UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

LETÍCIA BERLESE MELLO DOURADO

A TECNOLOGIA DE BLOCKCHAIN COMO FACILITADORA DOS SERVIÇOS CARTORÁRIOS BRASILEIROS

PORTO ALEGRE
2020

LETÍCIA BERLESE MELLO DOURADO

A TECNOLOGIA DE BLOCKCHAIN COMO FACILITADORA DOS SERVIÇOS CARTORÁRIOS BRASILEIROS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação da Faculdade de Direito da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção do título de Bacharela em Ciências Jurídicas e Sociais.

Orientador: Prof. Dr. Fabiano Menke

PORTO ALEGRE

2020

LETÍCIA BERLESE MELLO DOURADO

A TECNOLOGIA DE BLOCKCHAIN COMO FACILITADORA DOS SERVIÇOS CARTORÁRIOS BRASILEIROS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação da Faculdade de Direito da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção do título de Bacharela em Ciências Jurídicas e Sociais.

Aprovado em: ___ de _____ de 2020.

BANCA EXAMINADORA:

_____
Prof. Dr. Fabiano Menke (Orientador)
Universidade Federal do Rio Grande do Sul

_____
Prof. Dr. Luis Renato Ferreira da Silva
Universidade Federal do Rio Grande do Sul

_____
Prof. Dr. Guilherme Carneiro Monteiro Nitschke
Universidade Federal do Rio Grande do Sul

AGRADECIMENTOS

São muitas as pessoas que merecem menção nesse pequeno espaço, tanto aquelas que me acompanham desde o início da minha trajetória pessoal, quanto aquelas que foram se somando no caminho. Primeiramente, gostaria de agradecer a minha família, aqui representadas pelos meus pais, Sandra e Rafael, e pelas minhas irmãs, Natália e Caroline, que sempre me apoiaram em todas as decisões que tomei, mesmo que isso representasse diversos finais de semana longe do convívio social familiar. Em especial, gostaria de agradecer por todas as oportunidades que vocês me proporcionaram para que eu pudesse me desenvolver e por todo o suporte durante esse período. Gostaria de agradecer também o meu orientador nesse trabalho de conclusão de curso, Prof. Fabiano Menke, por ter aceitado o convite e ter sempre se demonstrado disponível com as dúvidas que tive ao longo do desenvolvimento do trabalho. É na pessoa dele que eu agradeço todos os mestres que fizeram e continuam fazendo parte da minha formação jurídica. Aos amigos que entenderam todas as desculpas acadêmicas que foram dadas e aos amigos que fizeram parte dos momentos que compuseram essas desculpas – equipe de arbitragem, empresa júnior, Enactus UFRGS, intercâmbio, entre outras iniciativas – fica aqui o meu agradecimento por fazerem parte dessa trajetória. Não poderia faltar o agradecimento aos chefes e colegas de estágio/trabalho por terem compartilhado momentos que agregaram e muito a minha formação como a profissional de direito que eu espero me tornar. A todos que fizeram parte dessa trajetória de alguma forma, fica aqui registrado o meu sentimento de gratidão por todas as experiências que me trouxeram até aqui.

RESUMO

Os serviços cartorários brasileiros possuem uma má fama, por serem considerados mais burocráticos do que o necessário, envolvendo altos custos e grande de tempo de espera para a realização do ato. Apesar de este cenário não refletir completamente a realidade dos cartórios atualmente, ainda há diversas melhorias que podem ser feitas na prestação desses serviços, a fim de facilitar a utilização destes por seus usuários. A tecnologia de *blockchain* pode ser uma aliada nessa busca. Criada em 2008 pelo pseudônimo de Satoshi Nakamoto, a tecnologia pode funcionar como um livro-razão distribuído e descentralizado, em busca de uma maior segurança contra falhas e fraudes no sistema. Assim, o presente trabalho pretende verificar se é possível conferir toda a segurança jurídica provida por cartórios extrajudiciais no Brasil para documentos digitais criados em uma plataforma que se utiliza de *blockchain*. Dessa forma, estuda-se primeiro o funcionamento da tecnologia e a possibilidade de conceder os atributos de validade e eficácia aos documentos digitais e, após, verifica-se iniciativas brasileiras que tentam criar um sistema notarial e registral mais racional, inteligente e eficiente. Por fim, analisa-se se a solução proposta – de utilização de tecnologia de *blockchain* em um sistema cartorário para a criação, armazenamento, registro e transferência de documentos digitais – pode ser implementada.

Palavras-chave: *Blockchain.* Cartório. Registro. Documento Digital.

ABSTRACT

The Brazilian notary system has a bad reputation since it presents an image of a bureaucratic, costly and time-consuming service. Although the described scenario does not reflect the entire system, such services could suffer some significant improvements in order to facilitate their users' experience. Blockchain can be an ally in this journey. Satoshi Nakamoto has presented this technology in 2008 as a distributed and decentralized ledger, characteristics that allow the system to recognize and prohibit flaws and frauds faster than the notary model available today. In this sense, this paper intends to analyze whether documents created in a Blockchain platform can provide the same security as the notary offices while reducing the time and the costs involved. The first part focuses on the operation of the Blockchain and on if this technology can provide the same attributes as the digital signatures to digital documents. The next chapter presents an analysis of Brazilian notary offices' current scenario as well as other tech initiatives. Finally, the proposed solution will be analyzed against the presented background, in order to verify if it can or not be implemented.

Key-words: Blockchain. Notary office. Notary service. Digital document.

LISTA DE ABREVIATURAS

ANOREG	Associação dos Notários e Registradores do Brasil
AR	Autoridade de Registro
CNH	Carteira Nacional de Habilitação
CNJ	Conselho Nacional de Justiça
CNNR/RS	Consolidação Normativa Notarial e Registral do Rio Grande do Sul
CONARQ	Conselho Nacional de Arquivos
DBVN	Nação Descentralizada Sem Fronteiras e Voluntária[1]
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ID	Identidade/Identificação
INPI	Instituto Nacional de Propriedade Intelectual
ITI	Instituto Nacional de Tecnologia da Informação
LGPD	Lei Geral de Proteção de Dados
MP	Medida Provisória
PACDigital	Prova de Autenticidade de Conteúdo Digital
PACWeb	Prova de Autenticidade de Conteúdo Web
QRCode	Código de Resposta Rápida [2]
RG	Registro Geral
SERPRO	Serviço Federal de Gerenciamento de Dados
STJ	Superior Tribunal de Justiça
STN	Secretaria do Tesouro Nacional
TD	Tesouro Direto
UNCITRAL	Comissão das Nações Unidas para o Direito Comercial Internacional[3]

[1] Em inglês: Descentralized Borderless Voluntary Nation (tradução nossa).
[2] Em inglês: Quick Response Code (tradução nossa).
[3] Em inglês: United Nations Commission on International Trade Law (tradução nossa).

SUMÁRIO

1. INTRODUÇÃO

Apesar de o acesso à internet ter crescido exponencialmente desde o início do século, os seus recursos ainda não são tão explorados ou utilizados quanto poderiam ser. Por exemplo, a produção de documentos, especialmente aqueles que possuem um cunho oficial, permanece muito analógica e, muitas vezes, extremamente burocrática.

Considerando-se um contrato, para que ele tenha validade de título executivo no futuro, é necessário que pelo menos quatro pessoas - as partes que estão se obrigando e duas testemunhas - o assinem em três vias físicas. Além disso, caso deseje se obter mais segurança - e, em alguns casos, essa é uma exigência formal - é necessário que esse contrato seja registrado em um cartório, a fim de se obter fé pública no referido documento.

Tal dinâmica envolve uma quantidade relevante de tempo e dinheiro, tornando os negócios engessados. São diversas preocupações e agendamentos até que se tenha um contrato assinado, válido e eficaz. Ocorre que, após todos esses trâmites, ainda permanecem questões importantes, como o lugar onde o documento será armazenado ou a possibilidade de fraude desse arquivo, seja em seu conteúdo ou, até mesmo de uma assinatura.

Por isso, devemos considerar as tecnologias já existentes para criar uma dinâmica mais simples, célere e conectada com a nossa realidade. Vejamos o seguinte exemplo: utilizando-se de um procedimento digital para assinatura de documentos, a parte que redigiu o contrato, assina-o eletronicamente e o encaminha para a outra parte que faz o mesmo. Após assinado o documento, poderiam registrá-lo diretamente em uma plataforma digital do cartório.

Além da diminuição de custos financeiros e tempo gasto com o procedimento, outra vantagem seria a desnecessidade de testemunhas, visto que o Superior Tribunal de Justiça (STJ) já decidiu que, no caso de instrumento particular assinado eletronicamente pelas partes, a assinatura de testemunhas não é mais um requisito, tamanha é a confiança no sistema de criptografia das assinaturas digitais (2019).

Veja-se que um simples exemplo, totalmente imaginável em nossa sociedade atual, evita deslocamentos e gastos desnecessários, possibilitando processos menos burocráticos e demorados.

Um sistema de troca/transferência de informações por meio de uma rede interligada sem qualquer terceiro intermediador, que se demonstra, entretanto, altamente segura e confiável. Em linhas gerais, assim foi definida a tecnologia de Blockchain por Corales *et al* (2019).

A Blockchain é considerada como a próxima grande revolução tecnológica após a *internet*, conforme sustentado por diversos autores como De Fillipi e Wright (2015) e Corales *et al* (2019), uma vez que pode modificar completamente o modo como nos comportamos como sociedade. Isso porque são diversas as funcionalidades trazidas pela Blockchain, muitas delas ainda não exploradas.

Assim, no presente trabalho, pretende-se demonstrar uma dessas aplicações: a possibilidade de armazenar documentos com segurança, conferindo a mesma validade e eficácia perante as partes que as assinaturas digitais e os cartórios. Contudo, apesar de não ser, pode parecer muito arrojada para pessoas que sequer estão acostumadas com a dinâmica já existente.

Por essa razão, o objetivo do presente trabalho é demonstrar, inicialmente, que a solução é verdadeiramente mais segura do que o modelo atualmente utilizado - conferindo os mesmos atributos da assinatura digital, qual sejam, a autenticidade, a integridade e o não repúdio do documento. Em um segundo momento, pretende-se apresentar os casos que já existem no Brasil e se é possível implementar a solução de uma forma ampla e geral em todo o território nacional.

O método de abordagem será o dedutivo, no sentido estudar a funcionalidade da tecnologia de *Blockchain* atualmente para comprovar a sua potencialidade em garantir os atributos que conferem validade a vontade das partes pelas assinaturas digitais e a eficácia a esses documentos, demonstrando que seus usos podem ir muito além das criptomoedas.

Por buscar uma solução tecnológica a um problema jurídico criado por uma norma pouco pensada para a realidade brasileira, realizar-se-á revisão bibliográfica da temática. Relevante destacar que a matéria ainda é incipiente no Brasil, de forma que a literatura analisada, em relação à *blockchain* será, em grande parte, estrangeira.

Necessário apresentar, primeiramente, conceitos básicos da tecnologia de *Blockchain*, a qual ainda é tratada com um tom de mistério e misticismo, principalmente para aqueles que não são da área da informática. Ainda, será necessário estudar a realidade dos cartórios brasileiros e seus atos.

Como método de procedimento se utilizará o comparativo. Para isso, será realizado um estudo de casos, tanto daqueles amplamente utilizados por cartórios no Brasil, quando das inovações que surgiram com fim semelhante ao do presente trabalho. Apresentar essas iniciativas demonstrará, na prática, se a implementação de uma plataforma como a que se pretende seria possível em nossa realidade.

Para tanto, o trabalho foi dividido em dois grandes capítulos. O primeiro capítulo representará o estudo da tecnologia de *blockchain* e seu funcionamento, bem como a possibilidade de garantir os mesmos atributos conferidos pela assinatura digital. No segundo capítulo, realizar-se-á um estudo de casos, comparando a realidade cartorária brasileira e iniciativas que pretendem facilitar a realização de atos notariais e registrais.

2. TECNOLOGIA DE *BLOCKCHAIN*

Nessa primeira parte do estudo, pretende-se explicar a tecnologia de *blockchain* de forma simplificada, para que um leitor leigo no assunto tenha capacidade de entender o seu funcionamento. Não há intenção de apresentar todos os detalhes computacionais por trás da tecnologia, tão somente dar um contexto geral acerca de suas funcionalidades a fim de verificar se serve como solução ao problema apresentado.

Ainda, na segunda parte do capítulo, pretende-se verificar se a tecnologia de *blockchain* pode garantir os atributos de autenticidade, integridade e não-repúdio ao documento nela depositado, com o objetivo de verificar se a solução pode substituir o modelo físico utilizado por cartórios brasileiros atualmente.

Desse modo, poderá se ter uma ideia de como uma tecnologia criada para realizar a transação de moedas pode garantir os atributos de um documento digital, mesmo quando este é transferido a outra pessoa.

2.1. Funcionamento e aplicação do Blockchain

As transações financeiras, iniciadas com o fim das trocas diretas por produtos, sempre tiveram a necessidade de um terceiro que intermediasse a relação, com o intuito de assegurar confiança ao processo.

É possível verificar que a criação dos bancos ocorreu exatamente por este motivo, de forma a possibilitar que comerciantes de cidades diferentes pudessem vender seus produtos e ter a certeza de que aquele pedaço de metal correspondia ao valor da mercadoria. Isso porque havia uma instituição que certificava que aquele metal correspondia ao valor do produto que havia sido comercializado, o que facilitava a troca por outros produtos de maior necessidade ao comerciante.

Em razão disso, surgiram complexos sistemas bancários e monetários, de modo a conferir cada vez mais confiança ao sistema. Sendo assim, a transferência de uma quantidade de dinheiro de uma parte para a outra, por qualquer meio disponível atualmente (transferência bancária, pagamento com cartão de crédito/débito, empréstimo de quantias, entre outros), necessita de um terceiro mediador dessa relação com o objetivo de “fiscalizar” se o valor transferido não foi utilizado em outra operação anterior, trabalho geralmente desempenhado por uma instituição financeira.

Isso ocorre pois vivemos em um sistema de confiança e, para tanto, nos tornamos dependentes de um terceiro intermediador que verifique todas essas transações e garanta que o valor, de fato, possa ser transferido.

Contudo, o custo dessa intermediação torna as transações mais caras em razão da necessidade de remunerar a ação desse terceiro. Esse custo, por sua vez, é aceito pela sociedade, pois se entende que este é o preço a se pagar pela confiança de que o processo de transferência desses valores não sofrerá fraudes.

Ainda assim, esse sistema não é integralmente confiável, pois está sujeito a ataques e fraudes, havendo dificuldades de coibi-los de forma eficaz. Além disso, o preço que se paga por essa mediação em certos tipos de transferência pode tornar a própria transação desinteressante, especialmente quando envolver transferência de valores baixos.

Isso é possível verificar, por exemplo, na quantidade de pessoas que ainda prefere enfrentar longas filas de banco e de caixas lotéricas do que realizar transações bancárias por outros meios mais cômodos, uma vez que estes meios geralmente impõem um custo maior. Aliás, esse exemplo também demonstra como as pessoas ainda não confiam plenamente na internet, especialmente quando se refere a dinheiro.

Por esta razão, muitos ainda pensam que um sistema de transferência de valores sem qualquer intermediação seria impossível, pois seria mais difícil de evitar fraudes, visto que as partes, quando não fiscalizadas, não são confiáveis.

Ocorre que, em 2008, Satoshi Nakamoto, pseudônimo do criador (ou dos criadores)[4] do *Bitcoin*,[5] trouxe, em seu manifesto de somente nove páginas, aquilo que hoje já é considerado como uma das grandes revoluções tecnológicas da atualidade. Nesse modesto artigo, Nakamoto apresenta um meio de transferir ativos sem a necessidade de mediação de um terceiro, ou seja, torna-se desnecessária a participação de uma instituição financeira em transações monetárias.

A *Blockchain*, por sua vez, é a tecnologia utilizada na plataforma em que os *Bitcoins* são trocados. Tal tecnologia é explicada por Tapscott e Tapscott (2016) como um sistema de registro ponto-a-ponto (*peer-to-peer)* para transferir valores – o que

[4] A real identidade de Satoshi Nakamoto permanece desconhecida. Não se sabe, inclusive, se é uma única pessoa, um grupo ou, até mesmo, uma comunidade.
[5] Moeda virtual formada por assinaturas digitais e funções *hash*. Seu valor é determinado livremente pelo mercado, não tendo uma autoridade central que a regule.

não implica necessariamente transação de dinheiro – sem a necessidade de um intermediário confiável para verificar, assegurar e realizar a ação.

Ou seja, conforme definido por Corales *et al* (2019) a transação é realizada diretamente entre as partes, as quais não precisam ter qualquer tipo de relação de confiança, sem o envolvimento de um terceiro para intermediar a relação. As informações ficam gravadas em blocos que são adicionadas ao sistema para fortalecê-lo, formando uma corrente de blocos, característica que dá nome à tecnologia.

Blockchain é a designação genérica dada a um esquema de algoritmos e criptografia que garantem a integridade e rastreabilidade de todas as transações que acontecem na rede sem depender de uma autoridade central, o que permite uma ampla descentralização e distribuição. Kacprzyk *et al* (2020) esclareceu que a tecnologia utilizada hoje é chamada de *Blockchain* 2.0, desenvolvida para comportar as demandas da indústria, sendo a geração da tecnologia que suporta os contratos inteligentes e os protocolos[6] de consentimento.

De forma mais detalhada, a *blockchain* é descrita como um "livro-razão distribuído" por Corales *et al* (2019), por possibilitar o registro de transações compartilhado, descentralizado e aberto, de forma que, se alguém tentar modificar seus dados, sinais de alerta serão enviados aos desenvolvedores do sistema.

O Serviço Federal de Processamento de Dados (2017) fez a ressalva de que a tecnologia, em si, não é um banco de dados, mas ela é utilizada na construção de uma plataforma que pode ser considerada um banco de dados replicado por um grande número de "nós", tendo a descentralização como medida de segurança, sem a necessidade de intermédio de terceiros para criar confiança e consenso.

A *blockchain* é criptografada pois se utiliza da criptografia assimétrica, que envolve chaves públicas e privadas para manter a segurança da rede. Pode ser considerada como pública também, uma vez que todos podem verificar o que reside na rede. Por fim, é distribuída, porque funciona em diversos computadores, chamados de servidores, disponibilizado por voluntários em todo o planeta, de forma que não possui um único centro que possa ser invadido e comprometer a operação da rede.

Assim, é entendida como uma tecnologia de validação inviolável, por ser praticamente impossível modificar as informações ali colocadas. Dessa forma, Singhal

[6] Protocolo, no contexto da telecomunicação, significa um sistema de regras que descrevem como um computador pode se conectar com, participar de e transmitir informação por um sistema ou rede.

et al (2018) considera que toda a entrada nesse registro é permanente. Isso porque qualquer mudança representaria uma nova transação que precisaria ser validada por todos os nós que contribuem com a corrente.

Os nós, capazes de estocar dados de transação e operações que podem validar esses dados, são os servidores que regularmente atualizam-se entre si com os dados presentes na corrente e permitem que pessoas autenticadas se conectem a eles. Quando um nó apresenta mau funcionamento, os desenvolvedores isolam esse servidor e o analisam para determinar o erro e corrigi-lo.

Esse erro geralmente se relaciona com uma falha de transmissão de dados válidos, de forma que o nó transmite informações que não fazem sentido aos demais nós. A vantagem é que, quando um nó precisa ser afastado, essa ação não acarreta em prejuízo a plataformas que precisam ser acessadas em tempo real, uma vez que os demais nós contornam a falha e o usuário pode reconectar-se a qualquer servidor que esteja funcionando, conforme explicado por Norton (2016).

Além disso, todos os nós da corrente possuem uma cópia própria da corrente em si, de forma que o trabalho computacional para modificar uma única transação seria “descomunal” e impraticável, de acordo com a explicação de Singhal *et al* (2018). Desse modo, quanto maior a corrente, especialmente de nós confiáveis, mais difícil é a possibilidade de alteração.

O bloco contém duas partes: a parte de cima, chamada de “cabeça”, que contém o valor *hash* do bloco anterior, impedindo que qualquer transação realizada nele seja modificada. O “conteúdo do corpo” (parte de baixo do bloco), por sua vez, traz a lista validada de transações, suas quantidades, os endereços das partes envolvidas, entre outros detalhes. Por essa razão é que se diz que é possível verificar toda a corrente verificando seu último bloco.

A cada transação da informação, uma chave criptografada é gerada, tornando a transição segura. Para a sua validação, esse código deve passar por uma série de servidores espalhados pelo mundo, os quais validarão a transação através de um processo conhecido como mineração.[7] Isso proporciona a criação de um código criptografado único, inviolável, imutável e resiliente, capaz de promover uma transação segura, rápida e sem intermediários.

[7] A mineração tem como objetivo resolver o valor de um novo algoritmo criado quando uma nova transação é solicitada.

Em decorrência dessa ação, os blocos são compostos por uma cadeia de assinaturas digitais, pois, a cada transferência da informação na corrente, ocorre a aposição de uma assinatura digital no *hash* da transação anterior e da chave pública do próximo proprietário, adicionando essas informações ao final da corrente.

O recebedor pode confirmar as assinaturas apostas a fim de verificar a cadeia de propriedade daquele bloco de informações. Nakamoto (2008) esclareceu que, dessa forma, passamos de sistema de confiança para um sistema de criptografia, que pode assegurar mais fortemente a impossibilidade de fraudes, uma vez que a tecnologia torna computacionalmente impraticável a reversão da transação.

Aliás, passamos de um sistema de confiança puramente em pessoas, e para um sistema em que a confiança é fornecida por criptografia, por meio de um protocolo confiável (*trust protocol*). Isso porque as informações na rede estão abertas e públicas, de forma que os usuários podem verificar o que é verdade e o que não é.

Nakamoto (2008) explica que, para aceitar um bloco que entendem como válido, os nós trabalham para aumentá-lo; já para rejeitar um bloco inválido, os nós apenas se recusam a trabalhar nele. Qualquer regra ou incentivo pode ser realizada por meio do consenso entre as partes envolvidas.

De acordo com Dannen (2017), a cada 10 minutos, em média – caso não ocorra nenhum erro de verificação -, todas as transações conduzidas são verificadas, esclarecidas e armazenadas em um bloco que se liga ao bloco anterior, criando uma corrente. Todo bloco deve se referir ao anterior para que seja válido.

Essa estrutura permanentemente carimba o tempo e armazena as trocas de valores, impedindo que alguém altere o registro. Por exemplo, para que alguém roube um *bitcoin*, é necessário que este usuário refaça todo o histórico da cadeia em plena luz do dia, o que torna quase impossível que isso ocorra.

Em resumo, a formação dessa corrente de blocos de informação possibilita o registro desses dados em diversos servidores e a corrente aumenta sempre que há uma nova transferência do valor. Os servidores, ou nós, são os responsáveis por validar essa operação por consenso e registro, o que torna a criptografia mais segura e dificulta a alteração dos blocos através de um ataque.

Dessa forma, uma vez que a tecnologia é utilizada para a transferência de valores, pode também transferir documentos digitais, pois estes nada mais são do que

um conjunto de *bits*.[8] Assim, segundo Norton (2016) uma vez que o documento original se mantém na cadeia, é possível prevenir a alteração de documentos ao comparar as informações de arquivos duplicados, para verificar se as informações seguem inalteradas.

Por isso, De Fillipi e Wright (2015) mencionaram que qualquer conteúdo ou dado eletrônico ou até propriedade pode ser registrado ou representado de maneira digital em *blockchain*, em forma criptografada, permitindo com que as pessoas consigam realizar a transação dessas informações diretamente e instantaneamente.

Outra curiosidade da *blockchain* é que a tecnologia possui um código aberto (*open source code*), o que possibilita que qualquer pessoa possa baixar o código sem custos e desenvolver suas próprias ferramentas de transações em rede.

Isso não significa, contudo, que todas as plataformas com *blockchain* podem ser replicadas gratuitamente. As ferramentas e plataformas desenvolvidas com base em *blockchain* podem ser fechadas, é o código base da tecnologia em si que é aberto, possibilitando a criação de novas funcionalidades.

A primeira grande dificuldade do sistema de transação por *blockchain* surgiu com a necessidade de verificar que o valor não havia sido transferido anteriormente para outro recebedor (*double spending problem*), porque, para isso, seria necessário ter conhecimento de todas as transações dessa informação realizadas até aquele momento.

E, para conseguir isso sem um terceiro intermediador, Nakamoto (2008) explica que as transações precisariam ser anunciadas de forma públicas, por meio de um sistema em que o recebedor tenha provas de que a maioria dos nós daquela transação concordam que ele foi o primeiro a receber. Ou seja, seria necessário um modelo em que todos os participantes concordassem com a ordem em que receberam a informação, de uma forma coesa contida um único histórico, chamado de mecanismo de consenso por Tapscott e Tapscott (2016).

Para resolver essa questão, a *blockchain* foi desenvolvida para manter os seus registros inalterados com base em carimbos de tempo (*timestamps*) e números *hash* criptográficos, também conhecido simplesmente como *hash*. O *hash* é um algoritmo matemático que resume um bloco de dados (*bits*) em uma sequência fixa de caracteres, tendo em uma saída única para este bloco. Qualquer alteração no bloco

[8] Menor unidade de medida de dados que pode ser transmitida ou armazenada.

original resulta em uma modificação na saída, conforme indica o parecer do Instituto Nacional de Tecnologia da Informação (2019).

O carimbo de tempo, por sua vez, comprova que a informação existia no momento de sua transação. Cada carimbo de tempo inclui o carimbo de tempo do *hash* anterior (ou seja, no bloco da corrente) em questão, de forma que se cria uma corrente em que o carimbo novo reforça o carimbo posto anteriormente. Assim, como explicado por Nakamoto (2008), conforme os blocos novos vão se juntando à corrente, alterar um bloco significa modificar todos os blocos que vieram após.

Isso permite com que os desenvolvedores inspecionem os registros na plataforma para verificar os fatos de qualquer transação ou para detectar tentativas de adulteração do registro. Em razão disso, é possível detectar e isolar, de forma confiável, uma tentativa deliberada de alterar os dados antes que uma fraude ocorra.

Em suma, conforme Santos *et al* (2017b), pode-se elencar as seguintes características da *blockchain*: (i) imutabilidade; (ii) atualidade; (iii) irrefutabilidade; (iv) prevenção contra a duplicação de transações (*double spending*); (v) transparência; (vi) visibilidade pública; (vii) descentralização; (viii) disponibilidade; e (ix) desintermediação.

Santos *et al* (2017b) caracteriza a imutabilidade como a impossibilidade de modificar os blocos e transações já realizadas. A atualidade é a atualização periódica do registro. A irrefutabilidade significa que o autor da transação não pode negá-la, caso todos os nós da rede tenham-na aceito. A prevenção contra a duplicação de transações é a garantia de que não há registro duplo de transação daquele valor.

A transparência e a visibilidade pública se complementam, sendo a primeira a capacidade dos nós da corrente de ver as transações ali registradas, enquanto a segunda é a capacidade destes nós de acessar o registro e verificar a legitimidade das suas informações.

A descentralização decorre do fato de não existir um proprietário centralizando todas as informações de dados e transações do registro. Já a disponibilidade se refere a capacidade da rede de se manter ativa e segura mesmo quando alguns dos nós estão *off-line*, pois os nós que seguem operando continuam decidindo por consenso. Por último, a desintermediação é exatamente a possibilidade de ter o sistema funcionando sem a necessidade de intermediação de terceiros.

Ademais, apesar de a publicidade da transação ser um ponto essencial para garantir a segurança desse método, Nakamoto (2008) esclarece que é possível

manter a privacidade das transações quando se coloca as chaves públicas de modo anônimo. Assim, é possível verificar que alguém está enviando algo a outra pessoa, mas não é possível verificar a identidade das pessoas envolvidas na transação.

Visto que os serviços financeiros requerem um sistema fechado, com permissão para utilizá-lo, os registros em *blockchain* já podem ser feitos de forma privada. Pensando sob a ótica do funcionamento de um cartório, é possível manter os documentos registrados acessíveis apenas àqueles que tenham permissão, de forma a garantir a segurança de armazenamento.

Inclusive, a tecnologia de *blockchain* já vem sendo adotada em plataformas para armazenar informações, uma vez que promove serviços mais rápidos, baratos, seguros e menos riscos de falhas ou fraudes que possam atrapalhar ser funcionamento – por meio da eliminação de um ponto central de armazenamento de informações.

Em que pese ser uma tecnologia criada com um intuito específico - facilitar as transações financeiras, em especial de *Bitcoin* -, hoje em dia a tecnologia de *blockchain* já possui diversas utilidades, sendo possível prever que muitas ainda estão por vir.

Como exemplos importantes ao direito, que vêm sendo amplamente estudados atualmente, temos os *smart contracts* e sistemas de governança, os quais estão sendo implantados em governos do mundo todo, tema este diretamente relacionado com o presente trabalho.

De Fillipi e Wright (2015) dão como exemplo de *smart contract* a possibilidade de um trabalhador ser pago por hora ou por dia, enquanto os valores que devem ser retidos do salário seriam encaminhados diretamente à entidade competente. Dessa forma, seria necessário comprovar que o empregado cumpriu com o requisito estabelecido no contrato – nesse caso, o cumprimento da jornada de trabalho disposto no instrumento -, que ocorreria a liberação imediata do pagamento, sem a necessidade de intermediador nessa relação.

Além da análise da própria tecnologia de *blockchain,* importante atentar-se mais detalhadamente ao funcionamento de outras partes que compõem a rede, a fim de verificar se a solução apontada no presente trabalho é adequada ao contexto brasileiro.

2.1.1. Criptografia assimétrica

A criptografia pode ser definida como o estudo dos sistemas matemáticos que buscam resolver dois problemas de segurança: a privacidade e a autenticação.

Um sistema privado previne a extração de informações por partes não autorizadas por meio de mensagens transmitidas por um canal público, garantindo que o interlocutor está sendo lido apenas pelo recipiente desejado.

Já um sistema de autenticação, segundo Diffie e Hellman (1976), previne a colocação não autorizada de mensagens no canal público, garantindo a legitimidade do interlocutor ao recebedor da mensagem.

A criptografia assimétrica, também conhecida como criptografia de chave pública, tipo de criptografia utilizado pela tecnologia de *blockchain*, veio para assumir o papel anteriormente ocupado pela chamada criptografia simétrica.

Um sistema de criptografia simétrica possui uma única chave que tanto codifica quanto decodifica a mensagem. Em razão disso, quando utilizada para enviar uma mensagem “secreta” ao receptor, necessita que ambas as partes tenham conhecimento da chave privada. Ocorre que, com o tempo, percebeu-se que a decodificação da chave privada era um procedimento relativamente simples, visto que o processo partia de uma sequência lógica, o que tornou o método inseguro.

Para solucionar o problema, Merkle, Diffie e Hellman criaram a criptografia de chaves públicas, também conhecida como criptografia assimétrica. O método consiste na criação de um par de chaves: uma privada, que deve permanecer secreta e com acesso restrito apenas ao seu detentor, e uma chave pública, gerada a partir da chave privada. Essas duas chaves, em conjunto, são utilizadas para validar transações.

Funciona da seguinte forma: o possuidor da chave privada e remetente da mensagem codifica o seu conteúdo e envia ao receptor. Este, com a chave pública, consegue ler a mensagem e verificar sua autoria, mas não consegue modificar seu conteúdo.

Apesar dessa ligação, Needham e Schroeder (1978) afirmam ser praticamente impossível obter a chave privada por meio da chave pública, por ser baseada em problemas matemáticos que não possuem soluções eficientes. Ainda, Merkle (1978) esclarece que o trabalho que alguém teria para descobrir a chave privada é exponencialmente maior do que o trabalho que as partes tiveram para escolher a chave. Por esta razão, quanto maior o trabalho para escolher a chave, mais difícil seria para descobri-la.

Uma das grandes vantagens desse sistema é que a chave pública não precisar de um canal seguro para a sua troca, pois a mensagem não poderá ser decodificada sem a chave privada, que deve se manter secreta.

Importante salientar, apenas, que, no caso de assinatura de documentos digitais por meio de criptografia assimétrica, o que é criptografado é o resumo do documento e não o seu conteúdo em si, uma vez que o processo de criptografia assimétrica é lento. Isso ocorre, conforme consta na Uncitral Model Law (2001), porque a assinatura digital se propõe a autenticar o documento, não o tornar confidencial.

Dessa forma, o destinatário consegue visualizar o conteúdo e quem apôs a assinatura – para verificar a autoria – com a chave pública, mas não consegue modificar seu conteúdo. A mudança de qualquer aspecto do documento, inclusive a mudança da forma do arquivo, implicaria na quebra da assinatura e, consequentemente, a sua invalidade.

Assim, por se basearem no modelo de criptografia assimétrica, as assinaturas digitais são consideradas, atualmente, mais seguras do que as assinaturas apostas em meio físico, de acordo com Menke (2005) e Pinheiro (2016), o que garante segurança à própria tecnologia de *blockchain* ao se utilizar delas.

2.1.2. Assinaturas digitais

A assinatura digital, por seu turno, é uma derivação da criptografia assimétrica. Enquanto o remetente possui uma chave privada, da qual se utiliza para assinar e criptografar o resumo do documento digital, o destinatário possui uma chave pública, para verificar se a autoria do documento condiz com o que o remetente informou. Para isso, um programa de computador irá verificar se a chave pública que o destinatário possui condiz com a chave privada do remetente.

Em caso positivo, o programa apontará que a assinatura é válida. Na prática, essa informação garante a integridade do documento, ou seja, garante que não houve nenhuma modificação desde a aposição da assinatura no arquivo até a sua chegada ao destinatário, e a presunção de origem deste documento.

Tal sistemática é a mesma utilizada pela tecnologia de *blockchain* em todas as transferências de informação. Como explicado anteriormente, a corrente ganha ainda mais força, pois as assinaturas digitais dos transmissores anteriores segue no bloco

e são reforçadas pela assinatura do novo transmissor, o que garante que a informação contida naquela corrente segue sendo a mesma desde o seu início.

Uma questão remanescente, no que diz respeito às assinaturas digitais e *blockchain*, é como será atestado que aquela pessoa é quem diz ser. No Brasil, as assinaturas digitais são realizadas por meio de certificados digitais, os quais são expedidos por autoridades certificadoras reconhecidas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Nesse caso, tem-se um terceiro confiável que irá atestar que aquele certificado pertence àquela pessoa. Atualmente, os certificados digitais possuem diversas formas, com opções inclusive que não são físicas - de maneira que as informações para a autenticação permanecem armazenadas apenas no computador.

Em uma plataforma com tecnologia *blockchain*, a forma de verificação da identidade da assinatura digital não foge desse modelo. É necessário também que alguém ateste a identidade daquela pessoa. Em razão disso, necessário salientar que esta “limitação” não contradiz a celeridade que se busca com a solução apresentada, apenas garante segurança aos atos praticados com certificados digitais.

Como se pode verificar por recentes iniciativas, a própria certificação por autoridades reconhecidas pela ICP-Brasil vem apresentando inovações e acelerando seus processos de verificação de identidade, sem, contudo, deixar de ter um processo confiável. Como esforços interessantes, pode-se destacar três regulamentações do Conselho Gestor da ICP-Brasil, aprovadas em outubro de 2020, conforme reportagem publicada no site do Governo Federal.

Todas as atualizações normativas representam os esforços governamentais em ampliar o acesso da população às assinaturas digitais. A primeira diz respeito à possibilidade de emissão do certificado digital para pessoas jurídicas diretamente através do Balcão Único para Abertura de Empresas.

Este serviço, que tem data de início prevista para dezembro de 2020, pretende viabilizar a abertura de uma empresa em até um dia, de forma virtual. Assim, no mesmo ato de abertura, será emitido também um certificado digital à pessoa jurídica, o que possibilitará a emissão imediata de notas fiscais, por exemplo. Caso a medida seja bem-sucedida, será um marco relevante para a desburocratização da constituição de empresas.

A segunda iniciativa difundiria definitivamente a utilização de assinaturas digitais pelo país. Trata-se a possibilidade da emissão de certificados digitais a

pessoas físicas diretamente pela Carteira de Identidade (RG) e pela Carteira Nacional de Habilitação (CNH). Essa medida pretende:

> [F]omentar a modalidade de emissão de certificados em nuvem. Esta modalidade de certificado digital é mais amigável para o cidadão, ao proporcionar seu uso através do celular. Ademais, objetiva-se viabilizar a mudança do modelo de negócio na comercialização de certificados digitais ICP-Brasil, ao permitir que a cobrança dê-se pelo uso do certificado e não mais pela sua emissão. A projeção é de que o cidadão não tenha custos para a emissão e utilização do certificado em serviços públicos digitais. (GOVERNO FEDERAL, 2020).

Por fim, uma medida que tem sido muito popular durante a pandemia, e foi recentemente regulamentada pela Lei 14.063/2020, é a permissão dada às Autoridades de Registro (ARs) de "realizar suas atribuições de forma não presencial, desde que mantida a equivalência do nível de segurança" (GOVERNO FEDERAL, 2020). Assim, é possível requerer um certificado digital de forma virtual e realizar a prova de identidade por meio de videoconferência, sem a necessidade de deslocamento.

Dessa forma, verificada uma vontade política em difundir a digitização dos procedimentos da vida civil, a tecnologia de *blockchain* pode ser fundamental para o cumprimento deste propósito.[9]

2.2. Desafios de autenticidade, de integridade e de não repúdio

Apesar de ser considerada uma tecnologia revolucionária, a *blockchain* ainda apresenta certo desconhecimento acerca de sua operacionalidade. Para o presente estudo, foi escolhida a análise dos atributos de autenticidade, integridade e não repúdio - conferidos por assinaturas digitais aos documentos digitais assinados com elas -, para verificar se documentos em *blockchain* poderiam garanti-los também.

Caso possa garantir esses atributos, há segurança de que esses documentos não sofreram modificações desde o seu envio pelo remetente. No caso de documentos transferidos pela *blockchain*, pretende-se verificar inclusive se é possível

[9] Necessária esclarecer acerca da diferença entre os procedimentos de digitização e digitalização, que serão discutidos mais amplamente na seção 2.3.1. A digitalização, mais conhecida, consiste no processo de transformar um documento nascido em meio físico para o meio digital, normalmente pela utilização de um escâner ou por foto. A digitização, por sua vez, é o processo de passar procedimentos que comumente são realizados no meio físico para o meio digital, automatizando-os.

que o destinatário consiga verificar que o documento é o mesmo desde a sua criação, mesmo que outras pessoas tenham participado da cadeia de envio.

2.2.1. Autenticidade

A autenticidade é definida pelo Conselho Nacional Arquivístico (CONARQ, 2016) como a qualidade do documento que lhe dá credibilidade, uma vez que estabelece que o documento não possui qualquer tipo de adulteração ou corrupção, permanecendo em sua forma original. A autenticação, por sua vez é uma declaração desta qualidade.

A autenticidade pode ser dividida entre identidade – definida como “o conjunto dos atributos de um documento arquivístico que caracterizam como único e o diferenciam de outros documentos arquivísticos” (CONARQ, 2012, pg. 2) – e integridade.

No caso das assinaturas digitais, a autenticidade decorre da segurança conferida ao sistema de verificação de identidade do usuário para a emissão do certificado digital, atrelada à tecnologia de criptografia assimétrica que impede, a princípio, que outra pessoa tenha acesso à chave privada deste usuário.

Por essa razão, a assinatura digital consegue garantir a autenticidade enquanto outros meios quando aplicados sozinhos, como o sistema usuário/senha por exemplo, não conseguem, de acordo com parecer desenvolvido pela ICP-BRASIL (2019).

Como forma de conferir autenticidade à sua identidade dentro de uma plataforma *blockchain*, recentemente foi noticiado pela Associação dos Notários e Registradores do Brasil (2019), um advogado requereu uma ata notarial, a qual é dotada de fé pública, para comprovar que ele era quem dizia ser dentro da rede. Assim, criou uma forma de atestar a autoria da transferência da informação dentro da plataforma, caso sua identidade fosse contestada em algum momento.

2.2.2. Integridade

A integridade de um documento é conceituada pelo CONARQ (2016) conceituada como a comprovação de que o conteúdo ali exposto não sofreu alterações após a sua criação, em especial corrupções maliciosas e não autorizadas.

A própria tecnologia de Blockchain possui a preocupação com a integridade de seus dados. Sendo um sistema ponto-a-ponto (*peer-to-peer*), temos uma tecnologia que pretende alcançar e manter a integridade da rede e de seus dados, de forma a não necessitar de um intermediário para fazer isso.

Para alcançar tal atributo, segundo Drescher (2017), o sistema em *blockchain* busca assegurar que os dados utilizados e mantidos nele estão completos, sem qualquer contradição ou erro (integridade de dados). O sistema também verifica se o comportamento de seus servidores está conforme o esperado e sem erros lógicos (integridade de comportamento). Por último, o sistema tem a capacidade de restringir o acesso a seus dados e suas funcionalidades apenas a seus usuários.

2.2.3. Não-repúdio

O não-repúdio tem um caráter de confiabilidade, no qual o receptor aceita a autoria do documento pelo emitente porque este é o único que teria acesso à chave privada que gerou a assinatura aposta no documento. Isso ocorre porque, em teoria, a chave privada deveria ser mantida secreta, de forma que apenas o seu titular tenha acesso, o que evitaria fraudes em nome do emitente.

O não-repúdio às assinaturas digitais, quando apostas por meio de certificados digitais emitidos conforme a ICP-Brasil, advém do §1º do artigo 10 da MP 2200-2. Sendo assim, a assinatura digital equipara-se à assinatura manuscrita, tendo os mesmos efeitos que esta, quando o certificado digital "for emitido por uma das autoridades certificadoras credenciadas pelo Instituto Nacional de Tecnologia da Informação" (MENKE, 2005, pg. 141).

Outros meios de comprovação de autoria do documento podem ter este atributo, desde que ambas as partes envolvidas no negócio assim convencionem, conforme previsto no §2º do mesmo artigo. Menke (2005, pg. 145) descreveu essa possibilidade como uma garantia à "autonomia privada e liberdade que os sujeitos possuem para utilizarem o meio mais adequado e proporcional à importância do negócio ou da comunicação encetada".

Menke (2005) ainda esclarece que o não-repúdio possui uma presunção relativa – ou *juris tantum* -, de que o signatário daquele documento é quem diz ser. Dessa maneira, cabe prova em contrário para demonstrar que a pessoa não está vinculada à vontade manifestada naquele documento, podendo o juiz decidir se as provas apresentadas pelo impugnante são suficientes para afastar a presunção de autoria do documento.

2.2.4. Pode a tecnologia de *blockchain* garantir esses atributos?

Em linhas gerais, sim. A tecnologia de *blockchain*, segundo Braga *et al* (2017b) pode garantir tais atributos pelo simples fato de que a cada transação uma nova assinatura digital é aposta, inclusive, garantindo assinaturas apostas anteriormente.

A única dificuldade que pode se mostrar é o atributo do não-repúdio, uma vez que nem sempre a assinatura digital será emitida nos moldes da ICP-Brasil. No entanto, caso a solução seja implementada diretamente por um cartório, a assinatura digital será conferida por alguém que possui fé pública, de modo que o problema mencionado acima pode ser facilmente resolvido.

Outra similaridade de acordo com Tapscott e Tapscott (2016) é a utilização de carimbos de tempo (*timestamps*) para o registro de evidências claras e incontestáveis, de forma que se possa verificar a temporalidade dos registros.

O carimbo de tempo constrói um depósito de segurança digital, tornando-se seguro e viável para o uso em redes globais ao empregar funções *hash* e assinaturas criptografadas digitais. Ademais, a possibilidade de auditar os dados dentro da corrente confere à *blockchain* a habilidade de arquivar dados de forma mais segura do que as bases de dado online existentes hoje em dia.

Além disso, a tecnologia de *blockchain* pode trazer ainda mais vantagens, pois alia os benefícios das assinaturas digitais com outras inovações. Quanto aos atributos em si, eles são garantidos também com funcionalidades próprias.

A corrente, por meio da tecnologia de *blockchain*, pretende proteger a integridade de cada bloco, tanto em referência ao bloco anterior, quanto ao bloco seguinte, e também busca manter a integridade do sistema como um todo. Isso acontece pela capacidade do bloco em manter todas as informações dos blocos anteriormente colocados na corrente. Assim, torna-se praticamente impossível que a corrente seja modificada e, consequentemente, a alteração do documento colocado na plataforma.

A identificação do documento surge no momento que ele é registrado em *blockchain*, por meio de um algoritmo que verifica todo o seu conteúdo. Caso o sistema desconfie que houve alguma alteração no documento, é preciso somente que ele seja verificado novamente pelo algoritmo, comparando com uma outra versão do documento.

Esse processo não permite determinar com certeza qual foi a modificação ou alteração que ocorreu no documento, mas, conforme esclarecido por Haber e

Stornetta (1991) consegue verificar pelo menos que o documento não condiz com a outra versão, ao detectar que algum *bit* foi alterado.

Ainda, a fim de evitar que alguns usuários permaneçam de forma centralizada com o carimbo de tempo, a tecnologia funciona com uma “confiança distribuída”, que nada mais é do que a distribuição simultânea de versões recentes da mesma informação, dado ou documento por um número de computadores individuais ou nós que não conhecem um ao outro, para fornecer uma atualização constante da corrente, segundo Casey e Vigna (2018).

No entanto, Herian (2019) alerta que dois problemas ainda subsistem em relação à *blockchain*: (i) o carimbo de tempo reflete apenas um dos lados dos dados, ou seja, só é possível verificar quando o dado é colocado na rede, mas não quando a informação foi criada, para objetivamente verificar a sua temporalidade; (ii) em razão da dificuldade em se modificar ou excluir a informação, a forma como esta foi colocada na rede pode se tornar “perpétua”, no sentido de que o trabalho para retirá-la da rede ou corrigi-la é muito grande.

Apesar de serem problemas que devem ser levados em consideração, para a solução que se busca no presente trabalho, tais questões podem ser contornadas. Isso porque, considerando um sistema de *blockchain* para os serviços notariais, temos que o documento terá fé pública, no momento que for aceito pelo cartório como verdadeiro.

Acerca da modificação do documento, pensemos em uma matrícula de um imóvel, por exemplo, a qual precisa ser modificada a cada vez que o bem é transferido. Neste caso, uma nova informação teria de ser colocada na rede, sem modificar a anterior, pois tal seria impossível.

Assim, ficaria registrado na rede que houve uma alteração de titularidade e o documento mais recente deve ser considerado para verificar a situação atual do imóvel. Assim como já ocorre atualmente nos cartórios, a solução seria apenas manter um banco de dados atualizados, a fim de ser ter organizado a matrícula válida para aquele documento.

Ainda, quanto à autenticidade do documento em *blockchain*, cumpre realizar alguns comentários. A identificação do usuário na rede, a princípio, não requer qualquer tipo de informação que comprove que o usuário é quem diz ser, o que poderia dificultar a verificação de autoria do documento.

Entretanto, essa falha é facilmente contornável, visto que muitas das iniciativas que serão analisadas no capítulo seguinte realizam um processo de identificação do usuário semelhante ao feito para a emissão de um certificado digital. Dessa forma, para poder utilizar a plataforma, no modelo pensado para uma solução em cartório, o usuário necessariamente precisaria apresentar credenciais para demonstrar ser quem diz ser, o que confere segurança ao documento assinado por ele.

A presença do carimbo de tempo também permite garantir que o documento existe daquele jeito desde que foi registrado na plataforma, garantindo, assim, a autenticidade do documento que ali se encontra. Dessa forma, se o documento foi aceito por todas as partes envolvidas naquele documento, entende-se que ele adquiriu todos os atributos para que tenha validade e eficácia, conforme artigo publicado pela plataforma OriginalMy (2018).

3. A TECNOLOGIA DE BLOCKCHAIN APLICADA AO SERVIÇO NOTARIAL BRASILEIRO

A análise realizada no capítulo anterior demonstra que a tecnologia de *blockchain* consegue garantir os atributos de autenticidade e de integridade de um documento nela armazenado por suas próprias características. Tendo em vista a MP 2200-2, o não-repúdio pode se tornar um atributo dos documentos gerados na rede caso seja assinado por um certificado digital emitido em ICP-Brasil (art. 10, §1º).

Caso o sistema não forneça uma infraestrutura baseada na ICP-Brasil, o não-repúdio ao documento depende do acordo realizado entre as partes ou aceitação pela parte a quem for oposto o documento (art. 10, §2º). Nesse caso, as partes poderiam simplesmente acordar que um ato ou diversos atos de uma negociação se desenvolverão por meio da *blockchain*, tornando-os oponíveis a ambos, sempre com a ressalva de que é importante ter provas deste acordo, visto que uma das partes pode impugná-lo posteriormente.

Em razão dessa conclusão, necessário verificar a solução proposta. Propõe-se utilizar a tecnologia de *blockchain* para criar uma plataforma de registro e armazenamento de documentos segura, que funcione nos mesmos moldes de um cartório. Assim, pretende-se verificar se a solução poderia conceder fé pública ao documento, garantindo a não oponibilidade deste perante terceiros.

Importante ressaltar que é possível que, em redes mais complexas, como a que se propõe no presente trabalho, apenas pessoas autorizadas tenham acesso e possam criar novos dados ou acessar as informações já existentes. Dessa forma, os usuários são organizados em grupos dependendo das permissões que possuem para acessar a rede.

Isso é possível porque as redes de *blockchain* podem diferenciar-se em redes públicas (não-permissionadas) e privadas (permissionadas). A primeira possui regras próprias, independente de aspectos legais ou regulatórios para o seu funcionamento.

Braga *et al* (2017a) esclarece que os validadores das transações são anônimos e a entrada para participar da rede de mineradores é livre. Já as redes privadas possuem regulamentação legal e os participantes são pré-selecionados, sendo as aplicações restritas a corporações fechadas.

Para tanto, uma vez que o trabalho se propõe a verificar o caráter jurídico da aplicação de *blockchain* a documentos digitais, e não o seu desenvolvimento

tecnológico, a segunda parte foca na análise de casos já existentes no país e como se essas iniciativas estão sendo aceitas.

A utilização de *blockchain* em serviços públicos não é nenhuma novidade. Como mencionado anteriormente, as aplicações de *blockchain* ainda não são completamente conhecidas e muito tem-se estudado para encontrar todos os potenciais dessa tecnologia. No entanto, há certo esforço por parte de diversos países, os quais estão desenvolvendo sistemas de governança completamente digitais, integrando diversos setores da sociedade por meio da tecnologia.

Um dos casos mais curiosos é o da Estônia. O país europeu se auto intitula como o primeiro país completamente digital do mundo. E os números dão suporte à afirmação, uma vez que 98% da população possui uma Carteira de Identidade digital, que permite a assinatura digital de documentos apenas com esta identificação, entre outras soluções digitais aos seus cidadãos.

Além de ser reconhecido pelo número de *startups* que vem atraindo nos últimos anos, o governo vem investindo em iniciativas na tentativa de desburocratizar a relação entre seus cidadãos. Esse esforço também pretende criar interesse de investimento no país, de forma a atrair empreendedores digitais.

Uma das iniciativas mais inovadoras é a e-Residency[10]. Com essa plataforma, qualquer pessoa no mundo pode requerer a abertura de uma empresa na Estônia, sem a necessidade de presença física. O *site* oficial da plataforma descreve o serviço como “uma identidade digital e um *status* que possibilita o acesso aos serviços digitais do país e um ambiente transparente para os negócios, lançado pelo governo” (ESTÔNIA, 2014).

Dessa forma, o país chama a atenção daqueles que querem abrir uma empresa dentro da União Europeia com o mínimo de burocracia possível. Para tanto, a governo desenvolveu um processo simples, com uma plataforma de fácil manuseio e com um sistema de envio de documentos simplificado.

No entanto, não é necessário ir a outro país para verificar esforços nesse sentido. Em 2017, o Serviço Federal de Gerenciamento de Dados (Serpro) já aventava a possibilidade de utilização da tecnologia de *blockchain* para a desburocratização dos serviços públicos no Brasil.

[10] Disponível em: https://e-resident.gov.ee/. Acesso em: 12 de agosto de 2020.

Em uma análise para a utilização da tecnologia no serviço Tesouro Direto (TD) da Secretaria do Tesouro Nacional (STN), foram elencadas funcionalidades de plataformas com a utilização de *blockchain*, que vão além de automatizar o processo e aumentar sua segurança. A tecnologia também aumenta a capacidade de análise de dados e de resposta, o que, em si, agiliza o processo.

A solução pretendia que o cidadão pudesse investir em títulos públicos mesmo sem conta bancária, diretamente do seu celular. Bases do governo seriam utilizadas para autenticar e conferir a reputação do investidor. Em análise à página oficial no TD, no entanto, mostra que o cidadão ainda precisa abrir uma conta em uma instituição financeira autorizada, o que leva a crer que a iniciativa ainda não foi implementada.

A falha na implementação de uma plataforma que parecia promissora, entretanto não é um sinal necessariamente ruim. O fato de o governo brasileiro ter investido em pesquisas sobre a implementação da tecnologia em um serviço público demonstra a sua abertura para aceitar iniciativas que estão em desenvolvimento ou até mesmo, que já estejam funcionando. Por isso é que se faz necessário analisar as inovações tanto do setor público, quanto do privado, a fim de verificar uma implementação da *blockchain* em larga escala nos serviços cartorários.

Antes de adentrar na realidade dos cartórios no Brasil, necessária fazer uma distinção entre os serviços notariais e registrais, visto que ambos são oferecidos por cartórios extrajudiciais, a depender de sua competência.

Os serviços notariais são aqueles prestados por um notário, também denominado de tabelião, e suas competências estão descritas na Lei 8.935/1994, entre os artigos 6º e 11:

> Art. 6º Aos notários compete:
> I - formalizar juridicamente a vontade das partes;
> II - intervir nos atos e negócios jurídicos a que as partes devam ou queiram dar forma legal ou autenticidade, autorizando a redação ou redigindo os instrumentos adequados, conservando os originais e expedindo cópias fidedignas de seu conteúdo;
> III - autenticar fatos.
> Art. 7º Aos tabeliães de notas compete com exclusividade:
> I - lavrar escrituras e procurações, públicas;
> II - lavrar testamentos públicos e aprovar os cerrados;
> III - lavrar atas notariais;
> IV - reconhecer firmas;

> V - autenticar cópias.
> Parágrafo único. É facultado aos tabeliães de notas realizar todas as gestões e diligências necessárias ou convenientes ao preparo dos atos notariais, requerendo o que couber, sem ônus maiores que os emolumentos devidos pelo ato.
> Art. 8º É livre a escolha do tabelião de notas, qualquer que seja o domicílio das partes ou o lugar de situação dos bens objeto do ato ou negócio.
> Art. 9º O tabelião de notas não poderá praticar atos de seu ofício fora do Município para o qual recebeu delegação.
> Art. 10. Aos tabeliães e oficiais de registro de contratos marítimos compete:
> I - lavrar os atos, contratos e instrumentos relativos a transações de embarcações a que as partes devam ou queiram dar forma legal de escritura pública;
> II - registrar os documentos da mesma natureza;
> III - reconhecer firmas em documentos destinados a fins de direito marítimo;
> IV - expedir traslados e certidões.
> Art. 11. Aos tabeliães de protesto de título compete privativamente:
> I - protocolar de imediato os documentos de dívida, para prova do descumprimento da obrigação;
> II - intimar os devedores dos títulos para aceitá-los, devolvê-los ou pagá-los, sob pena de protesto;
> III - receber o pagamento dos títulos protocolizados, dando quitação;
> IV - lavrar o protesto, registrando o ato em livro próprio, em microfilme ou sob outra forma de documentação;
> V - acatar o pedido de desistência do protesto formulado pelo apresentante;
> VI - averbar:
> a) o cancelamento do protesto;
> b) as alterações necessárias para atualização dos registros efetuados;
> VII - expedir certidões de atos e documentos que constem de seus registros e papéis.
> Parágrafo único. Havendo mais de um tabelião de protestos na mesma localidade, será obrigatória a prévia distribuição dos títulos.

Com base na descrição de sua competência, é possível depreender que os atos como a autenticação de firmas, a redação e autenticação de procurações, testamentos e inventários são exemplos de atribuição de um notário.

Enquanto isso, as atribuições de um oficial de registro, contidas nos artigos 12 e 13[11] da Lei dos Cartórios (Lei 8.935/1994), concede a estes funcionários públicos a função de registrar documentos atinentes a imóveis (transferência de propriedade, entre outros) e registro civil (certidão de casamento, nascimento, óbito, adoção, entre outros), por exemplo.

O Brasil possui, atualmente, 13.340 serventias extrajudiciais cadastradas e ativas, segundo dados atualizados do 1º semestre de 2020, sendo 770 serventias no Rio Grande do Sul.[12] Tendo em vista o contexto de pandemia, a Corregedoria Nacional de Justiça (CNJ) publicou o Provimento 100/2020, regulamentando a realização de atos notariais por videoconferência e assinatura digital.

Este provimento instituiu a utilização da plataforma e-notariado, que possui os seguintes objetivos elencados no artigo 7º da regulamentação:

> I - interligar os notários, permitindo a prática de atos notariais eletrônicos, o intercâmbio de documentos e o tráfego de informações e dados;
> II - aprimorar tecnologias e processos para viabilizar o serviço notarial em meio eletrônico;
> III - implantar, em âmbito nacional, um sistema padronizado de elaboração de atos notariais eletrônicos, possibilitando a solicitação de atos, certidões e a realização de convênios com interessados; e
> IV - implantar a Matrícula Notarial Eletrônica - MNE. (CNJ, 2020)

Apesar de ainda não ser o ideal, visto que muitos dos atos ainda necessitam a designação de horário com um notário, a possibilidade de realizar tal ato de casa já representa um grande avanço no sentido de desburocratizar os serviços notariais. Em relação às iniciativas que tentam implementar soluções digitais no país, temos, por

---

[11] Art. 12. Aos oficiais de registro de imóveis, de títulos e documentos e civis das pessoas jurídicas, civis das pessoas naturais e de interdições e tutelas compete a prática dos atos relacionados na legislação pertinente aos registros públicos, de que são incumbidos, independentemente de prévia distribuição, mas sujeitos os oficiais de registro de imóveis e civis das pessoas naturais às normas que definirem as circunscrições geográficas.
Art. 13. Aos oficiais de registro de distribuição compete privativamente:
I - quando previamente exigida, proceder à distribuição eqüitativa pelos serviços da mesma natureza, registrando os atos praticados; em caso contrário, registrar as comunicações recebidas dos órgãos e serviços competentes;
II - efetuar as averbações e os cancelamentos de sua competência;
III - expedir certidões de atos e documentos que constem de seus registros e papéis.

[12] Dados do CNJ. Disponível em: https://www.cnj.jus.br/corregedoria/justica_aberta/. Acesso em: 12 de agosto de 2020.

exemplo, os cartórios digitais. Em Porto Alegre, especificamente, há dois tabelionatos que já operam de forma remota e com toda a segurança que a legislação exige.

No que diz respeito a iniciativas com a utilização específica de *blockchain*, temos um setor privado, dominado por *startups*, algumas utilizando soluções apenas de autenticação do documento, outras desenvolvendo convênios com cartórios locais a fim de ofertar a tecnologia necessária para a transação.

Um dos grandes limitadores dessas iniciativas, no entanto, é a desconfiança das pessoas em serviços prestados online, uma vez que a assinatura digital, apesar de ser mais segura que um selo ou um carimbo físico, é invisível, o que faz com que parte da população não confie em documentos eletrônicos.

Tal crença, em realidade, não se sustenta, uma vez que um documento eletrônico, produzido de forma digital, e ainda por cima assinado por um notário ou oficial de registro, é muito mais seguro do que um documento físico.

Dessa forma, passa-se nessa parte do estudo a analisar casos concretos, que já estão em funcionamento no país, a fim de verificar a sua efetividade no que se propõem, a sua escalabilidade e a verificação de melhorias necessárias no sistema para que se alcance a solução proposta.

3.1. Casos existentes

3.1.1. Cartórios digitais

A imagem que se tem de cartórios extrajudiciais e de serviços notariais em geral no Brasil é a de uma atividade burocrática, demorada e cara. A necessidade que temos de autenticar praticamente todo e qualquer documento no país possui um caráter inclusive jocoso na visão popular, em razão do engessamento que isso traz aos negócios jurídicos realizados por aqui.

Nessa parte, inclusive, comenta-se apenas a autenticação de documentos simples, como uma procuração de plenos poderes ou qualquer outro documento que necessite de autenticação de firma. Não há referência a casos mais complexos como a abertura e fechamento de empresas, um dos conhecidos pesadelos dos empreendedores brasileiros.

No entanto, não se pode entender os cartórios como algo necessariamente ruim. A sua função é completamente necessária para um sistema que pretende conferir segurança jurídica aos seus negócios. A presença de um terceiro

intermediário que pode conferir fé pública tem o condão de diminuir fraudes e torna o nosso sistema como um todo mais confiável.

Contudo, como comentado anteriormente, o trabalho que se necessita para realizar um serviço relativamente simples – o de conferir se a assinatura física do documento confere com a assinatura real daquela pessoa – demanda mais tempo e dinheiro do que o necessário. Por essa razão, muitos estabelecimentos cartorários já começaram a repensar sua dinâmica de atendimento.

Apesar de ainda ter uma participação relativamente pequena no mercado notarial, já existem diversos cartórios que oferecem serviços digitais no país, inclusive na cidade de Porto Alegre. Esse processo foi acelerado com a pandemia se alastrou pelo mundo, obrigado com que as pessoas saíssem de casa o menos possível.

O artigo 1º da Lei 8.935/1994 descreve os serviços notariais e de registro como “os de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos” (BRASIL, 1994). Por essa razão, tais serviços são de extrema relevância para a realização de negócios jurídicos válidos e eficazes.

De forma a garantir que o país continue funcionando, uma vez que a realização de grande parte dos negócios jurídicos no Brasil depende de algum serviço notarial – como compra e venda de imóveis, autenticação de assinaturas, certidões de nascimento, óbito e casamento, entre outros serviços -, estes estabelecimentos precisaram se adaptar a uma nova realidade.

Importante mencionar, antes de analisar casos concretos de cartórios digitais pelo país, que a Lei da Liberdade Econômica (Lei 13.874/2019) encerrou com qualquer discussão acerca da equiparação entre os documentos digitalizados – nascidos físicos e passados para o meio digital em momento posterior -, e documentos produzidos em meio físico.

Tal entendimento, apesar de parecer óbvio em nosso contexto, trouxe maior segurança para os documentos produzidos por meio digital, uma vez que agora se tem certeza que estes possuem o mesmo valor de documentos físicos.

Mesmo tendo alguns aspectos que precisam ser melhor considerados – por exemplo, a possibilidade de descarte de documentos físicos após a digitalização destes -, a medida teve sua implementação bem pensada. Isso é demonstrado pelos critérios técnicos descritos no Decreto 10.278/2020, que regulamenta o art. 2º-A da

Lei 12.682/2012 – dispositivo que permite a digitalização de documentos físicos e seu posterior descarte.

A medida tem benefícios. Isso porque ela pode desburocratizar os serviços prestados por cartórios, permitindo com que os documentos notariais e registrais permaneçam de fácil acesso aos seus usuários.

Necessário ressaltar também que os serviços digitais não se relacionam com a digitalização de documentos. Isso porque os documentos criados por cartórios digitais são nascidos neste meio, e não transformados do meio físico para o digital, o que pode conferir eficácia, validade, autenticidade do documento e a oponibilidade deste perante terceiros.

Assim, podemos elencar as seguintes vantagens de se utilizar documentos digitais natos: integração dos documentos em um único sistema, o que diminui a necessidade de espaço físico para a guarda de documentos e facilita a sua catalogação; a eliminação de custos considerados “invisíveis”, como a impressão, cópia e envio dos documentos; segurança no armazenamento; diminuição de risco de perda do documento, entre outros.

De modo a exemplificar os benefícios, a plataforma Cryptoid (2019) analisou o caso da Leroy Merlin, empresa que trabalha no ramo de comércio de produtos de reforma e construção. A companhia estimou uma economia de R$ 200 mil anuais com a dispensa de reconhecimento de firma e impressão de documentos, além da economia de tempo de assinatura de documentos. A empresa constatou que a certificação de um contrato demorava, em média, 45 dias. Enquanto isso, quando assinado digitalmente, esse processo diminui para 2 dias.

Ainda, importante ressaltar outros diversos custos secundários, como deslocamento, impressão de folhas e encaminhamento do documento. Exposto assim, fica clara porque é necessária a mudança para um sistema mais digital, dado que se possa garantir os atributos aos documentos para que eles tenham validade jurídica.

Tendo essas premissas em mente, é possível verificar como essas iniciativas funcionam na prática.

Os atos notariais por meio eletrônico no Rio Grande do Sul estão regulamentados na Consolidação Normativa Notarial e Registral do Rio Grande do Sul-CNNR/RS:[13]

> Art. 960. São entendidos como atos notariais digitais, dentre outros, os seguintes:
> I – registro de assinatura eletrônica e de certificado digital: é o arquivamento no Tabelionato de Notas de certificado digital de pessoa física ou jurídica e respectiva assinatura eletrônica;
> II – reconhecimento de firma digital em cópia física: é a declaração, pelo Tabelião de Notas, de que o documento digital que deu origem à cópia física foi assinado pelo titular do certificado referido na assinatura digital e não foi alterado desde o momento da assinatura;
> III – reconhecimento de firma digital em documento digital: é a declaração, pelo Tabelião de Notas, de que o documento digital foi assinado pelo titular do certificado referido na assinatura digital e não foi alterado desde o momento da assinatura;
> IV – autenticação de documento digitalizado: é a atribuição de autenticidade, pelo Tabelião de Notas, a um documento digitalizado pelo Tabelionato a partir de um documento original em meio físico;
> V – autenticação de cópia física de documento assinado digitalmente: é a atribuição de autenticidade, pelo Tabelião de Notas, a uma cópia física de um documento assinado digitalmente pelo(s) titular(es) do(s) certificado(s) referido(s) na(s) assinatura(s) digital(ais) do documento;
> VI – autenticação de cópia física de documento digitalizado autêntico: é a atribuição de autenticidade, pelo Tabelião de Notas, a uma cópia física de um documento digitalizado previamente, conferido e autenticado por Notário;
> VII – autenticação de cópia de documento digital da Internet: é a atribuição de autenticidade, pelo Tabelião de Notas, a uma cópia física de um documento digital obtido na rede mundial de computadores;
> VIII – reconhecimento de página da Internet por Tabelião de Notas: é a declaração, através de ato notarial, da existência de determinada página na rede mundial de computadores e seus respectivos responsáveis;
> IX – emissão de traslado ou certidão digital: é a emissão, pelo Tabelião de Notas, de documento assinado digitalmente referente a ato por ele praticado. (CNNR/RS, 2020).

[13] Disponível em https://www.colegioregistralrs.org.br/wp-content/uploads/2020/01/CNNR.pdf. Acesso em: 19 de setembro de 2020.

Neste mesmo ato, é tratado acerca da utilização de certificados digitais por tabeliães, entre os artigos 951 e 958. Nestes dispositivos, pode-se destacar a necessidade de emissão dos certificados digitais pelas autoridades certificadoras ICP-Brasil (art. 952, §1º); a fé pública concedida aos documentos assinados digitalmente pelo Tabelião de Notas (art. 952, §3º); os atos notariais podem ser formados e conservados em meio eletrônico (art. 955); e a desnecessidade de selos, carimbos ou outras marcas oficiais para conceder validade ao certificado e à assinatura digital do Notário (art. 956).

Uma das iniciativas encontradas na capital gaúcha, o 5º Tabelionato de Notas de Porto Alegre, em sua página oficial na internet, elenca os seguintes benefícios de se utilizar do seu "cartório digital":

> - **Processo Simples**
>
> Solicite os serviços sem precisar ir até o Cartório. Você ganha mais tempo para desfrutar sua vida, sem abrir mão da segurança nos atos jurídicos que pratica.
>
> - **Documentos Digitais**
>
> Obtenha documentos digitais válidos legalmente. Os atos praticados na Cartório Digital possuem o mesmo valor jurídico de seus equivalentes em papel.
>
> - **Atualização em tempo real**
>
> Acompanhe os serviços solicitados de onde estiver, de forma ágil e simples, via internet. Você se mantém atualizado, sem precisar ligar ou ir até o Cartório.
>
> - **Pagamento simplificado**
>
> Pague os emolumentos via internet, com cartão de crédito, débito ou boleto bancário. Isso garante mais segurança para você e para os cartórios.
>
> - **Segurança na transação**
>
> Faça as transações de forma segura. Todos os documentos digitais adotam processos criptográficos para criação de uma assinatura digital.
>
> A Cartório Digital simplifica o acesso do cidadão aos cartórios. Com a plataforma os serviços continuam sendo prestados diretamente pelas serventias, sem intermediação.[14]

[14] Disponível em: http://www.tabelionatomanica.com.br/informacoes-cartoriodigital.php. Acesso em: 19 de setembro de 2020.

A descrição acima exemplifica bem as vantagens de se utilizar o serviço digital. Não é necessário o deslocamento para o envio ou retirada do documento, o pagamento pode ser realizado de casa, é possível realizar o acompanhamento da solicitação em tempo real, de forma que o documento digital possui o mesmo valor jurídico de um documento produzido em meio físico.

A despeito de todas as vantagens que o serviço oferece, no entanto, o local de solicitação de documentos pela *internet* encontra-se indisponível por tempo indeterminado, o que acaba por frustrar as expectativas daqueles que pretendem migrar para esta modalidade do serviço.

Iniciativas semelhantes, entretanto, aparentemente se tornaram comum pelo país. Apesar de não ter um sistema totalmente digital, cartórios vêm aceitando solicitações *online*, por meio de mensagens eletrônicas ou até plataformas especializadas em seus *websites*. Alguns ainda enviam os documentos por meio físico, sendo entregues diretamente na casa do requerente, o que, de certo modo, pelo menos facilita em tempos de distanciamento social.

Também há iniciativas que já encaminham documentos digitais natos, assinados por certificados digitais. Modelos como este são mais efetivos na digitalização do serviço, visto que documentos digitais assinados digitalmente possuem a mesma validade de documentos físicos.

Ademais, são mais práticos de armazenar, sendo facilmente acessíveis a qualquer momento. Isso se demonstra uma vantagem especialmente em tempos de pandemia, visto que o papel é potencial meio de condução do vírus. Além disso, possuem uma garantia mais substancial de autenticidade e integridade do documento, em face da possibilidade de validação da assinatura aposta por meio eletrônico.

A capital gaúcha, seguindo a tendência de digitização dos processos cartorários, conta com outra serventia que oferece serviços digitais. O 1º Tabelionato de Notas de Porto Alegre[15] integra o e-notariado, uma iniciativa do Colégio Notarial do Brasil – Conselho Federal. O e-notariado[16] consiste em uma plataforma em que o cidadão pode solicitar “a realização de escrituras, procurações ou qualquer outro ato notarial eletrônico diretamente no tabelionato de notas”.[17]

---

[15] Disponível em: https://1tabelionatopoa.com.br/. Acesso em: 19 de setembro de 2020.
[16] Disponível em: https://www.e-notariado.org.br/customer. Acesso em: 19 de setembro de 2020.
[17] Disponível em: https://www.e-notariado.org.br/customer/get-to-know. Acesso em: 19 de setembro de 2020.

Para possibilitar a utilização da plataforma, o cidadão se cadastra em um tabelionato de notas de sua cidade credenciado como uma Autoridade Notarial, levando seu documento de identidade e comprovante de residência. O serviço é gratuito e o certificado digital é instalado diretamente em seu celular, após a conferência dos documentos e a identificação presencial da pessoa.

Dessa forma, o usuário do serviço irá assinar o ato por meio de uma assinatura digital cadastrada na própria plataforma. A página do serviço oferece a validação do documento,[18] a fim de garantir que o documento possui validade jurídica e que este realmente possui fé pública como clama ter.

Além das vantagens elencadas para atos realizados por pessoas físicas, em especial, os condomínios edilícios aproveitaram as novidades trazidas em momento de isolamento social necessário. Esse é um exemplo relevante pois os condomínios dependem significativamente de serviços notariais em seu cotidiano. Ao longo dos meses, foram percebidos principalmente os seguintes benefícios: agilidade, praticidade, economia, segurança no trânsito de documentos e eliminação de espaços físicos para a guarda de documentos.

É inegável que essas iniciativas estejam contribuindo positivamente para a digitalização dos procedimentos cartorários e colaborando para a desburocratização desses serviços. Tais serviços devem ser incentivados, visto que são uma solução interessante e mais viável a curto prazo, mas ainda há problemas que se acredita que podem ser resolvidos por plataformas construídas com tecnologia de *blockchain*, o que irá se analisar no próximo ponto.

3.1.2. Soluções em *blockchain*

Após a análise de serviços que já se utilizam do meio digital para funcionar, resta a verificação de iniciativas que se utilizem de *blockchain* para realizar serviços típicos de um cartório.

Conforme explicado no ponto anterior, a *blockchain* funciona como um livro-razão, no qual são registradas todas as transações daquela rede, sendo reconhecida como a tecnologia mais avançada para guardar e registrar informações atualmente.

Ainda, essas informações são consideradas imutáveis e não podem ser apagadas da rede uma vez nela posta, o que garante a segurança tecnológica do

[18] Disponível em: https://assinatura.e-notariado.org.br/validate. Acesso em: 19 de setembro de 2020.

documento. Por sua vez, a fé pública, que garante a segurança jurídica do documento, no Brasil é adquirida por meio do registro deste em um cartório competente.

A tecnologia de *blockchain* pode resolver problemas cartorários com soluções digitais, como a verificação da transferência do documento eletrônico, a preservação do conteúdo e a legitimidade das partes que subscreveram o documento. A integridade do documento pode ser garantida pela utilização de carimbos de tempo (*timestamp*), o que atesta que o documento não foi alterado. A autenticidade do documento, por sua vez, torna-se ainda mais fácil de assegurar do que a de um documento físico, em razão da autenticação por um código computacional.

A fim de visualizar melhor o procedimento que ocorre no meio digital, o documento eletrônico recebe uma assinatura digital, a qual é capaz de assegurar os atributos de validade jurídica de um documento digital nato. Ainda, é possível acrescentar um selo digital, emitido pelo Tribunal de Justiça de cada Estado da federação, e encaminhar o documento conjuntamente com uma certidão do próprio oficial escrevente.

Este documento, então, fica arquivado em um livro digital, constituído por um disco rígido[19] aprovado pelo Tribunal de Justiça, o qual passa por constantes auditorias.

Tendo em vista os pontos apresentados acima, passa-se a analisar as iniciativas que já existem no Brasil, apontando as similaridades com a solução proposta e as melhorias necessárias para uma ampla implementação no sistema cartorário brasileiro.

Importante salientar que a análise dos casos abaixo foi feita de forma imparcial, sem nenhum cunho mercadológico. Pretende-se apenas observar as propostas sob o ponto de vista de seus funcionamentos, funcionalidades, vantagens e desvantagens.

3.1.2.1. OriginalMy Blockchain

Fundada em 2015, considera-se a primeira empresa brasileira a apresentar soluções por meio da tecnologia de *blockchain* para eliminar a burocracia desnecessária, a fim de promover “acesso à justiça e tornar a governança mais

[19] Local de armazenamento de informações, como arquivos, programas, jogos, entre outros, funcionando como uma memória do computador, ou externa a ele.

transparente através de nossas ferramentas para comprovar a autenticidade de pessoas, contratos, documentos e arquivos digitais".[20]

Em razão da parceria criada com alguns cartórios extrajudiciais, é a iniciativa mais semelhante à proposta de solução que se busca incentivar com o presente trabalho. Tal parceria já rendeu a emissão de certidões de registros civis, como a primeira certidão de nascimento e as primeiras certidões de união estável do país.

A plataforma oferece quatro serviços distintos:

- Blockchain ID: permite o acesso a *sites* e lugares sem a necessidade de cadastro. É o meio utilizado para assinar documentos por meio da plataforma. A criação da ID se dá por meio de aplicativo próprio, podendo ser utilizado por pessoas físicas e jurídicas. Empresas podem utilizar a base de dados do sistema para realizar uma série de serviços, sendo possível a criação de classificações de acordo com o perfil recebido. Em atenção à Lei Geral de Proteção de Dados (LGPD), o usuário deve consentir com a utilização de seus dados pessoais.

- OMySign: capaz de provar autoria da assinatura, podendo ser assinado de qualquer lugar do mundo a qualquer tempo. Em razão da certificação em *blockchain*, consegue detectar fraudes nos documentos a serem assinados, de forma que o sistema impede a assinatura caso perceba alguma alteração. Com a Blockchain ID, é possível verificar que está assinando o documento, de forma a conferir o atributo de não-repúdio ao documento. Contanto que seja admitido pelas partes, a assinatura digital não precisa ser por certificado emitido pela ICP-Brasil. A plataforma, no entanto, não possibilita o armazenamento de documentos.

- PACDigital: nomeada como Prova de Autenticidade de Conteúdo Digital, é uma solução para proteger um arquivo digital. Ao armazenar o documento em *blockchain*, será emitido um certificado contendo um número *hash*, junto com um carimbo de tempo, o que pode atestar a data e o horário da certificação, podendo posteriormente comprovar a existência e a autenticidade daquele arquivo. Importante ressaltar que está solução não substitui o registro no INPI (Instituto Nacional de Propriedade Intelectual).

- PACWeb: realiza a cópia do conteúdo de uma página da *internet* ou de uma conversa por mensagem de texto no celular, gerando um relatório que comprova a

[20] Disponível em: https://originalmy.com/about. Acesso em: 12 de agosto de 2020.

existência daquele conteúdo, por meio de certificação da data e da hora que a informação foi capturada.

Na sessão de perguntas e respostas da página oficial, é informado que provas produzidas pela ferramenta PACWeb foram aceitas em um processo judicial no Tribunal de Justiça de São Paulo demonstrando que a solução tem validade jurídica.

3.1.2.2. OwlDocs

É uma empresa brasileira que se propõe a proteger os dados do usuário, disponíveis na nuvem, *on premise*[21] ou *blockchain*, reduzindo os custos de infraestrutura. Com *blockchain*, eles se propõem a garantir a autenticidade, a integridade e a confidencialidade dos documentos depositados.

Por meio da *blockchain*, é possível realizar auditoria e prova de existência das informações depositadas. A auditoria significa verificar todas as atividades realizadas que envolvam o documento depositado, desde a simples visualização por um usuário, até a mudança ou realização de uma nova versão do arquivo.

Por meio da *OwlDocs Stamp*, um contrato inteligente baseado na rede *blockchain Ethereum*, a plataforma consegue descentralizar o processo de autoria de todos os eventos e registros de envio dos documentos, “de forma transparente e automática para o usuário, garantido a integridade, a autenticidade e aprova de existência do evento baseada na Hora Legal Brasileira”.[22]

3.1.2.3. GrowthTech

Especializada em contratos imobiliários, diz-se a pioneira no país em transações integralmente eletrônicas. Os contratos imobiliários privados são registrados em uma *blockchain* privada, sendo eles formalizados em um ambiente seguro e assinados por meio de QRCodes ou certificados digitais baseados na ICP-Brasil.

- Identidade digital: os dados cadastrais e biométricos são verificados em bases de dados oficiais do governo;

- Contrato digital: contratos 100% digitais, como promessas de compra e venda, contratos de compra e venda com alienação fiduciária, confissão de dívida e notas promissórias, entre outros.

---

[21] Sistema de armazenamento desenvolvido pela própria empresa.
[22] Disponível em: https://www.owldocs.com/blockchain. Acesso em: 05 de outubro de 2020.

- Assinatura digital: os contratos podem ser assinados por certificados emitidos pela ICP-Brasil ou por QRCode.

- Registro em *blockchain*: todos os contratos formalizados são registrados em uma plataforma de *blockchain* privada, para “tornar os processos mais seguros e transparentes”.

- DiGi: plataforma para facilitar a administração de condomínios edilícios. Promete criar um ambiente sem intermediadores entre as tarefas cotidianas do condomínio e o síndico e entre este e os condôminos, o que poderia evitar conflitos ao resolver questões pendentes.

Apesar de ter foco no mercado imobiliário, a empresa também busca inovações em outras áreas dos registros civis, como certidões de nascimento e de união estável.

3.1.2.4. Uniproof

Propõe-se a realizar o registro de qualquer arquivo eletrônico em cartório e em *blockchain*, eliminando a utilização de papel e evitando a ida ao cartório. Possui validade jurídica e fé pública dos documentos, a partir do computador do usuário.

O envio do documento é feito pelo próprio usuário em seu computador pela plataforma, assim como o retorno dos documentos registrados eletronicamente. O arquivo é analisado por um registrador e, se aceito, é registrado em *blockchain*.

O retorno ao usuário é do *hash* – para que possa verificar a sua validade - e do documento registrado em cartório. Ainda, oferece a guarda perpétua dos documentos registrados sem custos de armazenamento e possibilita a governança do documento por provar sua existência e seu conteúdo.

3.1.2.5. Bitnation

Apesar de não ser uma solução brasileira ou aplicada diretamente no país, esta plataforma merece menção no presente trabalho. Descrita como a primeira nação voluntária sem fronteiras descentralizada (DBVN)[23] criada em 2014, afirma ter realizado em *blockchain* a primeira certidão de casamento, certidão de nascimento, identidade emergencial de refugiado, cidadania mundial, constituição da DBVN, entre outros.

Dessa forma, a plataforma pretende ser uma organização autônoma descentralizada, possibilitando a criação de nações voluntárias, oferecendo muito

[23] Do inglês: Decentralized Borderless Voluntary Nation (DBVN) (tradução nossa).

mais do que somente serviços notariais. Não há barreiras à entrada, permitindo que qualquer um que deseje ingresse na equipe, a fim de se beneficiar da infraestrutura tecnológica da comunidade.

São mencionadas ainda a possibilidade de resolução de conflitos por meio de arbitragem e de criação de sua própria nação, com leis específicas, mecanismos de tomada de decisão, uma própria constituição e serviços de governança aos cidadãos.

Em razão do escopo do trabalho, não se pretende fazer uma análise jurídica completa da iniciativa, o que requer um estudo autônomo. Contudo, os objetivos e serviços da plataforma são capazes de demonstrar que é possível a realização de serviços notariais mais eficientes e mais inteligentes.

3.2. Relação entre *blockchain* e serviço notarial

Os exemplos expostos acima demonstram que, apesar de não ter um sistema completamente digital, o Brasil está em um caminho de digitização de seus serviços notariais e registrais. É importante notar que a situação atual de isolamento social acelerou o processo, em especial pelo aumento da procura de serviços desse modo, razão pela qual os processos desenvolvidos nesse momento devem permanecer e serem aprimorados com o tempo.

A análise nessa sessão se aterá às iniciativas que apresentaram a utilização de *blockchain* em suas soluções, deixando a análise do cenário cartorário brasileiro como um todo para a próxima sessão. Dessa forma, é possível verificar que já existem soluções promissoras para os serviços notariais no Brasil, tanto em relação ao registro do documento em si, quanto para o armazenamento deste documento após a sua autenticação.

Para o registro de documentos simples, a solução mais completa se mostra a da Uniproof. A partir dela, é possível enviar um documento produzido pelo usuário em seu computador por meio de uma plataforma do sistema. Após, o documento é enviado para a análise de registrador, que verifica os requisitos do documento e, se aceito, ele confere a autenticação necessária e armazena o documento em *blockchain*, encaminhando-o de volta ao usuário.

A dinâmica descrita se assemelha muito à prática cartorária cotidiana. O tabelião, quando requerida a certificação de um documento, precisa analisar se este arquivo atende às especificações legais, protegendo o documento com fé pública, se entender ser possível.

Nesse caso, temos uma vantagem para cada lado. A Uniproof, ao armazenar o documento em *blockchain* pode garantir a sua guarda permanente, de forma autêntica e íntegra. Registrar o documento em um cartório, no entanto, confere fé pública a ele, visto que o notário e o oficial de registro são os funcionários públicos dotados de tal atribuição.

Dessa forma, se o registrador da Uniproof for um tabelião ou um oficial, ou seja, se o sistema for utilizado por um cartório, é possível unir a facilidade de se encaminhar um documento diretamente por uma plataforma *online*, sem qualquer custo de deslocamento ou impressão, enquanto o documento é registrado em uma plataforma inviolável e ainda recebe fé pública.

Aqui, necessário fazer uma correlação com uma solução que já existe em cartórios brasileiros e pode ser utilizada em boa parte do território nacional, que é o e-notariado. Como explicado anteriormente, a plataforma permite com que os usuários realizem os atos cartorários sem se deslocar até o cartório.

A questão dessa solução é que, apesar do usuário já possuir uma certificação digital de sua identidade, a qual, pressupondo boa-fé, será utilizada somente por ele, este ainda precisa expressar sua manifestação de vontade a um notário, mesmo que de forma digital. Isso exige tempo e programação, além de deixar o processo mais demorado.

Por esta razão, uma solução totalmente digital para atos notarias, como a redação de procurações e de outros instrumentos particulares não necessitaria de uma nova manifestação de vontade, uma vez que a sua assinatura digital deveria representar tal manifestação.

É possível verificar também soluções específicas a um ramo dos serviços cartorários. A Growth Tech é uma *startup* especializada em registros de imóveis. Assim, ela permite que o contrato seja elaborado na própria plataforma e seja assinado pelas partes. Os contratos são assinados digitalmente, podendo ser por meio de QRCodes ou por assinaturas digitais, enquanto o documento permanece armazenado em uma plataforma de *blockchain*, com toda a segurança que a sua imutabilidade provê.

A iniciativa é de extrema relevância, visto que facilita o registro de imóveis por escrito, especialmente no momento de colher as assinaturas. O processo é seguro também pois todas as partes envolvidas devem ter uma identidade certificada na plataforma.

No entanto, não se pode esquecer que a transferência de propriedade de bens imóveis no Brasil requer, necessariamente, o registro dessa transação por escritura pública e, caso realizado por meio digital, requer a aposição de assinatura digital qualificada, conforme o art. 5º, §2º, inciso IV da recente Lei 14.063/2020.[24] Dessa forma, é imprescindível que o contrato seja registrado em um Registro de Imóveis para que seja oponível perante terceiros, visto que este é o requisito legal do nosso ordenamento jurídico.

Uma solução interessante seria a adoção dos próprios cartórios de registro de imóveis de uma base em *blockchain*; assim, o contrato de compra e venda de um imóvel, após assinado, já poderia ser registrado na rede para demonstrar a vontade das partes de transferir o bem de um para o outro.

Tal registro parece ser possível pela própria plataforma, quando se verifica que certidões de união estável e de nascimento foram realizadas pela iniciativa em convênio com cartórios. No caso da união estável, o casal compareceu ao cartório, no qual realizaram as suas identificações, para possibilitar a assinatura digital do documento, e responderam a um questionário. Após o documento foi certificado por dois notários, o que conferiu a fé pública à certidão. Além de ficar registrado na *blockchain*, uma cópia impressa foi entregue aos noivos.

A certidão de nascimento, por sua vez, ocorreu de uma parceria direta com o hospital e o cartório. Os pais aceitaram participar de uma iniciativa piloto para a realização deste tipo de certidão deste modo e o documento ficou registrado em uma plataforma com tecnologia *blockchain* após. Ambos os casos foram realizados com a aplicação *Notary Ledgers*, da *GrowthTech*, o nicho especializado para os serviços registrais dos cartórios.

Ainda, vale tecer breves comentários acerca da solução apresentada pela OriginalMy Blockchain. Embora não possibilite o armazenamento dos documentos certificados na plataforma, a iniciativa tem sido pioneira em serviços registrais no Brasil. Entende-se que o primeiro registro de nascimento em *blockchain* se deu pela

[24] Art. 5º No âmbito de suas competências, ato do titular do Poder ou do órgão constitucionalmente autônomo de cada ente federativo estabelecerá o nível mínimo exigido para a assinatura eletrônica em documentos e em interações com o ente público. [...]
§ 2º É obrigatório o uso de assinatura eletrônica qualificada: [...]
IV - nos atos de transferência e de registro de bens imóveis, ressalvado o disposto na alínea "c" do inciso II do § 1º deste artigo;

OriginalMy, certidão que foi posteriormente registrada em um cartório da região para ter fé pública.

Ainda, a aplicação PACWeb oferecida pela empresa pode funcionar como uma ata notarial eletrônica. Ou seja, é capaz de produzir provas do meio digital e comprovar que não houve modificações naquele meio após a "captura da tela", uma vez que essa captura acompanha todos os metadados[25] necessários para realizar a autenticação em juízo.

Estes metadados envolvem a data e horário da coleta, a localização do dispositivo e seu endereço de IP, entre outras informações. Após a coleta, os dados são guardados em *blockchain* e recebem um *hash*, de forma que, qualquer mudança que ocorrer após essa coleta, será apontada uma incongruência entre os arquivos.

A solução apresentada, assim, parece ser possível. Considerando que o documento pode ser criado dentro da própria plataforma com tecnologia de *blockchain* e assinado digitalmente pelas partes envolvidas, o documento possui os atributos de validade jurídica. Para ter fé pública, necessário que um notário ou oficial de registro o assine também. Por último, as transferências do documento poderiam ser feitas diretamente pela plataforma, uma vez que ficariam gravadas na rede.

3.3. Melhorias necessárias

Até a presente sessão, foram demonstradas diversas razões para ampla adoção da tecnologia de *blockchain* em serviços cartorários. Aqui vale ressaltar alguns, como a validade jurídica dos documentos criados e registrados em *blockchain*, visto que a Lei da Liberdade Econômica igualou o valor probatório de documentos digitais e físicos[26].

É inegável também que uma plataforma única com todos os documentos certificados facilitaria a comunicação entre os órgãos de registro público de diferentes competências e entes públicos. Além disso, representaria uma economia de tempo e dinheiro, visto que os atos poderiam ser comunicados instantaneamente de uma serventia a outra.

[25] Metadados são os "dados estruturados que permitem classificar, descrever e gerenciar documentos". Decreto 10.278/2020, artigo 3º, inciso II (BRASIL, 2018).
[26] Inclusão do artigo 2º-A, Lei 12.682/2012.

Aliás, uma plataforma acessível a qualquer tempo poderá prover cópias de documentos para o solicitante mesmo em momentos que o cartório esteja fechado, visto que o pagamento pode facilmente ser realizado por meio eletrônico.

A certificação de documentos por criptografia também tornará dispensável os selos, uma vez que a veracidade da certificação poderá ser conferida de forma computacional, um meio muito mais seguro.

Por todas essas vantagens, reforça-se a ideia de que o presente trabalho não pretende acabar com as serventias cartorárias, tendo em vista que elas prestam um serviço extremamente necessário para garantir a segurança dos negócios jurídicos promovidos no país. Aqui se pretende, única e exclusivamente, apresentar formas mais inteligentes e eficazes de promover estes serviços.

Por esta razão, após longa análise da tecnologia e de experiências existentes atualmente, cumpre mencionar as dificuldades para a implementação e as melhorias percebidas ao longo do estudo.

3.3.1. Dificuldade de digitização dos processos cartorários

O processo de digitização, diferentemente do processo de digitalização, busca automatizar o sistema, de forma que as atividades se realizem no meio virtual, sem a necessidade de impressão de documentos físicos ou aposição de selos e carimbos, por exemplo.

Apenas a título de curiosidade, o processo de digitalização, por sua vez, é apenas a migração dos documentos e arquivos que existem no meio físico para o meio digital. Nesse caso, a digitização dos processos cartorários é precisamente o centro da solução apresentada.

Apesar da existência de diversas iniciativas mais modernas e eficientes, como as apresentadas e analisadas nesse trabalho, é possível perceber pela sessão 2.1.1 que o modelo adotado como “digital” pelos cartórios brasileiros não condiz, nem de perto, com o estado de arte da tecnologia para serviços cartorários.

Muitos dos cartórios se utilizam da nomenclatura “digital” quando a solicitação do documento é feita por meio de um *website* ou de uma mensagem eletrônica, mas entregam o documento ainda pelo meio físico. Em um grande avanço, muitas das serventias já oferecem o encaminhamento de documentos no modo digital, tendo o tabelião assinado o arquivo com um certificado digital para dar-lhe fé pública.

Contudo, tal possibilidade só foi amplamente regulamentada recentemente, com o Provimento 95/2020 do CNJ, provimento este que surgiu apenas em razão do momento de isolamento social, o que ainda assim não fez com que processos digitais se tornassem regra nos cartórios brasileiros. Além disso, não é possível confirmar que as medidas tomadas durante esse período serão perpetuadas após.

É preciso reconhecer que os entes públicos têm se esforçado para trazer inovações para seus serviços, como é o caso da iniciativa e-notariado, regulamentado pelo Provimento 100/2020 CNJ. A possibilidade de realizar atos cartorários de casa, sejam eles notariais, sejam eles registrais, facilita-os e os desburocratiza. Contudo, tendo iniciativas que já mostram soluções mais desenvolvidas, a plataforma e-notariado fica aquém do esperado.

A digitização também enfrenta resistência por parte dos usuários dos serviços cartorários. Mesmo sendo os documentos eletrônicos mais seguros que os reproduzidos em meio físico, quando aqueles são certificados digitalmente, ainda há uma crença infundada de que o meio digital é mais suscetível a fraude. Para que o processo de digitização fosse efetivo, ele precisaria ser amplamente aceito e difundido pela população, o que ainda não acontece.

Dessa forma, a proposição da solução esbarra na vontade de digitização dos processos cartorários das duas partes envolvidas: os usuários dos serviços – população em geral – e os entes públicos.

3.3.2. Presença no território nacional

Embora seja uma solução remota – acessível em qualquer lugar, em teoria -, esta ainda não está disponível para todo o território brasileiro. Isso porque diversas atividades cartorárias exigem um cartório específico para realizar o ato. O registro de imóveis, por exemplo, precisa ser feito em um cartório na circunscrição do imóvel, não podendo o proprietário escolher aquele que desejar.

Como as soluções em *blockchain* estão limitadas aos cartórios com os quais elas possuem convênio, ainda não possível utilizá-las em todo o país, pois o usuário será obrigado a registrar o ato no cartório determinado pelo ordenamento, quando esta prescrever alguma regra.

Tal questão, no entanto, somente será resolvida com a popularização das soluções, o que depende de investimento e vontade por parte dos entes públicos em geral, de aceitação por parte dos usuários e de regulamentação por parte do governo.

3.3.3. Valor da realização dos atos

Com a proposta de uma solução tecnológica para um problema burocrático, pretende-se, além de diminuir o tempo para a realização de atos cartorários, diminuir os custos envolvidos também. Entende-se que tal seria possível, uma vez que não haveria a necessidade de guarda física e proteção destes documentos, enquanto o sistema será automatizado, não precisando de tantas pessoas para desempenhar aquela função.

Se pensarmos nos gastos secundários da realização do ato, tal quais os deslocamentos, as impressões e as cópias de documentos, temos, de fato, uma diminuição nos custos como um todo, o que é um ganho de um processo digital por *blockchain*.

Ocorre que os valores dos documentos digitais e físicos produzidos por cartórios são os mesmos. Nesse mesmo sentido, uma vez que as iniciativas que lidam com a tecnologia de *blockchain* são privadas em convênio com cartórios extrajudiciais, estas precisam ser remuneradas de alguma forma, quantia que não pode vir do valor inicial cobrado pelo ato.

Assim, serviços realizados digitalmente são mais caros, se considerarmos apenas o valor do ato. Dessa forma, seguindo o pensamento do exemplo do capítulo anterior, no qual as pessoas em geral preferem economizar o valor das transferências bancárias e passar horas em filas de banco e de caixas lotéricas, aqui entende-se que o mesmo pode ocorrer.

Embora o valor final do serviço cartorário realizado em *blockchain* muito provavelmente será menor, em especial quando lidar com atos complexos, com a necessidade de muitas cópias e assinaturas, é possível que ele seja preterido pelos atos físicos por um valor que apenas aparenta ser maior.

Isso ocorre porque o tempo gasto com as diligências e valores como armazenamento não são considerados no custo final do ato e a solução pode não ser tão efetiva quanto se propõe.

Por essa razão, a resposta para este problema é o mesmo para os outros dois apresentados acima: conscientização acerca do custo-benefício do sistema. É um trabalho, no entanto, que deve ser pensado a médio e longo prazo.

4. CONCLUSÃO

O Brasil é conhecido por ter um dos sistemas cartorários mais burocrático do mundo. A necessidade de comparecer diversas vezes em uma serventia para efetuar um ato simples ou, ainda, a falta de informação clara sobre os documentos necessários para realizar tal ato apenas corroboram a má fama dos nossos cartórios.

Contudo, as atividades notariais e registrais são de extrema importância para o funcionamento de um sistema com segurança jurídica, visto que são os tabeliães e os oficiais de registro que podem conferir fé pública a tais atos, sendo estes servidores indispensáveis para o nosso ordenamento jurídico.

Dessa forma, reforça-se a ideia de que o presente trabalho, em nenhum momento, teve o propósito de encerrar as atividades cartorárias, o que também não se acredita ser possível. Pretendeu-se, em realidade, demonstrar a sua importância no cotidiano de seus usuários e, por esta razão, tentou-se demonstrar que suas atividades poderiam ser desempenhadas de modo mais inteligente e eficiente.

Isso porque, como percebeu-se com o estudo, e sendo esta quase uma dedução lógica de quem vive no Brasil, o país ainda está muito atrasado na digitização de seus processos governamentais, em especial de seus cartórios. Apesar de iniciativas interessantes terem surgido nos últimos anos e, principalmente, meses, ainda há uma dificuldade de aceitação e utilização, por parte dos usuários, e implementação, por parte das serventias.

A pesquisa bibliográfica sobre a matéria foi relevante para perceber que se tem esforços por parte dos entes públicos em modernizar os serviços prestados pelos cartórios, com iniciativas que possuem grande potencial, como o e-notariado. Este cenário, no entanto, ocorreu em razão do isolamento social imposto em diversas cidades brasileiras, de forma que é preciso avaliar como será o seguimento dessas políticas nos próximos meses e anos.

Tendo em vista que a pesquisa pelas iniciativas brasileiras de digitização do setor iniciaram antes da decretação do estado de pandemia, é visível como a necessidade de isolamento e distanciamento social desencadeou uma série de medidas governamentais, acelerando esse processo, como a criação da plataforma e-notariado.

Contudo, é fundamental que este esforço político e da sociedade como um todo não seja esquecido após a retomada das atividades presencial, de maneira que se

siga pensando em como tornar as atividades cartorárias mais eficientes para a população em geral.

O presente trabalho serve como forma de incentivar esse desenvolvimento. Apesar de não se ter a pretensão de uma mudança brusca para um sistema completamente digital, o que requer tempo, dinheiro e aceitação por todos os envolvidos, o estudo propõe-se a trazer uma reflexão para as possibilidades de construção de um cenário mais racional quando se trata de serviços dos cartórios.

Além das funcionalidades e facilidade que um sistema completamente digital pode trazer, a implementação de uma plataforma em *blockchain* pode garantir mais segurança jurídica a todos estes atos, por meio de uma tecnologia revolucionária, diminuindo o tempo e os custos para a realização desses registros e certificações. Por isso, entende-se que, mesmo sendo uma realidade um pouco distante da que vemos hoje, ela é completamente possível.

A pesquisa, por óbvio, apresentou também dificuldades que uma implementação da tecnologia em sistemas cartorários pode enfrentar, sendo que as soluções para estes problemas podem apresentar certa contradição com a premissa da *blockchain*, qual seja, funcionar sem qualquer necessidade de intervenção por um intermediador.

Uma das maiores preocupações referentes à utilização de *Blockchain* para o armazenamento seguro de dados, bem como para a possibilidade de garantir autenticidade, integridade e não-repúdio dos documentos nele criados ou armazenados é a conferência de identidade dos usuários da rede, visto que não há uma autoridade centralizadora que controle essa entrada.

A necessidade de algum tipo de autoridade central de conferência das informações choca-se com toda a ideia da *blockchain*, que é eliminar o terceiro intermediário, de forma que é possível perguntar se uma solução que propõe a continuidade desse intermediário é de fato eficiente e eficaz. Entretanto, tendo em vista todas as iniciativas analisadas no presente trabalho, não se entende que a presença dessa autoridade acabaria com o sentido da proposta.

O intermediador seria necessário tão somente para conferir e verificar a identidade dos usuários da rede, o que não precisaria ser refeito toda vez que este usuário pretendesse realizar um ato dentro da plataforma, pois ele já teria sido reconhecido como quem diz ser. Sendo assim, os próprios notários ou oficiais de registro poderiam conferir as identidades.

Dessa forma, apesar de ainda utilizar a intermediação do servidor notarial ou registral, a sua função de verificar a vontade das partes fica mais restrita e mais segura, uma vez que a identidade delas já está no sistema. Acrescenta-se a isso o fato de que ainda não é possível garantir a identidade de alguém dentro da rede sem uma autoridade que confirme as informações essenciais do usuário, algo que pode nunca acontecer.

Sendo assim, se faz necessário, atualmente, que a assinatura digital utilizada pelos usuários em uma plataforma cartorária em *blockchain* tenha as mesmas características que a ICP-Brasil a fim de que se garanta a autenticidade, a integridade e o não repúdio ao documento; mas, resolvida essa questão, os procedimentos cartorários dentro da rede poderão se tornar muito mais simples, rápidos e seguros.

Ademais, a leitura sobre de *blockchain* e os serviços cartorários demonstraram caminhos promissores de pesquisas futuras, como a implementação da tecnologia em outros serviços governamentais e a iniciativa *Bitnation* e suas implicações jurídicas. O estudo da tecnologia demonstrou a imensidão de aplicações para a *blockchain*, razão pela qual pretende-se seguir no estudo acerca da cadeia de blocos, com o intuito de difundir a sua utilização e facilitar a nossa vida em sociedade, em especial as tarefas burocráticas.

REFERÊNCIAS

ASSOCIAÇÃO DOS NOTÁRIOS E REGISTRADORES DO BRASIL. *2º Tabelião de Notas de São Paulo faz sua primeira ata notarial de Blockchain*. São Paulo: 19 de novembro de 2019. Disponível em: https://www.anoreg.org.br/site/2019/11/19/2o-tabeliao-de-notas-de-sao-paulo-faz-sua-primeira-ata-notarial-de-blockchain/ Acesso em: 19 de agosto de 2020.

BRAGA, Alexandre Mello; FILHO, José Reynaldo Formigoni; LEAL, Rodrigo Lima Verde. *Tecnologia Blockchain: uma visão geral*. Brasil: CPqD, 2017. Disponível em: https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf Acesso em: 12 de julho de 2020.

BRAGA, Alexandre Melo; MARINO, Fernando C. Herédia; DOS SANTOS, Robson Romano. Segurança de Aplicações Blockchain Além das Criptomoedas. *In: XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. Brasília: [s.n] 2017.

BRASIL. *Decreto 10.278, de 28 de março de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10278.htm Acesso em: 02 de novembro de 2020.

BRASIL. *Lei 12.682, de 09 de julho de 2012*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm Acesso em: 15 de abril de 2020.

BRASIL. *Lei 13.874, de 20 de setembro de 2019*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm Acesso em: 15 de abril de 2020.

BRASIL. *Lei 14.063, de 23 de setembro de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm Acesso em: 02 de novembro de 2020.

BRASIL. *Lei 8.935, de 18 de novembro de 1994*. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8935.htm Acesso em: 19 de setembro de 2020.

BRASIL. *Medida Provisória 2200-2, de 24 de agosto de 2001*. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm Acesso em: 15 de abril de 2020.

CASEY, Michael; VIGNA, Paul. *The Truth Machine: The Blockchain and the Future of Everything*. Londres: HarperCollins, 2018.

CORREGEDORIA GERAL DE JUSTIÇA. *Provimento 001/2020 de 17 de Janeiro de 2020*. Disponível em: https://www.colegioregistralrs.org.br/wp-content/uploads/2020/01/CNNR.pdf Acesso em: 22 de outubro de 2020.

CONSELHO NACIONAL DE JUSTIÇA. *Provimento 100 de 26 de maio de 2020*. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3334 Acesso em: 22 de outubro de 2020.

CONSELHO NACIONAL DE JUSTIÇA. Provimento 95 de 01 de abril de 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3265 Acesso em: 22 de outubro de 2020.

CONSELHO NACIONAL DE ARQUIVOS. *Resolução nº 37 de 19 de dezembro de 2012*. Disponível em: http://conarq.gov.br/images/publicacoes_textos/conarq_presuncao_autenticidade_completa.pdf Acesso em: 06 de junho de 2020.

CONSELHO NACIONAL DE ARQUIVOS. *Glossário – Documentos Arquivísticos Digitais*. Brasil: 2016. Disponível em: http://conarq.gov.br/images/ctde/Glossario/2016-CTDE-Glossario_V7_public.pdf Acesso em: 02 de novembro de 2020.

CORRALES, Marcelo; FENWICK, Mark; HAAPIO, Helena. *Legal Tech, Smart Contracts and Blockchain – Perspectives in Law, Business and Innovation*. Singapura: Springer, 2019.

CRYPTOID. *Empresas economizam ao trocar cartórios por certificados digitais*. Brasil: 02 de dezembro de 2019. Disponível em: https://cryptoid.com.br/certificacao-digital/empresas-economizam-ao-trocar-cartorios-por-certificados-digitais/ Acesso em: 19 de setembro de 2020.

DANNEN, Chris. *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners.* Nova Iorque: Apress, 2017.

DE FILLIPI, Primavera; WRIGHT, Aaron. *Descentralized Blockchain Technology and the Rise of Lex Cryptographia*. Cambridge: Harvard University Press, 2015.

DIFFIE, Whitfield; HELLMAN, Martin. New Directions in Cyptography, *In: IEEE Transctions on Information Theory*. 1976.

DRESCHER, Daniel. *Blockchain Basics: A Non-Technical Introduction in 25 Steps.* Frankfurt: Apress, 2017.

GOVERNO FEDERAL. *Comitê Gestor da ICP-Brasil regulamenta novidades importantes para a emissão de certificados digitais de forma massificada e mais amigável para o cidadão brasileiro*. Brasil: 20 de outubro de 2020. Disponível em: https://www.gov.br/iti/pt-br/assuntos/noticias/indice-de-noticias/comite-gestor-da-icp-brasil-regulamenta-novidades-importantes-para-a-emissao-de-certificados-digitais-de-forma-massificada-e-mais-amigavel-para-o-cidadao-brasileiro Acesso em: 22 de outubro de 2020.

HABER, Stuart; STORNETTA, W Scott. How to Time-Stamp a Digital Document. *In: Journal of Cryptology*. Morristown: 1991.

HERIAN, Robert. *Regulating Blockchain: Critical Perspectives in Law and Technology*. Nova Iorque: Taylor and Francis Group, 2019.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. *Resposta ao Ofício nº 1.282/2019 – COTEC/SUCOR/RFB*. Brasil, 2019.

KACPRZYK, Janusz (ed.). Blockchain and Applications – International Congress. *In: Advances in Intelligent Systems and Computing*, Volume 1010. Cham: Springer, 2020.

MENKE, Fabiano. *Assinatura Eletrônica no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2005.

MERKLE, Ralph C. *Secure Communications Over Insecure Channels*. Berkeley: University of California, 1978.

NAKAMOTO, Satoshi. *Bitcoin. A Peer-to-Peer Eletronic Cash System.* [S.l.: s.n.], 2008.

NEEDHAM, Roger M.; SCHROEDER, Michael D. *Using Encryption for Authentication in Large Networks*. Palo Alto: Xerox Palo Alto Research Center, 1978.

NORTON, Jared. *Blockchain: Easiest Ultimate Guide To Understand Blockchain.* Califórnia: CreateSpace Independent Publisher, 2016.

ORIGINALMY. *Entenda como blockchain auxilia na assinatura eletrônica de contratos.* Brasil: 01 de outubro de 2018. Disponível em: https://blog.originalmy.com/entenda-como-blockchain-auxilia-na-assinatura-eletronica-de-contratos/ Acesso em: 06 de junho de 2020

PINHEIRO, Patrícia Peck. *Direito Digital*. 6ª edição. São Paulo: Saraiva. 2016.

SCHROEDER, Michael D.; NEEDHAM, Roger M. Using Encryption for Authentication in Large Networks. *In: Communications of the ACM*, Volume 21, Número 12. Palo Alto: 1978.

SERVIÇO FEDERAL DE PROTEÇÃO DE DADOS. *Serpro lança plataforma Blockchain*. Brasília: 10 de novembro de 2017. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2017/serpro-lanca-plataforma-blockchain-2 Acesso em: 19 de setembro de 2020

SINGHAL, Bikramaditya; DHAMEJA, Gautam; PANDA, Sekhar Priyansu. *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Delaware: SSBM Finance Inc., 2018.

SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso Especial n. 1.495.920 DF. Rel. Ministro Paulo de Tarso Sanseverino. Brasília, 15 mai. 2018. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201402953009&dt_publicacao=07/06/2018 Acesso em: 09 de novembro de 2020

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution*. Nova Iorque: Portfolio/Penguin, 2016.

UNITED NATIONS COMISSION ON INTERNATIONAL TRADE LAW. *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment*. Nova Iorque: 2001. Disponível em: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf Acesso em: 22 de outubro de 2020.