FUNDAÇÃO GETULIO VARGAS

ESCOLA DE DIREITO FGV DIREITO RIO

GRADUAÇÃO EM DIREITO

FELIPE VIANNA ROSSETO

Blockchain e sua implementação nos Cartórios de Registro de Imóveis.

Trabalho de Conclusão de Curso, sob a orientação do professor **João Pedro Barroso do Nascimento**, apresentado à FGV DIREITO RIO como requisito para obtenção do grau de bacharel em Direito.

Rio de Janeiro, dezembro/2019

FUNDAÇÃO GETULIO VARGAS

ESCOLA DE DIREITO FGV DIREITO RIO

GRADUAÇÃO EM DIREITO

FELIPE VIANNA ROSSETO

Blockchain e sua implementação nos Cartórios de Registro de Imóveis.

Rio de Janeiro, dezembro/2019

FGV DIREITO RIO

FUNDAÇÃO GETULIO VARGAS

ESCOLA DE DIREITO FGV DIREITO RIO

GRADUAÇÃO EM DIREITO

Blockchain e sua implementação nos Cartórios de Registro de Imóveis.

Elaborado por FELIPE VIANNA ROSSETO

Trabalho de Conclusão de Curso, sob a orientação do professor **João Pedro Barroso do Nascimento**, apresentado à FGV DIREITO RIO como requisito para obtenção do grau de bacharel em Direito.

Comissão Examinadora:

Nome do orientador: **João Pedro Barroso do Nascimento**

Nome do Examinador 1: **Gustavo Kloh Muller Neves**

Nome do Examinador 2: **Ivar A. Hartmann**

Assinaturas:

_____

João Pedro Barroso do Nascimento (Professor Orientador)

_____

Gustavo Kloh Muller Neves (Examinador 1)

_____

Ivar A. Hartmann (Examinador 2)

Nota Final: _____

Rio de Janeiro, _____de _____de 2019.

RESUMO:

O presente trabalho tem por objetivo de analisar a implementação *blockchain* no contexto dos Cartórios de Registro de Imóveis. Essa tecnologia tem a capacidade de descentralizar o sistema, democratizando seu acesso, enquanto também aumenta sua segurança frente a possibilidade de fraudes e erros humanos.

Para realização do projeto foi feita uma análise da confiabilidade da tecnologia, passando desde a explicação do seu contexto original, até demonstração estatística de sua confiabilidade. Além disso, seus benefícios como redução dos custos e das fraudes e os riscos inerentes a plataforma, como casos de avanço da tecnologia e integração do direito de posse e propriedade. Em sequência houve uma análise dos pré-requisitos para a implementação do modelo, além da demonstração de níveis distintos de integração do registro com o sistema, incluindo de análises de casos para exemplificação.

PALAVRAS-CHAVE: *Blockchain*. Cartórios. Registro. Propriedade. *Colored-Coins*.

ABSTRACT:

This paper aims to analyze the integration of blockchain in the properties registry. This technology has the power to decentralize the system, democratizing the systems acess, while making the registry more secure agains fraud and humam errors.

The Project starts with a trustability analysis, going from the explanantion of the first application of the technology to the statistics of its trustability. Moreover, it tries to cover the benefits of implementing it, as cost reduction, and risks, as the merge of possession of goods and property rights and the advance of technology. Furthermore, there is an analysis implementation's pre-requisites and the demonstration of different levels of complexity in integrating the systems, including some real cases for exemplifying the levels.

KEYWORDS: Blockchain. Notary. Registry. Property. Colored-Coins .

Sumário

I. INTRODUÇÃO

Em 2008, a publicação do artigo "*Bitcoin*: *A Peer-to-Peer Electronic Cash System*"[1] publicado por Satoshi Nakamoto começou a revolução disruptiva das criptomoedas. O que foi considerado como protocolo *bitcoin* aglomerou diversas tecnologias e tinha o objetivo de descentralizar o modelo de confiança necessário para o sistema financeiro. Uma dessas tecnologias, que pode ser considerada central no protocolo é a *Blockchain*, uma vez que seus princípios são eliminar a necessidade da terceira parte confiável, criar sequências de transações imodificáveis e promover comunicação ponto a ponto[2]. A tecnologia funciona como um grande livro-razão onde todas as partes do sistema possuem acesso a esse livro.

Como se pode ver, apesar de a tecnologia ter sido inventada para a solução de um problema específico do setor financeiro, ela é uma ferramenta com características próprias, que pode ser aplicada em outros segmentos. Assim, convém aplicar a ferramenta dentro de situações em que for conveniente. Nesse sentido, a tecnologia já foi aplicada, por exemplo, nos registros de terreno na Suécia[3] e nos registros clínicos de pacientes da Estônia[4].

As suas aplicações são inúmeras[5] e vêm sendo testadas e tendo seus resultados a todo momento. Embora exista aplicação em diversos setores[6], como o objetivo inicial é analisar a sua aplicação no cartório, apenas será analisado, especificamente, esse setor.

---

[1] Nakamoto, S. (2008) *Bitcoin*: A Peer-to-Peer Electronic Cash System. https://*bitcoin*.org/*bitcoin*.pdf
[2] MOUGAYAR, William (2017). Blockchain para Negócios: Promessa, Prática e Aplicação da Nova Tecnologia da Internet. Rio de Janeiro: Alta Books
[3] Prisco, Giulio (2018). Swedish Mapping Authority Pioneering Blockchain-based Real Estate Sales. Disponível em: <https://www.nasdaq.com/article/swedish-mapping-authority-pioneering-blockchain-based-real-estate-sales-cm935347>. Acesso em 02 de junho de 2019
[4] Kersti Kaljulaid (2019). Estonia is running its country like a tech company. Disponível em: <https://qz.com/1535549/living-on-the-blockchain-is-a-game-changer-for-estonian-citizens/>. Acesso em 02 de junho de 2019.
[5] Daley, Sam (2019) *31 Blockchain Companies Paving The Way For The Future*. Disponível em: <https://builtin.com/blockchain/blockchain-companies-roundup> Acesso em 01 de novembro de 2019.
[6] "Os setores que possuem alguma aplicabilidade, de acordo com a consultoria Mckinsey & Company são: Agricultura; Arte e recreação; Automotiva; Serviços Financeiros; Saúde; Seguros; Manufatura; Mineração; Propriedade; Setor Público; Varejo; Tecnologia, media e telecomunicação; Transporte e logística e Serviços de Utilidade Pública."
Carson, Brant. Romanelli, Giulio. Walsh, Patricia. Zhumaev, Askhat. Blockchain beyond the hype: What is the strategic business value. Digital Mckinsey, 2018. Disponível em: <https://www.mckinsey.com/business-*function*s/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value> acessado em: 2 de novembro de 2019.

Em primeiro plano, o artigo primeiro da Lei 8935/94[7], informa que as principais funções dos cartórios são de organização técnica e administrativa destinados a garantir publicidade, autenticidade, segurança e eficácia dos atos jurídicos. Ou seja, sua principal função orbita na relação de segurança jurídica e das bases para que os fatos se façam conhecidos. Dessa maneira, ele é o terceiro de confiança que faz com que as ações civis desde o nascimento até transferência de bens sejam possíveis.

No Brasil, os cartórios são prestadores de serviços notariais e de registro. Esses serviços são regulamentados pela lei nº 8935/94[8] e de acordo com o seu artigo 6º compete aos notários (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; e (iii) autenticar fatos. Enquanto aos tabeliães de notas também compete: (a) lavrar escrituras e procurações públicas; (b) lavrar testamentos públicos e aprovar os cerrados; (c) lavrar atas notariais; (d) reconhecer firmas; (e) autenticar cópias.

Por possuírem uma função tão ampla, os cartórios no Brasil são divididos em oito segmentos diferentes de acordo com o artigo 5º Lei 8935/94: a) cartório de notas; b) cartórios de protesto; c) cartórios de registro de imóveis; d) cartórios de registro de títulos de documentos; e) cartórios de registro civil das pessoas jurídicas; f) cartórios de registro civil das pessoas naturais e de interdições e tutelas; e g) oficiais de registro de distribuição. Seria impossível, pela brevidade do trabalho, discutir a aplicação da tecnologia em todos esses setores. Por esse motivo, será escolhido apenas um dos segmentos para sua aplicação.

O sistema de registro de propriedade deve ser confiável e seguro. Atualmente, 70% da população mundial não possuem o devido registro do seu imóvel[9]. A ausência de acesso formal

[7] Art. 1º Serviços notariais e de registro são os de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos.«http://www.planalto.gov.br/ccivil_03/LEIS/L8935.htm». www.planalto.gov.br. Consultado em 02 de junho de 2019

[8] «http://www.planalto.gov.br/ccivil_03/LEIS/L8935.htm». www.planalto.gov.br. Consultado em 02 de junho de 2019

[9] . "Why Secure Land Rights Matter." World Bank text/HTML, March 24, 2017. Disponível em: http://www.worldbank.org/en/topic/land. Acesso em: 25/11*2019

ao registro de imóvel gera não só problemas econômicos, como problemas de segurança, haja vista que três pessoas, em média, morrem por semana defendendo seus direitos ao seu imóvel ou terreno[10]. De maneira, que se torna urgente o registro correto de propriedade.

Além disso, 20% dos usuários de registro de imóveis admitem terem pago algum tipo de suborno para registrar ou verificar sua propriedade[11]. Isso demonstra o quanto o sistema atual, não vem funcionando da melhor forma possível por ausência de concorrência, na maioria das vezes. De forma, que percebe necessário a descoberta de novos modelos de registro de imóveis.

Os órgãos internacionais vêm reconhecendo o potencial da aplicação da tecnologia. A *World Bank Land and Poverty Conference* de 2016 tinha apenas um texto relacionado a *blockchain*, enquanto a de 2017 já possuía três sessões específicas e diversos artigos[12]. De forma, que mesmo as autoridades internacionais vêm pesquisando sobre os possíveis impactos dessa tecnologia no desenvolvimento dos registros de imóveis.

Nesse contexto, o presente trabalho, pretende apresentar o registro de imóveis por meio da *blockchain*, haja vista que ele tem o potencial de devolver para as pessoas o seu próprio direito de registrar seus imóveis. Para entender esse potencial, o trabalho irá apresentar o contexto inicial de criação do *blockchain*, para entender como funciona e qual são seus níveis de segurança. Em seguida, será apresentado os seus potenciais benefícios, riscos e desafios, para que possa ser feita uma comparação real entre o atual tipo de registro e o proposto com a ferramenta. Contudo, como se trata de implementação de uma tecnologia, isso pode ser feito de diversas formas. Assim, se faz necessário entender os graus de complexidade que já foram imaginados para a implementação, além dos exemplos reais de aplicação em diferentes níveis. Por fim, se pretende apresentar novos campos de exploração para futuras pesquisas e um breve resumo de tudo que foi apresentado.

---

[10] . Jochnick, Chris. “Land Rights and Global Development.” Foreign Affairs, February 7, 2017. Disponível em: https://www.foreignaffairs.com/articles/201 7-02-07/land-rights-and-globaldevelopment. Acesso em: 24/11/2019

[11] Avramov, Yuriy Valentinovich et al. “Registering Property: Using Information to Curb Corruption.” World Bank, December 1, 2017. Disponível em: http://documents.worldbank.org/curated/e n/270331513854675950/Registeringproperty-using-information-to-curbcorruption
Acesso em: 30 de novembro de 2019

[12] Graglia, Michael 2017, “*5 Myths About Blockchains*” NewAmerica Disponível em :https://www.newamerica.org/future-property-rights/blog/5-myths-blockchains-registries/ Acesso em 20/10/2019

2. O PROTOCOLO *BITCOIN*

A *blockchain* foi inicialmente introduzida pelo protocolo *bitcoin* de Satoshi Nakamoto[13]. O objetivo tanto da tecnologia, como do próprio artigo era resolver o "*double-spending problem*"[14], que é a possibilidade de invalidação de uma transação dentro da cadeia de transações (*transaction chain*) utilização dupla da mesma informação. A ferramenta *blockchain* foi introduzida para solução desse problema, o protocolo e o funcionamento da moeda *bitcoin* serão analisados como um todo, com o intuito de entender qual é a função precípua da tecnologia a ser analisada.

Inicialmente, o sistema no qual funciona a rede de *bitcoin*s, nada mais é que um protocolo de segurança. O objetivo final é fazer com que as transações que aconteçam dentro dessa rede tenham confiabilidade. A informação de que a transação de fato aconteceu é o que faz o sistema financeiro funcionar[15].Atualmente, para que ele tenha a confiabilidade, um terceiro independente é atribuído e para garantir que o terceiro funcione de forma idônea, existem leis que o sancionam em caso de má administração desse sistema e indenizam quem seja prejudicado. Nesse cenário, cada vez menos físico da moeda, se torna um desafio maior criar confiança sobre os novos modelos bancários[16]. Por isso, toda explicação abaixo se resume em tentar criar um sistema de transações em que os indivíduos confiem, demonstrando um protocolo de segurança e os motivos da não necessidade de um terceiro independente e de sanções a esse terceiro, por consequência.

2.1 *Bitcoin* Como Livro Razão

[13] Nakamoto, S. (2008) *Bitcoin*: A Peer-to-Peer Electronic Cash System. Disponível em: <https://*bitcoin*.org/*bitcoin*.pdf>
[14] Chohan, Usman W., The Double Spending Problem and Cryptocurrencies (December 19, 2017). disponível em SSRN: https://ssrn.com/abstract=3090174 ou http://dx.doi.org/10.2139/ssrn.3090174
[15] Curott, N. (2017). ADAM SMITH'S THEORY OF MONEY AND BANKING. *Journal of the History of Economic Thought, 39*(3), 323-347. doi:10.1017/S1053837217000396
[16] Singh, S. and Slegers, C. *Trust and electronic money*, Centre for International Research on Communication and Information Technologies, Melbourne, 1997

A tecnologia *blockchain*, e por consequência o *bitcoin*, é uma espécie de Tecnologia de Registro Distribuído (*Distributed Ledger Technology – DLT)* [17], ou seja, funciona, apenas para fins didáticos, como um livro-razão[18]. Sua principal função é registrar todas as transações em uma única plataforma em que todos consigam acesso. Desse modo, os números que constam no livro razão só possuem valor, a partir do momento que as pessoas resolvem que aquele livro tem a função de representar os bens e serviços que constam listados. Nesse caso, esse livro registra a entrada e saída de Bitcoin (BTC) de cada conta, que representam valor real, assim como qualquer moeda.

Para enviar qualquer quantidade de BTC, é necessário transmitir essa informação para toda a rede de *bitcoin*s. Os computadores, mais conhecidos como nós ("nodes") da rede, incluem a transação para dentro da sua própria cópia do livro razão, que repassam a mesma informação para todos os outros nós. Esse é um resumo, muito simplificado, de como funciona a rede de *bitcoin*s.

Apesar dessa explicação parecer muito com a essência do modelo de transferência bancária atual, ele possui uma grande distinção que é a descentralização do livro razão. Desse modo, todos os membros da rede de *bitcoin*s possuem uma cópia do livro razão, enquanto no modelo atual apenas as organizações bancárias possuem tal livro. A inexistência de uma terceira parte intermediadora reduz custos de transação, permite um controle maior e uma fiscalização individual.

2.2 A Transferência de Dinheiro na Rede *Bitcoin*

Em uma relação hipotética de transferência de BTC entre Alice e Bob, existem três problemas claros, relativos a veracidade da mensagem, que podem surgir com apenas essas informações sobre o sistema: (i) Como a rede sabe que a informação de que Alice transfere para Bob veio inicialmente de Alice (Autenticidade)?; (ii) Como se sabe se Alice de fato possui fundos para fazer a transferência?; (iii) Como se sabe se as transferências registradas são imutáveis?

[17] O termo não possui uma tradução clara para português ainda
[18] Driscoll, Scott. "*How Bitcoin Works Under The Hood*". Imponderable Things, jul 14, 2013. Disponível em: <http://www.imponderablethings.com/2013/07/how-*bitcoin*-works-under-hood.html

Se a rede é conectada e qualquer computador integrado na rede possui acesso ao livro razão e capacidade de alterá-lo, qualquer um deles poderia criar, alterar ou forjar novas informações dentro do sistema. Esse problema não existe quando um terceiro confiável detém o controle desse livro-razão e pode ser responsabilizado pelo mau uso dele. Entretanto, se sabemos que a informação é enviada pela pessoa por Alice, e que esta última possuía fundos compatíveis com a transferência e que o histórico de transferências é imutável, podemos afirmar que as informações nos livros razão são confiáveis.

2.2.1 Autenticidade da informação

Para solucionar o problema é preciso entender como solucionar o problema da autenticidade. Se Alice afirma que transferiu *bitcoin*s para Bob, precisamos inicialmente ver se Alice é de fato Alice, para então analisar a informação em si. A solução deste primeiro tópico é respondida pelo autor por meio da assinatura digital[19]

A assinatura digital possui as mesmas funções de uma assinatura física, que é a de dar autenticidade ao documento[20]. Ou seja, sua função central é a de conectar identidade a um pedaço de documento. Isso é feito por meio de um problema matemático que previne a cópia ou fraude. Por se tratar de informações e transações diferentes, a cada transação uma nova assinatura digital é utilizada. Essa assinatura funciona por meio de duas chaves diferentes e

[19] "We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a *hash* of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership" Driscoll, Scott. "*How Bitcoin Works Under The Hood*". Imponderable Things, jul 14, 2013. Disponível em: <http://www.imponderablethings.com/2013/07/how-*bitcoin*-works-under-hood.html>

[20] "A cryptographic primitive which is fundamental in authentication, authorization, and non repudiation is the digital signature. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information. The process of signing entails transforming the message and some secret information held by the entity into a tag called a signature.[...]
[...]Authentication is a term which is used (and often used) in a very broad sense. By itself it has little meaning other than to convey the idea that some means has been provided to guarantee that entities are who they claim to be, or that information has not been manipulated by unauthorized parties. Authentication is specific to the security objective which one is trying to achieve."
A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1997). p. 22-23.

conectadas. Enquanto a *private key* cria a *public key* há a verificação se a assinatura é verdadeira[21].

Como cada mensagem enviada é diferente, não há possibilidade de reutilização, o que impede que indivíduos mal intencionados tenham a possibilidade de forjar a mensagem enviada para a criação da assinatura. Assim, por meio dos problemas matemáticos originados da ECDSA[22] (*Elliptic Curve Digital Signature Algorithm*), apenas quem tem acesso a *private key* pode gerar novas assinaturas e as *public keys* podem verificar a veracidade dessa assinatura. Por isso, a autenticidade é atingida por meio da digital.

Cabe dizer que essa assinatura pode ser imaginada como a chave para abertura da criptografia. A criptografia é pública e o conteúdo que está por trás dela só pode ser acessado através da solução desse problema. Assim, é possível que mais de uma chave seja utilizada como solução do problema para que essa criptografia seja desfeita. Algo como o uso de duas chaves, ou três chaves de um total de quatro e assim por diante. Esse é o conceito de *multisignaturenature wallet* (multisig).

2.2.2 A Transaction Chain

Sobre a solução do segundo problema levantado, quanto a existência de fundos na carteira de Alice, esse é solucionado pela *Transaction Chain*. Nesse momento, é preciso revelar que, de fato, o livro razão que tem sido usado como referência para a explicação do modelo não existe. Na verdade, todo o histórico de transferências é guardado a partir da *transaction chain*.

---

[21] "To spend money, you must prove that you're the true owner of a public key address where money was sent, and you do that by generating a Digital Signature from a transaction message and your private key.[...]
Importantly, because the signature depends on the message, it will be different for every transaction, and therefore can't be reused by someone for a different transaction. This dependence on the message also means that no one can modify the message while passing it along the network, as any changes to the message would invalidate the signature"
Driscoll, Scott. "How *Bitcoin* Works Under The Hood". Imponderable Things, jul 14, 2013. Disponível em: <http://www.imponderablethings.com/2013/07/how-*bitcoin*-works-under-hood.html>

[22] Caso deseje mais informações sobre ECDSA : Moreira, Márcio Aurélio Ribeiro. "*ECDSA (Elliptic Curve Digital Signature Algorithm).*" Tese (Especialização em Segurança da Informação), Segurança da Informação, União Educacional Minas Gerais - Minas Gerais.

Ao invés dos balanços, que normalmente são utilizados para simplificar o registro das transações feitas, a verificação dos históricos de fundos é feita registrando e guardando todas as transações que ocorreram desde a primeira realizada na rede. Dessa forma, essa cadeia de informação tem a possibilidade de gerar um histórico, que pode ser verificado por qualquer máquina da rede.

Nesse contexto, para Bob enviar 0.5 BTC para Alice, ele precisa fazer referência a outras transações em que recebeu a totalidade de 0.5 BTC ou mais. As transações anteriores são chamadas de *inputs*, enquanto a nova transação é chamada de *output*. *Output,* são as novas saídas de dinheiro que estão sendo feitas a partir de *inputs,* que podem ser consideradas as entradas de dinheiro anteriores. Consequentemente, os *outputs* de Alice serão chamados de *inputs* de Bob.

Os pagamentos utilizados são antigas transações realizadas dentro da rede *bitcoin*. Por isso, haverá cenários em que os *outputs* somarão valores maiores do que os *inputs*. Nessa situação, por uma questão de simplificação do sistema e hermeticidade, sempre que os *inputs* forem maiores que os *outputs*, o sistema obriga o transmissor a fazer uma nova transferência de BTC com a diferença dos valores para si próprio. Esse novo *output* de A para o A poderá ser utilizado para novas transferências de *bitcoin*s.

A impossibilidade de se utilizar o mesmo *input* duas vezes faz com que os BTC enviados sejam permanentemente transferidos para a próxima carteira. Assim, o *input* de cada transação é o mecanismo que permite a percepção de fundos no sistema. Para verificar a existência de fundos basta olhar a *Transaction Chain* e perceber que os *inputs* que agora pertencem a um indivíduo na realidade são *outputs* de outra transação. Pode-se perceber, portanto, que a referência a antigas transferências é o que faz com que o sistema se feche e permite que se verifique os fundos de cada carteira.

2.2.3 Imutabilidade

A imutabilidade do sistema pode ser percebida pela análise da assinatura digital e da *transaction chain*. Se fosse possível alterar algum dos *inputs*, ou enviá-los duplamente, não seria possível acreditar na transferência deles. Por isso, o sistema faz com que todo novo nó que adentre ao sistema verifique todas as transações já feitas na história da rede[23].Não é possível

[23] What is a Full node. Disponível em: https://*bitcoin*.org/en/full-node#what-is-a-full-node Acesso em: 4 de outubro de 2019

criar *inputs* sem referência dentro do sistema, nem alterar partes da cadeia, uma vez que todo o processo de transferência depende das transações anteriores. Ainda que fosse possível, a verificação sendo refeita a todo o tempo, mostraria um erro dentro do sistema e impediria que tal transação fosse feita[24].

2.3 O Double-spending Problem e a *Blockchain*:

A transação de Alice para Bob, que foi usada como exemplo hipotético anteriormente, pode ser entendida, normalmente, como Alice paga Bob com dinheiro, no intuito de receber algum produto ou serviço em troca disso. Se tudo ocorrer corretamente, Alice recebe o produto ou serviço, Bob recebe os BTC e a obrigação é cumprida. Dessa maneira, não haveria necessidade de utilização do *blockchain*.

O *Double Spending Problem* consiste no envio da mensagem de que Alice enviou o comando de pagamento para Bob, ele por consequência envia o produto, mas enquanto a mensagem de pagamento de Alice é repassada para a rede, uma nova mensagem pode ser enviada dizendo que Alice pagou a própria Alice com o mesmo *input* utilizado para pagar Bob. A depender da velocidade de transmissão da informação dentro da rede, dois resultados podem acontecer: (i) ou a mensagem do pagamento de Alice para Bob será invalidada pela rede ou (ii) a mensagem de Alice para Alice será invalidada pela rede.

Um *double-spending attack* bem sucedido resulta na parte que deveria receber o dinheiro sem o seu produto e sem o pagamento. A mera insegurança de que ambos os processos podem ocorrer, a depender da velocidade de transmissão, faz com que a confiança dos pagamentos dentro da rede seja inviável. Esse é um problema de sincronização, que é resolvido por meio da *blockhain*[25].

---

[24] "Once a transaction has been used once, it is considered spent, and cannot be used again. Otherwise, someone could double-spend an *input* by referencing it in multiple transactions. So, when verifying a transaction, in addition to the other checks, nodes also make sure the *inputs* have not already been spent. To be explicit, for each *input*, nodes check every other transaction ever made to make sure that *input* has not already been used before. While this may seem time consuming, as there are now over 20 million transactions, it's made fast with an index of unspent transactions."idem 3

[25] "This is a problem of synchronization - there needs to be some universally accepted signal indicating that some transaction is final and that no conflicting transaction can ever be accepted. Given two conflicting transactions, it does not really matter which of them will be accepted, as long as there is a way to know that one transaction has been accepted and can no longer be reversed.

2.3.1 O *Blockchain*

A *blockchain* é usada para ordenar as transações, diferentemente da *transaction chain*. Enquanto a primeira ordena, a segunda mantém registro de quem possuiu os BTC no passado. Nesse sentido, a *blockchain* será apresentada em um contexto geral, antes de ser demonstrado como ele soluciona o problema do *double-spending*.

Cada bloco é composto por meio de um grupo de transações que aconteceram ao mesmo tempo. Nesse cenário, as transações podem ser divididas entre as confirmadas e as não confirmadas, sendo a primeira as que foram incluídas na *blockchain*, e a segunda as transações que serão incluídas a depender de sua validade. É preciso dizer também, que um bloco sempre possui referência ao seu bloco anterior, de maneira que estes se encadeiam a partir dessa linha histórica de formação de blocos.

Como qualquer bloco pode enviar informações sobre qual deve ser o próximo da lista, isso poderia gerar um problema de ordem. Por isso, os blocos não se organizam por meio de ordem de chegada. Eles são organizados por meio da ordem de resolução de um problema matemático, que envolve a leitura de um bloco somado a um *nonce (number only used once)* através de um *cryptographic hash*, com o intuito de o resultado dessa função ser menor do que um número em específico. Nesse sentido, a *Hash function* deve ser organizada da seguinte forma: Identidade do antigo bloco (*hash output*) + transações + *nonce* = *hash result*. O *hash result* deve ser menor do que um número X.

A *hash function* é uma função que transforma qualquer texto em um resultado encriptado. Nesse caso, se a função *hash* escolhida é a SHA256 e o resultado em questão é de 32 *bytes*, uma vez que se trata da *bitcoin*. Apesar disso, as funções *Hash* possuem outras estruturas com suas características próprias. Para alguns especialistas, a SHA 256 é a função

---

Bitcoin solves this with a proof-of-work system: Computational effort (consisting in the calculation of *hash*es) is spent on acknowledging groups of transactions, called blocks; and a transaction is considered final once sufficient work has gone into acknowledging the block that contains it. By linking the blocks to form a chain, the total work spent on any transaction is perpetually increasing, making it difficult to elevate any conflicting transaction to the same confirmation status without a prohibitive computational effort."
Rosenfeld, M. 2012a. Analysis of *hash*rate-based double-spending.pg 2. http://arxiv.org/abs/1402. 2009

que melhor combina velocidade e segurança[26], por isso deve ter sido a função escolhida por Satoshi Nakamoto, em detrimento de outras. Nessa função qualquer que seja a alteração, mesmo que um único dígito da mensagem, toda a sua estrutura é alterada.

A única forma de descobrir qual seria o resultado desse algoritmo é por meio de tentativas contínuas, uma vez que, apesar da estrutura do bloco ser sempre a mesma, a mínima mudança na estrutura do texto encriptado pode trocar completamente o resultado da função. Pela dificuldade de se solucionar um bloco, um cálculo é feito para que o tempo para todos os computadores da rede de *bitcoin*s, em conjunto, consiga resolver um bloco inteiro no tempo de 10 minutos. Isso tem o intuito de manter equilibrada segurança com a praticidade e velocidade do sistema. Tornando assim, o sistema quase impossível de possuir dois nós enviando o sinal ao mesmo tempo de qual deve ser o próximo bloco da *blockchain*.

Apesar disso, ocorre, mesmo que raramente, a solução de dois blocos ao mesmo tempo. Para solucionar isso, os blocos que são solucionados e recebidos ao mesmo tempo na rede serão entendidos por diferentes nós, como os corretos. Nesse caso, ambos os blocos seguem na rede, até que o próximo bloco seja solucionado.

A estatística diz que a chance dessa situação ocorrer duas vezes é ainda menos provável. Isso somado a regra de que sempre o maior ramo da cadeia seja preterido frente ao menor, faz com que a rede se estabilize rapidamente.

Isso porque, na ocorrência da possibilidade de ambos os blocos sejam solucionados ao mesmo tempo, cada nó entenderá um dos blocos como o correto. Todavia, o outro bloco não será descartado e ficará em espera. Como a rede sempre preferirá a maior cadeia, ele aceitará a maior cadeia em sequência que sair do resultado da segunda solução e invalidará as cadeias menores a partir de onde estiverem os erros. Isso resulta em apenas uma cadeia real e estável, solucionando, assim, o problema de ordenamento dos blocos.

2.3.2 A solução do *Double Spending Problem*:

[26] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1997).

O *double-spending problem* ocorre quando existem duas mensagens conflitantes, como já foi apresentado. A partir das informações que já temos, sobre a aceitação da maior cadeia de blocos, existem duas formas de se executar o *Double Spending attack*: (a) criando uma cadeia prévia maior do que a cadeia de blocos que vai ser conectada (b) processando as tentativas mais rápido do que a rede de computadores. Ambas as formas são impossíveis de acontecer por causa da *blockchain* como será demonstrado abaixo.

O primeiro tipo de ataque tem sua solução apenas com as informações que já foram explicadas até o presente momento. É impossível construir previamente uma cadeia de blocos. Isso porque, como explicado anteriormente, o *hash output* do último bloco da cadeia é utilizado como parte da fórmula para a solução do novo bloco. Dessa maneira, para criar uma cadeia, ela deve partir da informação da solução do último bloco já solucionado.

A única forma possível seria conseguir processar o bloco numa velocidade maior do que toda a rede de computadores em conjunto, que é a segunda opção de ataque sugerida. Nesse contexto, temos uma corrida entre o poder de processamento da cadeia com a informação fraudulenta (cadeia desonesta) e o da cadeia com informações reais sobre a transação (cadeia honesta).

Por se tratar da parte central da confiabilidade da ferramenta *blockchain*, esse será o único cálculo explicado dentro do presente texto. Sendo necessário informar, que se trata de calcular a probabilidade de um ataque bem-sucedido ocorrer. Por isso, Rosenfeld estuda o funcionamento dessa corrida entre as duas cadeias no seu paper "*Analysis of hashrate-based double-spending*" [27]. O objetivo desse cálculo é demonstrar o motivo por qual o *blockchain* é estruturado com o modelo de aceitar apenas a cadeia maior. Passo então a explicar o cálculo de Rosenfeld.

Para modelar isso é preciso, inicialmente, definir previamente dois pontos:

[27] Rosenfeld, M. 2012a. Analysis of *hash*rate-based double-spending.. http://arxiv.org/abs/1402. 2009

(i) A *hashrate*[28] da rede honesta em conjunto com a rede desonesta é constante[29]. Nesse sentido, o *Hashrate* total é chamado de H, onde pH é a *hashrate* da rede honesta e qH a da rede desonesta. Assim temos, p + q = 1 e H = pH + qH.

(ii) A dificuldade para solucionar um bloco é constante, como foi dito anteriormente, de forma que a *hashrate* sempre é H e o tempo para achar um bloco é sempre T.

Sabendo disso, podemos afirmar que Z = N - M[30]. Cabe dizer que toda vez que um novo bloco é solucionado o valor de Z muda, sendo o novo resultado Z_{+1} = Z + 1 caso o bloco seja da cadeia honesta e Z_{+1} = Z - 1, caso o bloco seja da cadeia desonesta. Assim, se N<M, ou seja, Z = - 1, a rede desonesta vence e *double-spending attack* acontece. Por se tratar de se Z se torna -1 em algum momento e não quando, estamos falando de uma Cadeia de Markov[31] com tempo discreto[32].

O resultado de tudo que foi exposto até agora é que o primeiro cenário em que Z_{+1} = Z + 1 tem a probabilidade "p" de acontecer, enquanto Z_{+1} = Z - 1 tem a probabilidade "q" de acontecer. Rosenfeld estabelece Az como a probabilidade de o *double-spending attack* ocorrer de forma bem-sucedida. Dessa forma, quando Z < 0, Az = 1, uma vez que quando Z for menor que zero o ataque já terá sido bem sucedido. Sabendo que a probabilidade do próximo bloco a ser solucionado de uma cadeia honesta tem a probabilidade de "p" e chance de sucesso de A_{z+1}, e que a probabilidade de um bloco da cadeia desonesta ser encontrada é de "q" e sua taxa de sucesso é de A_{z+1}, podemos ter a seguinte relação:

$$Az = pA_{z+1} + qA_{z-1}$$

[28] *Hash*rate pode ser definida, de forma simplificada, como a velocidade de processar a *hash function*, ou seja, a velocidade de se solucionar um bloco.
[29] O somatório de ambos é constante porque só existem as duas possibilidades, ou a rede desonesta irá ganhar ou a rede honesta irá ganhar, dentro de toda a *hash*rate do sistema.
[30] Z= número de blocos que a cadeia honesta tem a mais que a cadeia desonesta; N = número de blocos que já existem antes da indecisão na cadeia honesta e M = Número de blocos da cadeia desonesta
[31] O processo estocástico da cadeia de Markov possui características específicas. Cabe ressaltar apenas a propriedade que indica que numa cadeia de Markov apenas o estado anterior deve ser levado em consideração para realização dos cálculos e não todos os processos.
[32] Rosenfeld, M. 2012a. Analysis of *hash*rate-based double-spending.. pg 5 http://arxiv.org/abs/1402.2009

Sabendo que a relação de p + q = 1 e que se trata de uma cadeia de Markov com as características supracitadas pode-se entender que:

$$Az = \min\left(\frac{q}{p}, 1\right)^{\max(z+1,0)} = \begin{cases} 1, & se\ \ z < 0\ ou\ q > p \\ \left(\frac{q}{p}\right)^{z+1}, & se\ \ z \geq 0\ ou\ q \leq p \end{cases}$$

Nesse caso Rosenfeld se utiliza de dois gráficos para ilustrar as conclusões, que podem ser abstratas, acima. Os gráficos são os seguintes:

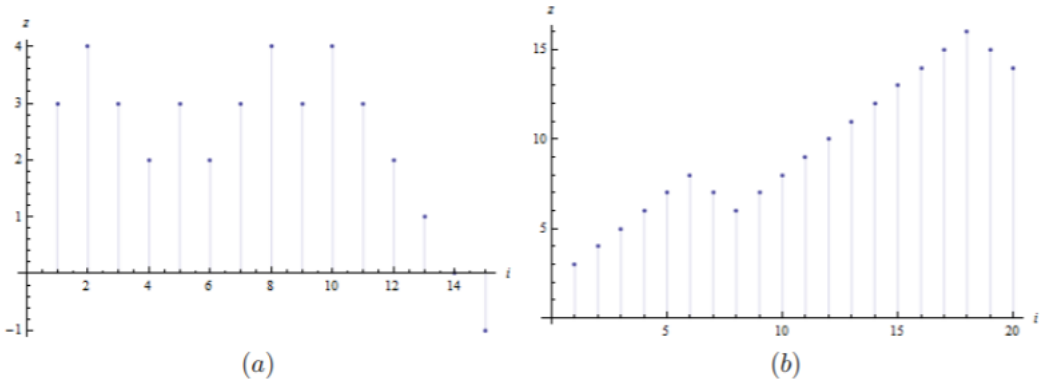

Figura 1 - *Rosenfeld, M. 2012a. Analysis of hashrate-based double-spending.. pg 06 http://arxiv.org/abs/1402. 2009*

Os gráficos pretendem demonstrar duas tentativas, ambas partindo de Z = 3, a primeira com 15 solução de blocos, sendo realizados tanto pela rede honesta quanto desonesta, e a segunda com 20 soluções. No gráfico (a) é possível ver uma tentativa bem-sucedida de ataque ao sistema, enquanto no gráfico (b) uma tentativa sem sucesso de ataque.

Três conclusões podem ser obtidas do conjunto dos gráficos, cálculos e informações anteriores. Rosenfeld afirma[33]:

“

- *The probability of success depends on the number of blocks, and not on the time constant $T_{0;}$*
- *If the attacker controls more than half of the total network hashrate, he always succeeds in catching up, from any disadvantage;*

[33] Rosenfeld, M. 2012a. Analysis of *hash*rate-based double-spending.. pg 06 http://arxiv.org/abs/1402. 2009

- *When q < p, the probability of success decreases exponentially with the disadvantage z; the lower the q is, the faster the decay*."

A primeira conclusão pode ser extraída tanto do gráfico, quanto da consequência de se tratar de uma Cadeia de Markov com tempo discreto. Enquanto as outras conclusões são vistas com o conjunto do gráfico com a fórmula para Az.

Sabendo que Z é o fator central para entender o quão confiável é a rede, é preciso em seguida entender qual o valor do número de blocos solucionados da rede honesta "n" faz com que a rede seja confiável o suficiente. Isso porque, é possível e comum, que negociantes esperem para enviar sua mercadoria após um número específico de confirmações, ou no caso em questão de solução de blocos em sequência.

Rosenfeld afirma que Nakamoto, no texto original do protocolo, aplica uma simplificação do modelo e por isso, não utilização uma Distribuição de Poisson como modelo, mas sim uma Distribuição binomial negativa. Assim, como a última distribuição pretende analisar o número de sucessos (pela rede desonesta) antes de falhar n vezes (pela rede honesta), com a probabilidade q de sucessos, esse será o modelo seguido. Assim a probabilidade para um valor de m (número de blocos pela rede atacante) específico é:

$$P(m) = \binom{m+n-1}{m} p^n q^m$$

Rosenfeld adota a corrida entre as duas redes a partir do resultado Z_{+1} = m - 1, uma vez que ele acredita que a rede desonesta deve começar o ataque a partir do primeiro bloco. Dessa forma Z = m – n – 1. Assim de acordo com o Rosenfeld, a probabilidade do double-spending *attack* acontecer, após n confirmações é:

$$R = \sum_{m=0}^{\infty} P(m) A_{n-m-1}$$

$$\sum_{m=0}^{n-1} \binom{m+n-1}{m} p^n q^m \left(\min\left(\frac{q}{p}, 1\right)\right)^{n-m} + \sum_{m=n}^{\infty} \binom{m+n-1}{m} p^n q^m$$

$$= \begin{cases} 1 - \sum_{m=0}^{n} \binom{m+n-1}{m} (p^n q^m - p^m q^n), & se\ q < p \\ 1\,, & se\ q \geq p \end{cases}$$

Como a equação é complicada de retirar conclusões a partir dela, a tabela abaixo reflete melhor a probabilidade de um ataque bem-sucedido, em função da *hashrate* da rede desonesta *q* e o número de confirmações:

q	1	2	3	4	5	6	7	8	9	10
2%	4%	0.237%	0.016%	0.001%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
4%	8%	0.934%	0.120%	0.016%	0.002%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
6%	12%	2.074%	0.394%	0.078%	0.016%	0.003%	0.001%	≈ 0	≈ 0	≈ 0
8%	16%	3.635%	0.905%	0.235%	0.063%	0.017%	0.005%	0.001%	≈ 0	≈ 0
10%	20%	5.600%	1.712%	0.546%	0.178%	0.059%	0.020%	0.007%	0.002%	0.001%
12%	24%	7.949%	2.864%	1.074%	0.412%	0.161%	0.063%	0.025%	0.010%	0.004%
14%	28%	10.662%	4.400%	1.887%	0.828%	0.369%	0.166%	0.075%	0.034%	0.016%
16%	32%	13.722%	6.352%	3.050%	1.497%	0.745%	0.375%	0.190%	0.097%	0.050%
18%	36%	17.107%	8.741%	4.626%	2.499%	1.369%	0.758%	0.423%	0.237%	0.134%
20%	40%	20.800%	11.584%	6.669%	3.916%	2.331%	1.401%	0.848%	0.516%	0.316%
22%	44%	24.781%	14.887%	9.227%	5.828%	3.729%	2.407%	1.565%	1.023%	0.672%
24%	48%	29.030%	18.650%	12.339%	8.310%	5.664%	3.895%	2.696%	1.876%	1.311%
26%	52%	33.530%	22.868%	16.031%	11.427%	8.238%	5.988%	4.380%	3.220%	2.377%
28%	56%	38.259%	27.530%	20.319%	15.232%	11.539%	8.810%	6.766%	5.221%	4.044%
30%	60%	43.200%	32.616%	25.207%	19.762%	15.645%	12.475%	10.003%	8.055%	6.511%
32%	64%	48.333%	38.105%	30.687%	25.037%	20.611%	17.080%	14.226%	11.897%	9.983%
34%	68%	53.638%	43.970%	36.738%	31.058%	26.470%	22.695%	19.548%	16.900%	14.655%
36%	72%	59.098%	50.179%	43.330%	37.807%	33.226%	29.356%	26.044%	23.182%	20.692%
38%	76%	64.691%	56.698%	50.421%	45.245%	40.854%	37.062%	33.743%	30.811%	28.201%
40%	80%	70.400%	63.488%	57.958%	53.314%	49.300%	45.769%	42.621%	39.787%	37.218%
42%	84%	76.205%	70.508%	65.882%	61.938%	58.480%	55.390%	52.595%	50.042%	47.692%
44%	88%	82.086%	77.715%	74.125%	71.028%	68.282%	65.801%	63.530%	61.431%	59.478%
46%	92%	88.026%	85.064%	82.612%	80.480%	78.573%	76.836%	75.234%	73.742%	72.342%
48%	96%	94.003%	92.508%	91.264%	90.177%	89.201%	88.307%	87.478%	86.703%	85.972%
50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Figura 2 *Rosenfeld, M. 2012a. Analysis of hashrate-based double-spending.. pg 10 http://arxiv.org/abs/1402. 2009*

A tabela levanta três pontos principais, em relação ao que pretende ser estudado nesse trabalho: (i) Se a rede desonesta possuir metade ou mais da rede global de *Bitcoin*s, o ataque sempre será bem-sucedido; (ii) Não há nada de relevante dentro do mito normalmente citado das 6 confirmações para as garantia das transações, é apenas o primeiro número que com 10% da rede, que se considerava muito improvável de se obter, que resulta em menos de 0.1% de chance de sucesso para a rede desonesta; (iii) Esperar por mais confirmações reduz exponencialmente a taxa de sucesso do *double-spending attack.* (iv) É possível que uma tentativa de *double-spending attack* ocorra com qualquer *hashrate* da rede desonesta. Com esses dados se torna possível comparar a probabilidade de se burlar tanto uma rede com um terceiro independente, quanto com o *blockchain* amparado no *Bitcoin*.

A partir de todo o exposto no capítulo, é possível afirmar que o *blockchain* é um mecanismo para registrar transferências, de forma que se tem todo o acesso possível, de forma descentralizada. Entretanto, ainda que digam que ele é um mecanismo inviolável[34], ele possui riscos inerentes, que precisam ser entendidos antes de se aplicar a tecnologia[35]. Além de que por se basear na estatística, mesmo que se trate de um evento extremamente improvável, na maioria dos casos, ainda não seria possível afirmar que o risco é inexistente, mesmo com o menor dos poderes de processamento pela rede desonesta. Dessa forma, é possível dizer que ele possui suas funções, elas são relevantes e disruptivas, mas não é inviolável.

3. APLICAÇÃO DE *BLOCKCHAIN* NO SETOR CARTORÁRIO

A *blockchain* não precisa ser aplicada apenas no seu contexto original. Ela possui o potencial de revolucionar o mundo digital permitindo que toda e qualquer transação *online* de qualquer coisa possa ser registrada e verificada a qualquer momento[36]. De forma que normalmente é vendido como uma Máquina para gerar Confiança[37]. Por isso, essa tecnologia vem sendo aplicada em diversos contextos tanto financeiros (como foi originalmente concebido), quanto não-financeiros.

Para cada um desses setores, existem modelos diferentes de *blockchain*s sendo estudados e utilizados através do mundo. A existência de *sidechains, alternative chains e Colored Coins*[38], viabilizam o uso de uma *blockchain* pública e já operante, sem necessidade

---

[34] "*Blockchain, a base de dados inviolável do mercado mundial"* INFOMONEY, Disponível em: https://www.infomoney.com.br/patrocinados/noticias-corporativas/blockchain-a-base-de-dados-inviolavel-do-mercado-mundial/ Acesso em: 29/11/2019

[35] Os riscos específicos para o setor Cartorário serão explicados, em seu contexto específico, nos capítulos 3 e 4.

[36] Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman (June, 2016). Blockchain Technology: Beyond *Bitcoin*. Applied Innovation Review. Issue No. 2. Pantas and Ting Sutardja Center for Entrepeneurship & Technology. Berkeley Engineering. UC Berkeley. pg. 8.

[37] The Trust Machine, ECONOMIST, 2015. Disponível em: <https://www.economist.com/leaders/2015/10/31/the-trust-machine> acessado em:2 de novembro de 2019.

[38] "Alternative blockchains: a system of using the blockchain algorithm to achieve distributed consensus on a particular digital asset. The system may share miners with a parent network such as *Bitcoin*'s, which is called merged mining. These Alternative blockchains have been suggested to implement applications such as DNS, SSL certification authority, file storage and voting.
Colored Coins: An open source protocol that describes a classes of methods for developers to create digital assets on top of *Bitcoin* blockchain by using its *function*alities beyond digital currency.
Sidechains: Alternative Blockchains which are backed by *Bitcoin*s via a *Bitcoin* Contract, just as dollars and pounds used to be backed by Gold. One can possibly have a thousands of sidechains "pegged" to

de criação da própria rede de *blockchains* privadas, o que possibilita a criação de *blockchains* que não necessariamente tem a finalidade financeira. Destaca-se, principalmente, a *Colored Coins*[39], protocolo utilizado para usar ativos reais no sistema que é digital, por meio da coloração.

Sabendo do escopo, que foi apresentado durante a introdução, pelos motivos já expostos, a presente seção irá demonstrar quais são os impactos positivos, riscos e críticas já imaginadas ao se aplicar tamanha mudança no sistema de registro de imóveis.

3.1 Benefícios

Qualquer transação de bens, atualmente, possui não só o custo de produção do bem, mas também envolvem os custos de transação[40]. De acordo com Coase, esses custos podem ser definidos em: (i) Custos de informação; (ii) Custos de Barganha e (iii) Custos de Policiamento. Assim, os custos de informação podem ser definidos nos custos de pesquisa para o melhor preço, ou de próprio conhecimento do produto, enquanto os custos de barganha podem ser definidos no consenso entre comprador e vendedor conseguirem achar um preço justo para o produto ou serviço sendo vendido. Por último, os custos de policiamento são os custos que visam garantir que o acordo definido venha de fato a ocorrer. Dessa maneira, os custos de transação que podem ser reduzidos por meio dos Registros de Imóveis são a redução dos custos com pesquisa sobre a situação do produto oferecido, principalmente se ele pertence a quem está vendendo, além de reduzir os custos de policiamento, que garante que o imóvel terá efetivamente sido transferido por meio de seu registro, ao fim da transação.

É fácil perceber que a presença de uma ferramenta que faz por si só o registro, pode reduzir parte dos custos de transação. A Goldman Sachs estima que essa tecnologia por si só, poderia ter impactos da ordem de 2 a 4 bilhões de dólares por ano[41] nos custos relacionados

bitcoin, all with different characteristics and purposes, and all of them taking advantage of the scarcity and resilience guaranteed by *Bitcoin* blockchain. In turn, the *Bitcoin* Blockchain can iterate to support additional features for these experiemental Sidechains, once they have been tried and tested."
Idem 35. Pg 13.

[39] *Colored Coins* é um protocolo para representar ativos reais dentro de uma plataforma de blockchain. Para mais informações sobre como funcionam as *Colored Coins* e o *Coloring Scheme*, em seu contexto original acesse: "*Colored : Coins Colored Coins Protocol Specification"* https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification

[40] Coase, R. H., The Nature of the Firm (1937). Economica (new series), Vol. 4, Issue 16, p. 386-405 1937. Available at SSRN: https://ssrn.com/abstract=1506378

[41] Goldman Sachs Group (2016) "Profiles in Innovation: Blockchain – Putting Theory into Practice" pg 7. Disponível em: <https://pgcoin.tech/wp-content/uploads/2018/06/blockchain-paper.pdf> Acesso em: 22 de outubro de 2019

com *title insurance*[42]. Isso porque, seriam eliminados os custos de confirmação dos títulos, haja vista que se trata de uma ferramenta que permite o registro distribuído e imutável, como previamente já visto.

Além de questões financeiras, situações de perda de documentos, e por consequência perda de direito, por motivos de catástrofes naturais, incêndios etc. poderiam ser evitados. No caso do Haiti, onde uma incontável quantidade de direitos de propriedade foi perdida durante o terremoto[43], os problemas com os registros que já haviam sido feitos e estavam mantidos por meio da rede de cartórios, não teriam sido perdidos, por não se tratar de algo físico. Há de se ressaltar, que como a própria matéria indica, os problemas com registro dos direitos de propriedade no Haiti são muito maiores do que apenas o terremoto, mas foram amplificados depois deles.

Soma-se a isso a redução dos custos das próprias transações, que hoje envolvem diversos intermediários. Inclusive, 10% de todo o custo da venda de uma casa nos Estados Unidos são gastos com custos de transação[44].

A segunda informação sobre o fracionamento do direito de propriedade, e por consequência, os dividendos provenientes do aluguel, não pode ser considerado uma novidade, haja vista que por meio dos Fundos de Investimento Imobiliários já é possível fazer isso sem a necessidade da tecnologia. O que vem de positivo para essa relação é a redução dos custos com administração e taxa de performance, que normalmente são cobrados dos quotistas desses fundos.

---

[42] O Title insurance não é desenvolvido no Mercado brasileiro de Imóveis. Entretanto, outras empresas estrangeiras trabalham com fazendo seguros desse tipo dentro desse mercado no Brasil.

[43] Moloney, Anastasia "Unclear land rights hinders Haiti's reconstruction", Thomsom Reuters Foundation News, 5 de julho de 2010. Disponível em: http://news.trust.org/item/20100705105000-axvt3/?source=spotnewsfeed Acesso em: 2 de novembro de 2019

[44] "In the longer term, blockchain-based registries could allow peer-to-peer asset transfers, reducing transaction times from months or weeks to minutes. Transaction costs could come down from thousands of dollars per sale to a modest service fee.The ease and security of transactions could also permit the efficient unbundling of property rights. A landowner could sell and easement to a neighbor quickly and cheaply. Investors could buy small shares in a rental property and receive their portion of the rent via an automated payment."
Graglia, J. M., and Mellon, C. 2018. "Blockchain and Property in 2018: At the End of the Beginning," Innovations: Technology, Governance, Globalization (12:1-2), pp. 90-116.

A oferta desse tipo de investimento também cresceria, uma vez que atualmente os Fundos de Investimento Imobiliários funcionam principalmente em torno de shoppings, lajes corporativas e galpões de logística. Nesse contexto, seria possível fazer o aluguel de uma casa para o *Airbnb*, por exemplo, por meio de dois donos, cada qual com sua participação do direito de receber dividendos dessa casa. Ainda seria possível automatizar esse contrato por meio dos *smart contracts*[45], e reduzir ainda mais os intermédios e a necessidade de realização de contratos físicos e contato entre as partes. Vale ressaltar também que, haveria uma maior democratização do acesso a esses fundos, já que não seria necessário a criação de uma pessoa jurídica nova, mas apenas fracionar a venda, ou aluguel de um bem, por meio do acesso a mais de uma carteira.

Ademais, a maior evolução de um modelo para o outro ainda consiste na redução da chance de acontecer qualquer tipo de erro humano durante as transferências, ou mesmo a possibilidade de haver fraudes. Atualmente, os *title insurances* existem principalmente por causa de quatro tipos de demanda[46], não necessariamente nessa ordem de relevância: (i) Erros no registro; (ii) Penhoras não descobertas; (iii) Heranças não descobertas e (iv) fraude. Não seria possível reduzir todo e qualquer problema. Heranças e penhoras que não se tornaram públicas ainda não poderiam ser resolvidas. Entretanto, num sistema que não circulasse informação apenas relacionadas a propriedade, mas que se relacionasse com outras informações judiciais, seria possível alterar a possibilidade de troca de um imóvel apenas com o aval de uma segunda carteira, como, por exemplo, o judiciário, por meio das *multisignaturenature wallets*. Dessa forma, seria possível solucionar problemas relacionados a outras informações que estivessem disponíveis na rede descentralizada.

Em relação a fraude, atualmente, as pessoas que têm acesso ao controle da plataforma central, seja honestamente, por meio de suas funções, ou desonestamente por meio de um ataque a rede, tem possibilidades de alterar o registro de qualquer propriedade dentro dessa rede. Isso levando em consideração apenas os cartórios que já estão completamente digitalizados. Os cartórios que operam apenas fisicamente, tem problemas maiores e não deveriam tentar fazer a

[45] Contratos automáticos que normalmente utilizam o Ethereum, uma outra criptomoeda, como base. Para mais informações: Buterin, Vitalik *Ethereum White Paper: A next generation smart contract & decentralized application platform.* Disponível em: <https://github.com/ethereum/wiki/wiki/White-Paper> Acesso em: 22 de outubro de 2019

[46] Lulich, Jordan (2018) What is Title Insurance and Why is it important? Forbes. Disponível em: < https://www.forbes.com/sites/jordanlulich/2018/06/21/what-is-title-insurance-and-why-its-important/#747a361612bb> Acesso em: 2 de novembro de 2019

transição direta entre cartório físico direto para uma estrutura sem cartórios, por exemplo, como será visto mais à frente.

Os erros humanos podem ser resolvidos reduzindo também o impacto dos seres humanos no trânsito de documentos, ou nas próprias alterações e confecções deles. Nesse caso, a aplicação da tecnologia reduzindo a quantidade de intermediadores, faz com que a troca de informações possa ser menos danosa.

Há de se dizer que o acionamento desses seguros tem uma taxa bastante elevada e esses erros podem ter impactos relevantes na vida de qualquer indivíduo, haja vista a importância do direito à moradia na vida de um cidadão médio. De acordo com a matéria sobre *title insurances* da Forbes[47]:

> "The reality is that title insurance has protected a large amount of insureds, but it really hasn't proportionality paid out that many claims. An estimated 4-5% of title insureds have been paid on their policy. However, these problems protected by the claims were unlikely to be detected by an ordinary purchaser. Only title insurance would protect the homeowner purchasers."

É possível possuir taxas muito menos significativas do que essas. Obviamente, também, esse valor entre 4% e 5% é apenas dos problemas ocorridos, que foram percebidos pelas seguradoras, dentro do contexto estadunidense. É possível imaginar que cartórios menos bem desenvolvidos possam ter problemas maiores e que existam problemas que não estão sendo levados em consideração, por não terem sido descoberto, o que faz essa taxa ser ainda maior.

3.2 Riscos:

Existem riscos inerentes a todas as plataformas, essa parte do texto pretende elencar os mais relevantes. Há de se mencionar, que alguns riscos podem ser solucionados com a própria noção dos pré-requisitos que serão apresentados na próxima sessão. Dessa maneira, apenas os riscos que não são resolvidos por eles serão apresentados nessa parte. O primeiro risco explicado será relativo à história do DAO (Decentralized Autonomous Organization) e sua

[47] Idem 45.

relação com o *Code is Law*, enquanto a segunda será a discussão sobre o risco de o computador quântico deturpar as estatísticas necessárias para o correto funcionamento do *blockchain* e a terceira sobre as *mining pools*.

3.2.1 *Code is Law*: o caso DAO.

O primeiro risco é relacionado a diminuição do conceito máximo que vem sido aplicado por trás das explicações da associação da programação ligada ao direito: o *Code is Law*[48]. O Incidente DAO, demonstra que erros humanos podem acontecer e o código pode não prever todas as situações, por mais que o *blockchain* seja válido ainda.

O DAO, Fundo de Venture Capital que tentou aplicar os *smart contracts* supracitados por meio da moeda Ethereum, com o valor total era de US$ 250.000.000,00 (cinquenta milhões de dólares). Acontece que uma das pessoas encontrou uma brecha[49] no sistema e conseguiu extrair US$ 60.000.000,00 (sessenta milhões de dólares)[50].

Por consequência disso, a Ethereum precisou aplicar um *hard fork*, que nada mais é que a troca de um código por outro, criado a partir de uma atualização. A partir dali duas seriam as possibilidades, as pessoas poderiam continuar com a rede nova ao instalarem a nova atualização com as novas regras, ou poderiam continuar com o modelo que já possuíam. As mudanças podem ser de várias ordens, mas nesse caso em específico, tinha o único objetivo de consertar os problemas criados pelo *hacker*.

---

[48] É a ideia de que o código por si só consegue implementar o enforcement necessário para o funcionamento adequado da lei. Caso queira ler mais sobre o assunto: Lessig, Lawrence (2000), Code and Other Laws of Cyberspace.

[49] O hacker utiliza o termo loophole, como no direito americano para brecha legal.

[50] "I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ehter. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the DAO for this reward. It is my understanding that the DAO code contains this feature to promote decentralization and encourage the creation of "child DAO's". I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law. For reference please review the terms of DAO"
Benito Arruñada, Blockchain's Struggle to deliver impersonal Exchange, 19 Minn, J.L. Scl & Tech. 55 (2018) Disponível em: <https://scholarship.law.umn.edu/mjlst/vol19/iss1/2> Acesso em: 27 de outubro de 2019

Independentemente do que houvesse a partir desse ponto, um resultado é claro: a descentralização máxima e a aplicação do *Code is Law*, não seria possível, ao menos não da forma em que foi concebida. Além disso, a imutabilidade do sistema também foi colocada em cheque, uma vez que na cadeia mais nova após o *fork*, teve sua ordem alterada por um dos membros, mesmo que aceito pelo resto da cadeia que continuou nessa linha do tempo da cadeia de blocos.

Em consequência do *hard fork* duas moedas seguiram, e em certo ponto a cadeia clássica começou a ser chamada de ETC (Ethereum Classic). Essa moeda chegou a ficar entre as três maiores criptomoedas[51], atrás apenas do *Bitcoin* e do Ether (moeda da rede após a atualização). Muitos dizem que esse pode ser um momento, após um *fork*, em que as pessoas escolhem democraticamente qual seria o melhor caminho para seguir para a moeda, demonstrando seu verdadeiro caráter descentralizador.

Entretanto, isso só aconteceria, em um mundo onde todos têm conhecimento da programação em questão, e que possuísse apenas cidadãos completamente racionais. Sabemos por meio da Economia Comportamental[52] que isso não verdade. Por meio da ignorância, ou mesmo da comodidade, as pessoas poderiam continuar na rede original, por não saber do que se trata a atualização, ou por ser mais confortável para elas do que mudar para a nova rede, mesmo que ela seja a mesma, apenas com a aplicação da correção.

Arruñada afirma que após isso, a parte de execução da lei não deva ser realizada por meio do *Code is Law*, mas ainda por meio do poder judiciário.[53]

---

[51] Idem 50 pg 72

[52] KOROBKIN, R. B. e ULEN, T. S. Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics, California Law Review, vol. 88, n. 4, jul. 2000. p. 1074-1075.

[53] "However, even if the goal of Ethereum Classic was to preserve the immutability of the blockchain and the conclusiveness of transactions, its claims of code-as-law were somehow diluted, by recognizing that 'the infrastructure is not there to enforce and uphold law, it's only a protocol that allows execution of immutable transactions and programs. Despite being presented as a decentralized, non-governed blockchain system, Ethereum Classic also relied on third-party enforcement, only in the more conventional form of state intervention. As argued by one of its developers, the solution for failures should be based on 'Legal recourse. If anything goes wrong the infrastructure cannot be controlled into changing its state. Recourse for financial crime and other illegal activities needs to take place through normal channels. It can be concluded that, at least for fraud cases, Ethereum Classic relies on standard

Todo o caso gira em torno da ideia de que uma lei não é apenas o que está no código. Mesmo a legislação comum possui discussões sobre o que cada palavra quer dizer dentro do contexto e a linguagem possui sua textura aberta muitas vezes, conteúdos que são sub ou sobre inclusivos e suas interpretações jurídicas. Embora o código tenha sua própria execução, ele é similar a interpretação literal de um dispositivo, não se pode resolver todos os casos por meio desse recurso. Se haverá futuramente um novo modelo tecnológico capaz de se adequar ao *Code is Law*, é indefinido. Todavia, a *Ethereum Classic* ainda precisa de interpretações mais amplas por meio do judiciário para funcionar. Como esses casos não foram isolados, tendo ocorrido com outras criptomoedas[54] e foram solucionados também por meio de um *hard fork.* Se essa é a de fato a melhor solução possível ainda são necessários mais estudos e análise das consequências.

3.2.2 Direito de Propriedade e Posse:

Esse grau de descentralização que pretende eliminar os Cartórios de Registro de Imóveis, irá transformar o direito de posse e o de propriedade, significativamente, na mesma coisa. Apesar da disputa entre as duas teorias da posse entre Savigny e Ihering[55] e suas formas distintas de aplicação no direito através do mundo, a única definição que é necessária para entender essa sessão é: O direito de posse é baseada na relação de fato, enquanto o direito de propriedade é baseado na relação jurídica[56].

No cenário hipotético, de duas pessoas brigando pelo direito de propriedade de um imóvel, apenas uma delas tem a posse desse imóvel, a segunda tem apenas o direito de propriedade. Esse direito, na sociedade atual, é garantido por meio da informação de que, apesar de não haver posse de um bem, ele detém o direito de propriedade confirmado por um terceiro independente, seja o cartório de registro de imóveis, ou o poder judiciário.

---

legal recourse (what could also be understood as a form of third-party contract completion) and blockchain integrity is dissociated from self-enforcement”

[54] Reif Nathan (2019) Investopedia Disponível em: https://www.investopedia.com/tech/history-*bitcoin*-hard-forks/ Acesso em 2 de Novembro de 2019.
[55] Neves, Gustavo Kloh Muller. *Propriedade.* Apostila do Curso de Propriedade na Escola de Direito Rio da FGV, 2017.
[56] Diniz; Maria Helena, Curso de Direito Civil Brasileiro: Direito das Coisas, Ed. Saraiva, 2010, p. 36

A *blockchain* em conjunto com o projeto de s*mart contracts*, pretende eliminar essa necessidade do terceiro, uma vez que a sua organização funciona da prova da existência de uma transferência. Seria impossível, nesse caso, a disputa entre duas pessoas com direito a propriedade que afirmam tê-la recebido de transações diferentes. Isso porque, apesar de não ser possível provar que algo não aconteceu por meio de certidões, é possível provar por meio da rede que não só a transferência de A para B aconteceu, mas que C por exemplo nunca recebeu essa propriedade. No cenário em que essas transferências são feitas por meio de *smart contracts*, a posse e o direito de propriedade andam juntos todas as vezes também, uma vez que ao adquirir uma propriedade, você está aceitando um contrato que provará também a sua propriedade desse bem.

Isso torna o direito de propriedade e da posse indissociáveis, e isso tem implicações sérias. Ora, grande parte da nossa economia possui base na dissociação desses direitos, o que poderia limitar as trocas a itens de baixo custo[57]. Com as informações que possuímos no presente momento, ainda não há como equacionar grandes transações. Embora isso seja verdade, ainda há que se descobrir novas especializações que irão surgir a partir desse novo modo de se organizar a propriedade, benefícios como a operacionalização de direitos fracionários[58] e a redução de custos e intermédios pode ser superior aos óbices que a conexão do direito de posse e propriedade devem gerar.

3.2.3 Fundo de Investimentos em Mineração (*Mining Pools*) e Computadores Quânticos

As fragilidades relativas a *Mining Pools* e Computadores Quânticos tem relação com a estrutura de defesa original dos *blockchain*s. Enquanto as *Mining Pools* são um problema mais urgente, nesse momento, os Computadores Quânticos podem invalidar toda a criptografia

[57] "[…]The block chain transaction doesn't merely represent a change in ownership of the car: it additionally transfers actual physical control or possession of the car. When a car is transferred this way the earlier owner's key fob stops working and the new owner's key fob gains the ability to open the locks and start the engine. Equating ownership with possession inthis way has profound implications[…] The implications are indeed profound but they are achieved by transforming ownership into possession – that is, by enforcing only a single right in the asset. The price being paid is huge: the modern economy is based on the specialization(or some would say, separation) of ownership and control (that is, in its simplest sense, possession). If blockchain's smart property is limited to possessory rights, the word merely in the preceding quotation should be excised and the word 'additionally' replaced by 'only'. In practical terms, this limits stand-alone (no trusted this parties) applications of smart property to low-value assets " Id 45

[58] Tradução livre de Fractional rights.

anterior a "*post-quantum*"[59], ou seja, a maior parte dela. Por isso, entender esses riscos é essencial antes de aplicar qualquer tecnologia *blockchain*.

Uma *Mining Pool* pode ser definida por um grupo de pessoas que juntam esforços para poder minerar blocos numa única rede de nós. Elas funcionam de forma similar a um fundo de investimento, onde as pessoas recebem, proporcionalmente, os *bitcoin*s, por exemplo, como resultado de seu investimento. As *Mining Pools* são problemas claros de *blockchains* públicas (como o *Bitcoin* ou a *Ethereum*), já que qualquer computador que participa da rede pode tentar aplicar um *double-spending attack* nela.Como vimos anteriormente a *hashrate* de *q* é de suma relevância para o desenvolvimento de uma cadeia desonesta. Assim, quanto maior o poder de uma única pessoa ou grupo, maior é o potencial dessa pessoa ser bem-sucedida em um ataque a rede.

Esse não é só um risco elevado para o futuro das *blockchain*s, como já está sendo um problema nesse exato momento. Gnash.io, uma *mining pool* de *bitcoin*, obteve 45% de todo o *hashrate* da rede e seus membros voluntariamente decidiram migrar para outros fundos e equilibrarem o sistema[60]. Esse não foi um caso isolado BTC Guild, outra *mining pool* de *bitcoin* conseguiu solucionar 6 blocos seguidos e voluntariamente também limitou os seus membros[61]. Vale relembrar, que assim que a notícia de que algum fundo conseguiu 50% do *hashrate* total, toda a moeda colapsa. Por isso, não é interessante para um grupo de pessoas possuir todo esse poder, haja vista que as pessoas iriam, consequentemente, parar de apostar nesse mecanismo de confiança. Isso teria como resultado o fim da moeda e o fim de todo os esforços que essa pessoa, ou grupo, teve para reunir todo esse *hashrate*.

Ainda que existam diversos desincentivos para que as *mining pools* cheguem a ter esse potencial de ataque. Ainda parece ser necessária a regulação desse setor, para que *mining pools*

---

[59] There are several classes of encryption algorithms that, as far as we know, are not significantly faster to solve on a quantum computer. These are known collectively as post-quantum cryptography, and provide some hope that the world can transition to cryptosystems that will remain secure in a world of quantum encryption.
Infante, Andre (2014) *Quantum computers de end of cryptography* Make Use of Disponível em: https://www.makeuseof.com/tag/quantum-computers-end-cryptography/ Acessado em 1 de outubro de 2019.

[60] Onur, Deler (2017) *End to end bitcoin blockchain with examples* Medium Disponível em : https://medium.com/@onurdeler/end-to-end-*bitcoin*-blockchain-with-examples-52eba6ee7caf

[61]Mineforeman.com (2013). *BTC Guild voluntarily limits their hash rate* Disponível em: https://mineforeman.com/2013/04/06/btc-guild-voluntarily-limits-their-*hash*-rate/ Acesso em: 3 de novembro de 2019.

não possam ultrapassar uma determinada taxa de *hashrate* em relação ao total da rede. Coibindo assim a possibilidade da *blockchain* se auto destruir.

Situação análoga pode ocorrer com o desenvolvimento dos computadores quânticos. Como dito anteriormente, a solução da criptografia do *bitcoin*, no caso de não possuir a chave, só pode ser feita por meio de tentativa e erro. Os computadores quânticos, não são necessariamente mais rápidos em solucionar um problema, mas podem resolver um problema por diferentes ângulos[62].

Com essa capacidade seria possível resolver o teste em uma velocidade muito maior do que o normal, o que invalidaria todo o sistema de criptografia do *blockchain*. Isso porque, ele depende da dificuldade de solução desses problemas matemáticos para ser considerado seguro. Assim, a inovação trazida por meio desse computador, poderia acabar com a segurança da *blockchain*, mas não só isso como de grande parte da criptografia existente. Nesse sentido, criptografias *post-quantum* precisam ser desenvolvidas para o futuro do *bitcoin*. Na atualidade já existem alguns desenvolvedores de *blockchain* que afirmam já ter soluções para esse cenário[63].

Vale ressaltar que as notícias recentes afirmando que a Google está prestes a desenvolver o computador quântico[64] que está sendo falado nessa seção são muito otimistas. O

---

[62] "Quantum computers work because they can have multiple internal states at the same time, through a quantum phenomenon called "superposition". That means that they can attack different parts of a problem simultaneously, split across possible versions of the universe. They can also be configured such that the branches that solve the problem wind up with the most amplitude, so that when you open the box on Schrodinger's cat, the version of the internal state that you're most likely to be presented with is a smug-looking cat holding a decrypted message. […]
For a concrete example, Shor's Algorithm, which can only be executed on a quantum computer, can factor large numbers in log(n)^3 time, which is drastically better than the best classical attack. Using the general number field sieve to factor a number with 2048 bits takes about 10^41 units of time, which works out to more than a trillion trillion trillion. Using Shor's algorithm, the same problem only takes about 1000 units of time."
Idem 56, pgs 3-4.

[63] "There has been news of blockchain builders putting out quantum-resistant chains, such as E-cash inventor David Chaum and his latest cryptocurrency, Praxxis. QAN is another project that says it is ready for the quantum computing age […]".
Pollock, Daryn (2019) *Google's Quantum Computing Breakthrough Brings Blockchain Resistance Into the Spotlight Again* Forbes Disponível em: https://www.forbes.com/sites/darrynpollock/2019/09/24/googles-quantum-computing-breakthrough-brings-blockchain-resistance-into-the-spotlight-again/#3019e8374504 Acesso em: 3 de novembro de 2019.

[64]Redação Galileu (2019) *Cientistas afirmam que Google está prestes a revolucionar a tecnologia com computador quântico* Disponível em:

motivo é, a Google apenas alcançou o primeiro passo[65], que é ultrapassar o computador mais rápido existente, mas ele ainda não soluciona as criptografias na velocidade que está sendo descrita acima.

4. PRÉ REQUISITOS PARA IMPLEMENTAÇÃO DO *BLOCKCHAIN*:

Esse capítulo irá tratar dos pré-requisitos básicos que podem evitar riscos na implementação do *blockchain*, no contexto de registro de propriedade, como o do cartório de registro de imóveis. O cerne desse capítulo é baseado no texto "Prerequisites for Incorporating *Blockchain* into a Registry" dos autores Michael Graglia, Christopher Mellon, e Evan Akin.[66], de forma que será uma paráfrase. Os argumentos dos autores são de extrema relevância e tem grande potencial otimização da integração.

Os pré-requisitos são: (i) Identidade Digital; (ii) Existência de um registro digital; (iii) Utilização de Múltiplas assinaturas por carteira (*multisignaturenature wallets*); (iv) Uso de *blockchain*s híbridas ou privadas; (v) Dados mais precisos possíveis; (vi) População com conectividade e conhecimento tecnológico adequado; (vii) Profissionais treinados e informados sobre o assunto. Cada um dos pré-requisitos supracitados tem a função de reduzir as chances ou eliminar um dos riscos.

4.1 Identidade Digital

Existem dois tipos de informação que precisam ser conectadas para se ter um registro de imóveis: o indivíduo e a propriedade. A propriedade pode ser incluída no sistema por meio dos *hash*es e pela solução das *Colored Coins*, previamente citadas e isso será carregado pela *blockchain* durante suas transações. Entretanto, não é possível fazer o mesmo processo para a

https://revistagalileu.globo.com/Ciencia/noticia/2019/09/cientistas-afirmam-que-google-esta-prestes-revolucionar-tecnologia-com-computador-quantico.html Acesso em : 20 de outubro de 2019.

[65] Idem 63.

[66] Graglia, Michael. Mellon, Christopher e Akin, Evan. (2017) *Prerequisites for Incorporating Blockchain into a Registry* New America Disponível em: https://www.newamerica.org/future-property-rights/blog/prerequisites-incorporating-blockchain-registry/ Acesso em: 19 de outubro de 2019

validação de identidade de uma pessoa. Sendo assim, é preciso solucionar o problema da identidade antes de se implementar um *blockchain* ao registro de imóveis.

No presente momento, existem soluções que provém tanto de uma base digital de dados fornecida pelo poder público[67], integrados com uma *blockchain* com as informações do registro dos imóveis, quanto da extração das informações por meio da tecnologia *blockchain* aplicado para o registro de Identidade[6869]. Cabe dizer, que se trata, na segunda opção, de uma segunda *blockchain* que tem a função de registrar pessoas e não de uma única *blockchain* que faz ambos os serviços. Apesar disso, Dubai afirma conseguir conectar todas essas *blockchain*s de forma que Dubai será a primeira cidade completamente conectada por meio de *blockchain*s até 2020[70].

Independentemente da forma, o que importa é que no fim, exista tanto a *blockchain* para registro dos imóveis, quanto os dados válidos sobre os indivíduos que os possuem. No brasil por exemplo, a informação poderia ser dada por meio da Registro de CPF, já existente na base de dados da Receita Federal. Como indica Graglia, Mellon e Akin[71]:

> "It is far better to use an existing, validated identity system than to create a new one just for a registry. This is both because identity management is a separate skill set and because using an established system or systems (if a federated identity verification approach is used) will result in higher quality information.' "

É claro que é melhor a aplicação de um sistema de identidade já existente, do que a criação de um novo somente para o registro de imóveis. Só seria conveniente a criação de um sistema novo, baseado em *blockchain*, para a identidade no caso de esse ser um outro objetivo, que beneficia lateralmente o projeto de *blockchain* para o registro de imóveis. Não é necessário que outro sistema seja criado, desde que o já existente possa ser considerado válido.

---

[67] Id 41.
[68]SecureKey 2017 "IBM and SecureKey Technologies to Deliver Blockchain-Based Digital Identity Network for Consumers" https://securekey.com/press-releases/ibm-securekey-technologies-deliver-blockchain-based-digital-identity-network-consumers/
[69] Graglia, Michael (2017) Will Blockchain Work in Ukraine? Disponível em: https://www.newamerica.org/future-property-rights/blog/will-blockchain-work-ukraine/ Acesso em: 28 de outubro de 2019.
[70] Smart Dubai Disponível em: https://www.smartdubai.ae/initiatives/blockchain Acesso em: 28 de outubro de 2019
[71] Id 66

4.2 Existência de um Registro Digital

A *hash function* já foi explicada previamente. É o processo de incluir um "carimbo" digital que só pode ser resolvido por meio da resposta do seu problema matemático. Cabe lembrar, que por envolver a resposta da função *hash* do bloco anterior da cadeia, todos os blocos só podem ser alterados a partir do conhecimento do último bloco solucionado. Assim, para todo o resto da rede precisa da informação sobre o último bloco para que a cadeia de transferências ande.

O registro de um documento por meio da *blockchain* depende da inclusão do *hash* nesse documento. É óbvio que não é possível colocar um *hash* em algo físico. Por isso, é preciso que todos os documentos que estão sendo enviados para o sistema já estejam digitalizados. Todos os outros nós precisam receber a informação de que esse documento com o *hash* está na *blockchain* e agora, qualquer outro documento incluído no sistema igual a esse pode ser descartado, haja vista que o original possui esse "carimbo digital" único. Assim, não é possível alcançar o funcionamento do projeto de um registro de imóveis com integração da *blockchain* sem a completa digitalização dos documentos. Tanto o projeto da Georgia, quanto o da Suécia[72] possuíam seus sistemas completamente digitalizados antes da implementação da *blockchain* no registro de imóveis das suas respectivas regiões.

4.3 Utilização de Múltiplas assinaturas por carteira (*multisignature wallets*)

Esse pré-requisito tem a intenção de permitir segurança contra o roubo, furto, ou mesmo desaparecimento de *private keys*. Somente a pessoa que possui a *private key* poderá registrar ou mesmo transferir seus bens, ou seja, o direito de propriedade está atrelado ao uso de *private keys*. Caso a dono da *private key* a perca por qualquer motivo, outra pessoa passaria a ser a dona do que houvesse sob o domínio dela. Nesse contexto, uma pessoa poderia ser forçada a transferir seus próprios bens e com isso perder parte do seu patrimônio.

Para solucionar o problema, os autores sugerem o uso de *Multisignature wallets*, que são, como explicado anteriormente, *public keys* que demandam mais de uma assinatura para a

[72] Graglia, Michael (2017) *Tbilisi agreement heralds significant expansion of blockchain to manage property registries* Disponível em: <https://www.newamerica.org/future-property-rights/blog/blockchain-for-property-rights-georgia/> Acesso em: 28 de outubro de 2019.

realização da transferência ou registro. Nessa toada, os autores sugerem que um terceiro confiável, ou que fez parte da transação, como um banco, ou mesmo o cartório, em casos de menor integração com a plataforma *blockchain*, sejam utilizados para verificar a transação. É claro que, a partir dessa etapa mais tempo seria necessário para que uma transferência fosse feita, haja vista que agora são necessárias a aprovação de duas pessoas e não só uma, mas ainda assim, é um preço pequeno frente a segurança de ter seus títulos roubados.

Como os próprios autores alertam, novos problemas podem surgir com o uso das *multisignaturenature wallets*, como casos antigos de má programação que facilitaram o ataque de hackers. Entretanto, eles ainda afirmam que novos códigos surgiram e ele são mais confiáveis, prevenindo mais problemas do que gerando. Vale ressaltar também, que o uso de *multisignatures* não deve ser obrigatório, mas um serviço extra que o dono da *private key* pode desejar utilizar ou não.

4.4 Uso de *blockchain*s híbridas ou privadas

As *blockchain*s privadas, podem ser definidas de forma simples, como as tem seu controle feito por meio de um terceiro[73]. Enquanto as *blockchain*s híbridas são o uso de duas *blockchain*s conectadas, sendo uma privada e uma pública. As *blockchain*s citadas até o presente momento (*Bitcoin* e *Ethereum*) são públicas.

De acordo com o autor do texto, três são os problemas centrais que a utilização da *blockchain*: (i) O judiciário ou um terceiro independente precisa ter a capacidade para alterar a *blockchain*; (ii) As redes públicas não conseguem trabalhar com todo o volume de dados envolvidos; (iii) O anonimato não é uma opção.

De acordo com os autores, os problemas como morte de um usuário sem a revelação de sua chave, disputas judiciais entre cônjuges que dividem bens e proprietário que é expropriado e não revela a sua chave, podem ser solucionados por meio do controle da *blockchain* privada.

[73] The Luxtag Project (2018) Private vs. Public Blockchain: What are the Major Differences? Disponível em: https://medium.com/luxtag-live-tokenized-assets-on-blockchain/private-vs-public-blockchain-what-are-the-major-differences-d92a504f3a4a Acesso em: 10 de novembro de 2019

Além disso, os exemplos anteriores como o do DAO, ou mesmo no caso de roubo de uma chave, citado no tópico acima, podem ser solucionados também por meio desse controle[74].

Esse modelo permitiria que voltássemos transações indesejadas após decisões judiciais, o que é positivo, haja vista que haverá decisões e elas precisam ter eficácia. Entretanto, não é possível afirmar que isso aconteceria por meio de uma *multisignaturenature wallet*, haja vista que uma *private key* não tem autoridade para desfazer uma transação. O que acontece é, provavelmente, a mesma atualização do sistema dado pelo *hard fork*, mas sem necessidade de aceitação alheia.

Em relação a capacidade de armazenamento, Graglia, Mellon e Akin afirmam que não é possível o armazenamento de tantos documentos dentro de uma rede descentralizada. É claro que um modelo em que apenas o *hash* é salvo dentro do sistema e os documentos são salvos por meio de outra parte digital, não seria necessária a utilização da private key. Todavia, se o desejado é a integração de toda a plataforma, é preciso a utilização de uma *blockchain* privada, pelo menos para a parte de armazenamento dos títulos, mapas e etc.

Sobre a questão o anonimato, é preciso entender que os cartórios têm a função dar publicidade aos atos jurídicos[75]. As ações que acontecem dentro de uma *public chain*, diferentemente do que é veiculado, não são anônimas, mas pseudônimas[76], onde é possível rastrear as atividades realizadas por uma *private key*, mas não por parte do indivíduo. Uma *blockchain* privada pode criar condições para que uma identidade seja conectada a *private key*, permitindo, por exemplo apenas uma *private key* por usuário e associando essa chave ao dono por meio do primeiro requisito.

4.5 Dados mais precisos possíveis

[74]"[...]But in a hybrid chain -- where decisions are tracked on a private chain with *hash*es of key documents recorded on a public chain-- they can be addressed by granting appropriate authorities to the Registrar and Judiciary, which is critical when managing real assets. This could take the form of a special variation of a multisig where an ombudsman has a key allowing it to create reverse transactions on the private chain. Accenture has made a similar observation in the context of financial services" Id 44

[75] Art. 1º Serviços notariais e de registro são os de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos.
Lei 8935/94 Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8935.htm>

[76] Id 50. Pg 59

A imutabilidade dos dados de uma *blockchain* é um dos seus principais benefícios. Ela mantém a informação que já existindo, impedindo potenciais erros ou fraudes que ocorram naquela transação. Entretanto, se uma informação já está corrompida, ela tem impactos ao ser registrada dentro do sistema.

Em um sistema de *blockchain* pública, a única solução possível seria carregar essa informação. Isso porque, a informação que é incorreta dentro do sistema, provavelmente vem dos blocos de um momento antigo na cadeia, e aplicar um *hard fork* a partir dali, pode ter implicações inúmeras frente as transações que ocorreram depois, já que estamos tratando de direitos reais. Além disso, o impacto de um *hard fork* numa rede em que as pessoas não são obrigadas a aceitá-lo permitiria a divisão de duas linhas do tempo, como no caso do DAO, uma em que a fraude é real e outra em que a fraude não é real. Essa discussão sobre o direito de propriedade pode ser de duas pessoas ao mesmo tempo, inutilizaria todo e qualquer motivo para se registrar os documentos por meio da *blockchain*. Diferentemente do que acontece com uma criptomoeda, como foi explicado anteriormente.

É claro que é possível alterar uma informação lá dentro, se o modelo aplicado for um de rede privada com acesso ao poder judiciário, por exemplo. Contudo, numa rede privada colocada dentro de um sistema imutável, a noção do que é correto ou não dentro da rede, que deveria ser imutável fica comprometida a partir disso. Dessa maneira, é preciso que antes de implementar a *blockchain* dentro do seu cartório uma rede digital de informações já esteja funcionando, onde é mais fácil descobrir os possíveis erros[77]

Assim, ao invés de utilizar os recursos para a aplicação da tecnologia *blockchain*, é recomendado que a eles sejam aplicados anteriormente na criação de um registro válido e confiável.

4.6 População com conectividade e conhecimento tecnológico adequado

[77] "*If a registry is in use, functioning as the public record, it should be on the best available technology. If transitioning to a new technology surfaces erroneous or conflicting records, they can be addressed in a systematic manner. Records can be flagged, and a process giving all parties a voice can be initiated without delaying implementation. If, however, the registry is riddled with errors, resources may be better utilized addressing those errors before incorporating blockchain into the registry*" Id 43.

É possível ver por toda a explicação, principalmente do primeiro capítulo, que uso desse *software* não é simples. Apesar disso, todas as pessoas devem poder fazer o registro de imóveis e sua possível transferência. Um dos maiores desafios de aplicação dessa tecnologia frente a todos os cidadãos de uma área é que todos eles devem ser capazes de conseguir executar suas transferências, haja vista que nos últimos níveis de implementação dessa tecnologia, haverá cada vez menos contato com outras pessoas. Contudo, nem todos os cidadãos possuem tecnologia suficiente para a execução disso, ou mesmo os que possuem tem pouco contato com a tecnologia ao ponto de conseguir se sentir seguro a executar a venda de seu imóvel.

Por isso, a proliferação de IaaS (*Infraestructure as a Service*) SaaS (*Software as a Service*) e BaaS (*Blockchain as a Service*) está cada vez maior. Com esses serviços é possível conseguir, por meio do pagamento da assinatura dos programas, ou dos equipamentos necessários para a execução do que é desejado.

Cabe dizer também que o treinamento das pessoas de início também parece ser um óbice. As plataformas devem ser bem transportadas, de forma que os cidadãos consigam entender o modelo do que é proposto, sem necessitar entender as questões intrínsecas da *blockchain*. Se parte significativa da população não possui qualquer contato com o uso da internet, por exemplo, não seria possível a aplicação da tecnologia nos registros. Além disso, a população não acreditará na solução que foi desenhada para garantir a confiança das transferências de imóveis[78], o que poderá ter impactos econômicos negativos. Nesse caso, é recomendado, como no anterior a digitalização e a democratização do acesso à internet antes da implementação da tecnologia.

4.7 Profissionais treinados e informados sobre o assunto.

O texto afirma que inicialmente, não será possível acabar com os intermédios, e por exemplo, advogados ainda entrarão com processos contra as transações ocorridas dentro da *blockchain* e os juízes irão julgar. Nesse cenário, é preciso que a informação para os futuros profissionais que trabalhem no futuro da área e nas áreas anteriormente citadas sejam bem informados e entendam sobre o que estarão enfrentando. Eles ainda afirmam[79]:

[78] Id 16.
[79] Id 44. Pg 15

> *All of these parties will need to be trained on the new system in order for it to function properly. The importance of engaging the professional communities who will interact with the blockchain early on in the transition cannot be overlooked. Blockchain lawyers such as Andrew Hinkes remind us that lawyers will need to understand a number of issues, including how to present records from the blockchain, how to interpret records, and how to harmonize evidence rules with output from the blockchain. To do any of those things, they will first need to be trained in the fundamental concepts, capabilities, and vocabulary of the blockchain. Even with a clear picture of the technical and structural requirements for a blockchain registry, a great deal of work will remain in the form of education and capacity building.*

5. NÍVEIS DE COMPLEXIDADE NA INTEGRAÇÃO DA TECNOLOGIA

Após entender o funcionamento da tecnologia, a aplicação genérica nos cartórios de registro de imóveis, benefícios e os riscos e pré-requisitos para mitigação dos riscos centrais e melhor aproveitamento dos benefícios, é necessário entender que existem diversas maneiras de se aplicar a tecnologia, haja vista existem diversos *blockchains* e diversos modelos de se organizar a propriedade, como já foi visto até aqui. O presente capítulo pretende apresentar quais são os níveis de integração do direito de propriedade com a tecnologia *blockchain*.

Para isso, os oito níveis apresentados por Graglia e Mellon em "*Blockchain and Property in 2018: At the End of the Beginning*"[80], tem o intuito de organizar em grau de complexidade de aplicação da tecnologia. Não se trata de uma escala, mas sim de diferentes níveis de complexidade da integração. A tabela abaixo resume, simplificadamente, o que irá ser tratado nesse capítulo:

Nível	Nome	Descrição	Exemplo
0	Nenhuma integração	Não usa a *blockchain*	Maior parte do mundo
1	Armazenamento por meio da *Blockchain*	Uso de *blockchain* para registro da transação	Suéca, *Dubai Properties (landstream)*
2	*Smart Workflow*	Blockchain usada para registrar o processo de uma transação	Propy

[80] Graglia, J. M., and Mellon, C. 2018. "Blockchain and Property in 2018: At the End of the Beginning" Innovations: Technology, Governance, Globalization (12:1-2), pp. 90-116 Disponível em: https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00270

3	*Smart Escrow*	Uso de *Smart Contract* para pagamento de *escrow*	Dubai, Georgia
4	Registro pela *Blockchain*	Base de dados central substituída pela *blockchain*	Não possui exemplos
5	*Disaggregated Rights*	Vários direitos diferentes são geridos por meio da *blockchain*	Pangea
6	*Fractional Rights*	Direitos são fracionados via *blockchain*	Não possui exemplos
7	Transações ponto a ponto	Direitos são transacionados sem intermediários em um sistema de nível 4	Não possui exemplos
8	Interoperabilidade	*Blockchains* diferentes se fundem	Não Possui exemplos

Figure 1 Tabela baseada no artigo: Graglia, J. M., and Mellon, C. 2018. "Blockchain and Property in 2018: At the End of the Beginning" Innovations: Technology, Governance, Globalization (12:1-2), pp. 90-116

Obviamente, o primeiro nível tratado pelo autor é o de não aplicação, que mantém a relação atual do país com seus registros de propriedade, o que não será analisado nesse texto. Os níveis seguintes podem ser divididos em dois subgrupos de quatro níveis cada: (i) os realmente aplicados; (ii) os que possuem aplicação especulativa.

Além disso, o maior destaque desse capítulo deve ser dado para o primeiro subgrupo, já que esses são níveis já palpáveis e que já possuem estudos mais conclusivos sobre as suas aplicações. Nesse sentido, apenas o primeiro grupo será apresentado nesse trabalho, haja vista sua aplicação mais direta nos Cartórios de Registro de Imóveis. Apesar disso, o futuro da tecnologia não deve deixar de ser explorada e nem deve ser limitado pelo que foi concebido pelo autor desses níveis.

Cabe ressaltar ainda que, a existência do Cartório só é dispensada a partir do nível quatro. Por isso, os três primeiros níveis partem da aplicação inicial da tecnologia incorporada à um sistema de cartórios, como poderá ser visto abaixo com o exemplo do brasileiro. Um estudo mais específico do quarto nível, que demonstra distância significativa dos outros três níveis, pela inexistência dos cartórios, também se faz necessário, mas a aplicação do projeto de Dubai e Georgia ainda não foram completamente incorporadas até a presente data.

5.1 Primeiro Nível: O Registro por meio de *Blockchain*

Esse é o nível inicial de complexidade, o cartório ainda executa grande parte de suas funções, tendo apenas seu registro simplificado por meio da tecnologia *blockchain*. O Cartório de Registro de Imóveis ainda possui todas as suas atribuições e competências. Contudo, a

tecnologia é implementada por meio da utilização da *hash function* para registro permanente de suas informações. Para maior segurança, uma rede pública maior e conhecida, como a *Bitcoin* ou Ethereum, pode ser utilizada para armazenamento dessas informações.

Por registrar permanentemente a prova de existência de um documento, numa determinada condição, ela tem o potencial de reduzir a probabilidade de falsificação dos registros, como foi dito anteriormente. Essas características são perfeitamente adequadas para países que tem problemas com falsificação de registros ou corrupção, haja vista que um documento está permanentemente registrado, sem qualquer possibilidade de alteração do registro, sem a posse da *private key* adequada. Soma-se a isso, países que tem grandes preocupações com a transparência, uma vez que sua descentralização da informação, permite que todos com acesso a rede possam acessar as informações disponíveis nela[81].

Destaca-se que esse grau de implementação não necessita de integração em todo o país, por se tratar da implementação em apenas um cartório, podendo ser aplicado como projeto piloto. Além disso, isso permite que diversos cartórios tenham modelos diferentes de integração, com utilização ou não de SaaS (*Software as a Service*), com uso de *blockchain*s diferentes, não os fazendo dependentes de uma uniformização. Soma-se a isso, que possui menor quantidade de pré-requisitos para sua implementação, haja vista que nem todos os países possuem essa uniformização e digitalização total do sistema.

Entretanto, é necessário alertar que nem todos os benefícios explicados no texto serão aproveitados por meio dessa aplicação. Obviamente, que para o melhor funcionamento e maior integração seria necessário avançar níveis acima, tendo novos desafios e riscos a partir de cada nível alcançado.

5.1.1. O cartório de Pelotas-RS

Por se tratar do primeiro nível, que inclui a tecnologia com menor nível de complexidade e depende de menor integração a ideia de descentralização do registro dos direitos de propriedade, esse nível terá a apresentação de um estudo específico.

A apresentação visa demonstrar apenas como funciona o modelo, para se ter uma melhor visualização de como seria a implementação do modelo no primeiro nível de complexidade. A tecnologia aplicada e suas falhas não serão exploradas além do que foi apresentado até aqui.

[81] Id 80.

Dessa forma, não se pretende analisar os riscos da *Colored Coins*, *torrent*, armazenamento em nuvem e outros modelos que forem explicados abaixo.

O Cartório de Pelotas no Rio Grande do Sul teve seu projeto, idealizado pela Ubitquity, analisado pelo estudo "Registro de Transações imobiliárias em *blockchain* no Brasil (RCPLAC-01) – Estudo de Caso 1"[82]. Os autores analisaram desde o contexto do Cartório em relação a parte Jurídico-administrativa, procedimental, documentário e tecnológica até modelo que está sendo aplicado por meio da Ubiquity trazendo os processos que cada usuário terá que exercer para realizar o novo registro. Assim, é possível entender melhor como se dá esse nível de integração que já está sendo realizado no Rio Grande do Sul.

Destaca-se que se trata de um projeto piloto que está sendo realizado com apenas "meia dúzia de documentos para testar a segurança que a metodologia que a *blockchain* oferece"[83]. Ainda se ressalta também, que o Oficial de Registro de Imóveis do Cartório de Pelotas afirma que a sua aplicação real só seria possível num futuro distante, haja vista os custos altos e a necessidade de se fazer um cálculo de custo-benefício.

O entendimento do contexto nacional de registro de imóveis, a partir da ótica da pesquisa realizada por Lemieux e Flores, antes da explicação do modelo de implementação no cartório de Pelotas, se faz necessário. Dessa maneira, os principais pontos a serem destacados sobre o cenário nacional dentro do contexto da pesquisa, são[84]:

(i) "O Brasil não possui um sistema integrado de gestão de propriedades. Portanto, a gestão de propriedades é fragmentada e ocorre em níveis governamentais diferentes, dependendo do tipo de propriedade e seu uso ";
(ii) "O processo implica em pelo menos 13 passos separados. O banco de dados Cadastral e o banco de dados de Registros mantidos pelos cartórios de registro de imóveis não estão integrados e identificadores diferentes são usados para o mesmo pedaço de terra, criando incertezas em torno da identificação da propriedade. ";
(iii) "Também não há banco de dados eletrônico para verificar embaraços (embargos, hipoteca, restrições, etc.) ";
(iv) "De acordo com algumas fontes, a falta de integração e de sistematização do sistema brasileiro de registro de imóveis abre uma porta para o abuso de proprietários ricos que, às vezes, subornam o cartório de registro de imóveis para registrar a propriedade de outra pessoa em seu nome. ";
(v) "Não há plano de classificação. Não há arquivista na instituição, porque, de acordo com os entrevistados neste estudo de caso, a gestão de documentos no escritório é pragmática. "

[82] Lemieux, Victoria & Flores, Daniel & Lacombe, Claudia. (2018). Registro de transações imobiliárias em Blockchain no Brasil (RCPLAC-01) - Estudo de Caso 1. 10.13140/RG.2.2.16022.45123.
[83] Id 82 pg 10
[84] Id 82 pg 7-10.

Nesse contexto, é possível dizer que apenas o primeiro nível de integração seria possível, pelo que já foi visto sobre os pré-requisitos e que será visto abaixo sobre os níveis de integração, nos próximos subtópicos. Além disso, é possível afirmar por todas essas ausências que este cartório em específico, e até mesmo o cenário nacional como um todo, não possui a parcela dos requisitos necessários para se ter total confiança nos registros que já possuem. Assim, não poderemos retirar o risco das informações antigas não serão fraudulentas, mesmo após o registro no sistema. No entanto, essas condições foram favoráveis para que a Ubiquity, tivesse a oportunidade de testar um projeto piloto com apenas um cartório dentro do Brasil.

A solução então será a aplicação da *blockchain* em primeiro nível, para garantir a autenticidade das informações relacionadas a propriedades imobiliárias. Ela utiliza o modelo de negócios SaaS (*Software-as-a-Service*), por consequências taxas são cobradas para adicionar ou modificar documentos da plataforma em questão. O acesso do usuário a plataforma funciona com o modelo *front-end web*:[85]

> "A solução usa o front-end web, que captura informações tomadas do 'Livro 2' – o registro geral de imóveis do cartório de imóveis, assim como um servidor web e armazenamento de backup. Livro 2, o registro geral de imóveis, existe como um bando de dados, contendo o número de registro da propriedade, o nome do dono, o endereço da propriedade, assim como a imagem da propriedade, fotos de livros e a certidão."

Front-end pode ser definido como a relação do usuário com a plataforma até o seu processamento[86]. Assim, destaca-se que o usuário, que pode ser tanto o próprio cartório, quanto o usuário, preenche suas informações que serão incluídas no registro. Esses componentes são conectados a Colu's API, que funciona por meio do protocolo das *Colored Coins*[87]. de maneira que essas informações sobre os ativos e suas transações possam ser enviadas para uma *blockchain*.

O texto afirma ainda que o plano é conectar diretamente ao plano de *Colored Coins Open Assets* e não ao *Colu*, uma vez que assim seria possível adequar o protocolo a todas as

[85] Id 82
[86] Souto, Mario (2019) "*O que é front-end e back-end?*" Alura Disponível em: https://www.alura.com.br/artigos/o-que-e-front-end-e-back-end Acesso em: 13/11/2019
[87] Como já dito anteriormente, *Colored Coins* é um protocolo para representar ativos reais dentro de uma plataforma de blockchain. Para mais informações sobre como funcionam as *Colored Coins* e o *Coloring Scheme*, em seu contexto original acesse: "*Colored : Coins Colored Coins Protocol Specification"* https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification

regras sobre armazenamento de dados da legislação brasileira. O principal risco relacionado ao armazenamento de dados é relativo a Lei Geral de Proteção de dados[88] (Lei 13.709/18), haja vista sua preocupação geral com privacidade e anonimização desses dados.

Destaca-se que, a plataforma *Colored Coins* anexa os metadados também a *multisignaturenature wallet* (multisig), que permite que mais de uma pessoa seja necessária para a confirmação de uma transação. Esse número de assinaturas é combinado anteriormente a criação do endereço. É importante relembrar, que a opção pelo uso de *multisig* permite a redução dos perigos de perda do acesso a carteira, no caso de o proprietário ser o único possuidor de *private key*.

Cabe ressaltar que pela incapacidade do sistema de armazenar a quantidade total de dados que um usuário deseja incluir com uma associação, o *coloring scheme* do Colu, permite a associação dessas informações por meio de metadados ao protocolo *Torrent*. O texto de Lemieux e Flores demonstra que o *torrent* é usado da seguinte forma:

> "Desta maneira, dados ou metadados relacionados aos ativos podem ser armazenados e associados com a transação usando o Bit*Torrent*. Isto é um protocolo peer-to-peer no qual os pares coordenam a distribuição dos arquivos solicitados, assim como os nós do *Bitcoin* coordenam o registro de transações em um ledger distribuído. [...]
> Em teoria, Colu maneja o upload do conteúdo dos metadados para o Bit*Torrent*, processo chamado de 'seeding'(semeando), testado pela Ubitquity de forma bem sucedida. Contudo, por ora, Colu está armazenando os metadados do projeto piloto em um servidor que não pode ser acessado pela internet e apenas semeará dados para o Bit*Torrent* por um pedido da(o) Ubitquity."

O armazenamento desses dados da rede *torrent* é feito por meio de outra rede descentralizada, IPFS (*Inter Planetary File System*), que chamamos comumente de armazenamento em nuvem. Em decorrência disso tudo, para adquirir essas informações é preciso acessar um link magnético (demonstrado na figura abaixo no campo Meta *Torrent*), que permite que essas informações sejam baixadas por meio de e-mail e aplicativos de mensagens, desde que o usuário possua um cliente *torrent* e o arquivo esteja sendo semeado na rede *torrent*. A figura abaixo demonstra como funciona isso:

[88] Brotto, Natália e Ribeiro, Aleff. (2019) "*A LGPD e a tecnologia blockchain são compatíveis?"* Jota Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-lgpd-e-a-tecnologia-blockchain-sao-compativeis-05112019 Acesso em: 06/11/2019

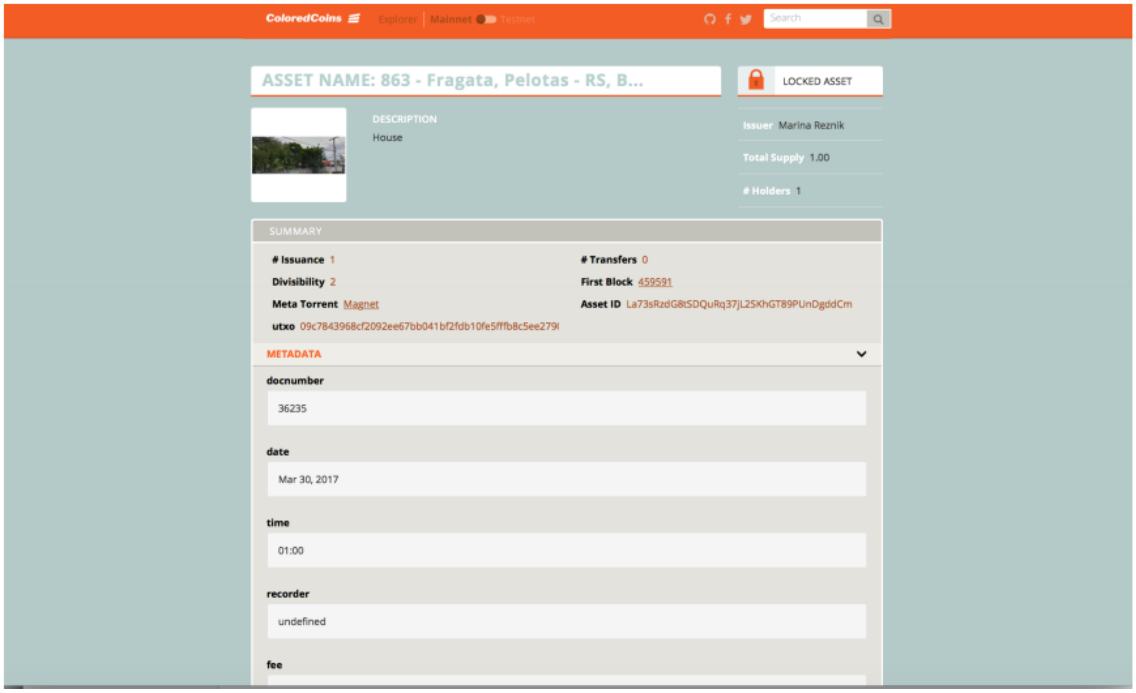

Figure 21Lemieux, Victoria & Flores, Daniel & Lacombe, Claudia. (2018). Registro de transações imobiliárias em Blockchain no Brasil (RCPLAC-01) - Estudo de Caso 1. 10.13140/RG.2.2.16022.45123. pg 15

"Colorir" os ativos permite, assim, que eles sejam identificados por meio de seu ID, como indicado na figura. Nesse contexto, é possível ter acesso a todas as transações que o envolvem, inclusive, visualizar todas as transferências antigas desse imóvel. Cabe ressaltar que essa imagem é de uma casa que não teve transferências desde que foi incluída dentro do sistema. O *hash utxo* também permite que essa transação possa ser pesquisada dentro da *blockchain* do *bitcoin*, aumentando ainda mais a validade da informação.

5.2 Segundo Nível: "Smart Workflow".

O segundo nível de integração tem o intuito de reduzir mais ainda a necessidade de terceiros de uma relação de transferência e registro de imóveis. Nesse caso, a existência de uma base conjunta das informações e um sistema integrado se faz necessário. A integração de todos os sistemas é a base para a redução dos intermediários, já que a muitos desses intermediários funcionam como meios de se garantir que a transação seja feita corretamente, por meio da utilização das informações que estão espalhadas em uma rede não integrada de informações. Sobre isso, Graglia e Mellon afirmam[89]:

[89] Id 76

> "[...] By publishing the completion step of the transaction on a permissioned chain and making those events visible to other participants in the transaction, timelines can be compressed dramatically. Along with mid-transaction transparency, hand-offs between parties become easier since everyone is using the same workflow rather than integrating numerous existing systems, which often introduces errors.
>
> In the case of a real estate transaction, the steps - bank-approved credit line, offer accepted, deposit received, contract signed, etc. – involve numerous entities who need to interact and be certain that each has done their part. Collaborating via a *blockchain* will allow them to collapse the timeline and realize significant efficiencies. […]
>
> In the case of real estate development, the documents required to develop a project-sales and purchase agreements, progress reports, and master plans – need to move back and forth between developers and approving agencies. Having a trustless *blockchain* that can track these documents and increase visibility to all parties will expedite the process and reduce confusion."

Este nível ainda pretende aglomerar novos tipos de documentos que não só os documentos necessários para uma transação. Como é possível ver no texto acima, todos os documentos necessários para a realização do desenvolvimento de um projeto imobiliário podem ser incluídos na integração do sistema. Isso tem consequências positivas para a integração do sistema e permite que os custos de transação sejam menores ainda, como explicados pelo texto.

Realça-se que esse novo nível de aplicação dessa modernização permite a integração de outros setores na rede, uma vez que os fazem serem mais familiarizados com a rede *blockchain*, reduzindo assim, a sua rejeição inicial ao modelo.

5.3 Terceiro Nível: "Smart Escrow"

O terceiro nível de complexidade na integração exclui a necessidade de um terceiro independente que realize serviços relacionados a uma *escrow account*[90]:

[90] "Escrow é uma garantia prevista em um contrato ou acordo comercial que é mantida sob a responsabilidade de um terceiro até que as cláusulas desse acordo sejam cumpridas por ambas as partes envolvidas no negócio.Normalmente, essa garantia é feita na forma de um depósito em dinheiro em uma conta criada especificamente para isso - uma escrow account, que em português poderia ser traduzida como 'conta-caução' ou 'conta de garantia'. "
Dicionário Financeiro. "O que é escrow? " Disponível em: https://www.dicionariofinanceiro.com/escrow/ Acesso em: 12/11/2019

O terceiro nível é chamado de Smart Escrow, mas acredito que a melhor nomenclatura para ela deveria ser Smart Contracts. O que os autores sugerem é a aplicação de Smart Contracts[91] para a realização dos contratos relacionados com a transferência de imóveis, como os contratos de aluguel e compra e venda. Ele sugere que sua automatização pode reduzir os custos relacionados ao uso de *escrow accounts*. Isso porque, não existe necessidade da utilização da garantia de contratos que são executados automaticamente por meio do que estiver no código que rege essa relação. Todavia, seus impactos são muito maiores do que esses. A depender do nível de utilização do *smart contracts*, quase todos os intermediários podem ser eliminados, inclusive os que fabricam os contratos, restando apenas a associação da programação a um contrato base, que é replicado para todos os casos que utilizem aquela base de *smart contract*.

Existem riscos que já foram discutidos no capítulo 3 em relação as possíveis conclusões do uso do *Code is Law*, e como consequência dos *Smart Contracts*, para solução desses problemas. Apesar disso, o autor sugere que pode resultar em uma redução da quantidade de processos levados à justiça[92]:

> "Aside from the clear implications of replacing a set of professionals with code, level 3 *blockchain* integration is significant because, as Andrew Hinkes argues, the impact of *blockchain*s on contract law may minimize litigation exposure as well. Hinkes points out that oracles – external data sources upon which smart contracts may rely – remain a vulnerability. Oracles are susceptible to fraud or manipulation and although many project seeks to address oracle information sources, they have many moving parts where they can break, be faked, or be manipulated. Smart Contracts open a Pandora's box of legal issues if they do not behave appropriately."

Pode ser que a abertura dessa "caixa de pandora" retorne em mais exposição das redes a novos ataques, como foi o caso da interpretação literal narrada no caso DAO. Todavia, pode ser também que a utilização dos *smart contracts* resulte em um novo entendimento do direito, considerando-se que a utilização de contratos automáticos reduz espaço para a discussão de zonas cinzentas de entendimento. Por isso, o *Code is Law* tem impacto direto sobre como se entende o direito em seu aspecto filosófico, mais especificamente sobre a filosofia da

[91] A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible. Jake Frankenfield, Investopedia (2019) "*Smart Contracts*". Disponível em: https://www.investopedia.com/terms/s/smart-contracts.asp Acesso em: 11/12/2019

[92] Id 80

linguagem. Pode ser que seja útil apenas em casos muito simples, que estejam dentro da moldura, ou que não funcionem em caso qualquer. Novos estudos são necessários sobre a aplicabilidade do *Code is Law*, métodos de funcionamento e solução de seus riscos, além dos seus custos e benefícios.

5.4 Quarto Nível: *Blockchain* Registry

O quarto nível é o último que já foi realmente implementado. Ele apresenta a real descentralização do registro de imóveis. Nesse caso, o cartório é completamente substituído pelo pela ferramenta *blockchain*. A real descentralização é a única que consegue eliminar totalmente o terceiro independente que dá a confiança final a transação, como foi feito, por exemplo, com as transações via *Bitcoin*s explicadas no primeiro capítulo desse texto.

A sugestão do texto organizador dos níveis sugere, que seja realizado por meio de uma *blockchain* híbrida. A primeira seria privada e garantiria o armazenamento dos dados, por questões de segurança, custos de armazenamento, privacidade seletiva e eficiência. Enquanto a segunda seria uma rede pública como a dos *Bitcoin*s, sendo utilizada para o registro permanente das informações.

5.4.1 Registro de Imóveis e Georgia

A implementação da tecnologia na Georgia foi dada em duas etapas. A primeira feita em 2016, implementada pela Bitfury e a NAPR, órgão de registro de imóveis do país, tinha os mesmos conceitos do primeiro nível, ou seja, somou o sistema de cartórios já existente com a *blockchain*. Enquanto a segunda etapa já engloba a transações de imóveis feitas por meio da *blockchain*, ou seja, sem a necessidade de registro em um Cartório de Registro de Imóveis.

Cabe ressaltar que a Geórgia possuía um dos melhores sistemas de registro de imóveis do mundo, ficando na terceira colocação do *ranking Doing Businesess* de 2016[93]. O sistema atualizado decorreu dos problemas antigos que a Geórgia possuía com corrupção relacionado

[93] World Bank Group. 2016. Doing Business 2016 : Measuring Regulatory Quality and Efficiency. Washington, DC: World Bank. © World Bank. https://openknowledge.worldbank.org/handle/10986/22771 License: CC BY 3.0 IGO.

ao registro no início dos anos 2000[94]. Com isso, é possível ver que eles possuíam o pré-requisito principal para a aplicação correta da tecnologia: a base de dados confiável e digitalizada. Além disso, por já possuírem a base digitalizada e interação por meio da internet para fazer o registro, foi possível implementar esse nível apenas no *back-end*, mantendo o *front-end* da mesma forma que antes.

A segunda fase de implementação começou em 2017, com a boa impressão criada pelo projeto piloto do ano anterior. De acordo com o Shang e Price[95]:

> "[...] Georgian Citizens will be able to access their property information on the NAPR website and put it up for sale. The nodes of the network will verify that the buyer has sufficient funds and that the seller owns the property before the transaction is concluded. With the new technology, all land sales and transfer information will be accessible to the public and it will not be easily altered by government agencies."

Assim é possível entender, de forma geral como funciona, o sistema. Vale ressaltar que a rede escolhida é a *Exonum*, uma rede privada que se ancora na *blockchain* do *bitcoin*, armazenando apenas do *hash* na rede pública, aumentando sua segurança, como foi previsto também nos pré-requisitos. Enquanto isso, ainda é possível armazenar os dados sensíveis na rede privada, sem torná-los públicos, evitando problemas com leis gerais de proteção de dados.

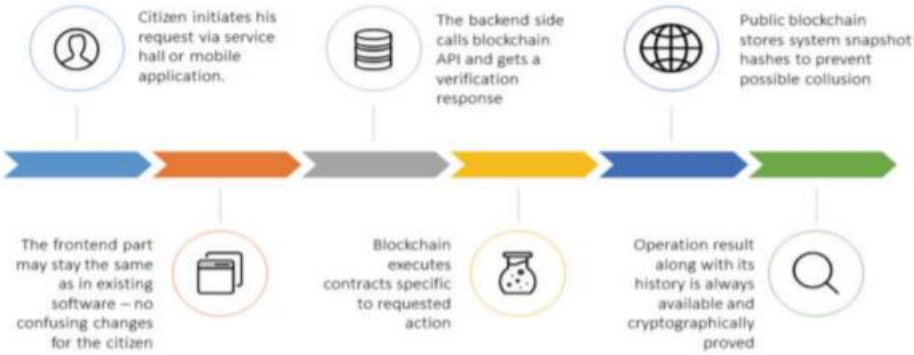

Figure 3 Shang, Q., & Price, A. (2018). *A Blockchain-based Land Titling Project for the Republic of Georgia*. Innovations, 12(3/4), 75

O gráfico acima, também ilustra como é o fluxo das ações necessárias para registrar um imóvel na Geórgia.

[94] Shang, Q., & Price, A. (2018). A Blockchain-based Land Titling Project for the Republic of Georgia. Innovations, 12(3/4), 72-78
[95] Id 94 pg 77.

Cabe dizer ainda que, o resultado tem sido muito positivo até o presente momento, uma vez que houve 1.5 milhões de registros de imóveis somente em 2018. Além dos índices de corrupção divulgados pelo banco mundial e estar em 4 lugar na colocação atualmente.[96] Apesar dos problemas gerais com transparência em outros setores do país[97].

6. CONSIDERAÇÕES FINAIS

Após a pesquisa relacionada ao tema é perceptível que a aplicação de *blockchain* é uma alternativa viável. Apesar dos mitos referentes a sua segurança, o estudo sobre o funcionamento da *blockchain* da *Bitcoin* demonstra que sua aplicação depende de uma rede complexa, e de como a rede é utilizada, haja vista a diferença visível de segurança correlacionado com o número de confirmações. É possível também entender através do capítulo a moeda por trás de tudo isso, sem as simplificações demasiadas.

Não só isso, a parte técnica de escolha ferramental para compor tanto uma rede privada, híbrida, ou pública também fazem diferença considerável nos resultados. E isso necessita de estudos mais específicos relacionados a programação e direito, principalmente no setor de armazenamento de dados. Isso porque, os dados precisam de garantia de segurança para que estejam cumpridas as novas preocupações relacionadas a disponibilização e utilização de dados referentes as leis de proteção de dados.

Foram vistos ainda os benefícios e os desafios associados a implementação da tecnologia. Com ela, seria possível evitar, por exemplo, que um único servidor de armazenamento seja destruído por fatores externos, haja vista a descentralização do centro "livro-razão". Além disso, a redução dos custos de transação pode ser considerada um dos maiores pontos positivos. E a redução da corrupção, que é dada por meio de fraudes e subornos pode ser radicalmente reduzida, caso exista uma aplicação correta, como está sendo o caso da Georgia, que vem atualizando seus registros desde o início dos anos 2000.

Existem riscos inerentes a plataforma, como a aplicação cada vez maior do *Code is Law*, já que vários contratos seriam automatizados com a maior implementação das trocas por meio

[96] The World Bank, 2018. Ease of Doing Business Report. [Online] Disponível em: http://www.doingbusiness.org/en/data/exploretopics/registering-property
[97] Transparency International, 2019. Transparency International-. [Online] Disponível em: https://voices.transparency.org/from-concentrated-power-to-state-capturegeorgias-backsliding-anti-corruption-reforms-c94d76bb2b21 Acesso em 24/11/2019

da *blockchain*. É um campo de estudo da associação do Direito com tecnologia, que apesar de já existir certo nível de pesquisa, ainda é muito novo e precisa de debates que ainda não foram traçados. O principal ponto que precisa desenvolvimento futuro é relacionado a junção de direito de propriedade e posse, a partir do quarto nível de complexidade de implementação.

Para evitar vários desses riscos, foram elaborados os pré-requisitos de Graglia, Melon e Akin. Eles visam mitigar problemas já levantados por outros estudos através dos seus pré-requisitos e evitar casos como a implementação falha dada em Honduras. Dentro deles é possível ver que ainda assim existem desafios, como a atualização da população em relação a digitalização. Georgia deve o seu sucesso, principalmente, a sua digitalização e integração da população com o próprio atendimento pela internet. Isso porque, existe certa desconfiança e dificuldade com a troca de qualquer sistema. Essa atualização apenas da *back-end* e não da *front-end* faz com que a interação com o usuário seja quase imperceptível, o que reduz essa desconfiança e dificuldade inicial.

Os níveis de complexidade na integração entre o registro e a tecnologia também desenvolvidos por Graglia, apontam para diversos caminhos que podem ser trilhados. O Brasil, como pode ser visto, tem tentado aplicar junto a *Ubitquity* o primeiro nível, enquanto a Suécia e Geórgia, já podem ser encontradas em outro grau de complexidade nessa escala. Cabe informar que cada país terá seus próprios desafios e os níveis que ainda não tiveram aplicação, tanto os já pensados pelo autor, quanto outros possíveis também merecem estudos futuros, que não cabiam no escopo deste trabalho.

Por fim, cabe dizer que o intuito de entender sua aplicação, discutir seus principais pontos e entender seus impactos no direito e na sociedade foi cumprida apenas parcialmente. Como foi dito ainda são necessários diversos estudos e as consequências da aplicação de cada *blockchain* tanto no nível de programação, como no caso de DAO, como os impactos reais na sociedade ainda estão para acontecer nos próximos anos, com a maior integração do mundo com essa tecnologia.

7. BIBLIOGRAFIA:

A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, ***Handbook of Applied Cryptography*** (CRC Press, 1997). p. 22-23.

Avramov, Yuriy Valentinovich et al. "***Registering Property: Using Information to Curb Corruption."*** World Bank, December 1, 2017. Disponível em: http://documents.worldbank.org/curated/en/270331513854675950/Registeringproperty-using-information-to-curbcorruption

Benito Arruñada, **Blockchain's Struggle to deliver impersonal Exchange**, 19 Minn, J.L. Scl & Tech. 55 (2018) Disponível em: <https://scholarship.law.umn.edu/mjlst/vol19/iss1/2>

Bitcoin Organization. **What is a Full node**. Disponível em: https://*bitcoin*.org/en/full-node#what-is-a-full-node

BRASIL. **Lei 8935, de 18 de novembro de 1994**. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF. Disponível em: .«http://www.planalto.gov.br/ccivil_03/LEIS/L8935.htm». www.planalto.gov.br.

Brotto, Natália e Ribeiro, Aleff. (2019) ***A LGPD e a tecnologia blockchain são compatíveis?*** Jota. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-lgpd-e-a-tecnologia-blockchain-sao-compativeis-05112019

Buterin, Vitalik. ***Ethereum White Paper: A next generation smart contract & decentralized application platform.*** Disponível em: <https://github.com/ethereum/wiki/wiki/White-Paper>

Carson, Brant. Romanelli, Giulio. Walsh, Patricia. Zhumaev, Askhat. Blockchain beyond the hype: **What is the strategic business value**. Digital Mckinsey, 2018. Disponível em: <https://www.mckinsey.com/business-*functions*/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value> acessado em: 2 de novembro de 2019.

Chohan, Usman W., **The *Double Spending Problem* and Cryptocurrencies** (December 19, 2017). disponível em SSRN: https://ssrn.com/abstract=3090174 ou http://dx.doi.org/10.2139/ssrn.3090174

Coase, R. H., The Nature of the Firm (1937). Economica (new series), Vol. 4, Issue 16, p. 386-405 1937. Available at SSRN: https://ssrn.com/abstract=1506378

Colored Coins White Paper ***Colored Coins: Colored Coins Protocol Specification*** https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification

Couto Silva, Alexandre & Mafra, Ricardo. (2018). **O blockchain como ferramenta de governança corporativa para redução de custos de agência nas sociedades anônimas** em Direito, Tecnologia e Informação. 1. 697-724. Disponível em: https://www.researchgate.net/publication/335243843_O_blockchain_como_ferramenta_de_governanca_corporativa_para_reducao_de_custos_de_agencia_nas_sociedades_anonimas_in_Direito_Tecnologia_e_Informacao/citation/download

Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman (June, 2016). **Blockchain Technology: Beyond *Bitcoin***. Applied Innovation Review. Issue No. 2. Pantas and Ting Sutardja Center for Entrepeneurship & Technology. Berkeley Engineering. UC Berkeley. pg. 8.

Curott, N. (2017). **ADAM SMITH'S THEORY OF MONEY AND BANKING**. *Journal of the History of Economic Thought, 39*(3), 323-347. doi:10.1017/S1053837217000396

Daley, Sam (2019) **31 Blockchain Companies Paving The Way For The Future**. Disponível em: <https://builtin.com/blockchain/blockchain-companies-roundup> Acesso em 01 de novembro de 2019.

Dicionário Financeiro. **O que é escrow?** Disponível em: https://www.dicionariofinanceiro.com/escrow/

Diniz; Maria Helena, **Curso de Direito Civil Brasileiro: Direito das Coisas**, Ed. Saraiva, 2010

Driscoll, Scott. ***How Bitcoin Works Under The Hood***. Imponderable Things, jul 14, 2013. Disponível em: <http://www.imponderablethings.com/2013/07/how-*bitcoin*-works-under-hood.html

ECONOMIST. **The Trust Machine**. 2015. Disponível em: <https://www.economist.com/leaders/2015/10/31/the-trust-machine> acessado em:2 de novembro de 2019.
em: <http://www.imponderablethings.com/2013/07/how-*bitcoin*-works-under-hood.html>

Frankenfield, Jake. Investopedia (2019) ***Smart Contracts***. Disponível em: https://www.investopedia.com/terms/s/smart-contracts.asp

Goldman Sachs Group (2016) "**Profiles in Innovation: Blockchain – Putting Theory into Practice**" pg 7. Disponível em: <https://pgcoin.tech/wp-content/uploads/2018/06/blockchain-paper.pdf>

Graglia, J. M., and Mellon, C. 2018. "**Blockchain and Property in 2018: At the End of the Beginning**" Innovations: Technology, Governance, Globalization (12:1-2), pp. 90-116 Disponível em: https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00270

Graglia, Michael (2017) **Tbilisi agreement heralds significant expansion of blockchain to manage property registries** Disponível em: <https://www.newamerica.org/future-property-rights/blog/blockchain-for-property-rights-georgia/>

Graglia, Michael (2017) **Will Blockchain Work in Ukraine?** Disponível em: https://www.newamerica.org/future-property-rights/blog/will-blockchain-work-ukraine/

Graglia, Michael 2017, ***5 Myths About Blockchains*** NewAmerica Disponível em :https://www.newamerica.org/future-property-rights/blog/5-myths-blockchains-registries/

Graglia, Michael. Mellon, Christopher e Akin, Evan. (2017) ***Prerequisites for Incorporating Blockchain into a Registry*** **New America** Disponível em: https://www.newamerica.org/future-property-rights/blog/prerequisites-incorporating-blockchain-registry/

Neves, Gustavo Kloh Muller. **Propriedade**. Apostila do Curso de Propriedade na Escola de Direito Rio da FGV, 2017.

Herrera-Joancomartí, Jordi. (2014). **Research and Challenges on Bitcoin Anonymity**. 8872. 10.1007/978-3-319-17016-9_1

Infante, Andre (2014) ***Quantum computers de end of cryptography***. Make Use of Disponível em: https://www.makeuseof.com/tag/quantum-computers-end-cryptography/

INFOMONEY.“***Blockchain, a base de dados inviolável do mercado mundial***”, Disponível em: https://www.infomoney.com.br/patrocinados/noticias-corporativas/blockchain-a-base-de-dados-inviolavel-do-mercado-mundial/

Jochnick, Chris. “=**Land Rights and Global Development**.”= Foreign Affairs, February 7, 2017. Disponível em: https://www.foreignaffairs.com/articles/201 7-02-07/land-rights-and-globaldevelopment.

Kersti Kaljulaid (2019). **Estonia is running its country like a tech company**. Disponível em: <https://qz.com/1535549/living-on-the-blockchain-is-a-game-changer-for-estonian-citizens/>.

KOROBKIN, R. B. e ULEN, T. S. **Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics**, California Law Review, vol. 88, n. 4, jul. 2000. p. 1074-1075.

Lemieux, Victoria & Flores, Daniel & Lacombe, Claudia. (2018). **Registro de transações imobiliárias em Blockchain no Brasil (RCPLAC-01) - Estudo de Caso 1**. 10.13140/RG.2.2.16022.45123.

Lessig, Lawrence (2000), Code and Other Laws of Cyberspace.
Lulich, Jordan (2018) **What is Title Insurance and Why is it important?** Forbes. Disponível em: < https://www.forbes.com/sites/jordanlulich/2018/06/21/what-is-title-insurance-and-why-its-important/#747a361612bb>

Mineforeman.com (2013). ***BTC Guild voluntarily limits their hash rate*** Disponível em: https://mineforeman.com/2013/04/06/btc-guild-voluntarily-limits-their-*hash*-rate/

Moloney, Anastasia **Unclear land rights hinders Haiti's reconstruction**, Thomsom Reuters Foundation News, 5 de julho de 2010. Disponível em: http://news.trust.org/item/20100705105000-axvt3/?source=spotnewsfeed

Moreira, Márcio Aurélio Ribeiro. ***ECDSA (Elliptic Curve Digital Signature Algorithm)***. Tese (Especialização em Segurança da Informação), Segurança da Informação, União Educacional Minas Gerais - Minas Gerais.

MOUGAYAR, William (2017). **Blockchain para Negócios: Promessa, Prática e Aplicação da Nova Tecnologia da Internet**. Rio de Janeiro: Alta Books

Nakamoto, S. (2008) ***Bitcoin*: A Peer-to-Peer Electronic Cash System.** https://*bitcoin*.org/*bitcoin*.pdf

Onur, Deler (2017) **End to end *bitcoin* blockchain with examples**. Medium Disponível em : https://medium.com/@onurdeler/end-to-end-*bitcoin*-blockchain-with-examples-52eba6ee7caf

Pollock, Daryn (2019) **Google's Quantum Computing Breakthrough Brings Blockchain Resistance Into the Spotlight Again Forbes** Disponível em: https://www.forbes.com/sites/darrynpollock/2019/09/24/googles-quantum-computing-breakthrough-brings-blockchain-resistance-into-the-spotlight-again/#3019e8374504

Prisco, Giulio (2018). **Swedish Mapping Authority Pioneering Blockchain-based Real Estate Sales**. Disponível em: <https://www.nasdaq.com/article/swedish-mapping-authority-pioneering-blockchain-based-real-estate-sales-cm935347>.

Redação Galileu (2019) ***Cientistas afirmam que Google está prestes a revolucionar a tecnologia com computador quântico*** Disponível em: https://revistagalileu.globo.com/Ciencia/noticia/2019/09/cientistas-afirmam-que-google-esta-prestes-revolucionar-tecnologia-com-computador-quantico.html

Reif Nathan (2019) **A History of *Bitcoin* Hard Forks** . Investopedia Disponível em: https://www.investopedia.com/tech/history-*bitcoin*-hard-forks/

Rosenfeld, M. 2012a. **Analysis of *hashrate*-based double-spending**. Disponível em : http://arxiv.org/abs/1402. 2009

SecureKey 2017 **IBM and SecureKey Technologies to Deliver Blockchain-Based Digital Identity Network for Consumers** https://securekey.com/press-releases/ibm-securekey-technologies-deliver-blockchain-based-digital-identity-network-consumers/

Shang, Q., & Price, A. (2018). **A Blockchain-based Land Titling Project for the Republic of Georgia.** Innovations, 12(3/4), 72-78

Singh, S. and Slegers, C. **Trust and electronic money, Centre for International Research on Communication and Information Technologies**, Melbourne, 1997 SmartDubai Disponível em: https://www.smartdubai.ae/initiatives/blockchain

Souto, Mario (2019) **O que é front-end e back-end?** Alura Disponível em: https://www.alura.com.br/artigos/o-que-e-front-end-e-back-end

Transparency International, 2019. **From concentrated to state capture: Georgias backsliding anti-corruption reforms** Disponível em: https://voices.transparency.org/from-concentrated-power-to-state-capturegeorgias-backsliding-anti-corruption-reforms-c94d76bb2b21

World Bank. **Why Secure Land Rights Matter**. 24 de Março, 2017. Disponível em: http://www.worldbank.org/en/topic/land.

World Bank Group. 2016. **Doing Business 2016 : Measuring Regulatory Quality and Efficiency.** Washington, DC: World Bank. © World Bank. Disponível em: https://openknowledge.worldbank.org/handle/10986/22771

World Bank Group, 2018. **Doing Business 2018: Ease of Doing Business Report.** Disponível em: http://www.doingbusiness.org/en/data/exploretopics/registering-property Acesso em :