Atualmente, as informações cadastrais bancárias de seus clientes eventuais, do proprietário e do destinatário dos recursos envolvidos na operação ou serviço financeiro são constantes fiscalizadas e controladas por instituições financeiras através de sistemas sigilosos ao público. A instituição financeira verifica os saldos dos grupos de negociação no livro de registro e os atualizas sempre que uma transação ocorrer. Esse é um sistema com uma autoridade centralizada pela respectiva instituição financeira.

A tecnologia *Blockchain* traz um controle diametralmente diverso, na medida em que utiliza o sistema de autoridade distribuída entre os usuários de forma a permitir a comercialização de ativos digitais (NAKAMOTO, 2012).

**A autoridade distribuída por permitir que todo usuário do sistema possa verificar as negociações possui uma razão pública, transformando o sistema em uma lista crescente de registros ordenados de transações (ALLEN, 2016). (não entra )**

Sempre que uma negociação é contratada, as partes envolvidas verificam se a parte que realiza a transação possui o saldo mínimo para concluir a operação e, dessa forma, se as razões públicas observadas.

2.3.1 CARACTERÍSTICAS DO BLOCKCHAIN

Allen (2016) enfatiza a importância da tecnologia *blockchain* que, inclusive sustenta o *Bitcoin,* não necessita armazenar informações sobre a moeda. Qualquer tipo de informação que requer um intermediário entre os agentes para verificação pode, teoricamente, ser armazenada em um *blockchain* para torná-la independente da figura do terceiro. Nessa visão, Mougayar (2016) define a tecnologia *blockchain*, de forma ampla, compreendendo como uma gama de “rede de troca de valores” que mantém o potencial de armazenamento e transmissão de informações descentralizadas.

O *hype* e o primeiro nível de compreensão em torno da tecnologia *blockchain* são as principais razões pelas quais ela está sendo introduzida no mercado com tanto êxito. Gartner (2016), que relata que o *blockchain* está próximo do pico do ciclo de *hype* para tecnologias emergentes. Esses fatores tendem a deixar o mercado aquecido pela vultosa participação de empresas iniciantes com casos de uso excessivos de propagandas para seu benefício de marketing (LINDEN; FENN, 2003).

Quando se trata de áreas de aplicação específicas, ainda não se encontrou um consenso na literatura sobre quais as áreas podem ser consideradas de uso definitivo para a tecnologia *blockchain*, exceto pelo óbvio caso do uso de moeda, como visto no *Bitcoin*. Muitos autores, entretanto, pretendem mapear e listar os possíveis casos de uso e aplicações para o *blockchain*, em que pese as possibilidades da tecnologia sejam pouco exploradas (TSCHORSCH; SCHEUERMANN, 2016). Atzori (2015) afirma que existem aplicações “potencialmente incontáveis” do *blockchain*.

Por outro lado, a P2P *Foundation* possui uma lista de, aproximadamente 33 (trinta e três) aplicativos que atualmente utilizam a tecnologia *blockchain,* não havendo consenso sobre quais as áreas de aplicação mais proeminentes. (não)

Há uma concordância de ideias sobre a tecnologia estudada quanto a possibilidade de divisão de áreas de aplicação, geralmente, em quatro categorias. Ledra Capital (2014) e P2P *Foundation* (SOO, 2016) elencaram algumas listas de aplicações atuais e potenciais. As 4 (quatro) categorias principais são mostradas no quadro 2, a seguir: (não)

|  |
| --- |
| **QUADRO 2** - **DIVISÃO DAS APLICAÇÕES DE TECNOLOGIA BLOCKCHAIN DA BLOCKCHAIN TECHNOLOGIES (2016) Finanças, razão distribuída e serviços financeiros:** Foco principal na aplicação original e na inovação do *blockchain* através do *Bitcoin*, ou, como alternativa, que as instituições financeiras criem seus próprios *blockchains* privados. |
| **Propriedade inteligente e propriedade autônoma:** A propriedade inteligente permite que a propriedade física ou não seja verificada, programada ou negociada no *blockchain*. Exemplos físicos de propriedade inteligente incluem veículos, telefones e casas que podem ser ativados, desativados, rastreados e mantidos. |
| **Lei programável e contratos autoexecutáveis:** Discute o conceito de Corporações Autônomas Descentralizadas (DAC), Organizações Autônomas Descentralizadas (DAO), capacitação de artistas para expandir a propriedade de suas obras, e o *blockchain* imobiliário permitindo uma atualização simultânea e eficaz dos registros. |
| **Identidade segura de verificação de identidade:** Introduz o conceito de aplicativos de identidade *blockchain*, permitindo a verificação, autorização e gerenciamento inalterados de identidades, resultando em eficiências significativas de redução de fraudes. (não) |

referencias

NAKAMOTO, S. *Bitcoin:* A peer-to-peer electronic cash system, 2008., 2012. Disponível em: < <https://bitcoin.org/bitcoin.pdf> >. Acesso em: 19 janeiro 2017

ALLEN, D.W. *Discovering and developing the blockchain cryptoeconomy,* 2016. RMIT University.

MOUGAYAR, W. *The Business Blockchain*: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons, 2016.

GARTNER. *Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage.* 2016. Disponível em: < <http://www.gartner.com/newsroom/id/3412017> >. Acesso em: 13 fevereiro 2017.

RIZZO, P. Gartner: *Blockchain Tech Hits Hype Cycle Peak*. [Online] CoinDesk.com., 2016. Disponível em: < <http://www.coindesk.com/gartner-blockchain-hits-hype-cycle-peak> /> Acesso em: 1 maio 2017.

LINDEN, A.; FENN, J. Understanding Gartner’s hype cycles. *Strategic Analysis Report*, N.R-20-1971. Gartner, Inc, 2003.

TSCHORSCH, F.; SCHEUERMANN B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *Ieee Communications Surveys and Tutorials*, 18(3), 2016. pp. 2084-2123.

LEDRA CAPITAL. *Bitcoin Series 24*: The Mega-Master Blockchain List., 2014. Gathered 2016-12-06. Disponível em: <http://www.ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list>

SOO, Aeze. *The Blockchains Application Directory*. Retrieved 6, 2016. Disponível em: <http://www.p2pfoundation.net/Blockchain#The_Blockchain_Applications_Directory>

Segundo a autora (DIULIANA FRANÇA,) o blockchain é uma espécie de livro razão digital, um recurso para se registrar transações de forma que se garanta a sua integridade. A tecnologia foi desenvolvida e é a base da moeda digital Bitcoin. Após o lançamento do Bitcoin em 2008, surgiram outras plataformas de moedas digitais baseadas em Blockchain e outros usos vem sendo aplicados.

Blockchain evoluiu de uma infraestrutura de moeda digital para uma plataforma de transformação digital

<http://www.eventos.momentoeditorial.com.br/wp-content/uploads/2018/04/DIULIANA-FRANCA.pdf>

Blockchain é um banco de dados distribuído, online, público e que pode ser atualizado por qualquer nó participante da rede peer-to-peer (P2P) baseado no consenso entre eles e assegurado por um algorítmo de uma prova de trabalho (Proof-of-Work), que tem o objetivo principal de dissuadir ataques cibernéticos (KYPRIOTAKI, ZAMANI; GIAGLIS, 2015). Utiliza-se de técnicas de criptografia para que cada participante possa manipular o ledger (livro digital onde informações são registradas regularmente) de forma segura e sem a necessidade de uma autoridade central. Uma vez que um bloco é adicionado ao blockchain é extremamente difícil alterar ou remover. Até agora, o blockchain tem atraído bastante atenção da indústria de serviços financeiros, mas a tecnologia pode ser adaptada para qualquer indústria onde seja necessário registrar, confirmar e transferir qualquer tipo de contrato ou propriedade. Blockchain é uma tecnologia tão disruptiva quanto a máquina a vapor e a eletricidade foram no século XX e espera-se que este novo paradigma seja capaz de modificar profundamente a maneira como a sociedade e a economia funcionam (UMALKAR, MACNEIL; LIGHT).

O mundo está passando rapidamente por uma mudança fundamental: está cada dia mais sendo impulsionado pelos dados. E esta transformação ocorre em todos os sistemas sociais através de diversos serviços que englobam tráfego, saúde, governo, logística, marketing, segurança entre outros (SHRIER, WU; PENTLAND, 2016). No entanto, problemas como vazamentos de informação por parte dos provedores desses serviços requerem que novos modelos de segurança sejam criados. Uma das tecnologias que surgiram recentemente e com grande potencial para atender a esta necessidade tem-se o blockchain. O blockchain consiste em uma cadeia cronologicamente ordenada de blocos protegidos pela resolução de Proofof-Work. O encadeamento é feito adicionando o hash do bloco anterior ao bloco atual. O alinhamento dos blocos de forma cronológica faz com que uma transação não possa ser alterada com antecedência sem alterar seu bloco e todos os blocos a seguir (AITZHAN; SVETINOVIC, 2016). Um grande benefício do blockchain é que ele é uma nova forma de tecnologia de informação descentralizada que pode ser aplicável em muitas situações além da criptomoeda e ativos financeiros. A natureza descentralizada do blockchain torna-o uma tecnologia da igualdade, que pode ser usada expandir a liberdade, possibilidade, atualização, expressão, ideação, e a realização para todas as entidades no mundo, humano e máquina (SWAN, 2015). O primeiro decentralized ledger para transações públicas foi desenvolvido por Satoshi Nakamoto (pseudônimo). No artigo Bitcoin: A Peer-to-Peer Electronic Cash System, de Nakamoto e publicado em novembro de 2008, o conceito foi introduzido pela primeira vez ao público (OBERHAUSER, 2014). O Bitcoin não foi o primeiro método de pagamento digital que foi desenvolvido, mas foi o primeiro que resolveu o double-spending (resultado de gastar algum dinheiro mais de uma vez) de forma descentralizada. Alguns exemplos de abordagens anteriores foram NetCash (1993), NetCents (1998) e uma patente com o nome de Method of electronic payments that prevents double-spending (1998). A abordagem apresentada no documento Bitcoin cria um ledger público descentralizado, denominado blockchain (OBERHAUSER, 2014).(não)

Referencias

AITZHAN, N. Z.; SVETINOVIC, D. Security and Privacy in Decentralized Energy Trading through MultiSignatures, Blockchain and Anonymous Messaging Streams. IEEE Transactions on Dependable and Secure Computing, Outubro 2016.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report, 2007

KYPRIOTAKI, K. N.; ZAMANI, E. D.; GIAGLIS, G. M. From bitcoin to decentralized autonomous corporations: Extending the application scope of decentralized peer-to-peer networks and blockchains. ICEIS 2015 - 17th International Conference on Enterprise Information Systems, 2015. 284-290.

OBERHAUSER, A. Decentralized Public Ledger as Enabler for the Gift Economy at Scale, 2014. SHRIER, D.; WU, W.; PENTLAND, A. Blockchain & Infrastructure (Identity, Data Security). connection.mit.edu, 2016.

SWAN, M. Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization). Texas Bitcoin Conference, 2015

UMALKAR, M.; MACNEIL, A; LIGHT, D. What every CEO Should Know About Blockchain. accenture. Disponível em: . Acesso em: 17 Setembro 2017.