Blockchain: Confiança em Transações Públicas e o Caso do BNDES

Gladstone Arantes Jr

- Quem diria?!... Você acaba de se tornar um pouco cypher punk.

- Punk, eu?!?!

O diálogo seria curioso mesmo se não tivesse o ocorrido entre um casal de férias:

ele, profissional de TI; ela, enfermeira.

A conversa era sobre um recém implantado sistema de prontuário eletrônico. Ela relatava a reação de uma colega de trabalho que, bem ao seu estilo insatisfeito, espalhava aos quatro ventos sua total descrença na segurança das informações do sistema, o que soava um pouco como teoria da conspiração:

- Quem é que me garante que eles não alteram aquilo tudo lá depois que a gente digita, Ana?!

- Eu não confio mesmo...!

Para a surpresa da nossa enfermeira, aquela peculiar conversa conjugal demonstrou que sua colega não estava tão equivocada assim. A verdade é que o funcionamento interno dos sistemas digitais e todo o entorno necessário para mantê-los em execução apresenta fragilidades que podem surpreender muita gente.

Aquela revelação acabou por aproximar o pensamento da nossa amiga do espírito dos questionadores e rebeldes em geral, sejam eles cypher punks ou sua colega de trabalho inconformada de plantão.

Nada como um caso da vida prática para introduzir uma questão relevante que, do contrário, poderia parecer apenas tecnicismo além do razoável!...

Minhas informações estão seguras, afinal?

Embora tenhamos a sensação de que a existência de uma senha para regular o acesso a um sistema seja suficiente para impedir alterações espúrias de suas informações, a realidade é bem mais complexa.

Nos sistemas que podemos chamar de convencionais, a barreira última para que as informações não sejam violadas é sempre humana. Isso porque, em geral, os mecanismos tecnológicos que impedem alterações de dados são ativados ou desativados por decisão humana, podendo ser revertidos a qualquer tempo. Assim, para evitar malversação, acabamos sempre dependendo de processos, controles, verificações, monitoramentos, incentivos, políticas, hierarquias, aprovações, auditorias etc.

Tudo depende do nível de confiança que temos nos esquemas de governança das instituições que proveem os sistemas que utilizamos. E confiança, muitas vezes, é matéria de foro íntimo.

Porém, é necessário se perguntar se, num futuro tão digital, a confiança continuará a ser analógica. Pior ainda, continuará a ser humana? Não existe mesmo uma garantia tecnológica, matemática, sobre o funcionamento de um sistema?

Sim, existe. E não é de se espantar que tenha sido criado por esse grupo tão singular...

A invenção dos *cypher punks*

Cypher punks não confiam em instituições: nem na sua competência, quanto mais em suas boas intenções!... Por isso, preferem sistemas descentralizados, sem um dono claramente definido, que sejam executados por uma rede inteira, não apenas por um nó.

Eles também advogam que a criptografia é uma arma para o empoderamento do cidadão comum contra o domínio dos poderosos digitais. Daí o cypher, que é um prefixo mais ou menos similar a cripto (Hughes, 1993). Radicais ou visionários? Talvez os dois... porque, embora possa ser excessivo

desconfiar de tudo e de todos, com o aumento avassalador da presença dos sistemas digitais no nosso dia a dia, não dá para criticar quem se incomode em ter que confiar em um número crescente de atores responsáveis por sistemas que, além de onipresentes, serão cada vez mais críticos e vitais.

Com esse *background*, a partir de ideias básicas sobre criptografia e descentralização, um grupo de *cypher punks* criou o Bitcoin (Nakamoto, 2008) e, por decorrência, a blockchain.

Curiosamente, seu proponente, Satoshi Nakamoto, nunca foi visto por ninguém. Ele simplesmente sumiu dos grupos de discussão que o ajudaram a implementar as versões iniciais da moeda criptográfica mais valiosa do mundo. Isso antes que ela viesse a se tornar conhecida do grande público. A singularidade da situação não implica relevância, dado que o código é aberto para o escrutínio de qualquer um, sendo conhecido, mantido e evoluído por um grande número de pessoas.

Embora tenha sido concebido quase como um ato de protesto contra o mercado financeiro em geral em meio à crise de 2008, com o tempo, percebeu-se que a ideia básica do Bitcoin poderia ser aplicada em situações que talvez nem o mais empolgado *cypher punk* pudesse antecipar (Tapscott & Tapscott, 2016). A comunidade entendeu que, pela primeira vez, tinha sido criado um mecanismo que garantia a integridade de um sistema sem que fosse necessário confiar em nenhuma pessoa ou instituição específica para isso. Uma garantia tecnológica de integridade! E se isso pode ser muito útil hoje em dia, imagine no futuro!...

O termo blockchain surgiu como uma forma de se referir à tecnologia em si, sem carregar o peso dos questionamentos específicos acerca do Bitcoin. O nome faz referência à forma como as transações de transferência de Bitcoins, assim como de diversas outras blockchains derivadas, são armazenadas pelos nós da rede. Estas são agrupadas em blocos que, por sua vez, são conectados em fila, formando, literalmente, uma cadeia de blocos, ou seja, uma block chain (Antonopoulos, 2017).

Hoje, existem literalmente milhares de implementações de blockchain (Butterin, 2013; Ben-Sasson et al., 2014; Hearn, 2016), muitas sem nenhuma relação direta com criptomoedas. A tecnologia deu origem a um sem número de variações e as inovações nesse domínio não param de aparecer.

Um livro de registro distribuído

É fácil notar que o termo blockchain diz muito pouco sobre o que realmente a tecnologia oferece e pode até ser considerado inapropriado, já que muitas implementações mais novas da tecnologia sequer contêm uma cadeia de blocos (Popov, 2018; Hearn, 2016; Baird, 2016; Bogliato, 2018). Apesar disso, blockchain ainda é uma palavra amplamente utilizada. O concorrente mais próximo na seara da nomenclatura é a expressão *Distributed Ledger Technology* (DLT), cuja obscura tradução seria tecnologia de livro-razão distribuído.

Ledger não é exatamente um conceito conhecido para as pessoas sem familiaridade com a ciência contábil ou congêneres. Trata-se de um instrumento onde são anotados as entradas e saídas de recursos de uma empresa para fins de auditoria e controle (Garryson et al., 2007). Generalizando-se um pouco o conceito para livro de registros, é possível realizar o acompanhamento de outros tipos de informação, como: as operações de compra, venda ou hipoteca de imóveis ou de terras; as medicações, exames e procedimentos aplicados a um paciente internado num hospital; e muitas outras mais.

Em um passado nem tão remoto, livros-razão empresariais, registros de imóveis, prontuários de pacientes ou quaisquer outros livros de registro eram cadernos de papel onde se anotava na próxima linha disponível os eventos que se queria acompanhar. Na sua versão digital convencional, ledgers são bancos de dados digitais onde registros antigos não podem ser apagados ou alterados e, portanto, apenas operações de inserção são permitidas. Como sabemos, em ambos os casos, a integridade do livro só pode ser garantida por controles institucionais. Vale notar, porém que, em termos puramente tecnológicos, um livro de registros de papel é até mais resistente à adulteração do que um digital. Uma rasura fraudulenta no meio de um caderno demanda que diversas páginas posteriores sejam também rasuradas. Uma dor de cabeça!... Já o *update* em um lote de registros de um livro digital é tecnicamente simples e pode não deixar rastro nenhum, se forem tomados os devidos cuidados.

Na sua versão blockchain, porém, um *ledger* simplesmente não pode ser alterado sem que um esforço realmente hercúleo e sofisticadíssimo seja engendrado! Isso ocorre porque cópias são distribuídas em muitos nós e o algoritmo garante que a versão vigente do *ledger* só pode ser alterada se um nó agressor obtiver mais de 51% do poder computacional da rede toda (Nakamoto, 2008). No caso do Bitcoin, são dezenas de milhares de nós, acumulando um poder computacional que se estima equivalente a centenas de Googles. Como regra geral, redes maiores trazem mais segurança e a do Bitcoin é a maior delas.

Esse algoritmo, usado no Bitcoin e em algumas das maiores blockchains do planeta, como Ethereum, Litecoin, Dash e muitas outras, é chamado de *Proof of Work,* ou Prova de Trabalho. O nome se dá porque, para que um bloco seja adicionado à cadeia, um nó precisa vencer uma competição para descobrir um número que resolve

um puzzle matemático, o que só é possível por força bruta, tentando o máximo possível de opções até achar um número que sirva. Ao encontrar o chamado *nonce*, o nó o envia a todos os outros, mostrando que realmente achou a resposta. Assim, ele literalmente prova que teve um trabalho enorme e que, portanto, está colaborando com a rede que, assim, aceita o novo bloco proposto pelo nó vencedor, incluindo-o como o próximo da cadeia. Em troca, o dedicado nó é recompensado com valiosos Bitcoins (Nakamoto, 2008).

Outros algoritmos vêm sendo criados e usados em outras blockchains para competir com o *Proof of Work*. Apesar de ainda ser considerado o mais confiável dos algoritmos de consenso distribuído, dado os serviços comprovadamente prestados ao Bitcoin, há diversas críticas quanto ao PoW, como a baixa escalabilidade (Nguyen & Kim, 2018) e o alto consumo de energia elétrica, cujas estimativas o igualam ao de um país como a Irlanda que podem ser observados estatisticamente pelo site https://digiconomist.net/bitcoin-energy-consumption

Um ledger criptograficamente protegido

Para completar o esquema de proteção, inserções no livro só podem ser executadas por aqueles que possuem chaves criptográficas privadas que atestam não apenas sua eligibilidade para a realização destas operações, mas também indicam quais informações podem ser alteradas. Por exemplo, uma chave privada define quais Bitcoins a pessoa possui. Se tentar transferir outros Bitcoins que não são seus, os nós da rede conseguem detectar a má intenção e terão prazer em rejeitar a transação (Nakamoto, 2008).

A técnica que garante isso, chamada de criptografia assimétrica, é amplamente utilizada nas comunicações seguras da internet (Rivest et al., 1978). Pode-se identificar facilmente quando ela está em ação pelo endereço que você está acessando: se começar com https, em vez do mais comum http, seu browser está usando criptografia assimétrica para garantir uma comunicação segura com o site.

Na criptografia assimétrica, você usa uma chave privada para encriptar um conteúdo e uma chave pública correspondente para desencriptar. A técnica foi criada baseando-se no fato de que certas operações matemáticas não são facilmente revertidas. Em particular, a multiplicação de dois números primos, mesmo muito grandes, é algo simples. Já decompor um número com centenas de dígitos nos seus fatores primos pode demorar mais do que a idade do universo. Assim, simplificadamente, a chave privada seria uma combinação dos primos e a chave pública seria a multiplicação entre eles (Rivest, et al., 1978).

No Bitcoin, uma pessoa tem uma chave privada e outra pública que se correspondem e às quais corresponde uma certa quantidade de Bitcoins. A chave pública é também conhecida como endereço. Sua carteira digital de Bitcoins assina (uma forma específica de criptografar) uma transação transferindo Bitcoins para algum outro endereço e envia transação e assinatura para a rede. Todos os nós, sabendo o endereço que quer transferir seus próprios Bitcoins, podem conferir se quem a enviou para a rede possui mesmo a chave privada que prova ser a pessoa a verdadeira dona dos Bitcoins. Isso sem que seja necessário conhecer a tal chave privada (Nakamoto, 2008).

Parece mágica, mas é matemática da melhor qualidade! É fácil perceber que a gestão das chaves privadas é crítica no uso da tecnologia. Toda notícia sobre problemas com Bitcoin que você vai encontrar certamente tem a ver com o roubo ou perda de chaves privadas, o que é de responsabilidade dos seus proprietários, sendo eles mesmos os únicos prejudicados por perderem seus Bitcoins.

Em 10 anos de operação, o ledger do Bitcoin nunca foi adulterado. O mesmo se pode dizer de outras DLTs de tamanho relevante já citadas, como o Ethereum e o Litecoin. Algumas redes menores, porém, já sofreram os chamados ataques de 51%, tendo seus ledgers revertidos[i]

Da internet da informação para a internet do valor e muito mais

Uma das características de tudo que é digital é a abundância, decorrência direta da irrelevância do custo marginal de replicação. Fazer uma música ou escrever um livro é algo bastante custoso. Mesmo que bem mais barato do que a produção do seu conteúdo, imprimir uma cópia do livro ou do DVD que contém a música tem um custo nada desprezível, demandando investimento prévio em maquinário, dispêndio de insumos etc.

Em formato digital, porém, cada cópia a mais produzida do livro ou do DVD tem custo praticamente zero. Daí que nada que é digital tem valor intrínseco. A valoração se dá pela propriedade intelectual ou pelo direito autoral. O arquivo digital em si não vale virtualmente nada!

Com as blockchains, a coisa muda de figura. Um Bitcoin é claramente um elemento digital que não se pode reproduzir indefinidamente. Não há como mandar uma cópia do seu Bitcoin para aquele seu amigo sem que você fique sem o seu. Claro que a existência do Bitcoin não prescinde da existência da rede, dos nós mineradores. Mas, o arquivo digital também não existe sem a infraestrutura subjacente, então, nesse sentido, não é tão diferente. Desta forma, com a blockchain, pela primeira vez, é possível criar um ativo digital autônomo, uma combinação anteriormente irreconciliável de termos!

Dentro da rede do Bitcoin é possível fazer bastante mais do que simplesmente transferi-los de um lado para outro.

Por conta de recursos já previstos pelos seus criadores, pode-se, por exemplo, marcar um Bitcoin e, desta forma, mudar o que este representa e, portanto, seu valor. Assim, já existem utilizações da rede do Bitcoin para emissão de títulos de propriedade de terra (Anand, 2018), recibos de commodities usadas como garantias (Chod et al., 2017), entre outros. É como se, além do Bitcoin, sua rede pudesse suportar outros ativos e quaisquer outros elementos que tenham valor.

Além disso, redes como a Ethereum permitem criar ainda mais facilmente um sem número de ativos. Esta apresenta um padrão chamado ERC-20 (Frozeman, 2015), exclusivo para a produção de tokens digitais, que são ativos digitais criptográficos que rodam sobre a rede Ethereum. É como se você pudesse criar o seu próprio Bitcoin só que reutilizando uma blockchain já existente e provada, bem mais simples do que criar uma rede do zero.

Assim, além da internet, que nos permite transferir informações pelos quatro cantos do mundo, agora temos as blockchains, que nos permitem transferir valores e ativos em geral, abrindo toda uma nova gama de possibilidades de aplicações.

É curioso notar que muitas operações sobre ativos como terras e imóveis, além de outros, são registrados e operados por cartórios e instituições similares. Aliás, tais instituições são basicamente responsáveis pela operação de livros de registros específicos, sejam registros de imóveis, registro civil, livros de notas, Diário Oficial etc.

Casas da moeda também pertencem a esse ecossistema. Elas fabricam não apenas cédulas de dinheiro, mas também diplomas universitários e outros documentos que nada mais são do que formas eficientes de acesso a registros. Isso porque formaturas são registradas em algum Diário Oficial e o diploma é como um documento comprobatório desse registro. Esse esquema geral é mais sujeito a problemas de falsificação do que os não iniciados no assunto supõem. Assim, não surpreende que algumas universidades, como o MIT (MIT, 2017), a Universidade de Nicosia (Nicosia, 2019) e a UFBP (UFPB, 2019) tenham lançado experimentos interessantes para substituir esses livros de registro e seus esquemas complexos por registros em blockchain.

Existe uma imensa expectativa de que a tecnologia possa permitir uma evolução nessas estruturas, tornando-as mais ágeis, confiáveis e automatizadas. Os mais entusiastas falam até em fim dos cartórios.

Não é possível afirmar que se chegará a tanto, mas o fato é que se tem investido muito tempo, esforço e pesquisa na busca de aplicações da tecnologia em setores da sociedade antes aparentemente imunes à tão temida disrupção tecnológica.

Pelo jeito, a tsunami digital tem um jeitão de ser bem democrática e não vai deixar, no longo prazo, ninguém de fora.

Lex cryptographia

A criatividade humana é virtualmente sem limites. O conceito de *smart contracts* ou contratos inteligentes não é nada novo. Nick Szabo o cunhou lá pelos idos de 1996 (Szabo, 1996), onde discutia o uso de códigos de computador como contratos no dia a dia. Algoritmos já estão regulando o relacionamento entre humanos há bastante tempo. Por exemplo, quando utilizamos um serviço de transporte ou de entrega mediado por aplicativos.

O código do aplicativo pode ser entendido como uma espécie de contrato, já que é responsável por controlar a relação entre as partes.

Tudo (ou quase tudo) o que é permitido dentro daquele contexto é especificado no software: desde o pedido de um motorista, passando pela aceitação da corrida, pelas regras de cancelamento de pedido e indo até o pagamento em si. Cada iteração do cliente ou do motorista com o aplicativo resulta em uma chamada ao código-contrato que corresponde à execução de uma cláusula prevista na ocorrência de um evento.

Existem motivos para acreditar que blockchain é uma excelente tecnologia para implementação dos *smart contracts*. Mesmo as transferências de Bitcoins não deixam de ser execuções de cláusulas de um contrato inteligente simples, que regula transferência de ativos. Mas, pode ser muito mais.

Existem blockchains específicas com esse fim. A Ethereum, por exemplo, permite que softwares complexos sejam armazenados na sua blockchain e sejam executados da mesma forma como descrito no exemplo do contrato de transporte mediado por aplicativos. A diferença é que, num *smart contract* do Ethereum, o código é executado e validado pela blockchain como um todo (Butterin, 2013).

A existência de um mecanismo tecnológico que rege relações entre seres humanos, com garantia de execução dentro das regras estabelecidas, criando ordem sem que seja necessário lançar mão de instituições, leis ou outros construtos sociais tem chamado a atenção de especialistas, que já cunharam a expressão lex cryptographica (a lei da criptografia) como uma forma de descrever essa inédita situação (De Filippi & Wright, 2018).

Sob o domínio da lex cryptographica, há possibilidade de ordem sem centralização nem assimetria de poder. Portanto, para todos os efeitos, não há possibilidade de conluio, nem de corrupção.

A máquina da confiança num mundo de desconfiança

Numa capa de 2015, a revista The Economist denominou a blockchain como a máquina da confiança (Berkeley, 2015).

Com o descrito até aqui talvez já seja possível entender a pertinência da denominação. Considere um *smart contract* na Ethereum. Todo o histórico da execução do contrato é armazenado de forma imutável para sempre e é acessível por qualquer pessoa pela Internet. Além disso, o contrato não pode ser alterado sem que o próprio processo de alteração tenha sido previsto no mesmo contrato originalmente estabelecido. E, caso ocorra a alteração conforme as normas estabelecidas, estas também ficam registradas (Butterin, 2013).

Desta forma, fica claro que podemos confiar no que é estabelecido por um smart contract. E que esta confiança é criada sem que tenhamos que confiar em ninguém. É o *trustless trust*.

A importância desse recurso não pode ser minimizada. Não estamos caminhando apenas para um mundo digital, mas também para um mundo onde confiança é um artigo de luxo.

A Edelman publica periodicamente uma pesquisa chamada Trust Barometer (Edelman, 2017), cuja manchete do sumário executivo de 2017 foi "Uma Implosão da Confiança". A confiança em todos as principais instituições pesquisadas caiu fortemente naquele ano e não há perspectiva de recuperação. Governos, empresas, imprensa e terceiro setor estão todos juntos, pelo menos nesse aspecto. A própria institucionalidade parece estar em cheque.

Especialistas já começam a relacionar o momento pelo qual passa nossa sociedade com aquele vivido com a criação da imprensa tipográfica por Gutenberg, ainda no século XV (Wheeler, 2019). A multiplicação não apenas das informações disponíveis para consumo na Europa (o número de livros publicados foi multiplicado por 20 num espaço de tempo relativamente curto), mas também do número de pessoas capacitadas a publicar, foi uma das bases para a derrocada da nobreza e da igreja, fustigadas por movimentos que não seriam possíveis antes daquela criação, como a reforma protestante e a revolução científica. O Iluminismo, a Revolução Industrial e as atuais democracias ocidentais são descendentes dessa invenção ou, no mínimo, foram habilitadas por ela.

Também naquela época, a população como um todo perdeu a confiança no sistema vigente e nos seus principais atores, já citados. Novos atores adentraram o palco e o que se seguiu faz parte da história. No longo prazo, as transformações foram extremamente benéficas, mas não sem muito tumulto e violência.

Por isso tudo, não se pode minimizar o nível de desconfiança das pessoas. Ele não é só conjuntural, é estrutural, principalmente num país como o Brasil. Nosso país não aparece diferenciado de outras democracias ocidentais na pesquisa da Edelman, exceto por um quesito: o setor público está entre os detentores de menor confiança em nível mundial. E isso sequer nos surpreende...

Crise e oportunidade

Em meados de 2017, fruto de uma reflexão interna, o BNDES entendeu que precisava inovar. Sendo já há muito tempo o maior investidor em seed capital e venture capital do Brasil, além de trabalhar com programas específicos para inovação há anos, poderia parecer fácil. Mas não era.

Inovar para fora sempre foi menos difícil do que inovar para dentro. Ao contrário de outras épocas, onde as chacoalhadas internas tinham sido empurradas principalmente pelo espírito intraempreendedor de heróis abnegados, agora era necessário implantar inovação como cultura, algo bastante mais desafiador.

Entre as diversas iniciativas, o IdeiaLab trouxe uma proposta um tanto simples: um concurso de inovação aberto a todos os empregados; com temáticas flexivelmente estabelecidas; com participação de equipes de até cinco pessoas, sem qualquer restrição quanto à sua formação; e cujo resultado final se daria por duas votações, sendo a primeira igualmente aberta a todos os funcionários e a segunda realizada por todos os superintendentes, responsáveis finais por escolher duas propostas para implementação.

Com 15% dos funcionários apresentando alguma ideia e 80% votando, a participação e a movimentação da casa podem ser consideradas um retumbante sucesso.

Escolhida para implementação, havia uma proposta de uso de blockchain para transparência no uso dos recursos do Banco. Inicialmente chamada de BNDESCoin, as iniciativas do BNDES se desdobraram em duas, conforme já havia sido proposto ainda em meados de 2017, no início do concurso: o BNDES Token e o TruBudget.

O BNDES Token é um token digital criptográfico, construído sobre a blockchain Ethereum, como um padrão ERC-20 (Arantes Jr, et al., 2018; Arantes Jr, et al., 2018). Como todo token da rede Ethereum, sua movimentação é totalmente transparente e pode ser acompanhada em tempo real por qualquer cidadão.

Já o TruBudget é um aplicativo para uma blockchain chamada Multichain (https://www.multichain.com/). Construído pelo banco de desenvolvimento alemão, KfW, o TruBudget foi criado pensando em melhorar a transparência de suas operações na África, através do registro do uso dos recursos no sistema. Ao contrário da Ethereum, do Bitcoin e das outras blockchains citadas, o Multichain (assim como outras, como Hyperledger, Quorum e Corda) não são redes abertas. Nelas, os nós que formam a rede são previamente conhecidos. Esse é um tipo bem mais simples e com implementações bem diferenciadas, chamadas de blockchains permissionadas, em contraste às blockchains púbicas referenciadas anteriormente.

As blockchains permissionadas têm sido muito usadas para integração entre sistemas de empresas (Arantes Jr, 2018). No caso do TruBudget, a equipe da iniciativa blockchain do BNDES propôs o uso para o Fundo Amazônia, cujos principais doadores são a Alemanha e a Noruega. Os nós da rede são o próprio KfW e o BNDES, tendo sido a Noruega convidada a fazer parte. Dessa forma, toda informação entrada sobre as operações ficam disponíveis para os doadores quase imediatamente, melhorando a capacidade de acompanhamento dos projetos. A proposta do BNDES Token, porém, é bem mais ousada.

BNDES Token

Ao liberar o token em vez de Real para um cliente, o BNDES se compromete a resgatá-lo dentro de certas condições definidas pelos smart contracts que implementam sua operação. O cliente, então, deve utilizar o token para adquirir os produtos e serviços previstos no contrato (tradicional, por enquanto) com o BNDES.

Apenas os fornecedores podem resgatar os tokens recebidos dos clientes. Na implementação em vista, o BNDES faz um depósito na conta corrente do fornecedor que corresponde ao valor total dos tokens resgatados. Esse valor é fácil de calcular, já que um BNDES Token tem o valor de um Real, o que o mercado costuma chamar pela alcunha de stable coin, ou seja, uma coin (moeda ou token) com valor estável. Quem garante a estabilidade, nesse caso, é o BNDES.

Todo o fluxo de BNDES Tokens fica transparente em tempo real para qualquer cidadão. Para assistir às transferências de recursos, o cidadão sequer precisa de um sistema do BNDES. Ele pode ver com "seus próprios olhos digitais", bastando para isso tornar-se um nó da própria blockchain Ethereum, o que é algo tecnologicamente viável para qualquer computador comum, bastando um pouco de conhecimento. Outras instituições ou cidadãos podem até construir suas próprias ferramentas para acompanhar os desembolsos.

Para melhorar a transparência do último passo, que é o depósito na conta corrente do fornecedor, a ideia é colocar uma prova desse depósito (conhecido tecnicamente como hash) na própria blockchain. Em implementações futuras, seria possível utilizar outra moeda criptográfica de amplo uso, o que garantiria a continuidade da transparência total. Todavia, isso depende de a adoção de alguma cripto moeda se difundir o suficiente para viabilizar essa evolução.

Os smart contracts garantirão que os BNDES Tokens só serão enviados para empresas que tenham sido cadastradas na própria blockchain. Além de garantir que o recurso se mantenha dentro do circuito esperado, o cadastro também é necessário para que o cidadão possa entender quais empresas participaram das transações. Isso porque transações de tokens ERC-20 na Ethereum normalmente se dão de endereço para endereço, o que não tem nenhum significado razoável para o cidadão. Para que as transferências sejam claras, é preciso associar os CNPJs das empresas a endereços da Ethereum que vão participar das transferências.

Por isso, os clientes do BNDES e seus fornecedores precisarão usar um certificado digital do tipo eCNPJ para assinar uma declaração digital onde declaram que são responsáveis pelos endereços que usarão para receber e repassar BNDES Tokens. O smart contract irá conferir a validade da declaração, o que dará garantia jurídica a qualquer um que estiver observando a blockchain de que os recebedores de recursos são efetivamente quem declaram ser. Isso porque o eCNPJ segue o chamado o padrão de certificados ICP Brasil e todo documento digital assinado com esse certificado tem validade legal (Arantes Jr, et al., 2018).

É muito importante destacar que esse processo de validação cadastral independe do próprio BNDES, pois o smart contract que valida a assinatura é publicado no Ethereum e seu funcionamento é transparente e garantido pela própria tecnologia. Assim, o cidadão pode confiar totalmente no processo, sem precisar confiar em nada além do padrão ICP Brasil e da própria tecnologia.

Todo o funcionamento do processo não é apenas transparente, é confiável. A implementação de smart contracts tem a preocupação de garantir a confiança do cidadão, mesmo que seja um cypher punk dos mais desconfiados.

Esse processo de construção tem a característica de *compliance by design*, ou seja, a própria arquitetura da solução garante sua correta execução e afasta, dentro do contexto daquilo que foi implementado como smart contract, qualquer possibilidade de desvio do previsto. Isso significa que as partes dos processos que possam ser automatizadas desta forma, sequer precisam ser auditadas, pois são confiáveis a priori!

Futuramente, pretende-se acrescentar outras avaliações na própria blockchain. Por exemplo, incluir as notas fiscais que comprovam as aquisições dos clientes perante os fornecedores, confrontando-as com as políticas operacionais do Banco. Isso significa que um empréstimo ou doação para aquisição de um equipamento nunca poderia ser utilizado para a compra de bebida ou armamento, por exemplo. Hoje em dia, estas proibições já existem e são garantidas. Mas as três melhorias a seguir mais que justificam a evolução do processo de acompanhamento.

A primeira é relevante: como o "*compliance*" é "*by design*", o impedimento da compra inadequada ocorreria em tempo real, ao contrário de hoje, que só é detectado e cobrado dias ou semanas. A segunda é de enorme interesse: sendo *compliant by desing*, é de se esperar que possa reduzir custos não

apenas de acompanhamento pelo BNDES, mas dos próprios órgãos de controle.

A terceira é muito mais importante e efetivamente revolucionária num mundo e num país de confiança em crise: por ser compliance by design, todo cidadão pode confiar a priori no processo e, mesmo se não confiar, pode ir lá ver ou rever com seus próprios olhos digitais. Essa possibilidade pode ser uma revolução no longo prazo.

Principais desafios

Nem tudo, porém, são flores em soluções baseadas em blockchain. A tecnologia, embora ofereça uma potencialidade inegável, ainda é um bocado imatura em diversos aspectos.

O mais importante primeiro. Ironicamente, algumas das maiores dificuldades são fruto de das próprias potencialidades da tecnologia e acabam gerando um problema relacionado exatamente àquilo que esta promete resolver: a segurança. A questão é que a imutabilidade e a transparência, combinadas, formam uma dupla explosiva. Não é só o cidadão ou o participante de um contrato que se beneficia da transparência no código.

Um hacker também fica muito satisfeito em conhecer seu *smart contract* em todos os detalhes. Isso o permite procurar brechas no contrato de forma a explorá-las para o seu benefício ou apenas para mostrar que pode. Por outro lado, se você perceber um problema no seu *smart contract* que poderá ser explorado por um hacker ou causar um enorme prejuízo a qualquer momento, atualizá-lo pode não ser nada simples e os impactos podem ser muito grandes para todos os envolvidos.

Num famoso caso de um conjunto de smart contracts da rede Ethereum que implementavam um novo modelo de negócios, chamado The DAO, a arrecadação de mais de 150 milhões de dólares de investimentos em Ethers, a moeda do Ethereum, depositadas diretamente no contrato publicado na rede, foi seguida pelo ataque de um hacker. Ele conseguiu transferir para uma conta pessoal algumas dezenas de milhões de dólares debaixo dos olhares aturdidos de todos. A comunidade de investidores e técnicos demorou um pouco até descobrir como evitar o pior e contra-atacou, numa trama digna de filme de ação. Ao final, um terço dos recursos haviam sido desviados e nunca mais foram recuperados. Mais desconcertante é que os recursos desviados não foram utilizados e encontram-se lá, parados até hoje. Aparentemente, o hacker estava só se divertindo.

No futuro, o mais provável é que sejam criados padrões bem estabelecidos para lidar com a questão do upgrade de algo que deveria ser imutável. Por agora, as saídas são precárias e, como todo código obrigatoriamente tem bugs, colocar qualquer software que não seja muito simples ou que não tenha sido profunda e custosamente testado em produção é uma atitude de coragem, desespero ou pura falta de noção.

Um outro problema técnico clássico é o desempenho. A rede Bitcoin processa algo como sete transações por segundo, contra algo menor do que 20 na Ethereum. Quando estas redes sofrem surtos de demanda, como no pico do valor do Bitcoin ou no hype do Cryptokitties (um joguinho de colecionar gatinhos digitais para o Ethereum), ambos no fim de 2017, as transações começam a demorar muito para ser completadas ou ficam simplesmente muito caras. Isso ocorre porque, em ambas as redes, o usuário paga para ter sua transação processada. O preço é livre e os nós tendem a priorizar quem paga mais. Se houver muita demanda, o preço sobe. Como se vê, embora técnico a princípio, o problema torna-se bem concreto ao se desdobrar em custos que podem inviabilizar alguns modelos de negócio.

Várias outras questões podem ser citadas fora do âmbito técnico, como um certo gap legal, principalmente no Brasil, ou os perigos de governança da rede. Por exemplo, como o Bitcoin não tem nenhum dono que decide em última instância o que fazer, discordâncias na comunidade quanto aos caminhos a seguir nas evoluções da rede podem levá-la a se dividir, num processo conhecido como hard fork. Tal evento, que já ocorreu algumas vezes no Bitcoin e uma vez na Ethereum, causa muita ansiedade entre todos os stakeholders, pois um hard fork mal executado pode causar um cataclismo na rede.

Não é à toa que implementações em blockchain tendem a ser muito diferente daquilo com o qual nos acostumamos vindo do Vale do Silício: softwares que são lançados ainda inacabados, com alguns bugs, que vão sendo corrigidos ao longo do tempo. Com criptografia, não existe essa possibilidade. Se houver um erro, pode-se pôr tudo a perder. As evoluções em blockchain costumam acontecer num ritmo muito mais controlado, sem o frenesi típico de uma nova versão do aplicativo a cada duas semanas. Blockchain não é aplicativo. É infraestrutura: se fizer errado, quebra e leva muita coisa junto, inclusive o valor de mercado da criptomoeda correspondente, o que não é aceitável.

Um começo modesto, um futuro em aberto

O TruBudget entrou em produção em maio de 2019, com um projeto piloto para acompanhar o uso dos recursos do Fundo Amazônia.

O BNDES Token tem previsto um piloto em produção em junho de 2019, porém numa versão muito simplificada, onde o token ainda funcionará como um registro parecido como o TruBudget e não como um ativo digital, o que ocorrerá no passo seguinte.

São experimentos que abrem uma janela para um futuro diferente, não limitado a uma única instituição, onde processos públicos poderão ser mais confiáveis, mesmo para o mais desconfiado dos cidadãos.

Onde a aplicação de recursos poderia ser acompanhada por lupa e em tempo real. Ou ainda melhor, onde ninguém se preocupará em acompanhar a execução do processo, apenas o seu desenho e seu desempenho, já que será possível acreditar que tudo está *compliance by design.*

Onde o debate poderá se concentrar nas ideias e a energia de todos não seja tão desperdiçada em apontar o dedo uns para os outros. Isso é um possível futuro distante. Muito distante, até...

Mas, se a gente tiver ajudado com um tijolinho que seja nessa construção, olhando para traz, vai ter valido a pena ter feito todo mundo virar um pouquinho *cypher punk.*

Referências

ANAND, S. A Pioneer in Real Estate Blockchain Emerges in Europe. Wall Street Journal, 2018.

ANTONOPOULOS, Andreas M. **Mastering Bitcoin: unlocking digital cryptocurrencie**s. " O'Reilly Media, Inc.", 2014.

ARANTES JR, G. M. Blockchain e o futuro da nova fase de integração nos negócios, Portal do Bitcoin. [Online], 2018 Disponível em: <https://portaldobitcoin.com/blockchain-e-o-futuro-da-nova-fase-de-integracao-nos-negocios/> Acesso em: 30/abr./2019.

ARANTES JR, G. M. et al., BNDESToken: Uma Proposta para Rastrear o Caminho de Recursos do BNDES. In: **Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações** (WBlockchain-SBRC 2018). SBC, 2018.

ARANTES JR, G. M. et al., Improving the Process of Lending, Monitoring and Evaluating Through Blockchain Technologies: An Application of Blockchain in the Brazilian Development Bank (BNDES), **2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)**. IEEE, 2018. p. 1181-1188.

BAIRD, L., The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance. **Swirlds Tech Reports** SWIRLDS-TR-2016-01, Tech. Rep., 2016.

SASSON, E. B. et al. Zerocash: Decentralized anonymous payments from bitcoin. In: **2014 IEEE Symposium on Security and Privacy**. IEEE, 2014. p. 459-474.

BERKELEY, J., 2015. The Trust Machine. The Economist, 31 Outubro.

CHOD, J. et al. Blockchain and the value of operational transparency for supply chain finance. **Mack Institute for Innovation Management, Working Paper Series**, 2018.

DE FILIPPI, P. Blockchain and the law: The rule of code. Harvard University Press, 2018.Edelman, 2017. 2017

GARRISON, R. H.; NOREEN, E. W.; BREWER, Peter C. **Contabilidade gerencial**. AMGH Editora, 2013.

HEARN, M. Corda: A distributed ledger. Corda Technical White Paper, 2016. Disponível em: <https://www.corda.net/content/corda-technical-whitepaper.pdf> Acesso em: 30/abr./2019.

HUGHES, E., A Cyberpunk's Manifesto. [Online] 1993. Disponível em : <https://www.activism.net/cypherpunk/manifesto.html> Acesso em: 30/abr./2019.

DURANT, E.; TRACHY, A. Digital Diploma debuts at MIT. Digital Diploma Debuts at MIT. [Online] 2017 Disponível em <http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017> Acesso em: 30/abr./2019.

NAKAMOTO, S., Bitcoin: A Peer-to-Peer Electronic Cash System. [Online] 2008 Disponível em: <https://bitcoin.org/bitcoin.pdf> Acesso em: 30/abr./2019.

NGUYEN, G.-T., KIM, K., A Survey about Consensus Algorithms Used in Blockchain. **Journal of Information Processing Systems, Fevereiro**, 14(1), pp. 101-128. 2018

POPOV, S., The Tangle, IOTA Academic Papers. [Online] 2018 Disponível em: <https://www.iota.org/research/academic-papers> Acesso em: 30/abr./2019.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, v. 21, n. 2, p. 120-126, 1978.

SZABO, N. Smart contracts: building blocks for digital markets. EXTROPY: The Journal of Transhumanist Thought,(16), v. 18, 1996.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world**. Penguin, 2016.

Wheeler, T. **From Gutenberg to Google**. Brookings Institution Press 2019.

Sites Acessados

ANON., s.d. Hyperledger. [Online] Disponível em: <https://www.hyperledger.org/> Acesso em: 30/abr./2019.

BOGLIATO, M. S., 2018. Hathor Network. [Online] Disponível em: <https://hathor.network/> Acesso em: 30/abr./2019.

BUTTERIN, V., 2013. Ethereum Foundation. [Online] Disponível em: <https://github.com/ethereum/wiki/wiki/White-Paper> Acesso em: 30/abr./2019.

Edelman Trust Barometer. Disponível em: <https://www.edelman.com/research/2017-edelman-trust-barometer> Acesso em: 30/abr./2019.

Frozeman, 2015. ERC Token Standard. [Online] Available at: https://github.com/ethereum/eips/issues/20

University of Nicosia <https://www.unic.ac.cy/iff/blockchain-certificates/ >Acesso em: 30/abr./2019.

UFPB, 2019. Lavid/UFPB vai desenvolver diploma digital para todo país em colaboração com outras universidades. [Online] Disponível em: <http://ci.ufpb.br/lavid-ufpb-vai-desenvolver-diploma-digital-para-todo-pais-em-colaboracao-com-outras-universidades/> Acesso em: 30/abr./2019.