revista Eptic
VOL. 22, Nº 2, MAI.-AGO. 2020

Rede descentralizada *blockchain*: cultura do "faça você mesmo" com estrutura matemática de algoritmos de consenso

Red descentralizada *blockchain*: cultura "hágalo usted mismo" con la estructura matemática de los algoritmos de consenso

Blockchain decentralized network: "do-it-yourself" culture with mathematical framework of consensus algorithms

Magaly Parreira do Prado

Doutora pelo Programa de Estudos Pós-Graduados em Comunicação e Semiótica da Pontifícia Universidade Católica de São Paulo (PUC-SP), pós-doutoranda na Escola de Comunicações e Artes da Universidade de São Paulo

Contato: magalyprado@usp.br

Submetido em: 02.04.2019
Aprovado em: 25.08.2019

Resumo

Em plena era da desconfiança, a sociedade se depara com um novo esquema: confiar seus dados a plataformas que alardeiam privacidade. Entre prós e contras, é preciso reflexão crítica. É impróprio da nossa cultura checar falhas e fraudes; sempre dependemos de mediadores de transações. A proposta é escrutinar o funcionamento de redes que se dizem seguras, sem taxas nem atravessadores, em sistemas para os quais fornecemos arquivos valiosos, na esfera econômica e fora dela, uma vez que a plataforma *blockchain* ultrapassa questões financeiras. A hipótese é que serão confiáveis ao controlar *bugs* e ataques. O método é traçar o estado da arte de uma comunicação com estrutura matemática na tentativa de criar uma cultura do consenso.

Palavras-chave: *Blockchain*. Privacidade. Economia. Redes. Confiança.

Resumen

En plena era de la desconfianza, la sociedad se enfrenta a un nuevo esquema de confiar sus datos: plataformas que alardean la privacidad. Entre pros y contras, se necesita reflexión crítica. Es impropio de nuestra cultura cheque fallas y fraudes, siempre dependemos de mediadores de transacciones. La propuesta es escudriñar el funcionamiento de redes que se dicen seguras, sin tasas ni atravesadores en los sistemas donde suministra archivos valiosos, en la esfera económica y fuera de ella, tanto que la plataforma *blockchain* sobrepasa cuestiones financieras. La hipótesis es que serán confiables al controlar *bugs* y ataques. El método es trazar el estado del arte de una comunicación con estructura matemática en el intento de crear una cultura del consenso.

Palabras clave: Blockchain. Privacidad. Economía. Redes. Confianza.

Abstract

In the age of distrust, society is faced with a new scheme of trusting its data: platforms that boast of privacy. Between pros and cons, it takes critical reflection. It is inappropriate for our culture to check for flaws and frauds; we are always dependent on transaction mediators. The proposal is to scrutinize the workings of networks that claim to be secure, without fees or cross-sellers in the systems where we provide valuable archives, both economically and externally, so much so that the blockchain platform overcomes financial issues. The hypothesis is that they will be reliable in controlling bugs and attacks. The method is to map the state of the art of communication with mathematical structure in an attempt to create a consensus culture.

Keywords: Blockchain. Privacy. Economy. Networks. Trust.

Crítica permanente

Em plena era da desconfiança entre pessoas e instituições, a sociedade se vê à frente de um novo esquema: confiar seus dados a plataformas que alardeiam privacidade das informações valiosas de seus indivíduos e empresas. Trata-se de um dos temas mais quentes da atualidade, e nós, da comunicação e da cultura, não podemos prescindir de nos colocar em diálogo permanente para um possível entendimento. Entre prós e contras − próprios de uma tecnologia recente −, concluímos que mesmo as pessoas fora da área estrita da economia, melhor dizendo, da nova economia, precisam ao menos dar início a uma reflexão crítica. Dizemos ao menos, pois não é próprio de nossa rotina ficar checando deslizes, falhas, nem mesmo fraudes, ou seja, sempre ficamos na dependência de mediadores de nossas transações. Assim, a proposta é que se comece a escrutinar os meandros de funcionamento de plataformas que se dizem seguras, sem ataques de hackers (do mal), sem cobranças de altas taxas de intermediação, bem como sem os atravessadores em sistemas para os quais fornecemos nossos arquivos. Aliás, arquivos de toda sorte, como documentos e outros que necessitam de um mínimo de privacidade, na esfera econômica e fora dela, já que a rede blockchain, que vamos procurar entender a partir deste artigo, ultrapassa questões meramente financeiras.

O método é a reunião das informações de autores e especialistas para traçar o estado da arte de uma comunicação com estrutura matemática na tentativa de criar uma cultura do consenso, quando a concordância vem da maioria. Não se trata ainda de fazer análises, não somente porque a estrutura é praticamente nova, mas também porque está em permanente adaptação. A hipótese é que esse tipo de plataforma numérica pode vir a ser confiável e infalível à medida que os hackers (do bem) possam ser remunerados o suficiente (não apenas com criptomoedas) no intento de oferecer o empenho necessário para desfazer possíveis bugs e ataques daqueles que vão tentar tirar vantagens nas empreitadas de menor porte, mais suscetíveis a deixar brechas.

"Descobertas recentes unificaram os campos da ciência da computação e da teoria da informação no campo da teoria algorítmica da informação", nos diz Szabo (1994)[1].

> A informação é usada para descrever as estruturas culturais da ciência, instituições legais e de mercado, arte, música, conhecimento e crenças. A informação também é usada para descrever as estruturas e processos de fenômenos biológicos e fenômenos do mundo físico. A aplicação mais óbvia de informações é para os domínios de engenharia de computadores e comunicações (SZABO, 1994).

Em 2008, no auge da crise financeira mundial e da bolha imobiliária, foi criado um sistema econômico alternativo na internet que visava a ser se-

1. "Tal método nos daria uma medida de conteúdo de informação absoluta, a quantidade de dados que precisa ser transmitida na ausência de qualquer outro conhecimento a *priori*. O método de descrição que atende a esses critérios é a *complexidade de Kolmogorov*: o tamanho do programa mais curto (em bits) que, sem dados adicionais, calcula a sequência e a termina" (SZABO, 1994).

guro para transferir itens de valor, tanto que foi denominado "protocolo de confiança". A inovação foi alardeada como uma rede sem burocracia, controlada e verificada pelos próprios participantes através de uma estrutura de dados chamada de *blockchain* − um registro de transações como um grande arquivo que serve para catalogar, rastrear, certificar, autenticar informações e objetos de valor acessível aos usuários interessados. As transações são armazenadas em blocos que estão acorrentados um ao outro. Trata-se de um banco de dados e uma cadeia de blocos (como diz o nome) que sempre carrega um conteúdo junto a uma impressão digital. O processo se dá de forma que o bloco posterior vai conter a impressão digital[2] do anterior mais o próprio conteúdo e, com essas duas informações, gerar a própria impressão digital, e assim por diante. No caso do Bitcoin, esse conteúdo é uma transação financeira (um mercado ainda não regulamentado no Brasil) que grava e registra de forma coletiva as negociações de compra e venda de moedas digitais sem vínculos com empresas, governos ou bancos, e guardadas em uma carteira virtual, que pode ser até mesmo o celular (QUINIOU; DEBONNEUIL, 2019; TORO INVESTIMENTOS, 2019; PRADO, 2018, tradução nossa).

> Dessa forma, é possível acessar essa base de dados pelo computador e ver uma negociação que ocorreu entre duas pessoas: uma na China e outra na Alemanha, por exemplo. Os detalhes sobre quem são os envolvidos não é possível saber, pois tudo é criptografado[3]. Mas dá para saber que aquela transação ocorreu e que ela está gravada na blockchain para sempre. E falamos para sempre no sentido literal. Afinal, não é possível desfazer ou alterar uma transação após ela ser inserida no sistema. Ou seja, não dá para voltar atrás caso tenha se arrependido de vender seus Bitcoins (TORO INVESTIMENTOS, 2019).

Na visão dos editores da *MIT Technology Review* (EXPLAINER..., 2019, tradução nossa), *blockchain* é "uma estrutura matemática para armazenar dados de uma maneira quase impossível de falsificar. Pode ser usado para todos os tipos de dados valiosos". Em definição de 2019 de Mike Orcutt (2019, tradução nossa):

> Um *blockchain* é um banco de dados criptográfico mantido por uma rede de computadores em que cada um armazena uma cópia da versão mais atualizada. Um *blockchain protocol* é um conjunto de regras que determina como os computadores na rede, chamados *nós* [futuros mineradores], devem verificar novas transações e adicioná-las ao banco de dados. O protocolo emprega criptografia, teoria dos jogos e economia para criar incentivos para os *nós* trabalharem para proteger a rede em vez de atacá-la para ganho pessoal. Se configurado corretamente, esse sistema pode tornar extremamente difícil e caro adicionar transações falsas, mas relativamente fácil verificar as transações válidas.

2. "O autor tira uma impressão digital do documento (sua *hash*) e a criptografa com sua chave privada. Assim, é suficiente para receber o documento para descriptografar com a chave pública do remetente a impressão digital (que garante o remetente), que é comparada com a impressão do documento a ser verificado quanto à autenticidade (que garante o conteúdo do documento)" (QUINIOU; DEBONNEUIL, 2019, tradução nossa).

3. "A criptografia permite que duas pessoas troquem mensagens sem que essas mensagens sejam interceptadas por terceiros. Isso consiste em determinar um algoritmo para criptografar as mensagens e outro para decifrá-las. A criptografia é uma disciplina fundamental para entender o desenvolvimento de *blockchains*" (QUINIOU; DEBONNEUIL, 2019, tradução nossa).

"I've been working on a new electronic cash system that's fully peer-to-peer[4], with no trusted third party."[5] Essas foram as palavras de Satoshi Nakamoto — pseudônimo do criador do Bitcoin em 2009 — em uma mensagem enviada para uma lista de discussão no final de 2008 cujo enfoque era criptografia. "Um *link* para um *white paper*[6] de nove páginas foi incluído descrevendo uma tecnologia que, segundo alguns agora estão convencidos, irá ocasionar uma disrupção no sistema financeiro" (NAKAMOTO, 2008).

Encadeamento de blocos

Um bloco contém, além de transações, o *hash* do bloco anterior. "A modificação de uma transação, portanto, modifica não apenas o bloco ao qual ele pertence, mas todos os blocos que o seguem. A estrutura do *blockchain* dá ao livro distribuído sua imutabilidade" (QUINIOU; DEBONNEUIL, 2019, p. 27, tradução nossa). Mas atenção: "muitas vezes, por abuso de linguagem, *blockchain* refere-se a qualquer tipo de livro distribuído e não apenas aqueles que são baseados em uma cadeia de blocos".

Cada bloco[7] encadeado é formado por várias informações sobre as diversas transações e possui uma assinatura digital única, chamada de *hash*[8] ou *proof of work* (*PoW*, na sigla em inglês). Essa assinatura funciona como uma impressão digital do bloco e ajuda a dar mais segurança ao processo, já que tudo é criptografado (TORO INVESTIMENTOS, 2019).

> O *hash* é uma função matemática que pega uma mensagem ou arquivo e gera um código com letras e números que representa os dados que o usuário inseriu. Essencialmente, o *hash* pega uma grande quantidade de dados e transforma em uma pequena quantidade de informações. É a "impressão digital" de algum arquivo, ou, no caso do *blockchain*, de um bloco. Nesse sistema de blocos encadeados, essa impressão digital é fundamental. O *hash*[9] vai assinar o conteúdo do bloco; caso qualquer informação seja alterada, o *hash* muda. Quando você gera um novo bloco que também contém o *hash* do anterior, cria uma espécie de selo: é possível verificar e sinalizar se algum bloco foi alterado, para então invalidá-lo (PRADO, 2018).

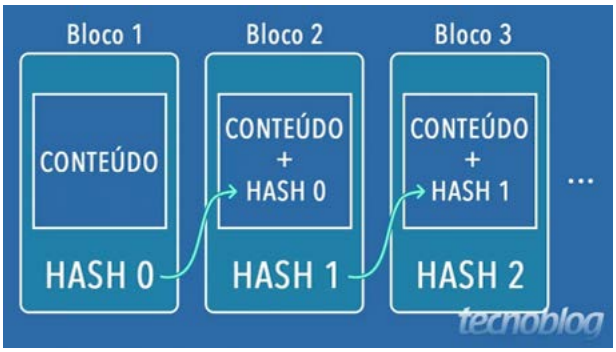

Figura 1 – Imagem usada por Ronan Damasco, diretor de tecnologia da Microsoft.

Fonte: Damasco (2017). No Tecnoblog

4. "Uma rede peer-to-peer é uma rede de computadores em que a comunicação acontece diretamente de um computador para outro. O modelo peer-peer se opõe ao modelo cliente-servidor, no qual um computador é o cliente e o outro é o servidor. A internet permite que os computadores comuniquem informações peer-to-peer (ou seja, sem intermediários). Tecnologias blockchain permitem que dois computadores troquem a escassez (ou o valor) peer-to- peer (sem ter que confiar em um terceiro)" (QUINIOU; DEBONNEUIL, 2019, p. 40, tradução nossa).

5. "Eu tenho trabalhado em um novo sistema de caixa eletrônico que é totalmente par a par [pessoa a pessoa, ponto a ponto], com nenhuma fonte ou host confiável" (tradução nossa).

6. De modo geral, trata-se de uma espécie de relatório usado em negócios ou marketing, de formato conciso, porém aprofundado, sobre um assunto complexo. Pode ser um documento oficial de governos ou organizações internacionais. Serve para divulgar informações, dados etc., mostrar a filosofia de uma empresa ou o propósito de um produto. A ideia é atrair um público-alvo, como os clientes.

7. "Cada bloco possui uma capacidade máxima e é criado em um ritmo constante. No caso do Bitcoin, são adicionados novos blocos à rede

O algoritmo de consenso mais comum é a prova de trabalho

Um algoritmo de consenso é um mecanismo pelo qual cada rede *blockchain* chega a um acordo. Redes públicas (descentralizadas) de *blockchain* são construídas como sistemas distribuídos e, como não dependem de uma autoridade central, os computadores da rede precisam concordar na validação das transações. É nesse ponto que os algoritmos de consenso operam, garantindo que as regras do protocolo estão sendo seguidas e que todas as transações ocorram de forma confiável, fazendo com que cada moeda seja gasta uma única vez (O QUE..., 2018).

"O algoritmo de consenso é um elemento fundamental na governança do *blockchain* e define as regras que a atualizam" (QUINIOU; DEBONNEUIL, 2019, p. 13). Assim, a rede descentralizada de blockchain é "segura por um mecanismo de consenso[10] de prova de trabalho (*proof of work*)[11], que usa poder de processamento para resolver cálculos matemáticos muito complicados para assegurar que o hash criptográfico do bloco seja válido" (PRADO, 2018)[12]. Em outras palavras: *PoW* é o primeiro algoritmo introduzido na rede de *blockchain*. "Muitas tecnologias de blockchain usam este modelo de consenso na comunidade blockchain para confirmar todas as suas transações e produzir blocos relevantes para a cadeia da rede" (PRADO, 2018). No entanto, "a prova de trabalho tem suas limitações. A rede parece crescer bastante e, com isso, precisa de muito poder computacional" (PRADO, 2018). O processo está aumentando a sensibilidade geral do sistema.

> Nakamoto combinou ferramentas de criptografia estabelecidas com métodos derivados de décadas de pesquisa em ciência da computação para permitir que uma rede pública de participantes que não necessariamente confiam uns nos outros concorde, e que um livro contábil compartilhado reflita a verdade. [...] Crucialmente, elimina a necessidade de uma autoridade central para mediar a troca eletrônica da moeda (PRADO, 2018).

"A consequência direta dessa descentralização é que o banco de dados deixa de ter um ponto central de falhas e vulnerabilidades", conforme pesquisa de Ferreira (2017, p. 7), que prossegue: "Um potencial hacker teria que atacar todos (ou no mínimo a maioria) os participantes para conseguir realizar qualquer alteração significativa, o que se torna cada vez mais impraticável à medida que o número destes participantes aumenta".

A tecnologia *blockchain*, além de gerenciar um registro de todas as transações, possui características inerentes à arquitetura e ao design blockchain que fornecem propriedades como transparência, robustez, auditabilidade e segurança (GREENSPAN, 2015; CHRISTIDIS; DEVETSIKIOTIS, 2016 apud CASINO; DASAKLIS; PATSAKIS, 2018). É uma estrutura vinculada e distribuída *peer-to-peer* que também pode ser usada para manter a ordem das transações e evitar gastos duplos (NAKAMOTO, 2008).

a cada 10 minutos aproximadamente. Assim sendo, neste período de tempo, são verificadas e adicionadas à *blockchain* diversas transações de compra ou venda de Bitcoin entre usuários. Só depois de um bloco inteiro ser preenchido e verificado é que uma quantidade da moeda pode sair da carteira virtual do usuário que vendeu e passar para a carteira de quem comprou. Se a pessoa estiver logada na rede, poderá ver a criptografia referente a essa mesma transação. Porém, sem conseguir ver a identidade dos envolvidos nem alterar esse processo. Como esses blocos são selados por códigos criptográficos complexos, é praticamente impossível violá-los e adulterar as informações contida neles" (TORO INVESTIMENTOS, 2019).

8. "Essa *hash* funciona como um elo de ligação [sic] entre os blocos, já que um bloco carrega sua própria *hash* e também a hash do bloco anterior. Com isso, vai se formando a cadeia, ou corrente, que liga vários blocos de informação entre si. Os responsáveis por reunir as informações em blocos e juntar um bloco ao outro são os mineradores. Essas pessoas reúnem as transações que ainda não foram inseridas em um bloco e as adicionam à blockchain com a *hash* certa" (TORO INVESTIMENTOS, 2019).

9. "Na maioria das vezes, tanto em razão do espaço de memória quan-

Os ataques e os gastos duplos

No final dos anos 2000, enquanto desenvolvia o Bitcoin, Nakamoto implementou o primeiro *blockchain* "para servir como livro-razão da sua moeda virtual. O objetivo de implementar este livro-razão inviolável era resolver o problema do gasto duplo de moedas virtuais, isto é, evitar que uma certa quantidade de moeda fosse gasta duas vezes em situações distintas" (FERREIRA, 2017, p. 7).

Em janeiro de 2019, reporta Mike Orcutt (2019) na *MIT Technology Review*, a equipe de segurança da plataforma de troca Coinbase notou algo estranho acontecendo na Ethereum[13] Classic, uma das criptomoedas que as pessoas podem comprar e vender:

> Na sua *blockchain*, a história de todas as transações estava sob ataque. Um invasor conseguiu controlar mais da metade do poder de computação da rede e estava usando-o para reescrever o histórico de transações. Isso tornou possível gastar a mesma criptomoeda mais de uma vez – o que é conhecido como "gastos duplos". O invasor foi visto fazendo isso em US$ 1,1 milhão. A Coinbase alega que nenhuma moeda foi realmente roubada de suas contas. Mas uma segunda *exchange*[14] popular, a Gate.io, admitiu que não teve tanta sorte, perdendo cerca de US$ 200.000 para o invasor (que, estranhamente, retornou metade disso dias depois)[15] (ORCUTT, 2019, tradução nossa).

Um dos problemas é o acesso desigual. O que torna a tecnologia *blockchain* desafiadora de se implantar e usar de forma eficaz em algumas partes do mundo é o fato de que requer acesso rápido e confiável à internet. Algumas plataformas ainda sofrem com infraestruturas de telecomunicações tremendamente fracas (MLOT, 2015 apud AL-SAQAF; SEIDLER, 2017). A atividade de mineração para verificar transações *blockchain* também requer poder de processamento. E o código também seria otimizado para ambientes que assumem um alto grau de desenvoltura, como alta largura de banda e armazenamento (AL-SAQAF; SEIDLER, 2017).

Importante lembrar que a Ethereum é na verdade um *fork* (bifurcação) do Ethereum Classic. O Ethereum Classic (ETC) é executado no mesmo protocolo fazendo uma função semelhante, mas tem algumas diferenças em sua comunidade. As duas criptomoedas "não apenas compartilham o mesmo nome, mas também compartilham uma história interessante que é um dos eventos mais cruciais em todo o histórico de criptomoedas. A batalha entre Ethereum e Ethereum Classic é de ética e ideologia", diz Moskov (2019, tradução nossa), do *Coin Central*. Antes que houvesse os dois "Ethereums diferentes que vemos agora, havia apenas um Ethereum. Desde então, US$ 50 milhões foram roubados por um hacker, e isso resultou em dois campos distintos de pessoas no mundo da criptomoeda sendo formadas" (MOSKOV, 2019).

to da confidencialidade, apenas os hashes dos dados são armazenados no blockchain e não os dados em si" (QUINIOU; DEBONNEUIL, 2019, p. 27, tradução nossa).

10. Para aspectos técnicos do design blockchain, como o seu protocolo de consenso, ver Sankar et al. (2017).

11. O PoW oferece proteção contra Distributed Denial of Service (DDoS), que reduz a quantia total do montante do minerador, e esses algoritmos do blockchain oferecem uma boa dose de dificuldade para que os hackers usem o sistema. Um DDoS é "um ataque de negação de serviço, é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na rede. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga" (WIKIPÉDIA, 11 abr. 2020. Disponível em: https://pt.wikipedia.org/wiki/Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o).

12. Quando alguém resolve a operação e consegue validar o bloco, recebe uma recompensa – as outras pessoas da rede também conseguem confirmar que o resultado é correto (PRADO, 2018).

13. "Ethereum é um *blockchain* programável descrito em dezembro de 2013 pelo seu criador, Vitalik Buterin. Esse é o pri-

meiro *blockchain* totalmente programável (no sentido de Turing). Permitiu o surgimento de aplicativos descentralizados chamados dApps [programas com vários *smartcontracts* em execução em um *blockchain*]. Os nós da rede formam um 'computador global' chamado de Ethereum Virtual Machine (EVM)" (QUINIOU; DEBONNEUIL, 2019, tradução nossa).

14. Na economia de troca, *exchange* é um termo técnico para descrever a interação entre vários agentes, que podem trocar produtos entre si com base em um sistema de preços.

15. "Desde o início de 2017, os *hackers* roubaram quase US$ 2 bilhões em criptomoedas, principalmente de trocas. Mas não foram apenas atacantes solitários oportunistas. Organizações de *cibercrime* também estão fazendo isso: a empresa de análise de dados Chainalysis disse que apenas dois grupos, ambos aparentemente ativos, podem ter roubado US$ 1 bilhão das trocas" (ORCUTT, 2019, tradução nossa).

16. O termo DAO designa um sistema de organização autônomo e descentralizado que usa regras de operação e participação que são fornecidas por um contrato inteligente registrado em um *blockchain*. Deve-se notar que o projeto Ethereum atualmente designa DAO como uma organização autônoma democrática.

Os *blockchains* são particularmente atraentes para os ladrões, porque as transações fraudulentas não podem ser revertidas como muitas vezes acontece no sistema financeiro tradicional, conforme reportagem na *MIT Technology Review* (ORCUTT, 2019). "Além disso, sabemos que, assim como os *blockchains* têm recursos de segurança exclusivos, eles também têm vulnerabilidades exclusivas. *Slogans* e manchetes de marketing que chamavam a tecnologia de 'inacessível' estavam completamente errados" (ORCUTT, 2019).

"Mas, quanto mais complexo for um sistema *blockchain*, mais formas existem de cometer erros durante sua configuração" (ORCUTT, 2019). Ainda em janeiro de 2019, a empresa encarregada da Zcash − uma criptomoeda que usa matemática extremamente complicada para permitir que os usuários realizem transações em particular − revelou que secretamente havia consertado uma "falha criptográfica sutil" acidentalmente incluída no protocolo. Um invasor poderia ter explorado isso para falsificar a Zcash de forma ilimitada. "Felizmente, ninguém parece ter feito isso" (ORCUTT, 2019). Ainda assim, a maioria dos *hackers* não fez ataques às *blockchains*, mas às exchanges. Ou seja, os *hackers* foram aos sites nos quais as pessoas podem comprar, trocar e manter criptomoedas.

Outra demonstração "da confiança aparentemente cega que alguns investidores e entusiastas de *blockchain* colocam na tecnologia foi o ataque ao primeiro sistema (DAO)[16] em junho de 2016" (AL-SAQAF; SEIDLER, 2017, p. 9, tradução nossa).

> O ataque explorou o contrato inteligente de código *buggy*, resultando na perda de mais de US$ 60 milhões em Ether, a moeda usada na Ethereum (Morris, 2016 apud Al-Saqaf; Seidler, 2017). Isso foi seguido por outros roubos em 2017 que exploraram *bugs* em *software* populares usados pela comunidade Ethereum, levando à perda de US$ 34 milhões em Éter (REIFF, 2017 apud AL-SAQAF; SEIDLER, 2017, p. 8, tradução nossa).

Um dos recursos da tecnologia *blockchain* é chamado de "contratos inteligentes". São programas de computador automatizados que podem ser acionados para transferir ativos digitais automaticamente dentro da mesma cadeia de blocos (FAIRFIELD, 2014, tradução nossa) ao se atenderem "certas condições de um contrato inteligente, que em si é imutável, já que seu código está no blockchain, o que torna possível fazer uma série de transações sem qualquer intervenção humana".

Quando se trata de prestação de contas, os contratos inteligentes

> podem levar os recursos da tecnologia blockchain ao próximo nível. Projetos baseados em contratos inteligentes foram implementados nos domínios imobiliário, de serviços financeiros, de mercados preditivos, de privacidade e identidade, de seguros, de entreteni-

17. Na definição de Orcutt (2019), da *MIT Technology Review*, um contrato inteligente é um programa de computador que é executado em uma rede blockchain. Ele pode ser usado para automatizar o movimento da criptomoeda de acordo com as regras e condições prescritas. Isso tem muitos usos potenciais, como a facilitação de contratos legais reais ou transações financeiras complicadas.

18. Já Szabo (1997 apud Casino et al., 2018) definiu em 1994 que um contrato inteligente (ou SC) é "um protocolo de transação computadorizado que executa os termos de um contrato", permitindo "cláusulas contratuais em código embutido".

> mento e de infraestrutura (CUMMINGS, 2016 apud AL-SAQAF; SEIDLER, 2017, p. 9, tradução nossa).

O AnChain.ai é uma das várias startups "criadas para lidar com a ameaça de *hackers* no *blockchain*. Ela usa inteligência artificial para monitorar transações e detectar atividades suspeitas, e pode escanear códigos de contrato inteligente para vulnerabilidades conhecidas" (ORCUTT, 2019, tradução nossa).

> Outras empresas, incluindo a ChainSecurity de Tsankov, estão desenvolvendo serviços de auditoria baseados em uma técnica de informática estabelecida chamada verificação formal. O objetivo é provar matematicamente que o código de um contrato realmente fará o que seus criadores pretendiam. Essas ferramentas de auditoria, que começaram a surgir no ano passado, permitiram que os criadores de contratos inteligentes eliminassem muitos dos bugs que tinham sido "frutos fáceis", diz Tsankov (ORCUTT, 2019, tradução nossa).

Em suma, "enquanto a tecnologia *blockchain* tem sido muito elogiada por sua segurança, ela pode ser bastante vulnerável sob certas condições", alerta Orcutt (2019, tradução nossa). Ele acrescenta que, às vezes, a execução de má qualidade pode ser "responsabilizada, ou erros de *software* não intencionais. Outras vezes, é mais uma área cinzenta − o resultado complicado de interações entre o código, a economia da *blockchain* e a cobiça humana. Isso é conhecido em teoria desde o início da tecnologia".

Vemos um afã de otimismo que precisa ser discutido, assim como ocorrências relacionadas a transparência, responsabilidade e limites do anonimato. Por enquanto, o discurso é de que "a corrupção e as violações dos direitos humanos muitas vezes prosperam em ambientes de sigilo, assimetria de informação e canais de comunicação opacos". Em contraste, "*blockchains* são projetados para trazer transparência total aos nós no sistema, de forma que cada pedaço de informação possa ser rastreado até sua origem e seguido com facilidade" (AL-SAQAF; SEIDLER, 2017, p. 9, tradução nossa).

Algoritmos de consenso formam a base das tecnologias de rede blockchain

"Os algoritmos de consenso são capazes de diferenciar todas as categorias de consenso que existem na *blockchain*", diz Lucas Lamounier (2018), do *101 Blockchains*. É a rede que movimenta informação para milhões e milhões de pessoas promovendo facilidades, cuja arquitetura inteligente é projetada tendo os algoritmos de consenso como ponto inicial. Os algoritmos de consenso deflagram um processo de tomada de decisão para um grupo no qual cada indivíduo constrói e apoia a decisão que funcionará para todos. "É uma forma de resolução na qual os indivíduos precisam apoiar a decisão da maioria, de forma consensual, quer tenham gostado ou

não. Os modelos de consenso do Blockchain são métodos projetados para criar igualdade e justiça no mundo online" (LAMOUNIER, 2018). Os sistemas de consenso usados para esse acordo são também chamados de "teorema de consenso". São os algoritmos de consenso que "tornam a natureza das redes blockchain tão versáteis. Sim, não há um único algoritmo de consenso do blockchain que possa afirmar ser perfeito, mas essa é a beleza da tecnologia que imaginamos – a constante mudança para podermos aprimorá-los", finaliza Lamounier (2018).

A partir dos pesquisadores Fabíola Greve, Leobino Sampaio, Jauberth Abijaude, Antonio Coutinho, Ítalo Valcy e Sílvio Queiroz, podemos exemplificar o esquema do algoritmo no *Consenso Nakamoto*:

> 1. Request: Clientes enviam transações para todos os nós da rede;
>
> 2. Collect: Cada nó pi da rede, ao receber as transações, as adiciona a um bloco bi;
>
> 3. Election: Em cada rodada k do consenso, um oráculo randômico escolhe um nó líder pl para propagar o seu bloco bl aos demais;
>
> 4. Validate: Cada nó pi aceita o bloco bl se ele é válido e se as transações contidas em bl são válidas.
>
> 5. Update: O nó pi, ao aceitar o bloco bl, irá adicioná-lo ao final do livro-razão e finaliza a rodada k. A posteriori, irá agregar o hash H(bl) ao próximo bloco a ser criado, mantendo assim a estrutura de corrente criptográfica (NAKAMOTO, 2008 apud GREVE et al., 2018, p. 17).

Além do dinheiro: contratos inteligentes

Os tecnólogos perceberam que as *blockchains* poderiam ser usadas para rastrear outras coisas além do dinheiro, como contam Casino et al. (2018):

> Em 2013, Vitalik Buterin, de 19 anos, propôs a Ethereum, que registraria não apenas as transações com moedas, mas também o status de programas de computador chamados "contratos inteligentes"[17] (SCs)[18]. Lançada em 2015, a Ethereum − e agora uma série de concorrentes e imitadores − promete tornar possível uma nova geração de aplicativos que se parece com os aplicativos da web atual, mas são alimentados por redes de criptomoedas descentralizadas, em vez de servidores de uma empresa.

Então, um contrato inteligente, ou *Smart Contract* (SC), é "um acordo entre partes que, embora não confiem umas nas outras, têm termos acordados que são automaticamente aplicados. Portanto, dentro do contexto *blo-*

ckchain, SCs são scripts rodando de forma descentralizada e armazenados no *blockchain*" (CHRISTIDIS; DEVETSIKIOTIS, 2016 apud CASINO et al., 2018, p. 56, tradução nossa), reforçando, "sem depender de qualquer autoridade confiável".

Assim, três gerações de *blockchains* podem ser distinguidas:

> Blockchain 1.0, que inclui aplicativos que permitem transações digitais em criptografia; Blockchain 2.0, que inclui SCs e um conjunto de aplicações que se estendem além das transações de criptomoeda; e Blockchain 3.0, que inclui aplicações em áreas além das duas versões anteriores, como governo, saúde, ciência e IoT [*internet of things*] (ZHAO et al., 2016 apud CASINO et al., 2018, p. 56).

Casino *et al.* (2018) trazem autores que aderem a essa linha de crítica e análise. Os autores ressaltam que "Há, de fato, algumas revisões focadas no papel particular de *blockchain*, incluindo o desenvolvimento de aplicações descentralizadas e intensivas de dados para a *IoT* (Conoscenti et al., 2016; Christidis e Devetsikiotis, 2016)" e "gestão de *big data* de uma forma descentralizada (Karafiloski e Mishev, 2017a). Outras análises enfocam questões de segurança do blockchain (Khan e Salah, 2017; Li et al., 2017a; Meng et al., 2018 apud Casino et al., 2018)". Atualmente, a tecnologia blockchain "é aplicada a uma ampla variedade de campos financeiros, incluindo serviços de negócios, ativos financeiros, mercados de previsão e transações econômicas" (HAFERKORN; QUINTANA DIAZ, 2015 apud CASINO et al., 2018, p. 56).

Mesmo que a tecnologia *blockchain* tenha sido introduzida com o Bitcoin como seu núcleo de tecnologia subjacente, levou vários anos para a comunidade de pesquisa se tornar totalmente consciente do potencial do blockchain e das vantagens de suas possíveis aplicações. Não é novidade que, durante os primeiros anos, blockchain foi considerado um sinônimo de Bitcoin (CASINO et al., 2018, p. 59).

Bitcoin: a mais conhecida das criptomoedas

No dizer de Casino *et al.* (2018), foi o Bitcoin que introduziu o algoritmo de consenso da *blockchain* antes de qualquer outra criptomoeda. Uma transação é a transferência de criptomoeda de uma pessoa para outra.

> No Ethereum, que inclui uma linguagem de programação interna que pode ser usada para automatizar transações, existem vários tipos. Um pode enviar criptomoedas para outro. Ou alguém pode criar uma transação que coloque uma linha de código, chamada de contrato inteligente, no *blockchain*. As pessoas podem, então, enviar dinheiro para uma conta que este programa controla, se determinadas condições codificadas no contrato forem atendidas (CASINO et al., 2018).

"Implementações bem conhecidas de blockchains públicos incluem Bitcoin, Ethereum, Litecoin e, em geral, a maioria das criptomoedas" (NAKAMOTO, 2008; HAFERKORN; QUINTANA DIAZ, 2015 apud CASINO et al., 2018, p. 57). "Uma de suas principais vantagens é não ter custos de infraestrutura: a rede é autossustentável e capaz de se manter, reduzindo drasticamente as despesas gerais de gerenciamento" (CASINO et al., 2018, p. 57).

"*Tokens* de segurança", "títulos com *tokens*" ou apenas "títulos digitais"

Há um tipo relativamente novo de ativo digital projetado com o uso de contratos inteligentes para cumprir automaticamente as regulamentações de valores mobiliários.

Na Figura 2, estão as diversas aplicações de *blockchain*.

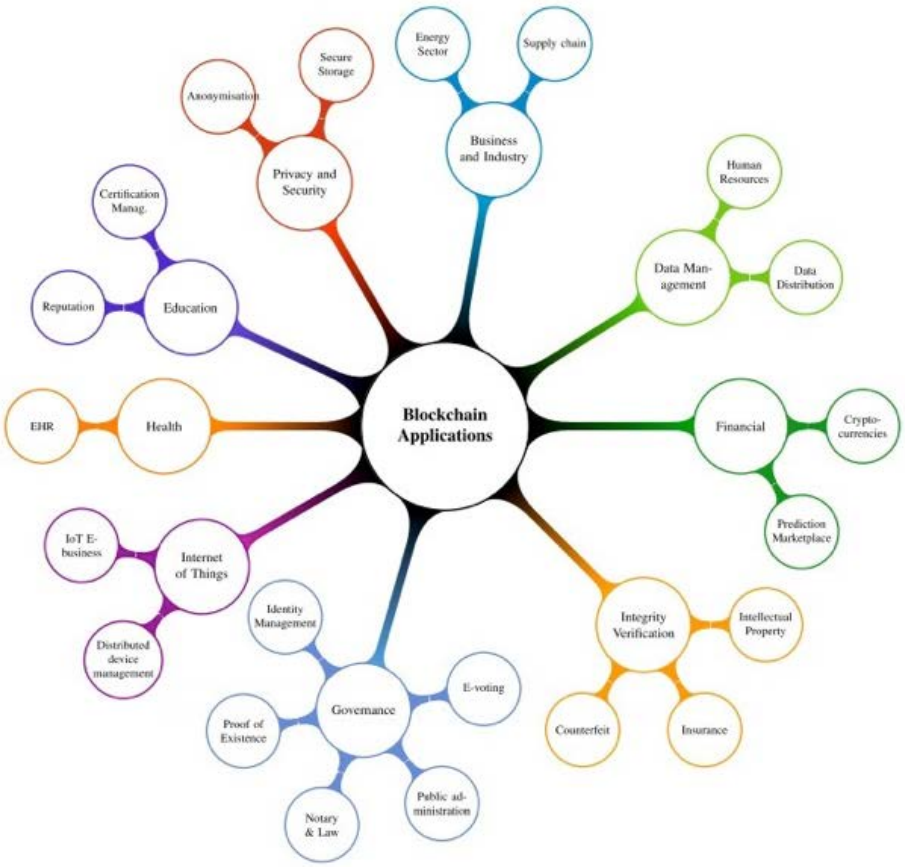

Figura 2 – Aplicações de blockchain. Fonte: Damasco (2017).

É nesse contexto que, segundo a visão dos que estudam tecnologias *blockchain*, a criação de redes de informação descentralizadas pode "transformar por completo a forma com que negócios serão feitos daqui para frente", ou seja, se atualmente a internet é considerada a forma mais eficiente de compartilhar informação com pessoas do mundo todo de forma veloz, a plataforma *blockchain* pode oferecer uma "nova proposta". Não necessa-

riamente é preciso se ater às transações que envolvem dinheiro e ativos financeiros. Acredita-se ser possível utilizar esse novo sistema para também arquivar e compartilhar música, arte, votos, documentos etc. (TORO INVESTIMENTOS, 2019).

Um entre diversos exemplos de como a tecnologia *blockchain* pode ser utilizada é "detectar a corrupção nos círculos do governo e limitar os abusos de poder de maneiras que os métodos tradicionais de contabilidade não podem" (AL-SAQAF; SEIDLER, 2017, p. 9, tradução nossa). Ao permitir que jornalistas e outros grupos de interesse público tenham acesso a dados públicos sobre o *blockchain*, "os direitos humanos podem ser um grande beneficiário. Os dados podem ser usados como irrefutável evidência para expor práticas criminosas dentro do Estado e, portanto, proteger membros vulneráveis da comunidade" (AL-SAQAF; SEIDLER, 2017, p. 9, tradução nossa). É importante notar que o grau e a implementação da transparência podem variar de um *blockchain* para outro: "Nos blockchains autorizados, é possível manter partes dos dados transparentes para alguns nós, mantendo o restante oculto. Isso pode ser crucialmente importante para algumas empresas e serviços que dependem de confidencialidade nos dados de transação" (AL-SAQAF; SEIDLER, 2017, p. 10, tradução nossa).

> O Hyperledger Fabric é uma das plataformas *blockchain* que permite a criação de *blockchains* autorizados nos quais os nós podem ser configurados para ter diferentes funções e configurações de permissão. Essas plataformas oferecem a possibilidade de abranger uma variedade de aplicações *blockchain* com diferentes graus e níveis de transparência (AL-SAQAF; SEIDLER, 2017, p. 10, tradução nossa).

Em uma visão de longo prazo e talvez hiperbólica do verdadeiro potencial da tecnologia *blockchain*, acreditam Huckle et al. (2016 apud AL-SAQAF; SEIDLER, 2017, p. 11, tradução nossa) que "poderíamos ir tão longe a ponto de imaginar um mundo onde governos e várias outras entidades têm suas legislações completas aplicadas automaticamente por meio de contratos inteligentes". Os autores evidenciam um aspecto caro à tecnologia ao complementar que isso poderia ser possível "devido aos rápidos desenvolvimentos em inteligência artificial, aprendizado de máquina, armazenamento em nuvem, largura de banda e poder de processamento", bem como "à proliferação de bilhões de dispositivos da Internet das Coisas (IoT) comunicando-se entre si de forma segura, automatizando muitos processos tradicionalmente manuais" (HUCKLE et al. 2016 apud AL-SAQAF; SEIDLER, 2017, p. 11, tradução nossa).

Vamos recorrer aos princípios do sociólogo Max Weber, em sua obra *Economia e sociedade*, escrita no início do século XX, quando assinalava que a economia capitalista exigia que "os negócios oficiais da administração fossem feitos com precisão, sem ambiguidades, continuamente, e com a maior velocidade possível" (WEBER, 1982, p. 250 apud SILVEIRA, 2018).

> É preciso destacar que "o fenômeno da governança algorítmica é parte de uma longa tendência histórica em direção à mecanização da governança" (Danaher et al., 2017, p. 2). Neste caso, a governança ou a regulação diz respeito ao controle, às maneiras ou formas de realizar, moldar e conduzir o comportamento das pessoas, de segmentos do mercado e da sociedade (SILVEIRA, 2018).

Ao utilizar a tecnologia *blockchain*, as transações eletrônicas poderão ser verificadas/registradas automaticamente a partir dos nós presentes na rede por meio do algoritmo criptográfico, conforme Staut (2018), que acrescenta: "sem qualquer tipo de intervenção humana, autoridade central ou qualquer ponto de controle que poderia interferir no processo, ou seja, qualquer tipo de entidade centralizada".

Em tempos de superexcitação em tornar tudo autônomo dentro da "cultura do faça você mesmo", na crescente usabilidade de códigos e na intenção de se apoderar da fricção entre rede — descentralizada, que garante um mínimo de privacidade — e mundo, estaria o propósito da plataforma *blockchain*. De acordo com Al-Saqaf; Seidler (2017, p. 13, tradução nossa), "Transparência, igualdade e autonomia são algumas das características da tecnologia *blockchain* que poderiam facilitar o progresso em áreas como identidade *on-line*, tráfico humano, corrupção, fraude, participação democrática e liberdade de expressão".

Disso se conclui, com Szabo (1994), que a teoria da informação algorítmica "é uma síntese abrangente da ciência da computação e da teoria da informação. Suas ressonâncias e aplicações vão muito além de computadores e comunicações, para campos tão diversos quanto a matemática, a indução científica e a hermenêutica".

Referências

AL-SAQAF, W.; SEIDLER, N. Blockchain technology for social impact: opportunities and challenges ahead. **Journal of Cyber Policy**, 2017. Disponível em: https://www.researchgate.net/publication/321012025. Acesso em: 30 maio 2019.

CASINO Fran; DASAKLISB, Thomas K.; PATSAKIS, Constantinos. A systematic literature review of blockchain-based applications: Current status, classification and open issues. In **Telematics and Informatics journal**. Homepage: www.elsevier.com/locate/tele. 2019. Disponível em: https://fardapaper.ir/mohavaha/uploads/2019/03/Fardapaper-A-systematic-literature-review-of-blockchain-based-applications-Current-status-classification-and-open-issues.pdf. Acesso em: 11 abr. 2020.

DAMASCO, R. **Conferência Web.br**. Blockchain: Conceitos básicos e aplicações da tecnologia. 24 out. 2017. Maksoud Plaza. São Paulo. Brasil. Dispo-

nível em: https://conferenciaweb.w3c.br/2017/home/. Acesso em: 11 abr. 2020. Acesso em: 12 abr. 2020.

DANAHER, J. et al. Algorithmic governance: Developing a research agenda through the power of collective intelligence. **Big Data & Society**, v. 4, n. 2, 2017.

EXPLAINER: What is a blockchain? **Technology Review**, Apr. 23, 2018. Disponível em: https://www.technologyreview.com/s/610833/explainer-what-is-a-blockchain. Acesso em: 27 mar. 2019.

FERREIRA, F. L. **Blockchain e Ethereum**: Aplicações e Vulnerabilidades. 2017. Monografia (Bacharelado em Ciência da Computação) – Universidade de São Paulo, São Paulo, 2017. Disponível em: https://linux.ime.usp.br/~fredlage/mac0499/Monografia.pdf. Acesso em: 03 jun. 2019.

GREVE, F.; SAMPAIO, L; ABIJAUDE, J; COUTINHO, A; VALCY, Í; QUEIROZ, S. Blockchain e a Revolução do Consenso sob Demanda. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, 36., São Carlos, 2018. **Minicursos**, capítulo 5. São Carlos: Sociedade Brasileira de Computação; Ufscar, 2018. Disponível em: http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/Capitulo5.pdf. Acesso em: 30 maio 2019.

LAMOUNIER, L. Algoritmos de Consenso: a Raiz que Sustenta a Tecnologia Blockchain. **101 Blockchains**, 04 out. 2018. Disponível em: https://101blockchains.com/pt/algoritmos-de-consenso/#pll_switcher. Acesso: 30 mar. 2019.

MOSKOV, A. Ethereum Classic vs Ethereum (ETC vs ETH): What's the Difference? **Coin Central**, 2019. Disponível em: https://coincentral.com/ethereum-classic-vs-ethereum/. Acesso em: 03 jun. 2019.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.

ORCUTT, M. Once hailed as unhackable, blockchains are now getting hacked. **MIT Technology Review**, Feb. 19, 2019. Disponível em: https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/?. Acesso em: 26 mar. 2019.

O QUE são os algoritmos de consenso das blockchains. **Binance Vision**, 2018. Disponível em: https://www.binance.vision/pt/blockchain/what-is-a-blockchain-consensus-algorithm. Acesso em: 30 mar. 2019.

PRADO, J. O que é blockchain? (indo além do bitcoin). **Tecnoblog**, 2018. Disponível em: https://tecnoblog.net/227293/como-funciona-blockchain-bitcoin/. Acesso em: 19 mar. 2019.

QUINIOU, M.; DEBONNEUIL, C. **Glossary Blockchain**. Paris: Unesco; Chaire Unesco Iten; Les Editións de l'immateriel, 2019.

SILVEIRA, S. A. Regulação algorítmica e os estados democráticos. **ComCiência**: Revista Eletrônica de Jornalismo Científico, dossiê 204, 06 dez. 2018.

Disponível em: http://www.comciencia.br/regulacao-algoritmica-e-os-estados-democraticos/. Acesso em: 23 mar. 2019.

STAUT, K. Saiba o que são os contratos inteligentes e como eles funcionam na prática. **Jus.com.br**, 2018. Disponível em: https://jus.com.br/artigos/68927/saiba-o-que-sao-os-contratos-inteligentes-e-como-eles-funcionam-na-pratica. Acesso em: 29 maio 2019.

SZABO, N. Introduction to Algorithmic Information Theory. **Nick Szabo's Papers and Concise Tutorials**, 1994. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/kolmogorov.html. Acesso em: 30 maio 2019.

TORO INVESTIMENTOS. Blockchain: O que é a tecnologia dos Bitcoins. **Toro Blog**. 21. jan. 2019. Disponível em: https://blog.toroinvestimentos.com.br/bitcoin-blockchain-o-que-e. Acesso em: 30 mar. 2019.