

Identificação digital baseada em *blockchain*: Um conceito disruptivo no ciberespaço.

Alex Oliveira Abreu Batista¹

Emillie Rebecca Bastos Dias²

Murilo Borges Silva³

Resumo

Um sistema de identidade digital baseado em *blockchain* pode proporcionar segurança de acesso e confiabilidade nas informações desde transações complexas, de caráter documental ou financeiro, a cadastros básicos em sites e redes sociais. *Blockchain* é um conceito de tecnologia que proporciona um sistema descentralizado de operações de forma segura, estável e sem intermediários, na qual todas as transações são registradas criptograficamente em uma rede distribuída *peer-to-peer*. Todos os eventos digitais são registrados em um livro público por meio de um consenso da maioria dos participantes, de maneira permanente, rastreável e transparente. A ascensão do *blockchain* vem provocando grandes expectativas de revolucionar os modelos de negócios adotados atualmente. No modelo de negócios tradicional, a autenticidade de informações sobre a identidade dos envolvidos em transações e a propriedade de bens é garantida por meio de documentos físicos e, em muitas vezes, reconhecidas por órgãos do governo ou profissionais dotados de fé pública em cartórios. Além disso, virtualmente, para ter acesso a conteúdos de sites e redes sociais, é preciso preencher cadastros com dados pessoais frequentemente. Usualmente, em meio digital, a validação desses dados cadastrais não é eficiente. A criação de perfis falsos e informações inverídicas na internet é uma prática fácil e comum.

Este trabalho visa apresentar um novo padrão de comportamento no ciberespaço, baseado neste protocolo de confiança. Analisando futuras possibilidades de aplicação, desde uma reputação social digital, identidade autêntica, até incentivos financeiros, onde poderá ser usada para recompensas por postagens, sendo uma abordagem radicalmente diferente dos modelos existentes.

Palavras-chave

Blockchain, identidade digital, internet das coisas.

¹ Alex oliveira abreu batista, UFG, alexoab@gmail.com

² Emillie Rebecca Bastos Dias, UFG, emillie.info@gmail.com

³ Murilo Borges Silva, UFG, muriloborgessilva@gmail.com

***Blockchain*-based digital identification: A disruptive concept in cyberspace.**

Abstract

A *blockchain*-based digital identity system can provide security of access and reliability of information from complex transactions, documentary or financial, to basic forms on websites and social networks. *blockchain* is a technology concept that provides a decentralized system of operations in a secure, stable and intermediated way, in which all transactions are registered cryptographically in a distributed peer-to-peer network. All digital events are in a public of records by consensus of the majority of participants, in a permanent, traceable and transparent manner. The rise of *blockchain* has raised great expectations of revolutionizing the business models currently adopted. In the traditional business model, the authenticity of information about the identity of those involved in transactions and ownership of assets is guaranteed through physical documents and often recognized by government agencies or professionals endowed with public records. In addition, to have access to content on websites and social networks, it is necessary to fill in personal data frequently. Usually, in digital media, the validation of these data is not efficient. Creating fake profiles and false information on the internet is an easy and common practice.

This paper aims to present a new pattern of behavior in cyberspace, based on the trust protocol *blockchain*, analyzing future possibilities of application, from a digital social reputation, authentic identity, to financial incentives, where it can be used for rewards for posts, with pretension to be a radically different approach to existing models.

Keywords

Blockchain , digital identity internet of things.

Introdução

Identidade, palavra derivada do latim *identitas*, é o agrupamento de atributos e particularidades que caracterizam um indivíduo, o reconhece e o diferencia dos demais.

“A identidade digital é o que somos na internet, ou melhor, o que a internet diz que somos para os demais. Esta identidade digital não está definida desde o princípio. Ela se constrói com a nossa participação, direta ou indiretamente, em diversos sites disponíveis na internet. As omissões, assim como as ações, também constituem parte de nossa identidade pelo o que deixamos de fazer. Os dados, as imagens, os contextos e o lugar onde estão acessíveis proporcionam nosso perfil online.” (Pantallas Amigas, 2018)

Constantemente, os sites solicitam a criação de perfis e senhas para permitir o acesso a conteúdos e serviços, como compras online, contas de e-mails, transações

bancárias, redes sociais, busca de empregos, comunicação com outras pessoas, solicitação de documentos ou serviços do governo, download de arquivos, cursos à distância ou até mesmo participação em sorteios online. Desta forma, é comum que um indivíduo possua uma numerosidade de identidades na internet. Não é possível garantir a autenticidade da identidade e das informações fornecidas pelo usuário. Esse fato favorece a criação de perfis falsos e a utilização destes perfis para disseminação de informações inverídicas, prática de bullying, fraudes, difamação ou simplesmente o acesso e a publicação de informações de forma anônima (Ardanaz, 2015).

A verificação da identificação digital é uma situação crítica. No setor financeiro, por exemplo, a confiança mútua entre os indivíduos envolvidos em operações é importante, além da conformidade com regulamentos, avaliação de limites de crédito e possibilidade de ofertas de produtos personalizadas ao consumidor.

“Hoje, uma transação que exige identificação – seja para um pagamento, um empréstimo ou outra operação – significa coletar comprovante físico por meio de um canal digital (como a fotografia de uma carteira de motorista) ou depender de processos de reconhecimento do cliente (KYC, *know your customer*, na sigla em inglês) pelas instituições financeiras.” (Deloitte, 2016).

Os problemas decorrentes da vulnerabilidade da identificação digital não ocorrem apenas no setor financeiro. Eles também são provenientes do comércio, entretenimento, educação, serviços do governo e todas as áreas nas quais é necessário se identificar para ter a permissão de acesso.

“O mundo de IDs de usuários, senhas e perguntas de segurança é um modelo falho. Não é questão de se, mas de quando isso vai mudar”, diz Gary McAlum (2017, *apud Yurcan*, 2017), chefe de segurança da USAA, uma organização financeira em San Antonio, Estados Unidos.

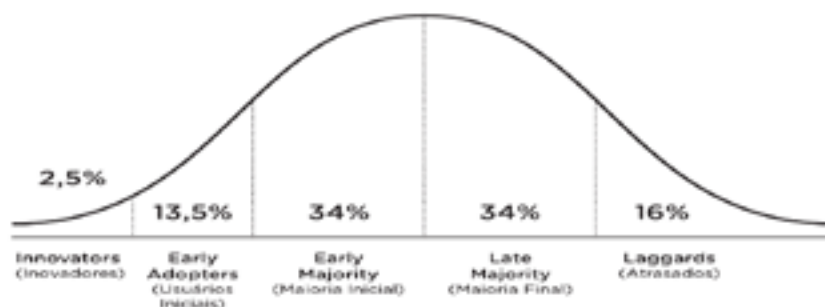
Neste cenário, a aplicação de *blockchain* para o tratamento das vulnerabilidades da identidade digital surge como uma alternativa inovadora e promissora, tornando-a mais segura e confiável.

Rogers (2003), em seu estudo, segmentou o processo de adoção de uma inovação em cinco grupos de indivíduos, que passam a ter contato e a usar essa inovação ao longo do tempo. O primeiro são os inovadores, público mais técnico, que propõe soluções de implementação para problemas complexos. Cerca de 2,5% são adeptos a testar ideias novas e disruptivas. Na sequência, 13,5% são *early adopters*, (tradução livre, usuários iniciais), pessoas não diretamente envolvidas na inovação, mas querem ter acesso mesmo que a ideia ainda não tenha sido testada. Neste ponto, do início da atividade da parábola, por alguma razão é desconhecida pela massa do mercado. Rogers (2003) responsabilizou os dois primeiros grupos iniciais, 16% uma minoria, segundo os seus estudos, de propagar ou não a anatomia de uma inovação as massas.

MAIO
9-11
UFG/BR

Popularizando a nova ideia, chegando até a maioria inicial (*early majority*) 34%, que representa uma fatia significativa para inovação. O processo continua, atingindo a maioria final (*late majority*) 34% e, fechando, na declividade da parábola, os atrasados (*laggards*), que simplesmente apenas adotam a inovação por falta de opção.

Figura 1: Classificação dos adotantes Rogers (2003).



Fonte: Rogers (2003).

Com essas divisões, e aprofundando mais a compreensão, na barreira formada entre os *early adopters* é a maioria inicial. Gladwell (2000) conceitua como ponto da virada, termo muito utilizado em seus livros, *The Tipping Point*, quando uma inovação deixa de estar restrita a um grupo pequeno formado pelos inovadores e os *early adopters*, passando a ser conhecida, já no ponto para a virada, a primeira fatia da massa de mercado. Nesse ponto a adoção praticamente triplica. É neste cenário que o *blockchain*, a inovação de Nakamoto se encontra. Cruzar essa barreira significa levar o conceito *blockchain* à massa do mercado e destravar um processo de adoção mais amplo.

Uma vez apresentados alguns momentos relevantes do potencial do marco histórico da internet de valor, aborda-se um paralelo entre o início do problema com soluções colaborativas no ciberespaço.

A gênese do blockchain e um novo padrão de comportamento no ciberespaço

A tecnologia *blockchain* teve a sua origem no âmbito financeiro e vem se tornando conhecida desde o surgimento da criptomoeda *Bitcoin*.

De acordo com Kikitamara (2017), em um fórum⁴¹ conhecido como "*The Cryptography Mailing*", Satoshi Nakamoto compartilhou a ideia precursora de um sistema econômico alternativo e descentralizado, sem intermediários, mas passível de verificação por todos os usuários da rede de nós (*peer-to-peer*). As transações efetuadas neste meio seriam registradas criptograficamente em um banco de dados distribuído, posteriormente denominado *blockchain*.

De forma simplificada, de acordo com Franco e Bazan (2018) podemos entendê-lo como um registro de dados extremamente confiável. Todos os membros da rede podem ter uma cópia desse registro e verificar as transações que são feitas. Nakamoto uniu a confiança entre os participantes na rede, graças o sistema robusto e seguro que foi descrito. Sendo ele o responsável por criar a maior parte do protocolo, aceitava raras contribuições de terceiros.

Não se sabe ao certo se Satoshi Nakamoto, pseudônimo, trata-se de uma pessoa desconhecida ou um grupo de pessoas responsáveis pelo desenvolvimento do bitcoin. (Gupta, 2017).

Em seu artigo, intitulado *“Bitcoin: a peer-to-peer electronic cash system”*, publicado em plena crise financeira de 2008 em uma lista de discussão sobre criptografia, Nakamoto propõe um sistema de moeda eletrônica *peer-to-peer* como solução para as complexidades, vulnerabilidades, ineficiências e custos das transações que ocorrem no sistema financeiro atual, o qual elimina os intermediários deste processo.

(..)O que é necessário é um sistema de pagamento eletrônico baseado em prova criptográfica em vez de confiança, permitindo que duas partes dispostas façam transações diretamente entre si sem a necessidade de um terceiro. As transações que são computacionalmente impraticáveis ao reverso protegerão os vendedores de fraude, e os mecanismos de custódia de garantia podem ser facilmente implementados para proteger os compradores. (Nakamoto, 2008, p.1, tradução nossa).

Três meses após o anúncio, Nakamoto disponibilizou gratuitamente o seu código-fonte aberto para quem quisesse baixá-lo e colaborar com a construção da rede do sistema.

Como reação inicial, demais ramificações da tecnológica *blockchain* levaram entusiastas a vislumbrarem um potencial ainda maior, capaz de transformar outras indústrias além do setor financeiro.

O conceito de blockchain está baseado na segurança de dados, o que torna desnecessário haver um órgão central para o estabelecimento de confiança entre as partes envolvidas. Em seu funcionamento, o *blockchain*, tem uma forma de registro que funciona em uma rede distribuída de usuários. Entende-se como um registro de dados extremamente confiável, onde os membros da rede podem ter uma cópia desse registro e verificar as transações que são realizadas. Assim, temos vários olhares direcionados para as movimentações financeiras ou informacionais. Para que uma transação seja efetivamente incluída no registro, usuários “especiais”, chamados mineradores, resolvem problemas matemáticos complexos para atestar a veracidade da transação, gastando, para isso, poder computacional e energia elétrica. Basicamente,

os mineradores precisam provar que uma transação é considerada verdadeira. Esse modelo é conhecido como prova de trabalho, do inglês *Proof-of-Work ou PoW*.

Dando sequência ao fluxo, todas as transações geram entradas e saídas que precisam condizer umas com as outras (um bloco de correntes sequenciadas). Todas as transações são anotadas e para cada uma delas é gerada uma saída, que indica se o valor envolvido foi atribuído ou não. Quanto mais blocos são adicionados à sequência, torna-se mais difícil a possibilidade de alteração dos dados, pois seria necessário alterar toda a sequência de blocos até chegar àquele em que informação pretendida registrada.

“O blockchain é como um nugget de frango. Você pega o animal (informação original) e o processa várias e várias vezes até chegar ao formato de um nugget (informação processada). Tentar reverter o processo é como tentar fazer o nugget voltar a ser um frango – o que, atualmente, é impossível.” (Franco e Bazan, 2018)

Devido à confiabilidade e segurança, estão surgindo várias oportunidades de aplicação desta tecnologia para vários setores da economia. Existem várias iniciativas de aplicações do *blockchain*, como na indústria da música e sua preocupação com direitos autorais, contratos inteligentes, identidade digital, auditoria, serviços de governo, combater a crise de refugiados, prevenção de fraudes eleitorais, saúde, educação, etc. (Tapscott, 2016).

Identidade Digital

A realidade digital e a realidade física estão se mesclando em um único modo de vida moderno e integrado. Nesse novo contexto, surge um novo modelo de identidade, a identidade digital. Essa identidade deve aprimorar questões relacionadas a privacidade e segurança em todo o mundo físico e digital. (Simons, 2018). Conforme O’alloran (2018, apud Mathuros, 2018), é preciso garantir que esta nova abordagem seja estabelecida de maneira sustentável, inclusiva e confiável, na qual governos, organizações internacionais, sociedade civil e empresas desempenharão um papel fundamental na criação deste futuro.

O conceito de identidade pode ser visto de diferentes perspectivas e é aplicável em diferentes contextos, dependendo do propósito para o qual a identidade digital é usada. Segundo Clark et al. (2016), o ciclo de vida da criação de uma identidade digital ocorre em três fases: registro (incluindo o cadastro e a validação), a emissão de documentos ou credenciais e a autenticação conforme mostra a Figura 2.

Figura 2: Ciclo de vida do gerenciamento de identidade.



Fonte: Kikitamara (2017), tradução nossa.

Na primeira fase, chamada de registro, inclui o cadastro (inscrição) e a validação dos dados. O registro é a parte mais importante da criação de uma identidade digital, onde são capturados e gravados os atributos de um indivíduo. Os atributos e a forma de capturá-los influenciam na credibilidade da identidade. Quando uma pessoa assume uma identidade durante o registro, esta identidade é validada confrontando os dados apresentados com os dados existentes. Essa validação pode ser realizada por meio de existência (quando é possível entrar em contato para confirmação de dados), por exclusividade (quando apenas uma pessoa reivindica a identidade, realizando combinações de atributos para determinar tal identidade) e por ligações (conferindo outras fontes existentes, como registros civis, fiscais, policiais, etc).

O registro de uma identidade passa pelo processo de emissão ou credenciamento, sendo esta a segunda fase. Para a identidade digital, os certificados devem ser eletrônicos, armazenando e permutando dados eletronicamente. Estas credenciais eletrônicas podem ser por meio de *smartcards* (cartões inteligentes), código de barras 2D, identidade digital móvel ou na nuvem, dentre outros. Após o registro e credenciamento, o indivíduo pode utilizar sua identidade digital para acessar o conteúdo desejado, sendo esta a fase denominada uso. Para acessar tais conteúdos, o usuário deve ser autenticado por meio de dados informados. De acordo com a IBM (2017), o

gerenciamento de identidade é um ponto crítico para a segurança da informação, pois a maioria dos tipos de controle de acesso e permissões é baseada neste gerenciamento. A identidade digital é fundamental para a realização de transações comerciais e as relações sociais na internet, permitindo formas de contato entre bilhões de usuários no mundo digital. Além disso, o gerenciamento de identidade tradicional favorece ciberataques, pois centraliza os dados em apenas um repositório de alto valor, gerando apenas um ponto passível de falha. Outro ponto de criticidade importante é a capacidade de criação de diversas identidades digitais pertencentes a um mesmo indivíduo, fato bastante comum na internet. Uma pesquisa realizada pela Intel em 2016 e citada pela IBM (2017, apud Bond, 2017) mostra que há uma pessoa atuante virtualmente possui em torno de 27 diferentes identidades digitais. Isso possibilita a criação de falsos perfis que podem ser utilizados de forma negativa e até mesmo criminoso. A criação de muitos perfis também pode comprometer a segurança, visto que os usuários costumam cadastrar senhas comuns a todos eles, o que aumenta o risco de acesso indesejado.

Identificação Digital baseada em *blockchain*

O modelo de confiança distribuída, *blockchain*, tem o potencial de ser aplicado ao sistema de identidade digital, permitindo que os usuários tenham controle sobre a própria identidade e compartilhem seus dados de forma consentida. Esse conceito é conhecido como identidade auto-soberana, do inglês *self-sovereign identity*. (Windley, 2018)

A utilização de *blockchain* associado à criptografia possibilita que os registros de identidade digital sejam imutáveis e que a vinculação de identidade a transações ou outros dados possa ocorrer somente mediante autorização explícita do usuário. Jehl (2017) explica que a arquitetura distribuída e descentralizada, utilizada pela maior parte dos sistemas de identificação baseados em *blockchain*, oferece mais segurança contra ciberataques, violações de dados e corrupção de dados. Além disso, o usuário evita que seja dado amplo consentimento de acesso a aplicativos e serviços, permitindo que sejam compartilhados apenas os dados mínimos necessários para cada transação e evitando a exposição de maiores informações pessoais com as empresas ou pessoas com as quais interage.

Kariuki (2017) explica que o *blockchain* enxerga a identidade autenticada de forma imutável, inquestionável e segura, por meio de assinaturas digitais baseadas em criptografia de chave pública. Desta forma, proporciona que transações sejam assinadas e a comprovação de informações e propriedades de ativos digitais sejam confirmadas em um ambiente seguro. Isso facilita o compartilhamento e integração de informações com as organizações e outros usuários, reduzindo custos envolvidos no modelo centralizado tradicional.

A identidade digital única baseada em *blockchain* também possibilita que os dados sejam sempre atualizados com as informações mais recentes do usuário. A proposta de aplicação do *blockchain* neste processo elimina a necessidade de interme-

diários, desta forma, evita-se que alguma instituição ou organização comprometa os dados de identidade do usuário.

Devido ao grande potencial apresentado pela aplicação do *blockchain*, empresas bastante conhecidas como Microsoft, IBM, Deloitte e governos estão investindo em projetos de identidade digital baseados nesta tecnologia. Segundo Bonde (2017), a identidade digital única já é realidade em alguns países como Estônia, Cazaquistão e a Índia. Na Estônia, por exemplo, esta identidade unifica o acesso a diversos serviços como transações bancárias, solicitação de benefícios estatais, declaração de impostos, registros escolares, etc. (Thompson e Yu, 2017).

Em agosto de 2017, o governo brasileiro anunciou uma parceria entre o Ministério do Planejamento, a Microsoft e a *ConsenSys*, empresa especializada em *blockchain*, no desenvolvimento de um projeto piloto de um sistema de verificação de documentos e identidades. O objetivo do projeto foi avaliar como o *blockchain* pode auxiliar na verificação de documentos registrados em cartório incluindo carregamento de documentos e aprovação de assinaturas. O governo brasileiro foi o primeiro sul-americano a realizar uma Prova de Conceito (POC) em *blockchain*. (Canaltech, 2017).

A Microsoft desenvolve outros projetos com a aplicação de *blockchain* em parceria com o governo brasileiro. Ruvic (2018, apud Soprana, 2018) afirma que a empresa acredita que essa tecnologia pode contribuir no combate a corrupção no país, pois proporciona a imutabilidade, o registro permanente, o controle e a rastreabilidade de transações realizadas dentro de um sistema.

Uma nova regra de negócio é apresentado a seguir, propondo uma abordagem diferente dos modelos existentes, alicerçada nos atributos básicos da segurança da informação, padrões internacionais (ISO/IEC17799:2005)^{5*}. São elas descritas detalhadamente a seguir (adaptado de Derin Cag , fundador da Richtopia):

1.Reputação social digital: Um sistema de monetização, para lidar com notícias falsas através do estabelecimento de um “sistema de classificação de crédito” para jornalistas e blogueiros ou contedistas de rede social , que poderiam ser incorporados a todos os sites, associando a reputação e o grau de especialidade do autor no assunto a sua identidade digital única.

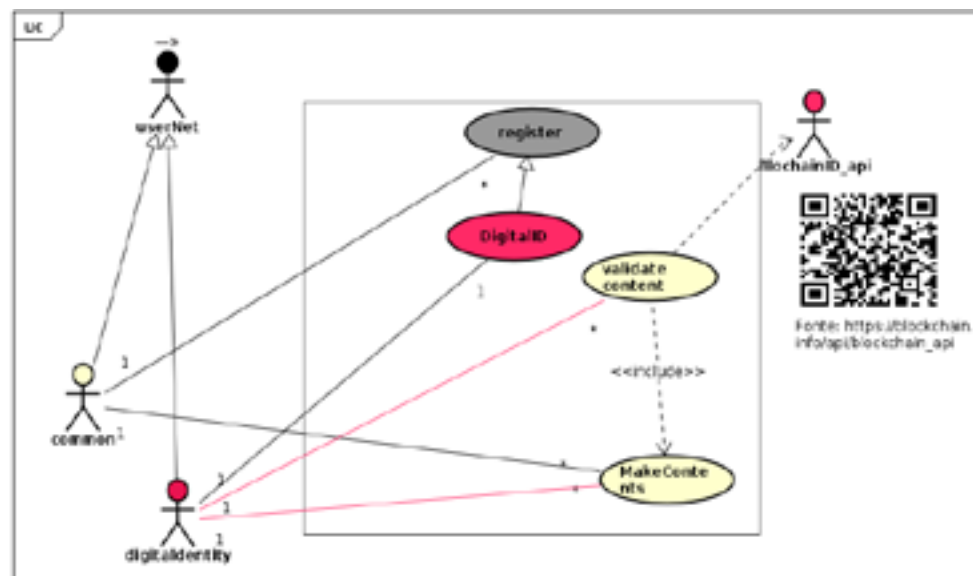
2.Autenticidade de conteúdo gerado: Todas as transações geram entradas e saídas que precisam condizer umas com as outras, formando um bloco de correntes seqüenciadas, garantindo dados proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

3. Identificação digital autêntica: Seria o atributo do não repúdio, propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormen-

te realizada. Quanto mais blocos são adicionados à sequência, torna-se mais difícil a alteração da informação, o que indica se o valor envolvido foi atribuído ou não.

Uma análise de caso de uso foi utilizada para cada abstração, definindo um conjunto de responsabilidades, conforme mostra a Figura 3.

Figura 3: Diagrama de caso de uso Identificação digital.



Fonte: Elaborada pelo autor.

Como podemos identificar, no ambiente virtual existiriam dois tipos de usuários, o *common user*, (usuário comum) e o *digital identify* (usuário com identificação digital), - sendo que este último criaria sua identificação digital única e exclusiva em uma plataforma (*DigitalID*). Ambos podem realizar cadastros e gerar conteúdos (*make contents*) no ciberespaço. Após de realizar seu cadastro, um fluxo de eventos será seguido.

Fluxo de eventos principais do caso de uso da identificação digital:

Caso de uso: A Identificação digital é adquirida após o usuário realizar cadastro na plataforma. O usuário terá posse de uma chave privada, e outra pública. Com a sua chave pública, o usuário a utilizará ou não para marcar seus conteúdos digitais. A assinatura digital só será validada após ser inserida ao bloco de correntes seqüenciadas, imutáveis e transacionais (*blockchain_api*). Sua chave privada estabelecerá a autenticidade do conteúdo gerado.

Fluxo excepcional de evento 1: O usuário, antes de registrar o conteúdo, no livro de registros, solicitará a "2FA"⁶⁵, como forma de identificação do usuário ao provedor de

serviço, utilizando uma combinação de dois métodos diferentes de autenticação. O dispositivo utilizado pode ser um *smartphone*, por exemplo, ou algum outro dispositivo que suporte esse tipo de operação e seja disponível ao usuário.

Fluxo excepcional de evento 2: O usuário poderá solicitar uma nova senha, via *e-mail*, mensagens de celular.

Fluxo excepcional de evento 3: O usuário poderá vincular sua monetização por meio de carteiras preexistentes no mercado de criptomoedas.

Fluxo excepcional de evento 4: A reputação social dependerá da interação das diferentes regras de negócios (redes sociais, por exemplo), por meio de contratos inteligentes, onde o *blockchain* poderia interagir com múltiplas plataformas simultaneamente em nome do usuário. Por exemplo, o *Facebook*, que poderia interagir com o *Twitter*, que poderia interagir com o *Instagram*, que poderia comunicar-se com qualquer outra por padrão, baseada em livros-razão distribuídos, melhorando a segurança, da internet de valor.

A tendência crescente de implementação com *blockchain* na indústria de rede social tem muitas possibilidades. Registrando entradas e saídas de forma concatenada como elos de uma corrente, é possível reduzir um comportamento muito comum no ciberespaço, a criação de perfis falsos e informações inverídicas, que são práticas fáceis e comuns na internet. Sem intermediações centrais, esse processo é um desafio, pois é a funcionalidade de controle geral que rende dividendos aos investidores. A ideia da confiabilidade sem a necessidade de um ente intermediário é bastante atrativa no meio digital e impactará como os negócios atuais são ditados atualmente. Pois, dessa forma, o controle de quem manusearia os dados e quanto mais tempo decorrido do registro, mais segurança seria possível ter sobre eles. Transações complexas, de caráter documental ou financeiro, podem ser realizadas de maneira intercontinental em poucos minutos, uma funcionalidade real aplicada no case de sucesso *Bitcoin*⁷.

Conclusão

A identidade digital é construída com a participação, direta ou indiretamente do usuário na internet, em diversos sites disponíveis e por meio de fornecimento de dados pessoais para a criação de perfis de usuários para acesso a conteúdos e serviços.

Com a identidade digital, surgiram problemas relacionados à segurança e a possibilidade de perfis múltiplos para um só usuário, que podem ser utilizados para diversas finalidades, como o anonimato, divulgação de informações falsas ou intenções fraudulentas. Dessa forma, surge o conceito de auto-soberania, no qual o indivíduo controla as suas próprias informações e quem as possui na rede. A utilização da auto-soberania

pode mudar a forma como os usuários gerenciam suas identidades digitais e dados disponíveis online.

A utilização de *blockchain* é uma proposta interessante para solucionar os desafios atualmente encontrados pela identidade digital. **O propósito deste artigo é continuar as possíveis funcionalidades para o futuro, da internet de valor, deixando o escopo aberto de modo colaborativo de ideias. Assim como ocorreu a ideia precursora de um sistema econômico alternativo descentralizada.** Os modelos de negócios existentes estão sendo redesenhados para se adaptarem aos novos tempos de grande avanço tecnológico. O *blockchain* tem o potencial de revolucionar a maneira de fazer negócios de uma forma eficiente e segura. Nesse cenário, onde a criação de uma identidade digital⁸⁸ única torna-se necessária, a tecnologia *blockchain* surge como alternativa para garantir a confiabilidade das transações sem a necessidade de intermediários ou autoridades centrais. Vislumbrando a grande potencialidade de suas aplicações em outras áreas, além do setor financeiro, empresas e governos estão investindo em pesquisas e desenvolvendo projetos para o desenvolvimento dessa tecnologia. As estruturas corporativas centralizadas terão que ser repensadas. O ambiente de negócios atual é volátil, incerto e complexo e passará por grandes transformações nos próximos anos, considerando o *blockchain* como uma tecnologia promissora para viabilizar esse avanço.

Notas

³ Site do fórum de criptografia disponível em: <http://satoshinakamoto.me/source/cryptography-mail-list>

⁴ Norma técnica disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306582>

⁵ Para saber mais acesse: <https://ssd.eff.org/pt-br/module/como-habilitar-autentica%C3%A7%C3%A3o-de-dois-fatores>

⁶ Mais informações: https://bitcoin.org/pt_BR; Pode ser acompanhado o tamanho deste registros já realizados neste: <https://blockchain.info/pt/charts/blocks-size>.

⁷ Participe do nosso em: <https://github.com/idigitalidentity0100/digital-ID.git7>

Referências

Pantallas Amigas. Disponível em: < <http://www.pantallasamigas.net/otros-webs/identidad-digital.shtm>>. Acesso em: 03 mar. 2018.

Ardanaz, Xabier Ferrer. **Riesgos de La identidad digital**, 2015. Disponível em: <<https://blogs.deusto.es/master-informatica/riesgos-de-la-identidad-digital/>>. Acesso em 01 mar. 2018.

Deloitte. **Picture perfect: A blueprint for digital identity**, 2018. Disponível em: <<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-digital-identity-online.pdf>>. Acesso em 03 mar. 2018.

- Yurcan, Bryan. **The Future of Digital Identity Is Up to Banks**, 2016. Disponível em <<https://www.americanbanker.com/news/the-future-of-digital-identity-is-up-to-banks>>. Acesso em 10 fev. 2018.
- Tapscott, Don. **How blockchains could change the world. McKinsey&Company**, 2016. Disponível em: <<https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world>>. Acesso em: 15 mar. 2018.
- Simons, Alex. **Decentralized Digital Identities and Blockchain – The Future as We See It**. Microsoft, 2018. Disponível em: <<https://cloudblogs.microsoft.com/enterprisemobility/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/>>. Acesso em 10 mar. 2018.
- Mathuros, Fon. **Digital Identity – Why It Matters and Why It’s Important We Get It Right**. World Economic Forum, 2018. Disponível em: <<https://www.weforum.org/press/2018/01/digital-identity-why-it-matters-and-why-it-s-important-we-get-it-right/>>. Acesso em 14 fev. 2018
- Clark, Julia et al. **Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation**. A joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper, 2016. Disponível em:<<https://secureidentityalliance.org/public-resources/4-july-2016-report-digital-identity/file>>. Acesso em 22 mar. 2018.
- IBM. **Identity management with blockchain**, 2017. Disponível em: <<https://www.ibm.com/blockchain/identity/>>. Acesso em 05 fev. 2018.
- Bond, Stewart. **It Was Only a Matter of Time – Digital Identity on Blockchain**. IDC Link – Real-time IDC Research, 2017. Disponível em: <<https://public.dhe.ibm.com/common/ssi/ecm/gi/en/gil12346usen/GIL12346USEN.PDF>>. Acesso em 03 fev. 2018.
- Windley, Phillip. **How blockchain makes self-sovereign identities possible**. ComputerWorld, 2018. Disponível em: <<https://www.computerworld.com/article/3244128/security/how-blockchain-makes-self-sovereign-identities-possible.html>>. Acesso em 22 fev. 2018.
- Jehl, Laura E. **Blockchain – The Future of Digital Identity?** Bloomberg Law, 2017. Disponível em: <<https://bakerlaw.com/webfiles/Privacy/2017/Articles/12-13-2017-Jehl-BNA-Blockchain.pdf>>. Acesso em 25 mar. 2018.
- Kariuki, David. **Blockchain Can Improve Digital Identification Greatly**. Cryptomorrow, 2017. Disponível em:< <https://www.cryptomorrow.com/2017/12/07/digital-identification-blockchain/>>. Acesso em 27 fev. 2018.

MAIO
9-11
UFG/BR

- Thompson, Kirsten; Yu, Eric. **Estonian Blockchain-Based ID Card Security Flaw Raises Issues About Identity**. CyberLex, 2017. Disponível em: <<https://www.canadiancybersecuritylaw.com/2017/09/estonian-blockchain-based-id-card-security-flaw-raises-issues-about-identity>>. Acesso em 25 mar. 2018
- Canaltech. **Ministério do Planejamento desenvolve projeto com tecnologia blockchain**. Canaltech, 2017. Disponível em: <<https://canaltech.com.br/governo/ministerio-do-planejamento-desenvolve-projeto-com-tecnologia-blockchain-99334>>. Acesso em 25 mar. 2018.
- Soprana, Paula. **Microsoft planeja usar blockchain para combater corrupção no Brasil**. O Globo, 2018. Disponível em: <<https://oglobo.globo.com/economia/microsoft-planeja-usar-blockchain-para-combater-corrupcao-no-brasil-22492159>>. Acesso em 25 mar. 2018.
- Kikitamara, Sesaria. **Digital Identity Management on Blockchain for Open Model Energy System**. Nijmegen: Radboud University, 2017. 74 f. Tese (Mestrado em Ciências da Informação), Nijmegen, 2017.
- Gupta, Manav. **Blockchain For Dummies**, IBM Limited Edition. Hoboken, NJ: John Wiley & Sons, Inc, 2017.
- Franco, André; Bazan, Vinicius. **Criptomoedas: Melhor que dinheiro**. São Paulo: Empiricus, 2018. 206 p.
- Gladwell, Malcolm. **O ponto da virada**. Rio de Janeiro: Sextante, 2009.
- Rogers, Everett M. **Diffusion of innovations**. 5th ed. New York: Free Pass, 2003.
- Nakamoto, Satoshi. **Bitcoin: A Peer-to-peer Electronic Cash System**, 2008. Disponível em: <<http://pdos.csail.mit.edu/6.824/papers/bitcoin.pdf>>. Acesso em 24 nov. 2017.
