A segunda era da Internet, as infraestruturas de assinaturas digitais e os entes confiáveis
KSI, PKI e Blockchain Permissionado

Por Eduardo Lacerda

Uma nova era da tecnologia, nascida na grande plataforma da informação digital, que ainda irá nos permear ao longo de certo tempo, surge e salta aos ávidos e ansiosos olhos de todos os segmentos. O novo, por vezes, mesmo com hodiernas formas criptográficas para embasamento da segurança nas transações e nos documentos eletrônicos, causa dúvidas, temores, inquietudes de não assentir sobre ser o protagonista do discurso e projetos ou na provável intervenção vertical nos próprios negócios de tema tão inovador, não só para os sistemas transacionais de ativos, mas, também, aos rumos das sociedades e governos.

Blockchain, uma Cadeia de Blocos Eletrônicos Permanentes ou, ampliando, uma Cadeia de Registros Eletrônicos Permanentes, enfim, dê-se o nome que desejar, é um engenhoso procedimento tecnológico para armazenamento de dados que envolve um protocolo de confiança e de consenso sobre uma rede, baseado na comunicação e autenticação de registros distribuídos ponto a ponto, comumente chamado de *Distributed Ledger Technology* (DLT). É construído por ligações criptográficas de blocos no sentido de recrudescer (para alguns garantir) os mecanismos a prova de violação e nesse ponto, inclusive, aos termos inseridos na competência da ilustre comunidade de assinaturas digitais. Não há segredos nos insumos tecnológicos por trás dessa esmerada forma de se registrar de maneira íntegra, com um robusto mecanismo de imutabilidade, um ativo digital, que pode ser conjugada com a legal manifestação de vontade nos documentos e transações eletrônicas.

Enganam-se aqueles que em uma inicial leitura permitam-se concluir que *blockchain* é estritamente uma plataforma anárquica, baseada em um Estado não regulado ou não legislado, embora a gênese procedimental, elegante do ponto de vista técnico, seja tangencialmente ou, com mais rigor, imbricada com a não regulação de transações em moedas virtuais ou criptomoedas, sem a necessidade de uma terceira parte confiável (provavelmente escrita, em 2008, pela enorme crise do *subprime* desencadeada em 2007; quem sabe?). É fato que estas, ainda ao arrepio legislativo e dúvidas dos órgãos reguladores, crescem e tomam espaços em diversos segmentos da sociedade, mas, não obstante, os governos começam a se inserir para de alguma forma "regulá-las" (será possível esta regulação ou basta que se fiscalize a origem – publicação de endereços pelos contribuintes aos órgãos competentes e mitigação de mascaramentos ou misturadores – e destino, ou seja, as transações das criptomoedas?), assim como as instituições que as operam. *Blockchain* é mais do que a plataforma que assegura as transações das criptomoedas mais conhecidas (*bitcoin*, *ethereum classic, dash, zcash, monero, fatcom*, entre outras); *Blockchain* é uma nova estrutura que

integra conceitos que serão tratados *a posteriori*, para garantir a imutabilidade de registros, confidenciais ou não, públicos ou privados, com autenticações e consensos permissionados ou não permissionados, que poderão incidir em mais ou menos regulação e que deve se desenvolver dentro de em um Estado Democrático de Direito. Nesse sentido, o governo do Reino Unido produziu um reluzente relatório chamado *Distributed Ledger Technology: beyond block chain*.

É importante destacar que as iniciativas e projetos, inclusive os já desenvolvidos, dos governos e empresas necessitam de maturação, principalmente no uso dos protocolos (tema que merece um artigo à parte, tratando sobre os códigos *hyperlegder, corda, ethereum – smart contracts, ripple, monero, bitcoin, chain*, entre outros) que, para cada tipo de negócio ou aplicação, podem garantir privacidade, escalabilidade, rastreabilidade, temporalidade e resiliência. Entretanto, vários destes protocolos atualmente conhecidos para criação de uma rede DLT não são condizentes com as premissas que visam a garantir autoria e a segurança na identificação, requisição, geração, emissão e guarda das chaves dos usuários, incluindo autorização e acesso às plataformas transacionais. Possuem seus próprios mecanismos de cifragem/assinatura, não permitindo que se utilizem outros tipos externos aos procedimentos embarcados originalmente nos respectivos códigos. Provavelmente, para as aplicações que se reduzem às transações bilaterais – e é fato que grande parte do segmento da sociedade da informação assim se combina –, esse é um modelo viável, mas quando esta imergir em garantias individuais, direitos e deveres de cidadãos e empresas, não há certezas, ainda, sobre a devida manifestação de vontade, proveniente de claros processos de identificação e uso das assinaturas digitais.

Neste momento, adentra-se à propositura deste texto e de conceitos mais relevantes ao papel das infraestruturas de assinaturas digitais e prestadores de serviço confiáveis nesta nova era. Aqui, portanto, relevar-se-á escriturado um estudo concatenado e resumido sobre dois eixos temáticos: (i) Public Key Infrastructure – PKI e Keyless Signing Infrastructure – KSI e (ii) *blockchain* permissionado, entre tantos outros conceitos que irão se inserir nesta esfera tecnológica de forma definitiva ao arcabouço técnico, legal e normativo das assinaturas digitais e credenciamento de entidades ou "mineradores" de confiança. Tratar-se-á de fundamentos para aplicações voltadas à sociedade (quem sabe a construção de uma rede *blockchain* de governo) e não privadas, embora possam ser utilizadas as mesmas soluções.

O primeiro eixo temático é sobre a infraestrutura de assinatura digital. Sussurra-se sobre *blockchain* terminando com a necessidade de chaves/assinaturas digitais ou algo do gênero de uma plataforma PKI. Não, ainda não, mas muito provavelmente transmutará o segmento. Visto que as plataformas de criptomoedas se utilizam de alguns modelos de geração e guarda de chaves, inclusive para calcular os "endereços" dos pontos, assinar ou dar confidencialidade nas transações, é possível que essa percepção terminativa citada tenha ligação ao que tem sido feito pelo governo

da Estônia e estudado pelo *Digital 5* – D5 (Reino Unido, Coreia do Sul, Israel, Nova Zelândia, Estônia e os Estados Unidos como observador) que é o uso de uma *Keyless Signature Infrastructure* – KSI. Para desfazer possível confusão, seguem as palavras de Ahto Buldas, Andres Kroonmaa e Risto Laanoja, no artigo *Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees*: "*The word keyless does not mean that no cryptographic keys are used during the signature creation. Keys are still necessary for authentication, but the signatures can be reliably verified without assuming continued secrecy of the keys.*".

Em princípio, KSI é uma solução díspar, com outros atributos, e, também, complementar às chamadas PKI. Notem: alternativa e não peremptoriamente substitutiva. "*KSI is intended to protect integrity of an asset while PKI is intended to protect its confidentiality. These are different attibutes.*", do *whitepaper*, *Keyless Signature Infrastructure® (KSITM) Technology - An Introduction to KSI Blockchain Technology and Its Benefits – Guardtime Federal, LLC Proprietary*. KSI é uma infraestrutura, de maneira resumida em algumas palavras, de assinaturas de tempo baseadas em árvores de *hash* (*hash-tree based time-stamp*). Congregam-se, por exemplo, estruturas de sistemas, como os *Gateways*, *Aggregator*, *Core Cluster* associados a um *Calendar Network*, que visam, além de permitir integridade e escalabilidade, com "n" chaves sendo geradas e somente utilizadas em um determinado momento, garantir a temporalidade e autenticidade das assinaturas digitais "sem necessitar" (e, aqui, o entre aspas é uma força de expressão) de um terceiro servidor confiável de tempo, de uma Autoridade Certificadora, LCR/OCSP, entre outros elementos de uma rede PKI. A verdade é que KSI é um grande Prestador de Serviço de Confiança, em que as chaves e assinaturas são geradas por meio de um algoritmo criptográfico, baseadas em um servidor de aplicação, e que, devido aos seus procedimentos e teoria matemática que pode a suportar, garantem temporalidade, escalabilidade, menos danos no caso de um comprometimento das chaves geradas e proteção a possíveis ataques quânticos (outro tema, neste cenário, que merece uma reflexão a parte). Questiona-se, substitui uma plataforma PKI?

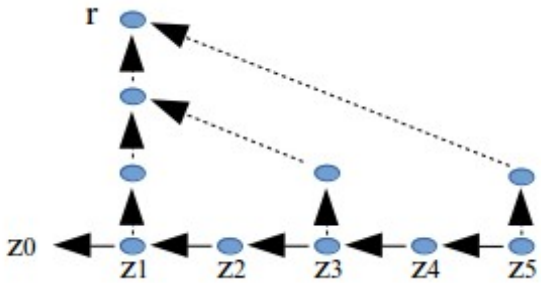
Ao contrário do que Martin Ruubel afirma em sua publicação *Privacy and Integrity on the Internet of Things. If all you have is a PKI hammer…*, a qual versa: "*After the invention of PKI a separate use case was proposed – digital signatures i.e. by signing data with a private key then others can verify the integrity of the data using the signer's public key. There are many problems with this. The first is that the proof of integrity is more of an attestation, i.e., it is true only because the signer says it is.*", a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil – agrega diversas funções de proteção da chave privada, desde requisitos técnicos e procedimentais para a Autoridade Certificadora até a indelével conexão entre esta e a pessoa física (inclusive com a atual prerrogativa do moderno e substancial sistema biométrico da ICP-Brasil, único em permitir que diferentes tecnologias biométricas se integrem, de forma segura, anônima, *online*, distribuída – sem

repositório central – e com a garantia de unicidade do cidadão), e aqui jaz a premissa irrevogável do controle e uso da mesma por parte do seu titular, ou seja, a garantida manifestação de vontade técnica e legal, dada até os limítrofes da MP 2.200/01 e das normas técnicas infralegais. Neste instante, incrementa-se às funções matemáticas de geração de chaves públicas e privadas em RSA, ainda o algoritmo mais usado na infraestrutura brasileira (deixa-se registrado que a cadeia V4 da ICP-Brasil é baseada na suíte ECC-Brainpool r1), os procedimentos de segurança física e lógica desta infraestrutura, ressaltando o rigor dos seus processos de identificação, solicitação, geração, emissão e armazenamento da chave privada. Na hermenêutica de suas normas, além dos parágrafos no seu ditame legal, encontrar-se-á postulados que produzem plena (destaca-se a luz da Teoria do Valor das Provas) validade jurídica às assinaturas digitais feitas nos documentos, ativos, transações e, também, nas autenticações digitais, ou seja, sem a necessidade de outro mecanismo para comprovação de sua autoria, integridade e autenticidade, que em conjunto com uma estrutura confiável de tempo, também regulada pela ICP-Brasil, entregam perenidade a qualquer assinatura digital. Uma parte: ressalta-se a importância da distinção técnica e legal entre as assinaturas digitais e as "autenticações eletrônicas", como "*login* e senha" ou assinatura biométrica – que servem somente para autenticação, com nicho específico de atuação, e não possuem atualmente as características matemáticas, procedimentais, de segurança e, portanto, legais de uma assinatura digital.

À vista do exposto, em que a tecnologia *KSI blockchain* pode ajudar? Em tudo. KSI, por exemplo, pode entregar, por si só, temporalidade às assinaturas digitais da ICP-Brasil. Como Prestadores de Serviço de Confiança, com o devido provimento à manifestação de vontade e autoria do demandante, as duas infraestruturas podem ser usadas mutuamente, visto que: "*In a keyless signature system, the functions of signer identification — and of evidence integrity protection — are separated and delegated to cryptographic tools suitable for those functions. For example, signer identification may still be done by using asymmetric cryptography but the integrity of the signature is protected by using keyless cryptography — the so-called one-way collision-free hash functions, which are public standard transformations that do not involve any secret keys.*", do artigo outrora mencionado. Ainda sim, torna-se necessária a criação de ambiente técnico, procedimental e legal para dar provimento a plena validade jurídica a estas manifestações digitais. Em que pese os debates sejam fundamentalmente voltados ao problema do comprometimento das chaves em uma solução PKI (não ignorando, subscreve-se, as questões da vulnerabilidade das assinaturas a ataques computacionais quânticos, do "complexo" sistema de revogação e da confirmação de autenticidade/integridade afetas a uma PKI, baseada em RSA, por exemplo), para se evitar uma prematura revelação da chave em KSI (vide a seguir, um exemplo de geração de chaves do algoritmo BLT, extraído do artigo citado) são necessários procedimentos extremamente rígidos,

como a manutenção de um dispositivo criptográfico dedicado para gerar as sementes randômicas, forte segurança e comunicação clara entre a aplicação cliente e o servidor KSI, assim como a configuração da estrutura de *Hash-Calendar* (*hardware* apartado, por exemplo), além de um mecanismo de identificação forte do lado cliente e servidor. Enfim, é necessária a criação de um Prestador de Serviço de Confiança para esse tipo de assinatura digital (que pode induzir procedimentos para certificados qualificados e não-qualificados, vide regulamento Europeu).

É fundamental considerar neste instante de avanços massivos em projetos mirando *Internet of Things* – IoT (e mesmo nesses casos, é fundamental endereçar a questão da identificação dos equipamentos), escalabilidade em assinaturas digitais, resistência a ataques quânticos, entre outros, uma discussão encaminhada pelo governo da Estônia e seu provedor de serviço (*Guardtime – BLT based KSI blockchain technology*), sobre a mudança na fundação matemática neste âmbito criptográfico. Nesse invólucro, para ilustrar, mostra-se o algoritmo BLT.

Geração da Chave	O dispositivo do lado cliente gera uma semente aleatória z_s. Para cada unidade de tempo t, a aplicação cliente gera uma senha (*one-time-password)*. As senhas são calculadas usando $z_{i-1} = f(z_i)$, para todo i = s … 1, em que f é a uma função de *hash*, construindo uma cadeia de chaves de *hash*: $z_0 \leftarrow z_1 \leftarrow z_2 \leftarrow \ldots \leftarrow z_s$. O cliente também calcula o *hash* raíz r da *merkle-tree*, conforme ilustrado:  A chave pública será dada por (z_0 e r) e enviada ao servidor de assinatura. O servidor só conhecerá z_{i-1} quando a aplicação cliente a utilizar, mas como o servidor conhece z_0, a senha pode ser verificada pela relação $z_{i-1} = f(z_i)$.
Certificado da Chave Pública	O certificado da chave pública enviado ao servidor de assinatura será: (IDc, z_0, r, t_0, IDs), em que IDc é o identificador do lado cliente, t_0 é a unidade de tempo que o certificado tornou-se válido, IDs é o identificador do servidor de assinatura autorizado. Para a revogação, basta o envio de uma mensagem de revogação ao servidor de assinatura deste certificado.
Assinatura Digital de um Documento	Para assinar uma mensagem m (calcular o *hash* de m), em que $t > t_0$: o cliente calcula x = h(m, z_i) e envia x junto com o IDc. O servidor de assinatura verifica se o certificado do cliente não foi revogado e cria um carimbo de tempo baseado em uma árvore de *hash* S_t = (x, IDc) e envia de volta ao cliente. A assinatura da mensagem m é (IDc, i, z_i, c_i, S_t), em que c_i é a comprovação que z_i está na posição i da cadeia de chaves de *hash*.
Verificação da Assinatura	Para verificar uma assinatura (IDc, i, z_i, c_i, S_t) de uma mensagem m: O identificador do cliente deve ser o mesmo do certificado. Com a chave z_i e a cadeia de *hash* c_i deve ser possível montar r.

	S_t é um carimbo de tempo válido em (h(m, z_i), IDc). O tempo t de S_t satisfaz t = $t_0 + i$. O identificador do servidor de assinatura em S_t e no certificado são os mesmos.

Conclusões do primeiro eixo:

(i) o conteúdo dos parágrafos anteriores, neste pequeno descritivo tecnológico, afetará as estruturas basilares de uma PKI, em consequência, por óbvio, a ICP-Brasil. Quando e em qual monta? Difícil a resposta.

Nota 1: Existem projetos que se utilizam de certificados digitais ICP-Brasil e outros que modelam uma PKI a estruturas *blockchain*, como podemos encontrar nos sítios:
-http://idgnow.com.br/internet/2017/05/25/empresas-ja-podem-usar-blockchain-para-validar-documentos-juridicamente-no-brasil/
-http://www.the-blockchain.com/2017/06/17/wisekey-partners-blockchain-interface-company-riddlecode-develop-innovative-solutions-securing-iot-via-blockchain-technology-crypto-hardware/?ct=t(RSS_EMAIL_CAMPAIGN).
-https://valid.com/pt-br/what-we-do/digital-certification/blockchain/

(ii) torna-se cada vez mais imprescindível uma nova e ampla regulação de um **sistema nacional de assinatura e identificação digital brasileira**, com diversos modelos, híbridos ou segregados, que sejam executados ao compasso de uma lei condizente com o futuro das assinaturas digitais, da identificação digital e dos registros digitais.

O segundo eixo temático é sobre *blockchain* permissionado e a construção de parâmetros para entidades ou "mineradores" confiáveis. A palavra permissionado neste contexto significa uma restrição da rede de quem pode participar do mecanismo de consenso na construção da *blockchain legder*, ou seja, a identificação inequívoca e transparente de quem são os endereços que expressamente tem a autorização para autenticar as transações no bloco e/ou calcular um determinado mecanismo de consenso. Ampliando o entendimento, pode-se inclusive determinar qual ponto possui permissão para criar *smart contracts* (em uma aplicação que demanda multisserviços) ou até mesmo endossá-los, pensando nas entidades regulatórias ou segmentos da sociedade em que os ativos devem por lei serem chancelados por estes e a própria transação em uma rede *blockchain*. Surgem, nesta discussão, questionamentos sobre a volta de bancos de dados centralizados; não chega a ser, mas, sem dúvida, conhecer o respectivo negócio, inclusive o impacto sobre armazenamento dos dados em blocos distribuídos, determinará qual é o tipo de aproximação tecnológica que deve ser feita, inclusive sobre os temas, já citados, como a imprescindibilidade de

autoria, privacidade e escalabilidade.

Nota 2: Destaca-se que diversas notícias e artigos publicados recentemente tentam resolver o problema da identificação em uma rede *blockchain* (atribuições de identidades descentralizadas e hubs na rede); não é simples a garantia de manifestação de vontade digital. A ICP-Brasil endereça esse tema de forma exemplar e cada vez mais torna-se referência mundial no negócio de uma identificação digital e dinâmica – vide a citação na audiência pública da Comissão de Comércio, Ciência e Transporte do Senado Americano, que pode ser encontrada no sítio eletrônico: https://www.commerce.senate.gov/public/_cache/files/9348f11b-49a4-4c47-922e-f5cc98d61b54/469C33D81041FAB151DC6B1E6608A18B.11.08.2017---wilkinson-testimony.pdf

Parte-se da premissa, para os fins de interesse público e garantias individuais, que qualquer abordagem de DLT, *blockchain*, *smart contracts*, entre outros conceitos, deve ser seguida de uma regulação e autoria da manifestação de vontade, em um Estado o qual se configura o poder de forma tripartite (principalmente a uma esfera em que o cidadão possa recorrer), emanado por um direito positivado e com regras democráticas. O primeiro eixo temático discorre tecnicamente sobre essa necessidade. Neste segundo, entrelaçado com a criação de uma legislação coerente, devem-se criar as condições mínimas de segurança e eficiência para que aplicações, principalmente as governamentais, possam, em um primeiro momento (i) atender a contento as leis vigentes e futuras adequações e (ii) suprir a sociedade da informação com serviços seguros e eficientes. É certo que uma rede *blockchain* de governo necessita endereçar os problemas relacionados à identificação dos seus cidadãos e empresas, privacidade das informações e resolver as nuances de escalabilidade (*mining*) dos protocolos que utilizam métodos como *Proof of Work – PoW –* e *Proof of Stake – PoS*. Sobre este último tema, segue o comentário de Vitalik Buterin, fundador da Ethereum, no sítio https://blog.ethereum.org/2017/04/01/ethereum-dev-roundup-q1/: "*After three years of trying to find solutions to the "nothing at stake" and "stake grinding" attacks, we have decided that the problem is too hard, and secure proof of stake is almost certainly unachievable. Instead, we are now planning to transition the Ethereum mainnet to proof of authority in 2018 (...).* No sítio *https://ethereum.stackexchange.com/questions/13968/are-miners-eliminated-in-proof-of-authority/13969,* aponta-se: "*For those not aware of how PoA works, it's a very simplistic protocol, where instead of miners racing to find a solution to a difficult problem, authorized signers can at any time at their own discretion create new blocks.*".

Em uma rede não permissionada, baseada em PoW, todos os nós de forma redundante participam de uma corrida para resolver um quebra-cabeça e autenticar as transações (blocos). O minerador que resolver a regra de consenso é recompensado (enquanto houver recompensa – é

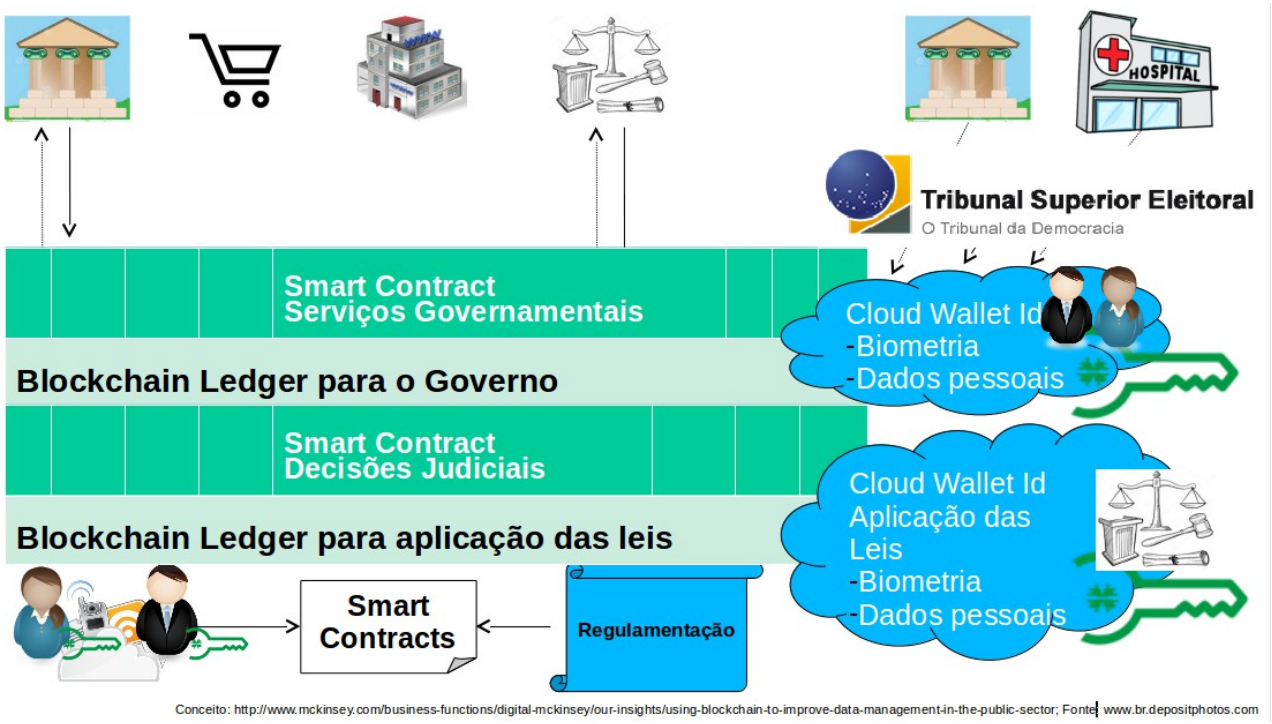
importante entender dos possíveis problemas de aumento das taxas, por exemplo, em uma aplicação *bitcoin* ou taxas advindas de um *smart contract*) e o novo bloco é distribuído para a rede. Como se sabe, um tremendo esforço computacional é consumido por diversos nós, sendo que somente um deles chegará ao resultado esperado e, assim, o esforço (tempo e custo) feito pelos outros entes será desperdiçado. Adotando PoS, recai-se sobre o problema do controle e habilidade de adotar critérios a revelia da rede.

Em sentido contrário a esse cenário, uma rede permissionada, além de não coexistir ao de baque recompensatório diminuto, poderá ter mais eficiência no trato computacional para uma determinada aplicação, visto que podem ser estabelecidos critérios, métodos e estrutura computacional para conhecidos "mineradores", que deverão se debruçar somente na resolução de temas atinentes àquela aplicação. Ademais, atualizações e evoluções nos protocolos de consenso podem ser estabelecidas mais rapidamente, visto que dentro deste consórcio transparente, principalmente para uma diretiva de governo, encaminham-se soluções tempestivas (obediência aos atos regulatórios) para um eventual impasse em detrimento de uma rede não permissionada. Importante ressaltar que conhecer o negócio a qual se pretende construir uma rede permissionada ou não (até mesmo a necessidade de usar uma plataforma *blockchain* DLT) é fundamental. Existem muitas aplicações, como consultas a dados abertos ou cadeias de suprimentos, nas quais existem necessidades de integridade dos registros, mas não sobre escalabilidade, que podem ser redes não permissionadas, adotando-se os critérios possíveis de recompensas e consenso, entretanto, quando a sociedade exigir eficiência e segurança, com a dependência de entrega de um direito ou cobrança de um dever, redes permissionadas adequam-se melhor.

Esta visão torna este consórcio transparente de endereços conhecidos, sejam entidades governamentais – que já possuem tais atribuições – ou do setor privado, em "mineradores" de confiança. A partir de uma determinada aplicação, o governo pode regular e acreditar (e todos os processos advindos de tal ato – divulgação, manutenção e auditoria de endereços, sistemas, métodos e esquemas criptográficos) entes de confiança que tratarão de autenticar os dados ou, se necessário e regulado, as ações cabíveis para o cidadão, empresas e esferas do Estado em uma *legder*, com a segurança regulatória e da própria tecnologia – sem a necessidade de um banco centralizado. São fundamentais, neste cenário, o desenvolvimento ou a possibilidade de uso de códigos abertos, mutáveis e auditáveis. O Instituto Nacional de Tecnologia da Informação (www.iti.gov.br) do Brasil possui em sua missão credenciar, auditar e fiscalizar entes confiáveis. Faz parte da sua natureza liderar este caminho.

Um modelo sugerido por este texto é a criação de uma rede *blockchain* de governo, em que diversos serviços – críticos, abertos, consultivos, contratuais, beneficiários, privados – se estabelecem e são protegidos pelas chaves dos usuários (e seus modelos de uso e assinatura),

permitindo acesso aos dados individuais, aos *smart contracts* (autorizando disparar múltiplos serviços) regulados e chancelados por entes fiscalizatórios ou estabelecidos em lei, registrando-se todos os atos e ativos em uma *legder* governamental. Nesse âmbito, satisfazem-se todos os critérios de autoria e a devida manifestação de vontade, integralidade nos documentos e transações, imutabilidade e perenidade, se for o caso, dos registros e privacidade nos dados e contratos que o ditame legal assim o positivar. Todos os segmentos da sociedade e do governo poderiam usufruir de uma rede como esta sem a necessidade de replicação de infraestruturas e dados, sem bancos de dados centrais, com a segurança institucional dada por uma rede *blockchain* permissionada de entes confiáveis.



Para a ICP-Brasil, embora existam diversas outras possibilidades, mencionadas no primeiro eixo temático (outro exemplo: uma plataforma blockchain para transparência de certificados SSL – cadastro positivo de domínios), aproximam-se dois cenários interessantes e açulantes. A regulação do *Trust Service Provider* – TSP e uma plataforma de *Know Your Costumer* – KYC. Nesta primeira área, foram exaradas normas que positivarão os conceitos de armazenamento de chaves dos usuários finais em HSM, com interoperabilidade devido à utilização do protocolo *Key Management Interoperability Protocol* – KMIP, e sobre o serviço de assinatura digital (portal de assinatura/verificação e armazenamento de documentos eletrônicos – referência o documento eIDAS 910/2014 e diretivas associadas). Estabelecem-se critérios para assinaturas digitais *on-line* em que as chaves estarão nos entes de confiança, podendo armazenar os milhares/milhões de

documentos assinados digitalmente, ou seja, ambiente adequado para estruturar um projeto de *Blockchain Ledger* da ICP-Brasil. Estudos aprofundados de quais plataformas e protocolos usar (ou o desenvolvimento de um com as universidades, empresas e governos) devem ser feitos, mas, certamente, será o empuxo para outros projetos, não só na ICP-Brasil, mas também em todo Estado brasileiro. A segunda, dada à resolução 131 de 2017 do Comitê Gestor da ICP-Brasil, que permite o uso de dados biográficos e biométricos pelas cadeias da ICP-Brasil de um cidadão já cadastrado, é criar uma plataforma de KYC, estudada por diversos segmentos, da ICP-Brasil. Com o uso de um certificado digital, provendo privacidade, segurança a garantias legais, ilustrado na figura acima, os entes credenciados poderiam fazer uso consensual e consumir os dados dos clientes, prevalecendo a irrevogável irretratabilidade de qualquer acesso, perenizado para toda cadeia.

Portanto, a criação de uma rede DLT *blockchain* deve ser planejada e necessária. Estudos e maturação são os cenários que perpassam atualmente todos os governos, empresas, ambientes acadêmicos e cidadãos, a fim de revistar a concepção dos respectivos negócios e em que essa nova plataforma tecnológica será útil. De fato, as aplicações e protocolos evoluem (a largos passos) e aparentemente será um caminho sem retorno, visto o tamanho dos investimentos e dos segmentos da sociedade que constroem modelos para transacionar e registrar ativos, estabelecer serviços e pagamentos, confirmar cadeias de suprimento, criar conceitos de identidade, entre outros nessa nova era da tecnologia. Concomitantemente, as infraestruturas de assinaturas digitais irão se alterar e é necessário seguir o compasso do que tem sido estudado por outros governos. Redes permissionadas para as aplicações públicas que afetam as garantias individuais e os deveres perante uma sociedade parecem ser a vereda a ser trilhada. As oportunidades eclodem-se e não se colidem. Conhecer o negócio – riscos e oportunidades – essa é a chave para o desenvolvimento.

Referências:

Blockchain for Identity Management
por Ori Jacobovitz, Technical Report #16-02, December 2016

Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World
por Don Tapscott & Alex Tapscott

Cryptocurrencies, Blockchains, and Smart Contracts
por Arvind Narayanan and Andrew Miller

Distributed Ledger Technology: beyond block chain
A report by the UK Government Chief Scientific Adviser

Distributed ledger technical research in Central Bank of Brazil – Positioning report
Technical consultants: Aldenio de Vilaca Burgos; Jose Deodoro de Oliveira Filho; Marcus Vinicius Cursino Suares; Rafael Sarres de Almeida
E-mail blockchain@bcb.gov.br
Research Manager: Aristides Andrade Cavalcante Neto
Chief Information Officer: Marcelo Jose Oliveira Yared
Authorized by Deputy Governor: Luiz Edson Feltrim
Central Bank of Brazil

Efficient Implementation of Keyless Signatures with Hash Sequence Authentication
por Ahto Buldas, Risto Laanoja, and Ahto Truu

Efficient Quantum-Immune Keyless Signatures with Identity
por Ahto Buldas, Risto Laanoja, and Ahto Truu

Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees
por Ahto Buldas, Andres Kroonmaa, and Risto Laanoja

Oward a philosophy of blockchain, Introduction
por Melanie Swan and Primavera de Filippi, Guest Editors

Proposta de uma Infraestrutura de Chaves Públicas construída sobre o blockchain do Bitcoin
por Antônio Unias de Lucena, Marco Aurélio Amaral Henriques

Sovrin Provisional Trust Framework - Sovrin Board of Trustees, 28 June 2017, Sovrin.org

State Management for Hash-Based Signatures
por David McGrew, Panos Kampanakis, Scott Fluhrer, Stefan-Lukas Gazdag, Denis Butin, and Johannes Buchmann

The iEx.ec project Blueprint For a Blockchain
based Fully Distributed Cloud Infrastructure, White Paper, March 18th, 2017, Version 2.0, Release Candidate

The Truth About Blockchain - It will take years to transform business, but the journey begins now.
por Marco Iansiti and Karim R. Lakhani

Using the Blockchain of Cryptocurrencies for Timestamping Digital Cultural Heritage
por Bela Gipp, Norman Meuschke, Joeran Beel, Corinna Breiting

Websites:

http://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract/

http://www.the-blockchain.com/2016/04/13/smart-contracts-the-good-the-bad-and-the-lazy/

https://www.law.ox.ac.uk/business-law-blog/blog/2017/04/how-blockchain-technology-will-impact-digital-economy

http://yalejreg.com/nc/the-firm-as-a-nexus-of-smart-contracts-how-blockchain-and-cryptocurrencies-can-transform-the-digital-economy-by-christian-catalini/

https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world

https://www.ethereum.org/

https://www.hyperledger.org/

https://www.r3.com/

https://guardtime.com/

https://www.coindesk.com/5-blockchain-developments-coming-2018/

https://blockchainhub.net/

https://www.evernym.com/

https://bravenewcoin.com

https://www.forbes.com/sites/jasonbloomberg/2017/10/06/can-blockchain-solve-the-quifax-identity-moass-heres-how/#bd05438296a7

https://br.cointelegraph.com/news/blockchain-digital-identification-in-canada-coming-in-2018

https://www.bloomberg.com/news/articles/2017-11-14/forget-iris-scan-canadians-to-use-blockchain-for-digital-ids