

O POTENCIAL DA TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA GERAÇÃO DE RECEITAS ACESSÓRIAS NO SUAC

POR GABRIEL ALEIXO – A STAR LABS.¹

O funcionamento da tecnologia blockchain

O objetivo central de uma base de dados distribuída construída a partir da tecnologia blockchain é a manutenção do consenso. Isso significa que ao longo de uma rede descentralizada, diferentes nós ligados a ela possuem uma cópia desse registro público de informações, estando todos livres para editá-la e propagar eventuais atualizações aos demais; e por isso diz-se que funcionamento do sistema independe de intermediários externos ou de confiança entre as partes, sendo estritamente regulado pela matemática por trás de seu código. O caráter revolucionário da blockchain reside justamente nos mecanismos que garantem, ao mesmo tempo, que todas essas cópias estejam em sincronia e que dados inconsistentes ou falsos não consigam ser mantidos nessa base informacional comum.

No caso do Bitcoin, por exemplo, sistema de moeda digital a partir do qual a tecnologia blockchain foi criada, há um registro público em que constam, grosso modo, o número de moedas digitais (os bitcoins) pertencentes a cada pessoa, bem como o histórico de transações por ela realizadas fazendo uso de um dado

¹ Graduado em Administração pela Escola Brasileira de Administração Pública e de Empresas da Fundação Getúlio Vargas (FGV EBAPE). Possui cursos de Inovação, Criptografia, Psicologia e Filosofia da Mente pela Universidade de Cambridge, Reino Unido. Co-fundador da A Star Labs. Co-fundador da federação Blockchain Hub Brasil. Co-criador e apresentador da websérie Bitcoin em Português. Pesquisador do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio), atuando desde 2013 nas frentes de moedas digitais, tecnologia blockchain e segurança digital.

endereço da rede. É justamente a operacionalização via blockchain a responsável por, concomitantemente, permitir que:

1. A rede seja permanentemente atualizada pelo próprio conjunto de usuários que a integra - com informações referentes às novas transações sendo adicionadas a todo momento e os saldos de bitcoins em posse de cada um alterados e sincronizados em todas as cópias desse balanço.
2. Seja extremamente custoso na prática, além de economicamente ineficiente, para um agente malicioso propagar informações falsas ou inconsistentes aos demais (como a de que ele está gastando bitcoins que na verdade não possui). Ou seja, a blockchain torna fraudes inviáveis na prática.
3. Os dados em posse de um usuário só possam ser alterados por ele mesmo (no caso, apenas o próprio usuário, ou alguém a quem ele cedeu sua chave privada, pode movimentar os bitcoins que constam sob seu controle na blockchain).

O resultado final desse processo é a efetiva geração e manutenção de consenso numa rede que não é individualmente controlada por ninguém, e que por isso tem sua figura de confiança distribuída entre todas as partes interessadas que rodam um mesmo código computacional. A operacionalização de uma blockchain

clássica ocorre, geralmente, através de códigos computacionais responsáveis por gerir os seguintes pilares²:

1. Imutabilidade: essa característica é assegurada por funções criptográficas, garantindo um traço importante da tecnologia: as informações, bem como suas autenticidade e autoria, são de fácil verificação, mas é impossível na prática se passar por outro indivíduo na rede, propagar informações fraudulentas ou mover os ativos digitais (como moedas) que não pertençam à pessoa devida.

2. Transparência: uma vez validadas pelo código do sistema e propagadas ao longo da rede, essas informações podem ter sua validade auditada por qualquer pessoa, bem como a data e hora de inserção e a autoria de quem as publicou, com total transparência.

A mais antiga das blockchains (a do Bitcoin) já opera em tempo integral desde janeiro de 2009 sem qualquer caso de falha sistêmica. Logo, assim como o protocolo TCP/IP permitiu a evolução bem como os múltiplos usos da internet de hoje, implementações de blockchains enquanto protocolos basilares abrem as portas para um conjunto de transformações radicais antes impossíveis. Como apontou Satoshi Nakamoto, criador da tecnologia, o grande trunfo da tecnologia blockchain é trabalhar com “provas criptográficas no lugar de confiança (centralizada)”. Por conta disso, uma série de novos campos se abre. Nesse processo, as características de destaque que tornam a blockchain uma tecnologia atraente pelo que pode trazer nos campos social, econômico e empresarial são

² Blockchain e o Futuro da Governança, disponível em:
<https://medium.com/@ITSriodejaneiro/blockchain-e-o-futuro-da-governanca-959265cc4d66>

descritas a seguir³ e ajudam a compreender o que se pode fazer a partir de aplicações nela baseadas:

O potencial da tecnologia blockchain reside em sua capacidade de oferecer serviços transparentes, livres de censura ou discriminação de uma maneira descentralizada para finalidades amplas; a partir do acesso mais equânime a um conjunto de instituições digitais (que permitem realizar votações, pagamentos, contratos, etc) cuja infra-estrutura irá revolucionar nossa forma de entender e construir ferramentas participativas. Como nós iremos guardar e gerir informações a partir de agora, uma vez que a tecnologia blockchain está aí, tornou-se uma questão de princípios de governança e tomada de decisões, baseadas em um consenso público e inviolável, por ser construído e mantido de forma descentralizada.

As possibilidades da tecnologia blockchain

Para os pesquisadores Aaron Wright e Primavera De Filippi, a mudança de paradigma trazida pela difusão da blockchain, seguida pela crescente implementação de sistemas descentralizados nela baseados, conduzirão à ascensão da *Lex Cryptographia*⁴, regras administradas através de contratos inteligentes auto-executáveis, capazes de permitir até mesmo o surgimento de corporações autônomas descentralizadas. Esse fenômeno tende a ocorrer como consequência da crescente transformação ou eventual redução no papel de intermediários legais e comerciais das diversas estruturas que compõem a

³ Blockchain e o Futuro da Governança, disponível em: <https://medium.com/@ITSriodejaneiro/blockchain-e-o-futuro-da-governanca-959265cc4d66> Acesso em 21/11/15 às 20:00

⁴ DE FILIPPI, P; WRIGHT, A. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Social Science Research Network. 2015.

sociedade tal qual a conhecemos hoje, uma vez que a blockchain permite “descentralizar a maneira como guardamos dados e gerenciamos informações”.

Se, no lugar de dados correspondentes a números ou informações financeiras - a exemplo do que ocorre na rede Bitcoin, uma base construída e gerada a partir da tecnologia blockchain armazena dados de outras naturezas, é possível manter uma vasta gama de novos serviços, muito mais ampla do que a de serviços estritamente monetários, com as mesmas qualidades do Bitcoin: imutável, seguro e descentralizado. O relatório *Blockchain Technology and Legal Implications of 'Crypto 2.0'*⁵ da Blomberg BNA já sinalizava com clareza essa tendência que cresceu vertiginosamente nos últimos meses.

Registros de propriedades, comprovações de autoria e propriedade intelectual, digitalização e automação de contratos, remessas internacionais de valor, emissão de títulos privados, mecanismos para o controle descentralizado de instituições, armazenamento remoto e distribuído de dados na nuvem e produtos financeiros diversos são alguns dos principais campos a serem transformados ou abertos nos próximos anos, segundo o relatório. O grande trunfo da tecnologia blockchain para o universo dos acordos e das transações é precisamente a capacidade de torná-los inteligentes, como evidenciado pela leitura de Aaron Wright e Primavera de Filippi⁶:

Using a distributed database, like the blockchain, parties can confirm that an event or condition has in fact occurred without the need for a third party. As a result, the

⁵ Blockchain Technology and Legal Implications of 'Crypto 2.0', disponível em: www.gibsondunn.com/publications/Documents/Lee-Long-Blockchain-Technology-BNA-Banking-03.31.2015.pdf

⁶ DE FILIPPI, P; WRIGHT, A. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Social Science Research Network. 2015, p.10.

technology has breathed life into a theoretical concept first formulated in 1997: digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention [...] In some cases, smart contracts represent the implementation of a contractual agreement, whose legal provisions have been formalized into source code. Contracting parties can thus structure their relationships more efficiently, in a self-executing manner and without the ambiguity of words. Reliance on source code enables willing parties to model contractual performance and simulate the agreement's performance before execution. In other cases, smart contracts introduce new codified relationships that are both defined and automatically enforced by code, but which are not linked to any underlying contractual rights or obligations. To the extent that a blockchain allows for the implementation of self-executing transactions, parties can freely transact with one another, without the technical need to enter into a standard contractual arrangement.

Isso é possível pois ela torna possível: digitalizar processos de controle e automatizar a tomada de decisões neles baseada, além de baratear e descentralizar a figura do agente mediador.

Protocolos abertos para aplicações baseadas em blockchain

Colored Coins

Protocolo que permite a programadores criar ativos digitais e registrá-los em blockchain. O procedimento consiste em criar um dado conjunto de unidades

digitais cuja distribuição e a titularidade ficam registradas na blockchain. Esses ativos mantêm todas as qualidades embutidas no Bitcoin, por exemplo, podendo ser utilizados de forma independente, da própria cotação de 1 unidade da moeda digital (1 bitcoin), com o propósito de servir aos mais variados fins: participação financeira em uma companhia (“ação”), pontos de milhagem ou fidelidade de uma loja ou rede específica, sistema descentralizado de votação (no qual cada unidade do novo ativo representa um direito a voto), registro de propriedade de bens digitais como domínios de websites, dentre outros. Além disso, especialmente quando combinados a plataformas mais avançadas que permitem a automação do comportamento de ativos digitais a partir de certas condicionantes pré-programadas e registradas numa blockchain, é imensa a gama de novos serviços propiciados, como a automação de pagamentos e empréstimos, concessão de heranças ou remuneração automática e atrelada a diversas moedas, bens ou ativos pelo desempenho de tarefas específicas.

Counterparty⁷

Plataforma criada sobre a blockchain do Bitcoin com o intuito de atrelar a ela novas funcionalidades, com destaque para produtos financeiros digitais e contratos inteligentes dessa natureza. Além de propiciar a criação e a gestão de ativos próprios, de forma semelhante à do protocolo Colored Coins, a Counterparty permite a automação de: pagamento de dividendos, câmbio entre diversos ativos ou moedas digitais e manutenção de mercados futuros

⁷ Counterparty, disponível em: <https://counterparty.io>

e derivativos⁸. Em especial, torna possível a criação de contratos inteligentes customizados que ficam armazenados e são validados a partir da blockchain do Bitcoin, uma vez que a plataforma possui interligado a seu sistema uma linguagem de *scripting* própria, a partir da qual usuários avançados podem programar ativos para que se comportem de uma certa forma quando uma ou mais condições são cumpridas.

Ethereum

Plataforma descentralizada que implementa uma blockchain para uso geral, criada com o intuito de que qualquer usuário tenha a liberdade de escrever códigos em sua base distribuída de dados, permitindo assim que contratos inteligentes sejam executados a partir dela. Pode-se compreendê-la como uma generalização da tecnologia blockchain. Tendo esta sido criada originalmente em 2009 para propiciar o adequado funcionamento do Bitcoin enquanto sistema de dinheiro digital descentralizado, ao longo dos anos a resiliência da tecnologia combinada a sua capacidade de manter consenso em uma rede distribuída foi validada e uma série de novas aplicações passou a ser proposta conceitualmente. Logo, a Ethereum hoje pode ser compreendida como a materialização em curso dessas discussões, conforme indicado pelo trecho abaixo, que abre o *paper* oficial de apresentação do projeto:

Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments ("colored coins"), the ownership of an underlying physical device ("smart property"),

⁸ About Counterparty, disponível em: http://counterparty.io/docs/about_counterparty/

non-fungible assets such as domain names ("Namecoin"), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules ("smart contracts") or even blockchain-based "decentralized autonomous organizations" (DAOs). What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

Há um time global responsável pelo desenvolvimento e as atualizações de todo o software que compõe a rede, criado como código aberto e livre. Desse modo, qualquer membro da comunidade pode auxiliar ativamente na evolução da Ethereum e suas funcionalidades, o que, naturalmente, vem levando indivíduos ou até mesmo grandes equipes e algumas empresas tradicionais a construir ferramentas implementadas sobre a rede.

Impacto econômico e social da tecnologia blockchain

Em artigo intitulado *Why Business Schools Need to Teach About the Blockchain*⁹, o pesquisador Kariappa Bheemaiah expõe com clareza os pilares que fazem da tecnologia blockchain um grande trunfo para a inovação nos negócios, tanto pelo que traz de inédito quanto pelo poder que possui de acelerar e ampliar os

⁹ BHEEMAIHAH, K. *Why Business Schools Need to Teach About the Blockchain*. Social Science Research Network. 2015, p.12.

efeitos positivos de outros arranjos descentralizados que a precederam, conforme anteriormente analisados:

[...] the Internet of Everything is increasingly becoming part of business reality. Today businesses and societies are noticing that the line between physical and virtual existence is beginning to blur at an increasing rate. In this transitional ambience, the centralized approach to building an IoT¹⁰ business model is expensive, lacks privacy and is not designed for endurance, as it fails to address the issues related to scale and complexity.

A secondary effect of the internet of everything is that it will also create an economy of everything (Panikkar, 2015), as every device capable of connecting to the internet becomes a point of transaction and economic value generation for consumers and prosumers in a sharing economy. In this form of a collaborative digital economy, a decentralized model is a sounder model to adapt, as it removes the fallacy of having a single failure point that is inherent of today's client-server based business models. On the contrary, in a decentralized structure, the addition of more nodes to the system actually decreases the risk of system failure as if one node fails to function, the whole network is not compromised.

As an increasing number of businesses, both large and small, begin to understand the advantage of having a decentralized system, the possibilities that are offered by the Blockchain technology begin to make economic sense. [...] In addition, decentralized architectures offer better cost benefits to companies as the peer-to-peer sharing of resources in a distributed network removes dependency on a central server, optimizes resource use and reduces costs. [...]

¹⁰ IoT ou internet of things, em tradução livre: internet das coisas.

As distributed networks begin to act as a channel of value-based transactions and in light of the afore mentioned advantages, a new breed of Blockchain based businesses are now beginning to show signs of disruption in various domains of the market.

Além de alguns anteriormente citados neste, Bheemaiah¹¹ destaca os seguintes setores nos quais implementações da tecnologia blockchain já são realidade:

Finanças:

Serviços de carteiras online para armazenamento e utilização de moedas digitais, a exemplo do Bitcoin, associados a ferramentas que propiciam empréstimos peer-to-peer, micropagamentos e remessas internacionais de valor com maior agilidade e menores custos.

Internet das Coisas:

A blockchain permite a criação e manutenção de criptomoedas que no mundo real funcionam como dinheiro programável. Exemplos práticos que começam a ser alvo de experimentos reais e construção de negócios futuros são: uma geladeira ligada a uma carteira de moedas digitais do proprietário capaz de encomendar novos alimentos online com base no orçamento disponível para o usuário e a quantidade de alimentos que armazena, além de poder propiciar a própria interoperabilidade entre entes inteligentes por meio da internet. Essa última linha, inclusive, foi alvo de experimentos do projeto ADEPT, idealizado pela gigante norte-americana IBM em

¹¹ BHEEMAIAH, K. *Why Business Schools Need to Teach About the Blockchain*. Social Science Research Network. 2015, p. 14.

parceria com a sul-coreana Samsung a fim de permitir, por exemplo, que uma máquina de lavar possa não apenas encomendar seu próprio sabão em pó, a partir de certo valor disponibilizado pelo dono em moeda digital, como negociar com a inteligência artificial de diversas lojas online com o intuito de tomar a decisão economicamente ótima. Ademais, o setor de tecnologia financeira (*FinTech*), pode se aproveitar dessa tendência para explorar possibilidades antes inviáveis em certos campos, como o controle compartilhado desses objetos inteligentes, a partir de uma carteira de bens/moedas digitais cujas movimentações só possam ser realizadas com base no acesso a múltiplas chaves, cada uma delas sob controle de diferentes agentes.

Contratos e Seguros:

A desintermediação propiciada pela implementação de contratos inteligentes ocorre como consequência da automação de processos nos quais os contratos tradicionais são dependentes de entidades garantidoras, como um terceiro de confiança capaz de assegurar o cumprimento de cláusulas acordadas entre duas partes que, em geral, não se conhecem. Nessa mesma direção, quando implementados sobre uma blockchain, tanto seguros usuais quanto novos produtos financeiros (derivativos baseados em criptomoedas, por exemplo) podem ser acionados automaticamente uma vez que determinada condição seja satisfeita. Embora ainda novas, cada vez mais estruturas com esse formato passam a poder ser traduzidas em código computacional, na forma de contratos inteligentes, e seus usos e consequências sobre os negócios são analisados nas próximas seções.

Princípios de como a tecnologia blockchain pode potencializar usos e novas receitas acessórias subsequentes na atividade do SUAC:

- Criação de um sistema de pontos que seriam distribuídos e mantidos numa blockchain, a fim de que se tenha total transparência e segurança quanto à emissão e à transferência desses pontos. Ademais, a construção de um sistema de pontuação em blockchain especificamente atribui significativa facilidade para integração desses pontos a plataformas de trocas, compras, dentre outros.
- Gamificação da plataforma, com a distribuição desses pontos como recompensa a atividades feitas mediante o uso do serviço: recarga do bilhete único, gasto da passagem, engajamento em pesquisas de marketing direcionado e afins.
- Complementar aos pontos trazidos previamente, e reforçando-os, a parceria com empresas privadas para a conversão dos pontos por brindes ou descontos pode alavancar as duas pontas envolvidas. Saem beneficiados tanto a SUAC mediante receita adicional dessas parcerias e, claro, os usuários do sistema que veriam seus pontos serem válidos como moeda de troca por determinados bens e serviços, estimulando a volta desse usuário a todo o ciclo de compra e gasto dentro do sistema.
- Os pontos teriam uma carteira atrelada de moeda digital que pode ser útil a várias outras funcionalidades no futuro, como micro-pagamentos, compra direta de bilhetes por meio de conversão direta e afins.

O estudo anterior mostra a vastidão do que é possível, sendo as últimas sugestões listadas acima apenas uma parte delas.

MATERIAL ADICIONAL

Blockchain Will Transform Customer Loyalty Programs. Harvard Business Review, disponível em: <https://hbr.org/2017/03/blockchain-will-transform-customer-loyalty-programs>

REFERÊNCIAS

About Counterparty, disponível em: http://counterparty.io/docs/about_counterparty/

Augur, disponível em: <http://www.augur.net/>

BHEEMAIAH, K. *Why Business Schools Need to Teach About the Blockchain.* Social Science Research Network. 2015, p.12.

Bitcoin P2P e-cash paper, disponível em:
<http://satoshi.nakamotoinstitute.org/emails/cryptography/1/>

Blockchain e o Futuro da Governança, disponível em:
<https://medium.com/@ITSriodejaneiro/blockchain-e-o-futuro-da-governanca-959265cc4d66>

Blockchain Technology and Legal Implications of 'Crypto 2.0', disponível em:
www.gibsondunn.com/publications/Documents/Lee-Long-Blockchain-Technology-BNA-Banking-03.31.2015.pdf

Colored Coins, disponível em: <http://coloredcoins.org/>

Counterparty, disponível em: <https://counterparty.io>

Cryptography Mailing List Emails, disponível em:
<http://satoshi.nakamotoinstitute.org/emails/cryptography/>

DE FILIPPI, P; WRIGHT, A. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia.* Social Science Research Network. 2015.

Ethereum Whitepaper, disponível em: <https://ethereum.org>