Instituto
de Tecnologia
& Sociedade
do Rio

RELATÓRIO

Blockchain para aplicações de interesse público

Apresentação

Nos últimos anos, a tecnologia blockchain esteve no centro de discussões sobre inovação, sendo apontada como uma das maiores transformações econômicas, sociais e técnicas das últimas duas décadas. Em que pese a quantidade de experimentos e prognósticos sobre o seu impacto na sociedade, há ainda um longo caminho a ser percorrido para que se possa vislumbrar os efeitos mais amplos da transformação que ela promove.

O Grupo de Estudos em Blockchain e Interesse Público do ITS Rio foi decorrente do olhar atento que o instituto lança sobre as implicações sociais de múltiplas tecnologias emergentes, acreditando sempre que inovações como esta pode ter um papel crítico em especial para as nações do Sul Global. Nelas, ainda mais, problemas relacionados à confiança perduram como um desafio de grandes proporções, pela forma como a falta desse atributo parece reforçar questões endêmicas a exemplo de corrupção e burocracia.

Ao longo de 12 meses, o grupo de pesquisadores foi conduzido por 10 encontros realizados ao vivo pela internet, promovidos com o intuito de lançar luz às relações que a tecnologia blockchain possui com múltiplos setores caros ao interesse público, contando sempre com a participação de atores de grande renome nos ecossistemas local e internacional. Os encontros contaram com palestras e debates envolvendo especialistas do tema oriundos de diferentes países, além de participantes convidados para os debates que tiveram a oportunidade de enriquecer a conversa a partir da apresentação de estudos de caso a respeito dos projetos baseados em blockchain que vêm construindo. O grupo foi formado depois de uma criteriosa seleção, de forma a identificar os principais nomes do cenário nacional, no que tange o potencial de impacto na interseção de tecnologia e sociedade. Composto por 20 pessoas, entre pesquisadores, acadêmicos e representantes dos setores público e privado, a seleção também teve como preocupação assegurar seu caráter multissetorial.

O presente documento foi construído a partir das relatorias e da contribuição voluntária dos integrantes do Grupo de Estudos sobre Blockchain para aplicações de Interesse Público, conduzido pelo Instituto de Tecnologia e Sociedade do Rio (ITS Rio) com o apoio do Instituto de Referência em Internet e Sociedade (IRIS-BH), entre os meses de agosto de 2017 e agosto 2018. Traz como resultado uma apresentação sobre a tecnologia blockchain e os que ela permite, focando-se, então, na proposição de um modelo para construção de aplicações blockchain integradas à preservação do interesse público.

Método e objetivos

DOCUMENTO PRODUZIDO A PARTIR DA RELATORIA DOS ENCONTROS DO GRUPO DE PESQUISA

DIAGNÓSTICO DOS RECURSOS DA TECNOLOGIA BLOCKCHAIN – CARACTERÍSTICAS E POSSIBILIDADES DE USO.

PROPOSIÇÃO DE UM MODELO – FRAMEWORK – DE IMPLEMENTAÇÃO DA TECNOLOGIA A PARTIR DO INTERESSE PÚBLICO

AO LONGO DE

12

MESES

TOTAL DE

11

ENCONTROS

11

ESPECIALISTAS DE DIFERENTES PAÍSES

MODELO MULTISSETORIAL

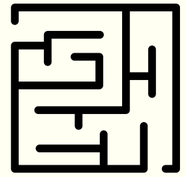
20

PARTICIPANTES: PRINCIPAIS NOMES DA ACADEMIA, SETOR PÚBLICO E PRIVADO

O QUE SIGNIFICA (PARA NÓS) INTERESSE PÚBLICO:

VALORES E DIREITOS UNIVERSAIS

DESENVOLVIMENTO ECONÔMICO E SOCIAL SUSTENTÁVEL



SOLUÇÕESPARAPROBLEMAS CONCRETOS DA REALIDADE POLÍTICA, ECONÔMICA E SOCIAL

Prefácio

Por Ronaldo Lemos

Já não é mais novidade. Vivemos um período de profundas mudanças em relação à "confiança". As pessoas têm perdido a confiança nas instituições, no setor privado e até mesmo na democracia. Existe uma demanda imensa por novas formas de se estabelecer confiança, seja ela em governos, empresas e até mesmo nas relações pessoais. A blockchain é uma tecnologia que surgiu exatamente para isso: gerar confiança, de forma distribuída.

Nosso modelo de confiança atual é baseado primordialmente em sistemas centralizados ou descentralizados. Se você quer saber quanto Alice tem em sua conta bancária, por exemplo, você precisa perguntar a uma instituição financeira — e confiar no que ela disser. A blockchain, no entanto, permite a criação de uma nova forma de confiança que não é centralizada (como no caso dos governos) nem descentralizada (como no caso do sistema financeiro global). É um modelo distribuído; e é por isso que esse sistema foi chamado de "confiança sem confiança", ou "trustless trust", no original em inglês.

Com esse propósito, a blockchain usa criptografia para assegurar a criação de um enorme banco de dados totalmente protegido contra adulteração (mesmo por seus operadores individuais). Gosto de dizer que ela pode ser descrita como um banco de dados, distribuído, capaz de produzir consenso e assegurar a integridade e unicidade das informações que nela são inseridas. Uma aplicação natural para isso é a criação de moedas virtuais, como é o caso do Bitcoin. Para saber quanto um usuário hipotético possui de saldo em bitcoins, não é preciso perguntar a nenhuma instituição intermediária, nem a nenhum banco. Pergunta-se à própria rede, que concorda de forma unânime sobre a quantidade de bitcoins que esse usuário possui.

Ao criar uma camada de consenso distribuído, a blockchain tem potencial para reconfigurar nossos sistemas de confiança em muitas outras áreas além do sistema financeiro. Uma das formas da blockchain criar consenso é por meio de um processo chamado "prova de trabalho" (proof of work), que consiste em resolver um desafio matemático, que é então demarcado no tempo, "assinado" criptograficamente e distribuído ao longo de toda a rede, o que impede sua adulteração.

E quais são suas aplicações? Como disse acima, gosto de pensar na blockchain como um grande banco de dados. Ela armazena pedaços de infor-

mação interligados entre si, em blocos (daí o nome); no entanto, essa informação é armazenada de forma distribuída. Toda a rede "concorda" com aquela informação, gerando, assim, consenso sobre ela em toda parte. Essas informações são imutáveis.Com isso, a probabilidade de adulteração da blockchain é praticamente zero. Além disso a integridade e unicidade das informações é assegurada em cada bloco.

Esse modelo de "blockchain" pode assumir muitas configurações técnicas e formatos operacionais nos dias de hoje. Em nossa visão, as blockchains mais promissoras são aquelas desenvolvidas por comunidades abertas e mantidas como um projeto open source, descentralizado, transparente e auditável.

No entanto, tecnologias nunca são neutras, e a blockchain não é nenhuma exceção. Ela foi originalmente concebida como uma tecnologia financeira, aplicada na criação do Bitcoin. Assim, não chega a ser surpreendente que os esforços em torno do seu uso hoje sejam majoritariamente para a promoção de ganhos econômicos. Isso é possível, por exemplo, por meio dos ganhos de eficiência promovidos por ela, ou ainda, pela redução dos custos de transação. Ela também desafia o papel dos intermediários nas mais diversas áreas, especialmente quando este intermediário é um "depositário de confiança" que se organiza de forma centralizada.

Assim como protocolos que permitiram a criação da internet como a conhecemos hoje, como o TCP/IP, a blockchain é também uma tecnologia livre e aberta, que não pertence a ninguém nem foi "patenteada" por seus criadores. Ao contrário, ela se tornou uma tecnologia aberta para o uso por parte de qualquer pessoa. Por isso mesmo ela se converteu em uma tecnologia fundacional, tal como foi o TCP/IP, ou ainda, a linguagem HTML que originou a World Wide Web (www). Por essa razão, a blockchain tem propriedades que podem ser descritas como "generativas", tal qual a Internet. Por isso, acredito que essa tecnologia pode levar ao surgimento de muitas aplicações de interesse público. Dentre elas, a possibilidade de votar pela internet, plataformas online de gestão de orçamentos participativos, ou ainda, um novo conjunto de ferramentas participativas e de organização social. Tudo isso terá como aliado a poderosa tecnologia de "provas criptográficas" em ambiente distribuído, transformando o modo como entendemos e vivenciamos a confiança.

1) Introdução

Ao longo dos últimos 20 anos, a expansão da internet comercial trouxe transformações estruturais na forma como a humanidade se relaciona, especialmente nos aspectos social e comercial. A redução em custos operacionais e a possibilidade de conectar novos mercados de modo mais eficiente foram alguns dos principais fatores que levaram à ascensão e à proeminência de certos modelos de negócio, característicos da economia digital. Dentre eles, destacam-se diversos serviços de intermediação online, que vão do e-commerce a grandes provedores de conteúdo e processadores digitais de pagamento.

A onda de inovações se acentua na atualidade, com recursos que trazem a possibilidade de descentralizar as interações humanas em diferentes aspectos, refletindo diretamente na forma de consumo e no potencial de colaboração. Operações de compra venda são simplificadas enquanto cresce a tendência de compartilhamento de serviços e afins.

A base da mais forte dentre essas mudanças possíveis está na capacidade que vem sendo construída de se criar aplicações descentralizadas em campos antes dominados por poucos.

CRIA-SE UM NOVO PARADIGMA:

O PROVIMENTO DE UM SERVIÇO PODE NÃO MAIS DEPENDER DA FIGURA DE UM SERVIDOR CENTRALIZADO, UMA EMPRESA OU UMA INSTITUIÇÃO TRADICIONAL. EM SEU LUGAR, UMA NOVA TECNOLOGIA, A BLOCKCHAIN, PERMITE QUE EM ALGUNS CAMPOS TUDO POSSA VIR A SER CONTROLADO DIRETAMENTE PELA MASSA DE USUÁRIOS DESSAS REDES.

Cria-se um novo paradigma: o provimento de um serviço pode não mais depender da figura de um servidor centralizado, uma empresa ou uma instituição tradicional. Em seu lugar, uma nova tecnologia, a blockchain, permite que em alguns campos tudo possa vir a ser controlado diretamente pela massa de usuários dessas redes.

Do ponto de vista prático, a compreensão geral desse fenômeno abre espaço para que novas oportunidades de negócio sejam evidenciadas, identificando ainda meios para a inovação em setores onde atualmente predomina a centralização, a burocracia ou os grandes custos operacionais. A sociedade como um todo tende a se beneficiar na medida em que novos serviços baseados na tecnologia blockchain surgem. Afinal, como demonstrado neste documento, o potencial dessas implementações é muito significativo, especialmente quando se trata de ampliar a transparência, a acessibilidade, e a segurança de operações baseadas em tecnologia da informação.

Contudo, as novas tecnologias quando pensadas como um fim em si mesmo têm um potencial limitado de transformar a sociedade. Por vezes, podem até mesmo gerar movimentos incontroláveis e incoerentes com sua visão inicial. Resguardar valores como a preservação do interesse público, a descentralização e a usabilidade em aplicações construídas a partir da tecnologia blockchain, a fim de que elas atendam ao mais amplo escopo possível de anseios das variadas facetas da sociedade, são obrigações permanentes. É precisamente por se tratar de um esforço contínuo, e não de um fator assegurado de antemão, que se faz valer o presente relatório e a construção do framework proposto, com o intuito de facilitar e guiar esse processo.

1.1) Blockchain: situando a tecnologia no tempo e espaço

Blockchain, a tecnologia que floresceu com o surgimento da moeda digital Bitcoin, carrega no próprio nome o seu significado central: trata-se de uma base de dados organizados através de blocos encadeados, ou seja: interligados sequencialmente e de forma ordenada, criando um histórico transparente e imutável de transações e registros nela armazenados. Vale notar, no entanto, que esta tecnologia engloba diferentes conceitos e tecnologias, dentre os quais alguns deles se encontravam no escopo das ciências da computação há mais de duas décadas, como a comunicação ponto-a-ponto (P2P) dos sistemas distribuídos e a criptografia assimétrica.

Numa blockchain, os blocos de dados que a constituem são interligados por elos sequenciais, sendo estes inquebráveis por um parte que tente fraudá-los. Essa importante característica assegura significativos graus de imutabilidade e temporalidade a tudo o que se registra a partir da tecnologia. Tal encadeamento é produzido e mantido de modo permanente, adicionando periodicamente novos dados consistentes com as informações previamente armazenadas na base. Antes de ser efetivamente registrado na blockchain, todo novo conteúdo informacional é previamente validado e resguardado por um mecanismo de consenso descentralizado, usualmente baseado na noção de um ou mais algoritmos de consenso, conceito explicado em detalhes a seguir. O banco de dados mantido a partir de voluntários conectados por meio de uma rede descentralizada, sem qualquer forma de autoridade central, permite a existência de sistemas autônomos e alternativos aos vigentes. Esta configuração confere a quaisquer dados armazenados a partir dela características singulares que são avaliadas individualmente adiante, e que podem dar base a uma gama de aplicações ampla, especial no que concerne à esfera do interesse público.

Trazendo tal complexidade e dinamismo, a blockchain se tornou a primeira tecnologia a materializar um potencial de mudança real nos paradigma econômico e social vigentes em alguns territórios, possibilitando a emergência de modelos mais descentralizados e distribuídos. No entanto, ela na verdade apenas inaugura a série de plataformas tecnológicas distribuídas que surgem a partir de então para variados fins, mudando a forma como a sociedade troca ativos ou informações de múltiplas naturezas.

Em 2014, um novo protocolo aberto para a construção de aplicações des-

centralizadas generalizadas (e não somente financeiras) foi inteiramente construído em torno da tecnologia blockchain e lançada com sucesso: a Ethereum. Nesta, tornou-se possível também a criação do que se conhece hoje por contratos inteligentes, trechos de códigos capazes de operacionalizar registros mais complexos de propriedade e a consequente emergência até mesmo das primeiras organizações autônomas (DAOs). Este feito evidenciou para um mercado que cresce exponencialmente o potencial das plataformas distribuídas, com a possibilidade de ir muito além dos sistemas de pagamento ou registros permitidos pela aplicação original da tecnologia no protocolo Bitcoin.

A BLOCKCHAIN ENGLOBA DIFERENTES CONCEITOS, COMO A COMUNICAÇÃO PONTO-A-PONTO (P2P) DOS SISTEMAS DISTRIBUÍDOS E A CRIPTOGRAFIA ASSIMÉTRICA. ALGUNS DELES SE ENCONTRAM NO ESCOPO DAS CIÊNCIAS DA COMPUTAÇÃO HÁ MAIS DE DUAS DÉCADAS.

1.2) A tecnologia a interesse de quem

Apresentado o breve histórico da Blockchain e a evolução desse tipo de tecnologia, os conceitos e aplicações tangíveis são abordados a seguir de forma a identificar benefícios e limitações, a fim de que seja estabelecido um conceito básico de onde e como de fato se pode atuar com ela. Para isso, interesse público estará aqui se referindo não estritamente ao setor público, mas ao proveito do grupo social ao qual uma solução tecnológica pode ser aplicada. Mesmo que para este fim o setor público seja impactado de forma direta ou indireta, a ideia de interesse público aqui utilizada se sustenta nos valores e princípios que permeiam o bem comum da sociedade, os valores e direitos universais e o desenvolvimento econômico e social sustentável[AB1] .

Levando este olhar em consideração, soma-se a isso o fato de a tecnologia ser uma ferramenta a ser compreendida e utilizada sempre que possível como tal. Aplicações de cunho tecnológico não solucionarão cada um dos complexos problemas da sociedade. Entretanto, o entendimento dessas ferramentas como instrumentos políticos guiados para a solução de problemas sociais reais é fundamental para o desenvolvimento equitativo de comunidades.

Além disso, se essas tecnologias de fato conduzirem a proposições para solucionar desafios da sociedade não há razão para ser contra. Sendo assim, são inúmeras as aplicações sustentadas por tecnologias como a blockchain que permitem uma maior participação popular nas tomadas de decisão e na elaboração de políticas públicas.

"YES, [WE WILL NOT FIND A SOLUTION TO POLITICAL PROBLEMS IN CRYPTOGRAPHY], BUT WE CAN WIN A MAJOR BATTLE IN THE ARMS RACE AND GAIN A NEW TERRITORY OF FREEDOM FOR SEVERAL YEARS."

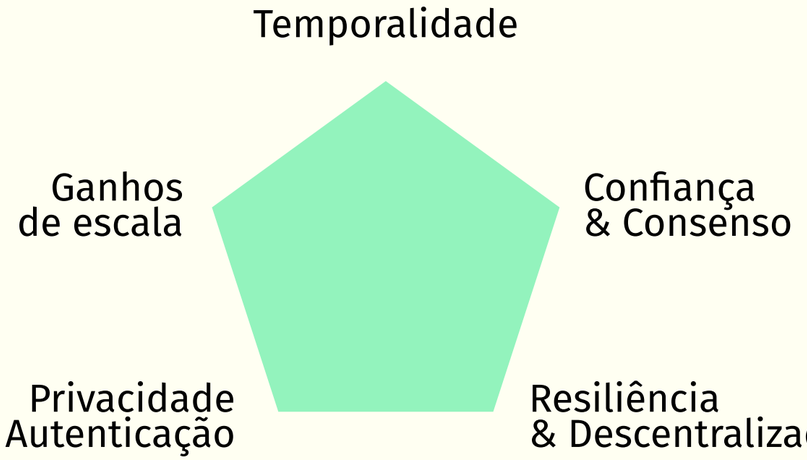
– SATOSHI NAKAMOTO, NOVEMBRO DE 2008.

2) Benefícios e desafios da tecnologia blockchain

Os benefícios de utilizar a blockchain estão intrinsecamente relacionados aos elementos que compõem a tecnologia. Essa tecnologia distribuída permite redução de custos e de burocracia, e aumento da confiabilidade e eficiência em sistemas de pagamento. É importante ressaltar, entretanto, que os benefícios atrelados à tecnologia blockchain não se resumem a um campo isolado.

2.1) A singularidade da Blockchain e seus principais benefícios

Os principais benefícios estão relacionados à promoção de **transparência**, **segurança** e *accountability*, logo reduzindo fraudes e corrupção, bem como de rastreabilidade. A propósito, **a imutabilidade, a inviolabilidade e resiliência** são uns dos principais fatores que fomentam o entusiasmo acerca da tecnologia. O caráter de descentralização do sistema permite que apenas dados verificados por nós independentes sejam



aceitos, o que torna impraticável e altamente custosas as tentativas de fraude na entrada e alteração de dados.

Diferentemente dos sistemas contábeis tradicionais, a blockchain trabalha com o conceito de contabilidade de tripla entrada, na qual a variável tempo é inserida e anexada a todas as transações, de modo que estas sejam localizadas e ordenadas em uma ordem específica. Essa **temporalidade**, isto é, o fato de cada transação ser codificada e "carimbada" com data e hora, permite o rastreamento de todos os "blocos da corrente", além de garantir que as transações não sejam alteradas. Essa lógica de encadeamento de blocos que possuem informações de transações passadas, somada ao caráter de imutabilidade do sistema permite que qualquer transação possa ser rastreada até, no limite, o bloco gênesis.

Uma característica que garante a **singularidade** da blockchain em relação a outros bancos de dados descentralizados é o mecanismo de consenso vigente e sua recorrente atualização. Isso ressalta a questão da **confiança**, de modo que participantes desconhecidos entre si podem confiar na outra parte de forma inequívoca, fato que é garantido pela criptografia e pelos algoritmos de consenso. Estes basicamente se tratam de um algoritmo que garante que os dados de uma rede sejam os mesmos para todos participantes, sendo crucial para legitimação das transações. A propósito, é importante frisar que o debate sobre governança descentralizada e distribuída está diretamente relacionado a esse mecanismo de consenso (normalmente influenciados por incentivos econômicos). Logo, muita atenção deve ser dada neste quesito. Sendo assim, a **resiliência** da rede é um ponto a ser enaltecido. No caso da Bitcoin blockchain, por exemplo, não há nenhuma ocorrência de queda total na rede ou de ataques que de fato tenham comprometido seu funcionamento. até o momento.

O principal mecanismo que provê tal resiliência é fruto da **descentralização** da rede que, desprovida de pontos centralizadores passíveis de ataques mal intencionados ou de erro interno, consegue operar mesmo em situações extremas, como em uma situação hipotética onde uma grande região fique sem acesso à internet. Característica fundamental de sistemas distribuídos, a arquitetura de rede peer-to-peer (P2P) garante que uma pessoa, uma instituição ou uma empresa se comunique diretamente de forma eficiente com outrem sem a necessidade de intermediários no processo. A propósito, em uma perspectiva filosófica e antropológica, isso pode ser inclusive classificado como sendo desenvolvimento.

É relevante mencionar também a questão da **privacidade**. Em algumas redes como a Blockchain, há a necessidade de que seus participantes sejam totalmente anônimos, o que é possível de ser alcançado em diferen-

tes níveis, de acordo com o protocolo utilizado. Na blockchain do Bitcoin, por exemplo, o usuário não precisa, a priori, se identificar por meio de dados pessoais, exceto os casos em que a aplicação toca às instituições tradicionais. O fator privacidade é no entanto variável, dependendo do modo de uso da rede. Em determinadas aplicações, se os membros de uma rede assim o quiserem, é possível definir que as identidades de cada membro seja verificável. Como cada participante tem acesso à sua chave privada única, qualquer um pode assinar digitalmente sua transação com ela, de modo que seja possível concluir matematicamente que quem executou tal assinatura foi o detentor daquela chave. Neste sentido, a dupla **privacidade-autenticação** é um campo que, sem dúvida, apresenta uma ampla gama de aplicações possíveis, a depender dos objetivos de um projeto.

Entre outras características da blockchain estão possibilidade de elaborar "pedaços de códigos" auto-executáveis, os chamados contratos inteligentes e as organizações autônomas descentralizadas. De tal forma, a **programabilidade** pode também ser considerada um benefício da tecnologia blockchain que permite, por conseguinte, a **previsibilidade**. Aliás, esta técnica possibilita não apenas a confecção de um sistema automático, mas também a criação de camadas onde é possível criar outros sistemas que rodam em paralelo a outras diversas aplicações. Dado que são altamente programáveis e automatizáveis, torna-se evidente os ganhos de escala da rede. Redes como a blockchain têm um potencial enorme de alcance com **ganhos de escala** crescentes e custos decrescentes de acordo com o tamanho de sua estrutura.

Por fim, é fundamental ressaltar que embora os benefícios inerentes à tecnologias como a Blockchain sejam inúmeros, ela não pode solucionar todos os problemas de forma tão simples. Trata-se de uma tecnologia relativamente nova, em estágio primário de desenvolvimento. Ainda que em processo de rápida evolução, vale lembrar que poucos dominam todas as suas complexidades, o que nos leva à necessidade de discutir também os desafios que ela representa.

2.2) Desafios e limitações da tecnologia blockchain

Apesar de todos os benefícios atrelados à blockchain, é importante enfatizar também que algumas das principais características da tecnologia podem representar, por vezes, uma de suas grandes limitações. Seu caráter **descentralizado supranacional** traz dificuldades para diversas jurisdições chegarem em consenso sobre a forma de atuar para garantir a estabilidade e legalidade da tecnologia sem comprometer potenciais ganhos de inovação. Por exemplo, como aconteceu no ínicio do Bitcoin com relação ao **anonimato**, levantando diversas preocupações, uma vez que este recurso pode hipoteticamente permitir que se reproduzam casos de uso ilegais, como o comércio de entorpecentes e a lavagem de dinheiro.

Cada uma destas questões pode ser contornada e respondida quando endereçadas de forma responsável em seus diferentes contextos regionais, e promovendo a devida discussão sobre os **aspectos jurídicos** em que esbarram. O principal desafio, neste ponto, é fazer com que tal responsabilidade se resolva a partir de processos participativos e multisetoriais que contribuam para um entendimento convergente entre diferentes jurisdições.

Outro desafio da tecnologia, mais ligado aos seus aspectos técnicos, diz respeito à emergência de diferentes tipos de redes distribuídas como a Blockchain. Esta multiplicidade de aplicações pode acarretar a expectativa de aumento do número de transações por segundo que cada rede suporta. De forma simples, cada transação tem um custo relativo ao seu tamanho e representa a capacidade computacional necessária para executar tal transação. A questão da velocidade da rede, portanto, está ligada ao valor das **taxas de transação**, ou seja, a capacidade da rede operar e seu valor intrínseco, que aumenta à medida que novas redes surgem com a intenção de ter desempenho melhor.

Apenas a título de comparação, até o momento as primeiras e principais redes públicas (Bitcoin e Ethereum) têm velocidades de pico ainda reduzidas, na casa de algumas dezenas por segundo. A NEO, uma rede chinesa lançada em 2014, mas se tornando popular na atualidade, tem anunciado até 10 mil transações por segundo.

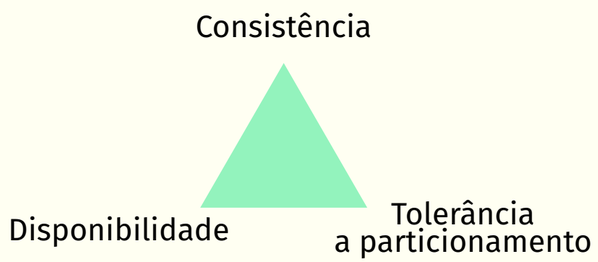
A **complexidade** é também um fator que representa as limitações da blockchain. Por ser, na verdade, uma combinação de diversas tecnologias, o seu entendimento para a ampla maioria do público ainda é muito restrito. Em geral, as pessoas nunca ouviram falar de redes ponto-

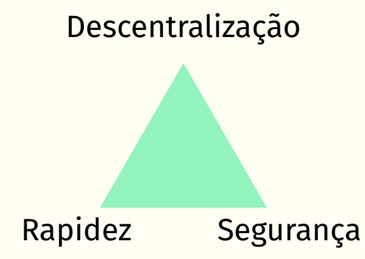
-a-ponto, computação distribuída, chave de criptografia assimétrica e seus hashs. Neste sentido, a Blockchain se torna um conjunto de complexidades que pode demandar anos para se popularizar, e principalmente, se consolidar.

Em certa medida, este fator pode ter dupla consequência. Se por um lado representa um desafio diretamente relacionado à **baixa experiência de uso da tecnologia**, podendo incorrer no seu potencial de **disseminação e custos de oportunidade** de novas implementações; por outro, pode ser interpretado como um benefício. No que tange ao surgimento de novos modelos organizacionais e de inovação, por exemplo, essa questão abre uma gama de oportunidade a serem testadas com potencial de implementações reais.

Alguns desafios técnicos são inerentes a essas complexidades, entre eles, o da computação distribuída (Teorema CAP) vale destaque. De acordo com o proposto por Eric Brewer, professor emérito de ciência da computação na Universidade da Califórnia, CAP significa *Consistency* (consistência), *Availability* (disponibilidade) e *Partition tolerance* (tolerância à partição). Conceitos que estão relacionados à veracidade das mensagens enviadas e disponibilidade de comunicação entre dois nós, e à tolerância de partição da rede em questão. O teorema CAP diz que jamais se poder ter essas três características de forma simultânea. Sendo a partição um fator intrínseco à sistemas distribuídos, seria necessário "escolher" entre consistência e disponibilidade.

Em suma, redes descentralizadas deverão obrigatoriamente sacrificar algum benefício em prol dos demais que configuram o trilema em questão, o qual também pode ser interpretado como uma impossibilidade de ter sistemas perfeitos no que concernem, ao mesmo tempo, descentralização, escalabilidade e rapidez. Normalmente, blockchains irão sacrificar em alguma medida rapidez/tempo em favor de níveis mais amplos para descentralização e segurança.





Basicamente, considerando o cenário apresentado em torno dos benefícios e desafios, podemos afirmar que o potencial da tecnologia blockchain é imenso. Seu impacto positivo, contudo, dependerá de como certas decisões forem tomadas, sobretudo no âmbito regulatório. Como se viu, muitas vezes tanto os benefícios quanto desafios podem variar de acordo com a perspectiva e modo de implementação. A questão que deve ser levantada, portanto, é sobre como organizações tradicionais, e principalmente seus governantes, irão se posicionar frente à adoção da tecnologia. Neste sentido, benefícios poderão ser alcançados e desafios superados à medida que estes atores se comprometem com o debate informado e responsável sobre a sua capacidade de inovação.

Contratos Inteligentes

Contratos evoluem constantemente e acompanham a sociedade, desde as relações de contratos na economia agrária, que era baseada em contratos individuais a distância. Passando pela sociedade industrial, onde os termos contratuais se padronizam, minimizando o envolvimento humano, avançamos para era digital em que contratos estarão cada vez mais dentro de agentes eletrônicos.

Quando falamos de contratos inteligentes, há primeiramente a identificação de que este seria um contrato dentro de um modelo eletrônico, o que é partcialmente verdadeiro. Quando Nick Szabo pensou em contratos inteligentes, pensou principalmente na segurança de formalização das relações entre pessoas, e nisso podem ser inclusos contratos, sendo a questão maior a de saberse eles eram, realmente, o melhor modelo que traria segurança nessas relações. Para ele, o principal pesquisador do assunto, contratos inteligentes são algoritmos de transação computadorizados que executam os termos de contratos. Podemos dizer que um contrato inteligente é um contrato cuja execução é automatizada. Isto é, um código que descreve uma regra de negócio capaz de fazer valer a si mesma sem depender, necessariamente, da interferência de terceiros.

Szabo pensou, sobretudo, no propósito da segurança, na relação disso com relacionamentos que construímos, e como o contrato é a formalização dessas relações, sendo então estes o modelo ideal de segurança nessas relações. Se analisarmos o comportamento de um sistema de segurança digital para cada tipo de protocolo de controle implementado e a evolução desses sistemas ao longo do tempo eles se assemelharam à lógica de contratos.

PODEMOS DIZER QUE UM CONTRATO INTELIGENTE É UM CONTRATO CUJA EXECUÇÃO É AUTOMATIZADA.

ISTO É, UM CÓDIGO QUE DESCREVE UMA REGRA DE NEGÓCIO CAPAZ DE FAZER VALER A SI MESMA SEM DEPENDER, NECESSARIAMENTE, DA INTERFERÊNCIA DE TERCEIROS.

Características de um contrato inteligente

Podemos então delinear os conceitos que possam delimitar o que são contratos inteligentes são:

- **Natureza exclusivamente eletrônica:** Contratos inteligentes não podem existir em qualquer outra forma do contrato (por exemplo, cópia impressa oral ou escrita) a não ser em formato eletrônico.
- **Implementado por software:** se formos analisar o contrato inteligente podemos dizer que ele tem uma representação dupla de sua natureza, a primeira é na lei, pois serve de "documento" que rege as relações contratuais entre as partes, e a segunda é objeto dos direitos de licença (leis de copyright para programas), representando o objeto da atividade intelectual.
- **Assertividade:** linguagem de programação é interpretada por máquina com base na lógica booleana (sistema numérico binário), e não permitem que a interpretação dos termos seja feita com base em critérios subjetivos e no modo de pensar análogo ao humano, que podem levar a ambiguidade.
- **Natureza condicional:** conforme análise dos estudos de Szabo contratos se baseiam em declarações condicionais. A natureza da linguagem de programação tem seu fundamento em declarações condicionais, isso demonstra a harmonia dessa abordagem para as clausulas e condições contratuais.
- **Auto-aplicabilidade:** os contratos são capazes de arrecadar dinheiro, realizar transações, distribuir recursos, emitir e gastar fundos para permitir uma maior capacidade de armazenamento e poder de computação sem a dependência de terceiros.
- **Resistente à adulteração:** Os contratos inteligentes não são focados em um servidor central, mas são distribuídos por vários pontos da rede, de modo que podem ser chamados de descentralizados, por isso resistem à adulteração.

Mas ainda existem questões a serem resolvidas, um contrato inteligente é um contrato com um significado atribuído a ele pelo direito contratual? Alguns pesquisadores acham que sim, pois são uma forma de autoajuda, porque não é necessário recorrer a um tribunal para que a máquina execute o acordo. Essa abordagem, apesar de ter fundamento, parece ser muito simples, não permitindo que o

PRINCIPAIS VANTAGENS DE USO

Redução da dependência de intermediários confiáveis, neutralidade do agente na assinatura de acordos;

Automação na assinatura de acordos, exclui a participação humana nas transações, tudo é feito pelo código de programa prescrito;

Custos de transação menores;

Garantia de um maior grau de segurança: dados no registro descentralizado não podem ser perdidos e atacados cibernéticos;

Precisão: nenhum erro pode ser cometido devido à ausência de formulários preenchidos manualmente.

DESVANTAGENS DE USO

Os usuários que desconfiam porque é uma nova tecnologia e eles ainda não a entendem;

Problemas na mudança dos registros executados, caso você queira mudar de ideia sobre alguma ação, como alugar um apartamento, e isso já estiver no contrato inteligente, pode haver problemas. Situações que devem ser levadas em conta na programação;

Segurança para salvar e manter dados. Só haverá erro caso, tenho existido imprecisão na construção do contrato;

Alguns agentes terceiros não desaparecerão, mas passarão a desempenhar um papel diferente. Advogados experientes certamente serão necessários em TI porque os programadores de contratos inteligentes precisarão consultá-los para fazer novos tipos de contratos.

contrato inteligente passe por uma análise mais profunda dentro da estrutura do direito contratual e definindo certas questões, dignas de serem respondidas.

O contrato inteligente no momento de sua execução passa então a ser extensivo para todas as partes, não sendo mais dependente de intermediários humanos. Após o lançamento de um contato inteligente, o iniciador da transação não precisa mais participar do processo.

Considerações Finais

Apesar de toda as possibilidades em torno de contratos inteligentes é necessário ainda avançarmos com relação as questões em aspectos jurídicos, pois eles ultrapassam a natureza jurídica, pois independem da jurisdição. A criação de framework legal que seja capaz de inserir os contratos inteligentes dentro dele é de fundamental valia para problemas futuros.

Outra questão está relacionada ao custo de execução, por estarem atrelados a sistemas que detém variação de custo de transação, esse tipo de característica não deve ser ignorado, pesquisar e identificar formas de contornar essas mudanças é fundamental para implementação dos contratos.

2.3) Análise SWOT

Tendo apresentado alguns dos principais benefícios e desafios da tecnologia de redes distribuídas como a blockchain e sua evolução, propomos aqui uma forma gráfica de apresentar os aspectos positivos e negativos de sua utilização, de modo a avaliar o seu real potencial e limitações possíveis de serem encontrados em diferentes aplicações.

A análise SWOT, técnica comumente utilizada para mapear e avaliar cenários de negócios, bem como sintetizar investigações científicas, foi a estratégia escolhida para este fim. Dessa forma, permite-se a identificação de prós e contras tanto no ambiente interno da tecnologia (fatores controláveis) como no ambiente externo (fatores incontroláveis), ao expor pontos fortes e fracos, e oportunidades e ameaças para determinado projeto.

No quadro apresentado a seguir, considera-se a blockchain como o objeto principal de análise, independente da evolução da tecnologia desencadeando-se em outros tipos de rede. Naturalmente, o processo de implementação de um projeto que se utiliza de uma tecnologia como essa tende a ser permeado por desafios e oportunidades particulares. Desta forma, a ferramenta proposta deve ser entendida como uma ferramenta estratégica dentro de um contexto de análise inicial para cada diferente processo iniciado.

Conforme o quadro mostra, há certa predominância de pontos fortes associados ao ambiente interno no processo de desenvolvimento e aplicação da blockchain. Isso provavelmente se deve à rápida evolução no número de trabalhos sobre o tema (no setor acadêmico e privado),

FORÇAS	FRAQUEZAS	OPORTUNIDADES	AMEAÇAS
Resiliência	Velocidade da rede	Regulação	Regulação
Descentralização	Taxas	Cooperação em comunidades de desenvolvedores	Ausência de vontade política
Temporalidade	Baixa experiência de uso	Adoção em países	Ataques à rede
Imutabilidade	Mindset da população	Adoção em empresas	Padronização massiva
Rastreabilidade	Escalabilidade	Adoção individual	Privacidade
Privacidade	Privacidade	Sustentabilidade do movimento Open Source	Transparência
Autenticação	Regulação	Erradicação da pobreza	Vigilância e monopólios legais
Transparência	Custos de implementação		Incontrolabilidade de atividades ilícitas
Programabilidade			Incapacidade de Interoperabilidade
Escalabilidade			Acessibilidade
Confiança			

assim como a atuação de comunidades de desenvolvedores dedicados ao aperfeiçoamento da tecnologia, contribuindo para o seu fortalecimento, tornando-a ainda mais promissora e robusta. Do ponto de vista do ambiente externo, ou seja, de fatores que são menos passíveis de serem controláveis num processo de desenvolvimento da tecnologia, percebe-se algum equilíbrio entre o número de ameaças e o de oportunidades.

Tal fato indica, sobremaneira, que a blockchain aparente estar em sua fase embrionária.

3) Aplicações em potencial

Nos tópicos anteriores buscamos expor os potenciais da Blockchain considerando suas principais características. Neste sentido, o quadro SWOT ajuda a construir um cenário geral sobre os aspectos envolvidos em torno dela. Vale aqui, contudo, dar um passo adiante, apresentando algumas das principais aplicações que podem ser pensadas a partir deste tipo de tecnologia. O título aplicações em potencial, é mais para chamar a atenção da importância destas aplicações, já que em todos estes campos já existem projetos em algum nível de desenvolvimento.

3.1) Identidade digital

A questão de identidades digitais tem sido abordada de forma recorrente no Brasil e já aplicada em diversas parte do mundo. Muitos países têm manifestado o interesse principalmente em infraestruturas digitais únicas, casos por exemplo da Estônia e o da Índia.

Apesar de nem todas as iniciativas tenham feito uso de plataformas em redes como a Blockchain, quando se fala em uma **infraestrutura única**, esta tecnologia tem um enorme potencial. No Brasil, em especial, uma infraestrutura que agregasse os diversos documentos que compõem o sistema de registros civis e de identidades em um **documento único e soberano**, significaria, em última instância, criar um banco de dados onde os dados de registro do cidadão ficassem em um mesmo "pedaço de código" imutável e facilmente rastreável. Além de promover uma série de avanços no que tange a eficiência e resiliência desses sistemas, permitiria a criação de uma identidade digital compreensiva possível de ser utilizada na identificação do indivíduo em todas as esferas, reduzindo drasticamente as perdas por burocracia e ineficiência de serviços, entregando, ainda, autonomia para o usuário final.

No caso do Brasil, existem atualmente certificados digitais de custo elevado, num valor médio de R$180,00 e válidos apenas por 1 ano. A blockchain pode apoiar a democratização das identidades digitais de forma rápida e com baixíssimo custo, além de possibilitar que elas sejam soberanas, conceito que está atrelado à capacidade de cada cidadão "fazer" e "representar" sua própria identidade. Vale mencionar o papel que identidades digitais podem ter em relação à inclusão social e no suporte de políticas públicas. A blockchain pode tornar essa questão extremamente mais eficiente e palpável, como foi no caso do *World Food Programme*, que a utilizou para o cadastro de refugiados.

3.2) Sistemas notariais

Dentre as aplicações de blockchain de interesse público, aquelas relacionada aos sistemas notariais é um dos casos de uso mais relevantes, principalmente no que tange ao contexto brasileiro. A razão é que a unificação digital do sistema notarial do país e, logo, seu reflexo direto sobre a questão das identidades, traz enorme potencial para transformá-lo em líder mundial de certificação digital.

Levando em consideração que a maioria dos processos realizados por cartórios se dão através de papéis e carimbos, tornar esse procedimento inteiramente digital é fundamental para aumentar eficiência, reduzir custos e fraudes. Fato é que a tecnologia blockchain em si pode, inclusive, ser interpretada como um tabelião de notas, ao se tratar de um sistema descentralizado e padronizado de registros de propriedade que armazena informações e realiza transações de maneira muito mais rápida, transparente e auditável.

O caráter da temporalidade de cada transação nesse banco de dados distribuído vale ser ressaltado, além do fato dessa informação ter sua integridade assegurada pelo uso de criptografia aplicada. A autenticação é um elemento intrínseco no mecanismo da blockchain e desta forma o reconhecimento de firmas e lavratura de testamentos e procurações públicas se dão de forma prática e segura. A tecnologia pode ainda ser utilizada como uma ferramenta auto-organizacional através dos contratos inteligentes.

3.3) Certificações

São inúmeras a áreas que trabalham com diferentes tipos de emissão e guarda de certificados que poderiam contar com um banco de dados descentralizado, imutável e rastreável para conferir agilidade, eficiência e transparência em suas operações. Escolas, cursos técnicos, cursos de idiomas, universidades e demais instituições de ensino podem digitalizar seus certificados e registrar os identificadores únicos como uma espécie de número de série de cada um deles na blockchain.

Essa prática torna muito mais fácil o combate a fraudes e a validação da autenticidade dos diplomas por parte de empregadores ou outras partes interessadas. Por se tratar de uma abordagem digital para a criação e o controle de certificações, adicionalmente podem ser dispensados outros gastos com segurança, impressão de diplomas, provisão de vias

adicionais dos certificados, entre outros.

Uma outra área de atuação em que trabalhar com certificados digitais poderia trazer benefícios é o da saúde. Nestes casos, indivíduos e empreendimentos podem emitir versões digitais de documentos e registrá-los em uma ockchain, pois isso faz com que seja atribuído a cada uma delas um registro imutável dando conta do dia exato em que foram gerados. Isso permite, por exemplo, que receituários médicos não sejam fraudados e nem reutilizados, além do registro privativo e incorruptível de resultados de exames e demais informações médicas que estarão acessíveis somente ao paciente, ao médico ou ao que for configurado em termos de permissões, já que tudo é inteiramente configurável.

3.4) Rastreamento da cadeia de suprimentos

Uma tecnologia como a blockchain poderia ser aplicada em diversos setores da economia no âmbito de cadeias de suprimentos. Por exemplo, na agricultura a autenticação e possibilidade de acompanhar todo trajeto de um determinado cultivo desde seu plantio até o destino final garante a transparência e benefícios não só para o usuário final, uma vez que teriam certeza quais foram as etapas e proveniência de tal produto, bem como autoridades na fiscalização.

Com relação à indústria, o processo de registrar cada etapa do processo de manufatura em uma blockchain permitiria tornar o trabalho dos profissionais da área muito mais eficiente. Isso porque, com a combinação dos registros de geolocalização e de sensores, é possível saber a exata localidade em que a mercadoria se encontra, possibilitando a liberação automática de espaço dentro do armazém, em proporção de quantidade e no tempo necessário para a informação chegar. Da mesma forma em que um carro que passa em um pedágio e o pagamento é captado através de sensores - famoso sistema Sem Parar -, é possível ter um sistema plugado em um contrato inteligente construído em blockchain que, ao receber a mercadoria, executa automaticamente o pagamento para o fornecedor, sendo o próprio contrato o “indivíduo” pagante. Além de garantir que a legitimidade da governança de parcerias entre multinacionais, retroalimentando o setor.

Qualquer grande negócio, em especial aqueles ligados à alimentação ou logística, cujo trajeto entre a produção e a entrega ao consumidor final passe por múltiplas etapas em que algumas ou a totalidade delas seja de

especial importância pode se beneficiar profundamente. Certificações de produção orgânica, rastreio detalhado de cafés especiais, rastreio de safras do produtor ao consumidor, selos de recebimento e envio para medidas ligadas à segurança da alimentação, rastreamento de entregas com registro infraudável, transparente e em tempo real, dentre outros casos possíveis.

3.5) Propriedade intelectual

De forma análoga ao que ocorre no rastreamento de cadeias de suprimento, no contexto cultural, redes descentralizadas como a blockchain poderiam ser utilizadas para o registro de produções artísticas e intelectuais como livros, músicas, peças, etc. Com isso, autores, editoras, veículos de comunicação entre outras organizações do setor poderiam se beneficiar "guardando" o registro de suas criações em uma base de dados digitalizadas que garantisse a validade daquela informação, assegurando a comprovação de sua autoria. Isso permite uma forma desburocratizada, rápida e barata de comprovar a criação de uma obra com a finalidade de validar não apenas sua existência, mas a sua origem como um importante mecanismo no combate ao plágio e na prevenção de fraudes documentais.

3.6) Auditoria

A tecnologia blockchain pode ser uma importante ferramenta para garantir eficiência e controle de gastos. Especialmente no âmbito público, dados referentes aos gastos públicos podem ser armazenados em uma rede aberta da blockchain de forma a criar um sistema auditável e rastreável. Isso torna possível que qualquer indivíduo monitore, por exemplo, se orçamentos públicos foram devidamente operacionalizados. Ao registrar dados referentes à prestação de serviços numa Blockchain, as instituições públicas podem ser auditadas pela população em tempo real, apoiando também o direcionamento dos gastos públicos de forma mais eficiente e participativa. Além disso, confere segurança à transação já que uma vez registrados, a blockchain assegura a integridade destas informações, de modo que elas não possam ser alteradas para fins de censura, fraude ou corrupção, venham elas do setor público ou privado.

3.7) Compliance e Transparência Política

Por ser à prova de fraudes na prática e conter alto grau de transparên-

cia em relação aos dados que carrega em seus blocos, a blockchain pode se tornar uma forte aliada na acessibilidade das informações referentes aos governos, em seus diferentes níveis. Usos mais inovadores da tecnologia blockchain no setor público podem abrir espaço, por exemplo, para maior participação dos cidadãos no processo político em diferentes esferas. Como uma plataforma digital e de transparência, ela dá apoio à prestação de contas em sistemas políticos e de votação. Ao permitir o registro de assinaturas em uma base digital confiável, imutável e verificável, viabiliza subscrição de projetos de lei de iniciativa popular, rastreabilidade do dinheiro público e criação de propostas online para orçamentos participativo. Essa questão pode ser aplicada a planos plurianuais da lei orçamentária, em salários de políticos e campanhas eleitorais, por exemplo. Já no setor privado, contratos inteligentes podem ser utilizados de forma a garantir que as empresas estão agindo de acordo com a legislação vigente.

3.8) Inovação cívica

A blockchain tem um grande potencial também para promover engajamento político, dar voz a comunidades e facilitar serviços comunitários. A democracia direta tem muito a ser beneficiada pela tecnologia, justamente pelo seu caráter fundamental de ser uma rede descentralizada alimentada por um mecanismo de consenso. Isso pode ser facilmente projetado para garantir participação cidadã em ambos processos de elaboração de políticas públicas, bem como nos processos de tomada de decisão.

Vale lembrar também que as criptomoedas podem ser utilizadas com diversas finalidades. Por exemplo, criando mecanismos de recompensa pelo envolvimento cívico e inovação social. Além disso, ao permitir a transferência de valores de forma transparente, a tecnologia poderia também, em alguma medida, fomentar o bem estar social a partir de plataformas distribuídas para captação de recursos que influenciam ações de altruísmo e filantropismo.

3.9) Economia do compartilhamento

Plataformas da economia do compartilhamento podem ser fortalecidas pela tecnologia de diversas maneiras. Levando em consideração os tradicionais sistemas centralizados, a blockchain tornaria possível redistribuir a capacidade computacional de seus bancos de dados e determinar tarefas auto-executáveis pelos contratos inteligentes. Seria pos-

sível até mesmo a criação de organizações autônomas descentralizadas, nas quais os códigos em vigor permitiria que beneficiários de um dado sistema fossem os que procuram e ofertam bens e serviços.

Vale mencionar também o papel das ICOs, "Initial Coin Offers", como importante mecanismo de captação de recursos coletivo. Esse processo acontece de forma a viabilizar a efetivação de projetos baseados na tokenização de ativos e podem, por exemplo, servir como financiamento de pequenas e médias empresas. Não obstante, a sua regulamentação é uma questão em debate pelas autarquias responsáveis, não havendo um posicionamento uniforme em relação a esses ativos digitais.

3.10) Organizações Descentralizadas

Embora ainda de forma incipiente e bastante tímida, o campo que envolve o surgimento de novas formas de organização social é um dos que apresentam grande potencial para aplicações da tecnologia. Devido às características dos contratos inteligentes e a descentralização como mecanismo principal da blockchain, aplicações podem ser desenvolvidas à medida que a tecnologia se consolide. Garantir que determinadas tarefas e processos industriais, por exemplo, sejam determinadas por um código resiliente e estruturado de acordo com a governança, princípios e valores de uma instituição. Definitivamente, esse caráter vai moldar o futuro das organizações no que tange a eficiência e controle de processos, bem como ganhos econômicos pela redução de comportamento oportunista, entre outros custos de transação. A blockchain e suas aplicações permitem uma estrutura de governança organizacional mais determinística, de tal forma que esforços humanos podem ser utilizados justamente para garantir a legitimidade e adaptar essas estruturas.

3.11) Inclusão financeira

A documentação necessária para passar por processos de inscrição e validação das instituições financeiras, é um grande empecilho na inclusão financeira dos desbancarizados. Em paralelo, a utilização de aparelhos celulares como forma de prover acesso à serviços financeiros têm se mostrado de extrema relevância. O caso do projeto M-PESA do Quênia, que permitiu que 9 entre 10 pessoas naquele país pudessem pagar contas, ter acesso a crédito, realizar transferências de maneira prática e segura é bastante ilustrativo neste sentido.

Inclusão financeira é sem dúvida um elemento chave para redução da pobreza. A tecnologia blockchain pode prover uma base comum de dados, e ainda interoperabilidade entre diferentes sistemas e entre instituições, às quais múltiplas empresas ou órgãos financeiros de uma determinada região possa se conectar. Logo, bastaria um único registro nacional ou similar para incluir de uma só vez milhões de cidadãos no sistema financeiro local. Este é o tipo de processo que facilitaria também as remessas internacionais de valores.

Outro aspecto no escopo de inclusão financeira e atenuação da pobreza é o de moedas complementares, que existem há um longo tempo em paralelo ao sistema monetário convencional, sendo conhecidas como moedas sociais, locais ou comunitárias. O objetivo principal desse mecanismo é utilizar o dinheiro como um acordo de uma comunidade para fins específicos, de forma a assegurar a economia onde é criada. Iniciativas como essa existem em diversas partes do mundo, sendo o Brasil um país chave no debate após 20 anos da criação do Banco Palmas. O Brasil, inclusive, é um caso único uma vez que os grandes propulsores dessas moedas complementares serem os Bancos Comunitários de Desenvolvimento.

Existe também nesse viés, como manifestado pela Rede Brasileira de Bancos Comunitários, o interesse de estudar a viabilidade e utilizar a blockchain. Nesse ponto, ressalta-se o potencial que a blockchain pode contribuir no que tange a escalabilidade dessas moedas, a criação de um aglomerado robusto que congrega diversas dessas iniciativas através de uma mesma plataforma, bem como a potencial troca com criptomoedas globais vigentes. Por outro lado, é fundamental colocar a governança como pivô de forma que as comunidades em si estejam sob controle da tecnologia. Caso contrário, os reais objetivos desses sistemas de moedas complementares, que são notadamente a coesão social e o desenvolvimento socioeconômico local, podem estar ameaçados.

4) Estudos de caso

BNDES Token

O Banco Nacional de Desenvolvimento Econômico e Social (BNDES) realizou sua primeira experiência com Blockchain no início de 2018. Após um longo período em que o banco vinha estudando os possíveis casos de uso, tanto em âmbito nacional quanto internacional, a Iniciativa Blockchain se estabeleceu a partir de dois projetos. O primeiro é baseado em uma rede privada desenvolvida em parceria com o Banco Alemão de Desenvolvimento (KfW), enquanto o segundo está emitindo tokens para os processos de financiamento público do banco usando a rede pública Ethereum.

O BNDES estabeleceu um Memorando de Entendimento com o KfW em fevereiro de 2018, permitindo que usassem e colaborassem no aprimoramento da ferramenta deles baseada em blockchain e chamada de TruBudget. O KfW fornece consultoria e suporte técnico ao BNDES e pretende consolidar suas licenças de software de código aberto. O Fundo Amazônia, uma iniciativa da REDD+ apoiada pelos governos da Noruega e da Alemanha - e administrado pelo BNDES - foi escolhido para ser a prova de conceito em ambiente de testes. Dados reais e informações de processos sobre os desembolsos do Fundo Amazônia serão documentados no TruBudget, uma ferramenta de gerenciamento de workflow. Isso permitirá compartilhar essas informações entre o BNDES e os doadores em tempo real e com altos níveis de confiança. O token do BNDES foi iniciado com uma ideia simples, mas muito impactante. Quando um empréstimo é liberado, ele é feito através de um ativo baseado em um token, de forma que o monitoramento de todas as transações pode sempre ser feito em tempo real, tanto pelos agentes do BNDES quanto pela sociedade civil como um todo. É importante enfatizar que, embora haja algumas desvantagens em qualquer aplicação como essa, o uso da tecnologia blockchain nesse caso garante transparência adicional e benefícios de rastreabilidade total.

Voto Legal

Inovação cívica

Voto Legal é uma plataforma digital que possibilita o financiamento de campanhas eleitorais. Lançado em 2016, é uma plataforma aberta que tem como objetivo promover e viabilizar o financiamento de campa-

nhas políticas por meio da aproximação entre candidatos e seus colaboradores. Dessa forma, a ferramenta ajuda a promover e facilitar a doação de recursos financeiros de pessoas físicas para candidatos políticos.

Além de facilitar a doação direta, a Voto Legal garante transparência dessas operações, bem como fomenta a participação política cidadã. Os financiadores, ou colaboradores, podem, e deveriam, monitorar o comportamento dos candidatos durante o período eleitoral. Entre as principais características da plataforma, ressalta-se o fato de utilizar a tecnologia blockchain para comprovar a autenticidade. Isso é feito por meio da criptomoeda Decred, que viabiliza a o carimbo temporal da Voto Legal.

Mudamos
Inovação cívica, Identidade digital

O Mudamos é um aplicativo que permite a coleta de assinaturas para projetos de lei de iniciativa popular no qual genuinidade da identidade digital de cada assinatura é garantida pela tecnologia blockchain. Só no primeiro ano em que se tornou disponível para iOS e Android, a ferramenta já conta com mais de 600 mil downloads. O App foi desenvolvido pelo Instituto de Tecnologia e Sociedade do Rio e se tornou realidade após vencer o Google Social Impact Challenge em 2016, o que garantiu o financiamento e implementação do projeto.

O aplicativo se baseia no artigo 61, parágrafo 2º, da constituição brasileira de 1988, em que garante que se 1% da população assinarem uma petição de apoio a uma nova lei, esta deverá ser votada e reconhecida pelo Congresso nacional como sendo legítima e popular. O problema é que hoje em dia assinaturas se dão de forma física, através do uso de papel. De tal forma, a falsificação e o complexo monitoramento dessas assinaturas são corriqueiros, o que, atrelado a outros fatores, explicam o fato de jamais um projeto de iniciativa popular ter sido discutido em plenário por meio dessa ferramenta constitucional.

A arquitetura multifatorial do aplicativo garante a sua legitimidade. Trata-se de um mecanismo de autenticação que congrega diversas informações dos usuários, como o CPF, o título de eleitor, o número de telefone, a localização geográfica, a conta no Facebook e o número IMEI, a identidade do dispositivo. Para cada assinatura de projeto de lei um hash criptográfico é gerado, permitindo associar um indivíduo com a ação de forma legítima.

O potencial é enorme no que tange a governança e o engajamento político. O Mudamos permite o surgimento de uma democracia participati-

va, horizontal e transparente.

DAOStack
Inovação cívica

DAOStack é um protocolo que fornece uma gama de ferramentas para implementação de organizações autônomas descentralizadas. A startup baseada em Israel fornece soluções para empresas que pretendem tornar certos processos internos completamente automatizados e inteligentes. De forma sintética, trata-se de uma plataforma que permite que um conjunto informações sejam processadas e distribuídas de acordo com regras previamente definidas de acordo com a finalidade da organização. DAOStack surge como uma proposta de transformar em realidade o que ainda só existe no campo teórico, favorecendo a colaboração em massa a partir da promoção de modelos que incentivam financeiramente a criação e a preservação de sistemas econômicos não-rivais.

Everledger
Rastreamento

Atua no registro e rastreamento de diamante. No projeto, cada diamante tem suas medidas registradas na blockchain, sendo atribuído a ele um número de série correspondente. Uma vez registradas as informações sobre o diamante na blockchain, se consegue realizar todo tracking do diamante, de modo a proteger o consumidor final contra fraudes informacionais sobre o produto. Referido projeto permite transparência em questões de interesse público, tais como as condições de trabalho durante o processo produtivo e as formas de exploração de recursos naturais, além de agregar valor ao serviço provido pela empresa que explorar diamantes registrados em blockchain.

5. Entendo a tecnologia blockchain

Este relatório teve até agora como objetivo principal, discutir os usos que têm sido feitos de uma das principais tecnologias da atualidade, e como suas aplicações podem e devem ser revertidas para o benefício público. No entanto, sabendo que questões técnicas da blockchain ainda representa um campo desconhecido para o público geral, dedicaremos esta parte final do relatório à uma explicação breve sobre alguns conceitos centrais envolvidos na tecnologia.

"Blockchain é um Sistema distribuído"

'Sistemas distribuídos' é um campo da ciência da computação que aborda a questão de diferentes aglomerados de redes de computadores com um objetivo comum. Cada processador tem, no entanto, sua própria memória.

Nas palavras de Tanembaum "um sistema distribuído é um conjunto de computadores independentes entre si que se apresentam aos usuários como um sistema único e coerente". Este conceito precisa estar bem difundido ao se pensar qualquer implementação da tecnologia blockchain.

"Blockchain é uma Distributed Ledger Technology (DLT)"

A tradução literal para ledger é livro-razão, o mecanismo base da contabilidade. Trata-se, simplesmente, de um livro de registros contabilísticos que agrupam seus dados dos por data, histórico e informações de transações realizadas. Isto é, um banco de dados sobre o recebimento, o pagamento e a transferência de ativos, a documentação de débitos e créditos.

"Blockchain usa Criptografia assimétrica"

Esse tipo de recurso tecnológico possibilita que pessoas possam usar ferramentas criptográficas para encriptar e provar/verificar autenticidade de informações trocadas sem a necessidade do compartilhamento de um segredo.

Na blockchain do Bitcoin, por exemplo, o que interessa de fato são as assinaturas digitais produzidas por este tipo de criptografia. Pode-se ao mesmo tempo provar que alguém possui um "segredo" (chave privada) e autenticar uma transação com este "segredo" sem a necessidade de compartilhá-lo, tendo apenas que compartilhar a chave pública. Dessa forma, apenas o detentor da chave privada correta poderá movimentar fundos na rede.

No ecossistema da blockchain existe mais de um método para assinaturas. O principal deles é o Algoritmo de Assinaturas Digitais de Curva Elíptica. Esse tipo de assinatura é o que permite que todos na rede possam comprovar que uma transação foi enviada pelo detentor de uma certa chave privada - que nada mais é que um número gigante de 256 bits obtido, se feito corretamente, de forma criptográfica e aleatória - sendo, assim, essencial para o funcionamento correto da blockchain.

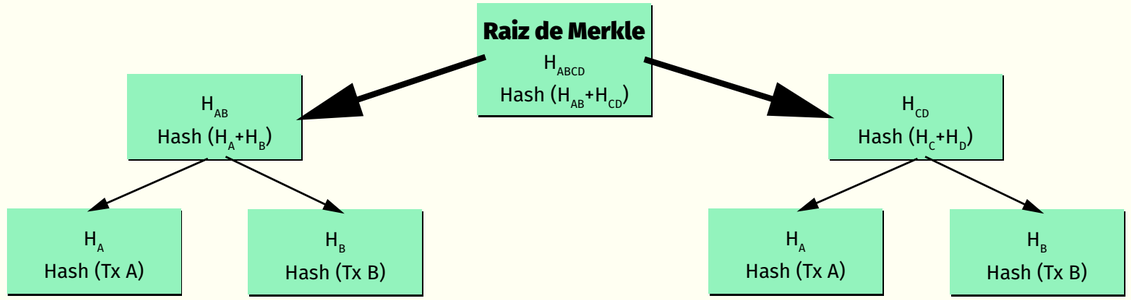
"Na Blockchain, os usuários da rede geram Funções Hash"

Este tipo de função é usado como bloco fundamental em muitas aplicações criptográficas e tem como comportamento básico receber um conjunto de dados de tamanho arbitrário como input e produzir um valor hash de um tamanho fixo como output que chamamos de digest como forma de representação do dado de entrada. Chamamos de funções hash criptográficas, todas as funções hash que atendem alguns requisitos básicos que os tornam quase impossível de ser modificados.

"As transações na Blockchain são como de Árvores de Merkle"

Árvores de Merkle são estruturas de dados utilizadas para criar um resumo de dados com integridade criptograficamente verificável de forma eficiente quando em poder da raiz de Merkle - que vai no cabeçalho de cada bloco - e de um caminho de Merkle.

Para formar a raiz desta árvore binária com as transações, cada transação tem o seu id (o hash da transação) concatenado ao id da transação vizinha na árvore é submetida a uma dupla rodada da função hash SHA-256 sucessivamente até chegar à raiz. A visualização torna simples:

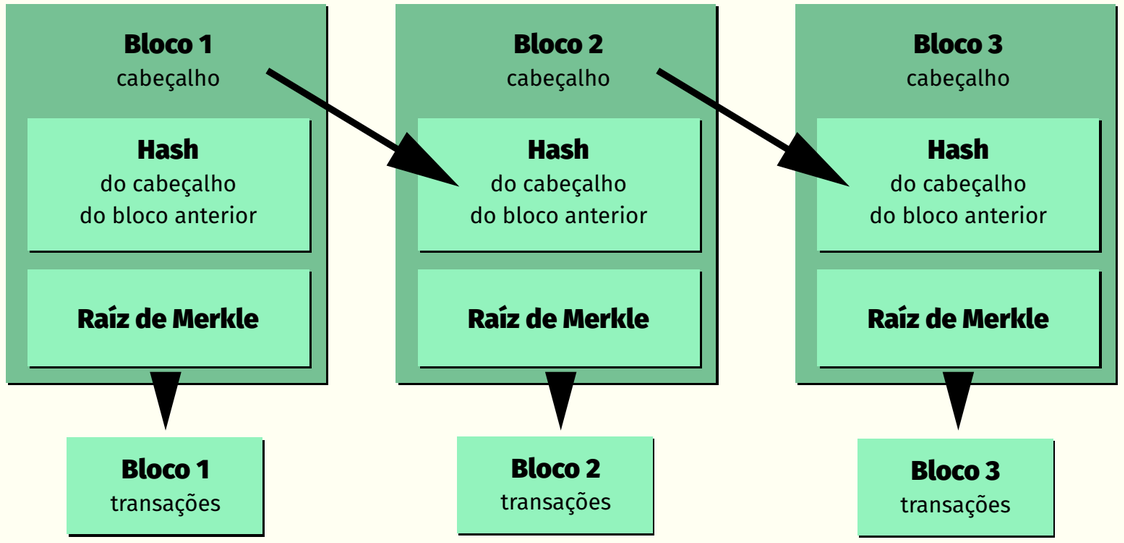


"Blockchain é uma cadeia de blocos"

Cada bloco é uma estrutura de dados que contém as transações a serem incluídas na blockchain por meio do trabalho dos mineradores na rede. De uma forma geral, o bloco é composto por um cabeçalho contendo

metadados sobre o bloco e uma lista de transações, e carregam todas as informações necessárias para servirem como páginas de um livro-razão das transações confirmadas na rede.

Cada bloco tem um identificador único que é criado a partir do hash de seu cabeçalho que serve tanto como identificador único deste objeto na rede quanto como prova de toda informação - incluindo as transações - contida nele. Esta característica faz com que a blockchain possa ser visualizada como uma corrente de blocos com os hashes do bloco anterior como elo criptográfico entre cada bloco:



“A cadeia de blocos da blockchain se forma a partir dos seus algoritmos de consenso”

Existem vários tipos de mecanismos de consenso, que são a principal atribuição nos bancos de dados distribuídos que caracterizam a tecnologia blockchain. Alguns deles são:

- **Proof of Work**

  É o mecanismo de consenso mais recorrente em redes públicas e conhecido como “mineração”. O protocolo emergiu para solucionar questões de segurança cibernética. No contexto da blockchain,trata-se de uma competição para resolução de um problema matemático traduzido em poder computacional. O primeiro minerador a ter sucesso na solução do problema recebe uma recompensa em troca dos esforços que fez.

- **Proof of Stake**

  Este tipo de algoritmo depende da participação de um validador na rede por meio de tokens como uma forma econômica, ou seja, há um conjunto de validadores que se revezam para propor ou votar

um novo bloco da cadeia. Estes votos por sua vez possuem determinados pesos de acordo com o montante do depósito realizado, este montante é a própria prova de participação.

Existem diversas variações de Proof of Stake, entre elas a Delegated Proof of Stake (DPoS), utilizada na blockchain Bitshares; delegated Byzantine Fault Tolerance (dBFT), proposta pela blockchain NEO de forma a evitar competição entre usuários; Proof of Importance (POI), utilizada pela blockchain NEM de forma a promover a atividade econômica; Proof of Stake Velocity (PoST); Proof of Stake Velocity (PoSV), entre outras várias. Neste relatório exploramos o Proof of Storage.

- **Proof of Storage**

  O Proof of Storage foi proposto em 2013 e se baseia na idéia de uma "árvore de blocos". De uma maneira bem didática, em cada "galho" dessa árvore, ou cada nó, ou cada computador ligado à essa árvore existe uma blockchain específica. Isto, basicamente, garante que o usuário apenas enxerga na rede aquilo que lhe convém e não cada transação presente na mesma.

- **Proof of Elapsed Time**

  O mecanismo de consenso Proof of Elapsed Time (PoET) é utilizado em redes permissionadas. Pode-se dizer que o este simula o Proof-of-Work, entretanto de forma adversa à competição para solucionar o desafio matemático, o usuário que tiver o menor tempo de espera para uma dada transação é eleito o validador da mesma. A propósito, este tempo de espera é distribuído de forma aleatória.

- **Practical Byzantine Fault Tolerance**

  Utilizado em blockchains permissionadas, o PBFT também funciona sob a ideia de um único validador conhecido para a criação de um novo um bloco. A ideia de consenso através de um mecanismo de voto, em que um número mínimo de nós na rede confirma o novo bloco.

- **Organizações Autônomas Descentralizadas**

  Organização Autônoma Descentralizada (DAO) é também um novo conceito que advém como a implantação da blockchain e que ainda não recebeu uma definição universalmente reconhecida. Podemos

dizer de forma simples que a DAO nada mais é do que um conjunto de contratos inteligentes de longa duração, em oposição a um contrato inteligente regular, com finalidades específicas e para um fim, uma vez que eles são atingidos. Além disso, alguns autores enaltecem a diferença entre organizações descentralizadas e DAOs, atribuindo ao segundo grupo elementos de inteligência computacional.

Ademais, as DAOs trazem à tona a questão da governança descentralizada, a mudança nos modelos de gestão vigentes. Entendemos como governança como regras, normas e ações de como as pessoas interagem umas com as outras. Ela regula o processo de tomada de decisão entre os atores envolvidos em um problema coletivo que leva à criação de normas. O grau de formalidade depende das regras internas da organização e, externamente, de seus parceiros de negócios.

É importante mencionar que uma DAO é definida como sendo sem fins lucrativos; apesar de você poder ganhar dinheiro em um DAO, a forma de fazer isso é participando de seu ecossistema e não fornecendo investimento à própria DAO. Obviamente, essa distinção é nebulosa, já que todas as DAOs contêm capital interno que pode ser possuído, e o valor desse capital interno pode facilmente subir à medida que a DAO se torna mais poderosa, de modo que uma grande parte das DAOs ao longo prazo será semelhante a uma DAC.

Se pensarmos que contratos são parte de uma parte da organização, e que, todas as organizações são conjunto de contratos complexos. Então podemos definir que as empresas são criadas usando uma série de acordos contratuais, que vão desde contratos que definem as relações com seus funcionários, a contratos de acordos com fornecedores e vendedores, além de obrigações para com seus clientes. Tradicionalmente, essas obrigações contratuais são bastante caras porque precisam ser aplicadas externamente pela sociedade na forma de um sistema legal confiável e através da aplicação legal, tendo a necessidade da existência de todo um ecossistema de execução de contratos.

Com um contrato “inteligente” baseado em blockchain, no entanto, muitos desses custos são grandemente reduzidos ou eliminados. Isso promete tornar as organizações baseadas em blockchain mais eficientes, rentáveis e competitivas em comparação às empresas tradicionais no mercado. Se pensarmos uma organização

com uma estrutura hierárquica gerenciada por um conjunto de pessoas interagindo e controlando a propriedade através regras definidas, uma organização descentralizada envolve um conjunto de pessoas interagindo entre si de acordo com um protocolo especificado em código e imposto no blockchain.

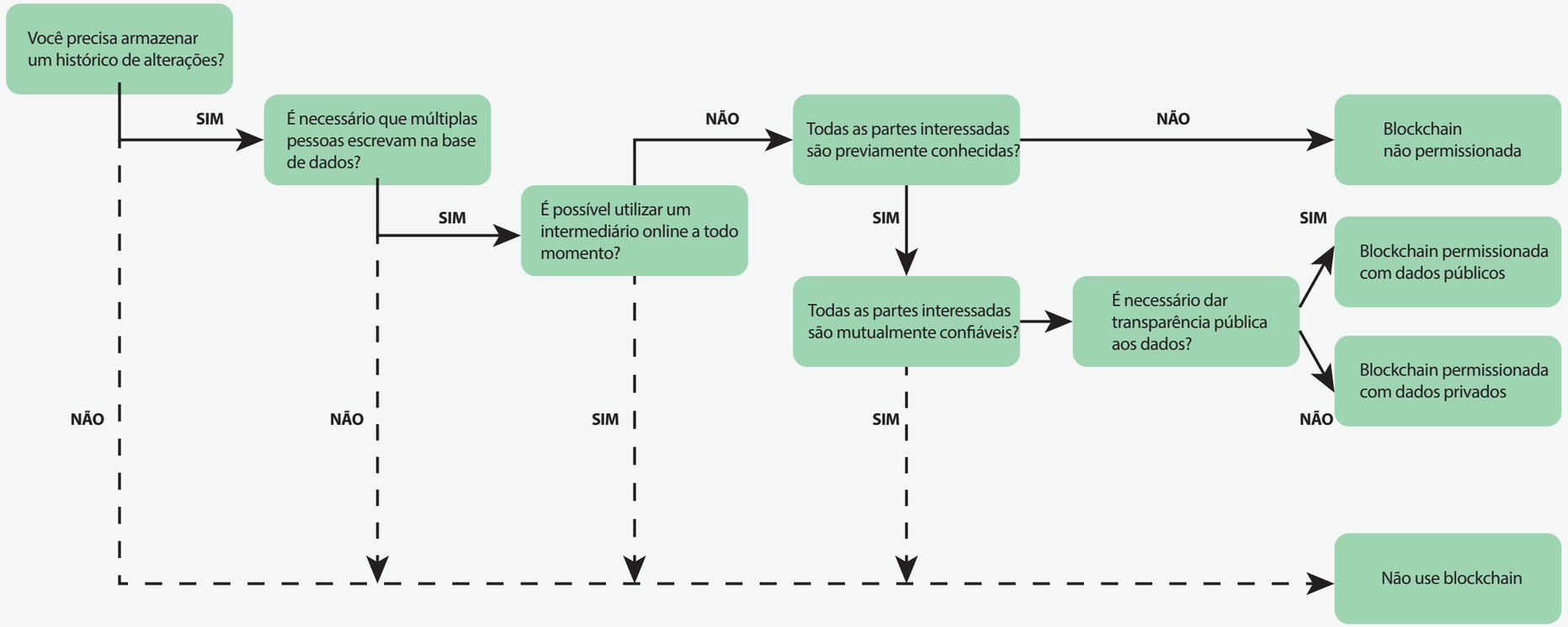
Também se podem usar esses contratos inteligentes para que controlem veículos, equipamentos e prédio. Um enorme potencial no que tange a Internet das Coisas. As DAOs são a mais complexa forma de smart contract e existe de forma autônoma, mas também depende de indivíduos para executar determinadas tarefas que o próprio autômato não pode fazer.

As DACs, corporações autônomas descentralizadas, podem ser definidas como uma subclasse das DAOs, pela definição de Daniel Larimer, as DACs pagam dividendos, quer dizer, há um conceito de ações em uma DAC que podem ser compradas e negociáveis de alguma forma, e essas ações potencialmente dão direito a seus detentores de recibos contínuos com base no sucesso do DAC.

1. FLUXOGRAMA: SUA APLICAÇÃO PRECISA DA BLOCKCHAIN?

Karl Wurst e Arthur Gervais, da ETH Zurich, publicaram um artigo em 2017 apresentando um framework para orientar em qual situação devemos utilizar blockchain. Em síntese, apenas em situação em que não temos uma confiança em terceiros e estes são, também, os responsáveis pela governança de um sistema, devemos utilizar blockchains públicas ou permissionadas. O trabalho analisa criticamente essas componentes e para fins deste relatório foi adaptado para o contexto brasileiro e de interesse público. Além disso, o modelo proposto servirá como a primeira condição a ser atendida no framework de aplicações utilizando a tecnologia blockchain.

Fluxograma: Sua aplicação precisa da blockchain?



2. QUADRO DE PERGUNTAS: DESCOBRINDO OS ELEMENTOS-CHAVE DE SUA APLICAÇÃO BLOCKCHAIN

1	2	3	4	5
Quais partes interessadas ("usuários") precisarão atuar ativamente com a base de dados; isto é, alterá-la e não somente lê-la? Quais partes interessadas deverão ter acesso permanente a uma cópia da base de dados sincronizadas com as demais? Dentre as partes interessadas, quais confiam umas nas outras?	Que eventos devem ser armazenados no histórico de alterações de sua base de dados? Você precisa de informações referentes às alterações lançadas por quais usuários?	A identidade de quais usuários precisa ser nominalmente conhecida? A identidade de quais usuários precisa ser verificada, ainda que de forma pseudônima?	Dentro do conjunto de tecnologias e serviços necessários ao funcionamento de sua aplicação, eventualmente para além do que já compõe a blockchain, quais podem ser providos por intermediários tradicionais?	Quais dados você precisa armazenar para o funcionamento de sua aplicação? Quais deles precisam ser publicamente conhecidos? Quais devem ser permanentemente atualizados como parte inerente à operação da blockchain?

CANVAS DE APLICAÇÕES BLOCKCHAIN
Inspirado diretamente pelo design do Business Model Canvas, metodologia amplamente adotada na construção de soluções inovadoras, o Blockchain App Canvas é voltado a estabelecer um fluxo permanente para construção e validação das hipóteses e fatores indispensáveis a uma aplicação integralmente funcional da tecnologia blockchain.

UTILIZAÇÃO
O preenchimento do Blockchain App Canvas deve ser feito seguindo de acordo com a ordem numérica indicada abaixo, a qual estabelece uma lógica condicional. Ou seja, uma dada dimensão só pode ser definida uma vez preenchida as anteriores. Por exemplo, não há como definir a dimensão de governança (3) de uma aplicação blockchain, sem antes definir a governança do quê (1) e entre quem (2). O centro de uma aplicação blockchain, e logo o centro do canvas, será sempre composto pelo ativo ao qual se pretende atribuir as funcionalidades da tecnologia. À direita do ativo estão as dimensões subjetivas da aplicação e à esquerda as dimensões objetivas.

Canvas de aplicações blockchain

Nome da aplicação

Finalidade da aplicação

7. Requisitos de Governaça

Todos os recursos-chave ao funcionamento do serviço, como e o quanto cada um deve ser protegido

6. Requisitos de Escalabilidade

Todas as atividades-chave ao funcionamento do serviço, bem como a escala que se espera dele.

5. Requisitos de Segurança

Todos os recursos-chave ao funcionamento do serviço, como e o quanto cada um deve ser protegido

1. Ativo

Um ou mais registros em sua blockchain ou contrato inteligente estão buscando operacionalizar. Exemplos variam de diamantes cuja cadeia de produção possui rastreabilidade em blockchain até registros de criação para fins de garantia de propriedade intelectual.

3. Governança

Trata-se dos incentivos econômicos que assegurem o funcionamento da blockchain de modo a corresponder às expectativas necessárias para a aplicação quanto a segurança, escalabilidade e descentralização.

4. Tecnologias adicionais

Tecnologias acessórias para o funcionamento da aplicação (como eventualmente internet das coisas ou inteligência artificial) até recursos imprescindíveis como mecanismos de identidade digital e outros.

2. Partes interessadas

Todos os agentes que farão parte da rede direta ou indiretamente. Compreende tanto as partes que se integram à manutenção da base de dados em si, quanto quem deve ter acesso parcial ou integral aos dados da blockchain.

8. Fatores de custo

Todos os principais custos que têm peso no financeiro e são derivados da construção e/ou da manutenção da aplicação

9. Fatores de receita

Todas as principais economias ou novas receitas consequentes da adoção da aplicação

Instituto de Tecnologia e Sociedade do Rio, através do grupo de pesquisa em aplicações da blockchain para interesse público. Leia o relatório completo em www.itsrio.org