, a utilização da tecnologia *blockchain* contribuiria para atenuar problemas relacionados à segurança e privacidade rastreando a história de cada dispositivo, que é única, registrando toda troca de dados feitas pelos mesmos e permitindo que atuem de forma independente em diversas transações.

Além dessas áreas, Formigoni (2017, p.16) fala sobre a possibilidade de aplicação no setor de energia elétrica e em "projetos estruturantes, que envolveriam diferentes atores de uma cadeia de valor", citando como exemplo o monitoramento e rastreamento de uma cadeia de produção, sistema de gestão de logística reversa de diferentes produtos e sistemas de gestão e controle da distribuição e venda de medicamentos de uso controlado.

6. Considerações finais

A plataforma *blockchain* surgiu da necessidade de um modelo de transações virtuais que respondesse de maneira mais satisfatória a evolução tecnológica em geral, que fosse menos burocrático, confiável e economicamente mais viável, e que fosse mais adequado para atender o crescente volume de transações ocorrendo em todo o mundo. Ainda que em seu começo tenha sido ofuscado pelo surgimento paralelo da criptomoeda *bitcoin*, a tecnologia *blockchain* e sua aplicação por meio de contratos inteligentes cresce não só no campo da informática como também vem se expandindo para outras áreas. Para Swan (2015) *apud* Formigoni (2017, p.27):

> Existe grande expectativa do mercado, de governos, assim como das comunidades acadêmica e de desenvolvedores de solução, em relação ao futuro da tecnologia *blockchain*. Alguns especialistas a consideram o quinto

> paradigma disruptivo da computação, que poderá trazer uma experiência ubíqua de internet do valor.

Por isso o propósito deste artigo foi apresentar um estudo teórico sobre o tema, trazendo entre outros assuntos: os conceitos iniciais, as ferramentas, o funcionamento e o potencial de múltiplas aplicações da plataforma *blockchain* como um sistema de segurança digital descentralizado, integro, transparente, privativo e imutável, que promete aliar essas características a possibilidade de diminuir custos, melhorar o acesso a diversos serviços existentes e oferecer novos serviços, essenciais a um mundo cada vez mais conectado e globalizado.

Ao fim, concluiu-se que a tecnologia *blockchain* possui grande potencial para mudar completamente a maneira como os usuários de internet, lidam com o compartilhamento e proteção de dados não só no âmbito pessoal, como empresarial e governamental. As vantagens que a plataforma tecnológica possui em relação aos sistemas convencionais atrai cada vez mais investimentos de empresas e organizações de vários setores, que buscam se beneficiar com seu uso. Com o aumento de investimentos, consequentemente aumentam as pesquisas no desenvolvimento da ferramenta e maiores são as possibilidades de evolução da mesma, o que demonstra grandes expectativas quanto ao seu futuro.

Referências bibliográficas

ACADEMY, Binance. **Vantagens e Desvantagens da Blockchain**. Disponível em: <https://academy.binance.com/pt/articles/positives-and-negatives-of-blockchain>. Acesso em: 22 mai. 2021.

CERQUEIRA, Aurimar Harry; STELER, Fernando Wosniak. **Tudo o que você queria saber sobre blockchain e tinha receio de perguntar**. Computerworld, 2017. Disponível em: <http://computerworld.com.br/tudo-o-que-voce-queria-saber-sobreblockchain-e-tinha-receio-de-perguntar>. Acesso em: 08 mai. 2021.

CERTISIGN. **O que é certificado digital?** Disponível em: <https://www.certisign.com.br/certificado-digital/o-que-e-certificado-digital>. Acesso em: 22 mai. 2021.

Figura 01. Disponível em: <https://www.gta.ufrj.br/ensino/eel878/redes1-2019-1/vf/blockchain/>. Acesso em: 24 mai. 2021.

Figura 02. Disponível em: < https://outraspalavras.net/outrasmidias/os-perigos-da-recentralizacao-mundo-de-pontas/>. Acesso em: 24 mai. 2021.

FORMIGONI, Filho José Reynaldo; BRAGA, Alexandre Mello; LEAL, Rodrigo Lima Verde. **Tecnologia Blockchain: uma visão geral**. Disponível em: https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-Blockchain-impresso.pdf. Acesso em: 10 abr. 2021.

GUPTA, Manav. **Blockchain for Dummies**®, IBM Limited Edition. Wiley Brand John Wiley & Sons, Inc., 2017.

MAÇOLI, Fábio. **Blockchain Advanced: Conceitos Blockchain**. Disponível em: <https://on.fiap.com.br/local/salavirtual/conteudo-digital.php>. Acesso em: 19 mai. 2021.

MAÇOLI, Fábio. **Blockchain Advanced: Fundamentação Tecnológica Blockchain**. Disponível em: <https://on.fiap.com.br/local/salavirtual/conteudo-digital.php>. Acesso em: 19 mai. 2021

MEYER, Maximiliano. **O que é P2P e como ela funciona?** Oficina da net, 2015. Disponível em: <https://www.oficinadanet.com.br/post/14046-o-que-e-p2p-e-como-ela-funciona>. Acesso em: 10 abr. 2021.

NAKAMOTO, Satoshi. **Bitcoin: A peer-to-peer Electronic Cash System**. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 08 mai. 2021.

SWAN, Melanie. **Blockchain: Blueprint for a New Economy**. Sebastopol, California: O'Reilly Media Inc., 2015.

SZABO, Nick. **The God Protocols**. Disponível em: <https://nakamotoinstitute.org/the-god-protocols/>. Acesso em: 18 ago. 2021.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution–como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo**. São Paulo: Senai-SP Editora, 2016.