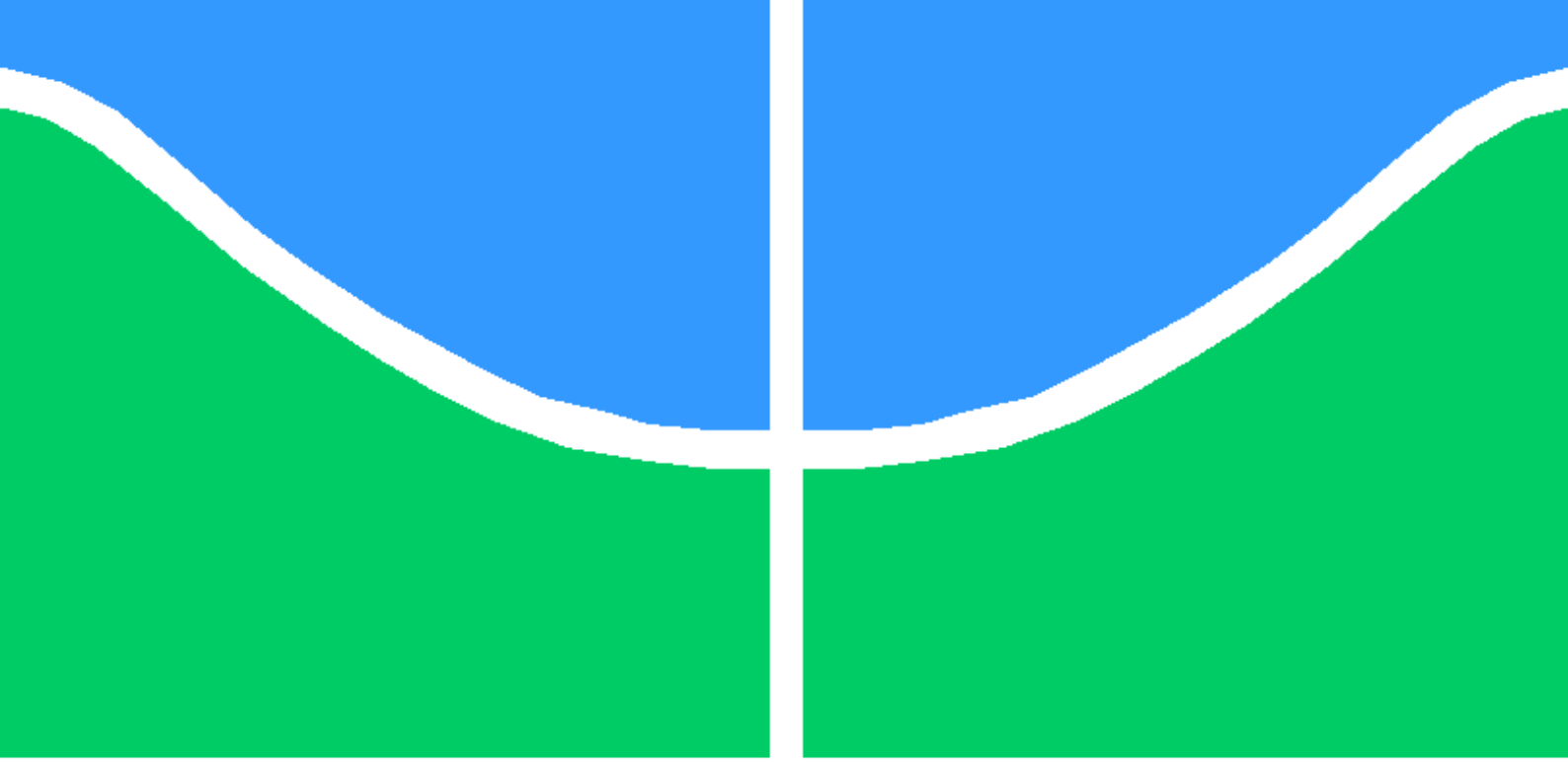

Trabalho Final de Graduação

Cadeia *Blockchain Ethereum*: Um Coadjuvante Para Segurança dos Registros de Imóveis no Distrito Federal.

Trajano Sousa de Melo

Matheus Ferreira de Almeida

Brasília, Dezembro de 2020

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia

Trabalho Final de Graduação

Cadeia *Blockchain Ethereum*: Um Coadjuvante Para Segurança dos Registros de Imóveis no Distrito Federal.

Trajano Sousa de Melo

Matheus Ferreira de Almeida

Relatório submetido ao Departamento de Engenharia
Elétrica como requisito parcial para obtenção
do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. PhD. Rafael Timóteo de Sousa Júnior, _____
ENE/UnB
Orientador

MSc. Francisco Lopes de Caldas Filho, _____
ENE/UnB
Co-orientador

Prof. Dr. Georges Daniel Amvame Nze, _____
ENE/UnB
Examinador

Agradecimentos

Ao Pai do Céu que me permitiu o retorno à Universidade de Brasília para a realização de um sonho. **A minha esposa Lilian**, que aguardou com amor a realização desse sonho. **Aos meus filhos, Luísa, Henrique e Saulo**, pela alegria do reencontro diário. **Aos meus familiares**, tias, irmãos e sobrinhos que sempre incentivaram esse estudante. Aos professores e servidores do Departamento de Engenharia Elétrica da Faculdade de Tecnologia da Universidade de Brasília, especialmente aos professores **Rafael Timóteo de Sousa Júnior, Georges Daniel Amvame Nze e Francisco Lopes de Caldas Filho** pela disposição de orientar e avaliar esse singelo trabalho. **A todos os amigos de 23 anos** que conquistei nesses inesquecíveis anos como graduando em Engenharia de Redes de Comunicação, especialmente ao **Matheus Ferreira de Almeida**, dileto amigo e companheiro inigualável nessa jornada.

Trajano Sousa de Melo

A **minha mãe Vaina, ao meu pai Manoel e minha madrasta Alipia** que tiveram um papel primordial para o meu ingresso na Universidade. Para **minha família, irmãos, tios** que sempre me apoiaram nas escolhas que fiz. Ao **professor Rafael Timóteo de Sousa Júnior** por me orientar neste trabalho, e para o **Francisco Lopes de Caldas Filho** pela determinação e disposição em nos dar suporte para assim melhorar ainda mais este trabalho. E por ultimo mas não menos importantes aos **meus amigos**, que estiveram do meu lado durante esses 5 anos, especialmente ao **Trajano Sousa de Melo** que teve um papel de protagonista em minha vida.

Matheus Ferreira de Almeida

Resumo

As cadeias de *blockchain* emergem como uma nova tecnologia para aplicações em diversas áreas. Desde a proposta do *blockchain* para funcionar como um livro-razão de transações financeiras formulada por Satoshi Nakamoto [25], inúmeros estudos foram produzidos e as virtudes das cadeias de *blockchain* alcançaram outros horizontes. As cadeias de *blockchain* se valem de instrumentos muito antigos como o processamento distribuído, a criptografia e soluções de consenso e a sua utilização nem sempre é recomendada. Aspectos de segurança em relação à modificação de transações realizadas nos remetem à sua utilização como instrumento coadjuvante na segurança de registros públicos, especialmente o referente ao registro de propriedades. O conhecimento de toda cadeia dos proprietários e ex-proprietários dos imóveis (cadeia dominial) e a sua manutenção para consulta da população é essencial para se garantir esse direito e preservar as relações jurídicas advindas de relações imobiliárias. Tal necessidade se compatibiliza com a ideia das cadeias de *blockchain* que podem servir como importante instrumento para a manutenção dos dados e a preservação da cadeia dominial, dificultando a possibilidade de fraudes nos registros públicos. O *blockchain Ethereum*, que permite a formatação de rotinas automatizadas por meio dos *smartcontracts* e a construção de cadeias privadas de *blockchain*, se apresenta como boa solução para auxiliar os sistemas atualmente utilizados para os registros públicos em cartórios brasileiros, conferindo uma maior segurança na manutenção das cadeias dominiais e facilitando a fiscalização dos serviços notariais.

Palavras-chaves: *Blockchain*, *Ethereum*, Cadeia de *Blockchain* Privada, *Smartcontracts*, Registros Públicos, Registros de Imóveis.

Abstract

Blockchain chains emerge as a new technology for applications in several areas. Since the blockchain proposal to function as a financial transaction ledger formulated by Satoshi Nakamoto, numerous studies have been found and the virtues of blockchain chains have reached other horizons. Blockchain chains use very old tools like cryptography and consensus solutions and their use is not always recommended. Security aspects in relation to the modification of transactions carried out refer to its use as a supporting instrument in the security of public records, especially regarding the registration of properties. The knowledge of the entire chain of owners and ex-owners of properties (domain chain) and their maintenance for the consultation of the population is essential to guarantee the right of property and preserve the legal relationships arising from real estate relations. This need is compatible with the idea of blockchain chains that can serve as an important tool for the maintenance of data and the preservation of the domain chain, making it difficult for fraud in public records. The Ethereum blockchain, which allows the formatting of automated routines through smart contracts and the construction of private blockchain chains, presents as a good solution for auxiliary systems currently used for public registries in Brazilian registries, providing greater security in the maintenance of chains and facilitating the inspection of notarial services.

Keywords: Blockchain, Ethereum, Private Blockchain Chain, Smartcontracts, Public Records, Property Records.

SUMÁRIO

LISTA DE FIGURAS

1 Introdução

A propriedade privada é um dos direitos fundamentais garantidos por nossa Constituição Federal. A importância deste direito em uma sociedade capitalista faz com que o Estado tenha uma especial preocupação para a sua instituição e salvaguarda. Para tal, quando tratamos de propriedade de bens imóveis, o Estado Brasileiro mantém uma grande estrutura de serviços públicos delegados para gerir e garantir a manutenção e transmissão desse direito. Graças a essa estrutura governamental delegada, os bens imóveis podem servir como garantias e incrementar a economia de toda a sociedade.

A importância desse sistema de gestão e garantias nos remete à reflexão de como a evolução das tecnologias poderia contribuir para a segurança das transações imobiliárias. Na realidade atual, cada Ofício de Registros de Imóveis administra um banco de dados próprio, com a obrigatoriedade de manutenção de um *backup* em lugar situado fora da sede do cartório. Temos, portanto, apenas uma instituição gerindo e zelando pelo banco de dados dos registros de imóveis de determinada localidade.

A obrigatoriedade de manutenção de um banco de dados em localidade diversa da sede dos cartórios de imóveis é exigência do Conselho Nacional de Justiça e busca ampliar a segurança relativa à manutenção dos dados armazenados. Tal preocupação dos órgãos fiscalizadores nos remete à discussão de como as novas tecnologias poderiam auxiliar na ampliação da segurança dos Ofícios de Registros de Imóveis.

As fronteiras para a aplicação das cadeias de *blockchain* em atividades não financeiras foram rompidas e a discussão sobre sua utilização em diversas atividades é uma constante [41], [40] [27], [44], [11] e [9]

O encadeamento de informações ou transações em uma rede distribuída que, após o consenso de seus participantes, torna o registro praticamente imutável é virtude que muitos buscam para suas aplicações [41]. O desafio da utilização dessas cadeias é instigante e muitas empresas renomadas buscam a construção de ferramentas para este fim [43].

O nascimento do *blockchain* que está ligado à substituição de entidades centralizadas de controle de atividade financeira [25], se volta agora, com a concepção de cadeias privadas, para o exercício dessas mesmas atividades de controle e fiscalização com a utilização das cadeias de *blockchain*. As cadeias privadas surgem como alternativas para a utilização dos benefícios do *blockchain*, mesmo em entidades controladoras de atividades estatais [41].

Verificamos que a execução de um sistema de banco de dados distribuíco, com menores custos de manutenção, maior segurança e maior confiabilidade é perfeitamente compatível com a tecnologia existente das cadeias de *blockchain*.As cadeias de *blockchain* privada onde o controle e processamento descentralizado se concentre em autoridades previamente definidas pode servir de um modelo para inclusão do *blockchain* como coadjuvante nos aspectos de preservação de dados

dos Ofícios de Registros de Imóveis.

Para a apresentação de um modelo de transição que objetiva incorporar as cadeias de *blockchain* às rotinas dos ofícios de registros de imóveis, optamos pela adoção de uma cadeia *Ethereum* privada, que permite a elaboração de *smartcontracts*, possibilitando a devida adaptação dos sistemas atualmente utilizados para o novo conceito.

No presente trabalho desenvolvemos uma explanação sobre as cadeias de *blockchain*, especificando as peculiaridades da cadeia *Ethereum* na formatação de *smartcontracts*. Apresentamos a realidade do direito imobiliário em nosso país, introduzindo conceitos mínimos para realçar a importância do direito imobiliário e a necessidade da segurança da preservação de dados dos registros imobiliários. Em seguida, discorremos sobre os procedimentos próprios dos cartórios de imóveis no Distrito Federal, realidade que é replicável para os demais Estados pois a legislação de regência é federal, para apresentar a nossa solução de uma cadeia de *blockchain Ethereum* que possa ser coadjuvante ao atual sistema de registros imobiliários, conferindo uma maior segurança aos registros públicos.

O trabalho proposto busca aliar as virtudes de segurança de uma cadeia de *blockchain* privada com a forma atual de trabalho dos cartórios do Distrito Federal, apresentando uma solução de transição do atual sistema registrário para um modelo em que as cadeias de *blockchain* possam prover os serviços de um banco de dados distribuídos, praticamente imutável, fato que trará uma maior segurança para os registros imobiliários.

Para a construção do modelo de transição, formatamos uma sistema *WEB* que representa os atuais serviços dos cartórios de imóveis e estruturamos *smartcontracts*, programados em linguagem *Solidity* 4.0, capazes de introduzir, em cadeia de *blockchain Ethereum* os dados obrigatórios pela legislação brasileira referentes a matrículas, registros e averbações de imóveis urbanos.

Para a validação do modelo apresentado optamos pela utilização da *IDE REMIX* como simulador da cadeia de *blockchain* com os dados que introduzimos no sistema *WEB*. As simulações realizadas permitiram a constatação da inclusão de dados na cadeia de *blockchain* e sua compatibilidade com a legislação atual dos registros públicos no Brasil.

1.1 Justificativa

O encadeamento de dados e transações que, com o auxílio da criptografia, permanecem de forma quase imutáveis nas cadeias de *blockchain* se mostram perfeitamente adequadas à realidade dos registros de imóveis que devem manter informações com as mesmas características, quais sejam: encadeadas no tempo e imutáveis.

A segurança na manutenção dos dados registrados nos cartórios de imóveis e a garantia da sua imutabilidade é que torna concreto o direito de propriedade em nossa sociedade.

As transações que envolvem imóveis costumam envolver recursos que, muitas vezes, decorrem de anos de poupança ou, até mesmo, enormes endividamentos. Tais recursos representam somas consideráveis de valor e, não raramente, decorrem de muitos anos de trabalho. Tais transações,

portanto, devem ser resguardadas pelo Poder Público para que os cidadãos possam, de forma transparente, buscar informações seguras sobre os bens negociados.

Os imóveis se prestam, igualmente, como garantia para empréstimos e, nessa função garantidora, os credores necessitam de informações seguras e transparentes sobre os bens recebidos em garantia.

No atual sistema legal brasileiro, as informações sobre os registros públicos é delegada aos Oficiais de Registros Públicos que mantém um banco de dados público para garantir a transparência de toda e qualquer negociação imobiliária.

A proposta de adotar uma cadeia de *blockchain* como coadjuvante na segurança dos registros públicos facilita o acesso às informações registradas e amplia a segurança jurídica das transações imobiliárias, além de se valer como um instrumento para a fiscalização das atividades delegadas aos Oficiais de Registros Públicos .

O registro de matrículas de imóveis, registros e averbações em cadeias de *blockchain* dificultará, igualmente, a possibilidade de fraudes decorrentes da alteração indevida nos registros públicos.

1.2 Objetivos

O presente trabalho apresenta os objetivos gerais e específicos descritos a seguir.

1.2.1 Objetivo Geral

- Propor o modelo de uma cadeia de *blockchain Ethereum* privada que possa auxiliar na segurança e fiscalização dos registros imobiliários.

1.2.2 Objetivos Específicos

- Analisar a situação do Distrito Federal para a implantação de uma modelo de transição para a utilização de cadeia de *blockchain Ethereum* como coadjuvante para a segurança e fiscalização dos registros públicos.
- Propor um modelo para essa cadeia de *blockchain Ethereum*.
- Elaborar simulações do funcionamento dessa cadeia de *blockchain* Ethereum para as finalidades especificadas.

1.3 Hipótese

As características das cadeias de *blockchain* se adequam às necessidades exigidas pela legislação brasileira para a manutenção dos registros de imóveis. Tais registros são essenciais à garantia do direito de propriedade e sua utilização pode servir para ampliar a segurança dos dados registrados e facilitar a fiscalização do Poder Público sobre essa atividade delegada.

Nos registros de imóveis, informações sobre o titular da propriedade e restrições que recaem sobre os imóveis são armazenadas de forma sequencial e devem permanecer imutáveis. Tais características sinalizam para a possibilidade de se utilizar cadeias de *blockchain* no armazenamento desses dados.

1.4 Metodologia

A pesquisa desenvolvida no presente trabalho é de natureza experimental, passando pela proposição do modelo de uma cadeia de *blockchain* para armazenar dados de registros públicos de imóveis.

Após a concepção do modelo da cadeia de *blockchain*, desenvolvemos os *smartcontracts* e uma ferramenta *WEB* para simular os atuais sistemas de gerenciamento dos ofícios de imóveis.

O sistema *WEB* formatado foi alimentado com dados reais de 50 (cinquenta) matrículas de registros de imóveis de um Ofício de Registro de Imóveis do Distrito Federal e simulações da cadeia *blockchain* foram executadas na ferramente *REMIX*.

1.4.1 Restrições da Pesquisa

- O sistema *WEB* formatado tem limitações e serviu para indicar a possibilidade de convivência e adaptação dos atuais softwares utilizados pelos ofícios de registros de imóveis com a cadeia de *blockchain* proposta.
- A validação da cadeia de *blockchain* proposta foi executada apenas no simulador *REMIX*.
- A simulação da cadeia de *blockchain* limita-se ao Livro nº 2, Registro Geral, que cuida dos principais dados dos registros de imóveis.

O presente trabalho está organizado da seguinte forma:

1. O Capítulo 1 traz uma apresentação da pesquisa realizada, reportando a importância dos registros públicos para o direito de propriedade e a adequação da utilização das de *blockchain* para o registro de imóveis.
2. O Capítulo 2 apresenta artigos que identificamos sobre os temas relacionados no projeto e o marco teórico do trabalho. Conceitos sobre *blockchain* e registros públicos são apresentados.
3. O Capítulo 3 descreve, de forma detalhada, os sistemas *WEB* e os *smartcontracts* concebidos em nosso projeto.
4. O capítulo 4, apresenta a validação da proposta. Demonstramos a inclusão e consulta de dados na cadeia *blockchain* e simulamos as funções fiscalizadoras.
5. No capitulo 5 são apresentadas as conclusões retiradas do trabalho e as contribuições futuras.

2 Revisão Bibliografica e Marco Teórico

2.1 Revisão Bibliográfica.

O tema central do trabalho, *blockchain*, diz respeito a uma tecnologia relativamente recente e objeto de inúmeros estudos nos últimos anos. Com sua origem em um texto de 2008, somente em 2013 teve desdobramentos para aplicação além do uso de uma criptomoeda. Os textos de Nakamoto (na verdade um pseudônimo de autor desconhecido) [25] e de Buterin [13] foram as bases da descrição dos modelos de *blockchain* do *Bitcoin* e do *Ethereum*.

Para uma melhor compreensão de conceitos básicos das cadeias de *blockchain*, nos valemos das abordagens de Nofer [27], Yaga [41], Zhang [34] e Cong [9].

Aspecto interessante em nossa pesquisa foi observar as discussões sobre aplicação ou não da cadeia de *blockchain* dada a presença de outras tecnologias. Yaga [41], Wüst [40] e Halaburda [16] apresentam interessante discussão sobre este aspecto. Nesse ponto verificamos diversos autores assinalando as virtudes do *blockchain* em sua aplicação para os registros de imóveis. Os artigos de Nofer [27], Zheng [44], Crosby [11], Wüst [40] e Cong [9] citam especificamente esta utilização.

Interessante abordagem sobre as relações entre smartcontract e o direito foram observadas em Rodrigues[31].

A utilização das cadeias de *blockchain* como serviço (*blockchain-as-a-service* também foram observadas como objeto de diversos estudos. Biswas [7] e Zheng [43] trazem olhares para esse ponto.

No outro tema do trabalho, registros imobiliários, para o qual optamos por ressaltar a importância do direito de propriedade que justifica a necessidade de manutenção de um sistema de registros públicos seguro, seguimos principalmente a renomada autora, Maria Helena Diniz em sua obra "Sistemas de Registros de Imóveis"[12], para apresentar a forma como se desenvolve a escrituração dos registros imobiliários, buscando trazer de forma didática o fluxo de procedimentos para esse registro. Ainda para o trato dos registros públicos a obra “Registros Públicos: Teoria e Prática”, de Loureiro [21] também serviu de apoio.

Uma grata surpresa foi o texto de Graglia e Mellon [15] que relaciona de forma explícita o direito de propriedade com a tecnologia *blockchain*. Os autores apresentam pré-requisitos para a utilização da tecnologia do *blockchain* em registros imobiliários e estágios para a implantação de um sistema totalmente operante em cadeia de *blockchain*.

Na busca de referências bibliográficas, identificamos um caso específico de utilização de *blockchain* para registros imobiliários que foi implementado em um cartório da cidade de Pelotas. Referência feita por Graglia [15] foi objeto de Estudo de Caso por Lemieux, Flores e Lacombe [20].

A experiência realizada em Pelotas encontra-se no estágio inicial indicado por Graglia, ou seja, limita-se ao armazenamento de documentos em cadeia de *blockchain*.

2.2 Marco Teórico.

2.2.1 *Blockchain Bitcoin*.

O *blockchain* foi inicialmente apresentado em um pequeno artigo de autoria atribuída a Satoshi Nakamoto[25]. O texto apresenta uma alternativa para o pagamento de transações realizadas na internet sem a necessidade de utilização de intermediários como acontece ordinariamente no sistema bancário tradicional (Yaga[41]). Diversas virtudes são descritas para a nova modalidade proposta, nelas incluídas a diminuição dos custos das operações de transferência de recursos e o decremento das taxas de fraudes (Yermark[10]). Um sistema de dados distribuídos, sem uma organização central reguladora, presente em uma rede de computadores, que encadeia bloco de transações utilizando criptografia em transações *peer to peer* - relação direta entre as partes (Zhang [34]).

O sistema bancário, que existe como garantidor das transações executadas, poderia ser afastado e a credibilidade das transações seria dado pelo conhecimento prévio e público das transações sem afastar o sigilo dos participantes (Zheng [44]). Uma nova e promissora modalidade de acreditação de transações poderia ser experimentada com muitos benefícios para seus usuários.

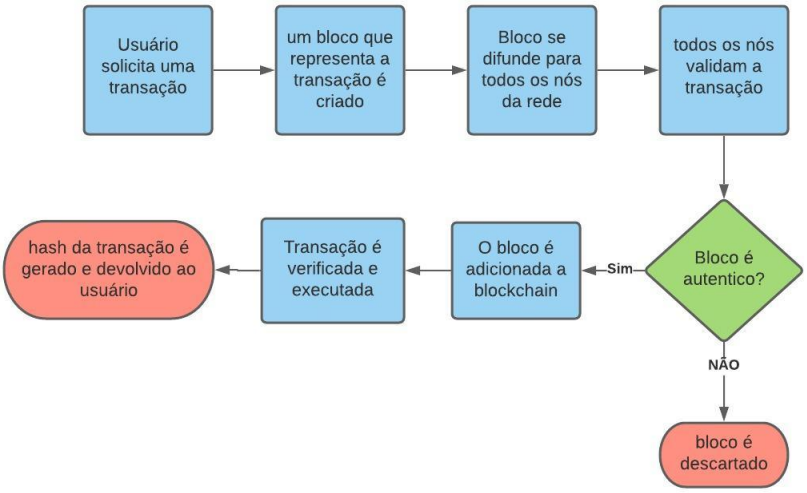

Figura 2.1 – Funcionamento do *Blockchain*.
Fonte: Autores.

Bruce, e outros [8], apontam como principais características do *blockchain Bitcoin* a sua transparência, disponibilidade, consenso, descentralização e segurança. Ainda segundo os autores, a tecnologia enfrenta desafios relacionados à falta de escalabilidade, exigência de um alto custo computacional, e excessiva replicação de dados.

O sistema proposto por Nakamoto [25] consiste em um bloco de transações, que se apresentam em uma linha de tempo, que são confirmadas por agentes anônimos, em um sistema de computação distribuída que utiliza de criptografia para assegurar a sequência dos blocos e as transações efetuadas. Os agentes anônimos confirmam *hashs* gerados das novas transações em troca de um valor residual da operação (este mecanismo é hoje denominado mineração). Os *hash* de cada nova

operação considera o *hash* da operação anterior, tornando cada vez mais confiável as transações mais antigas, transformando o bloco em algo praticamente imutável em sua totalidade.(Nofer [27], Yaga [41], Zhang [34])

Uma definição informal de blockchain, traduzida livremente, é apresentada por Yaga [41]:

> "Blockchains são livros digitais distribuídos, de transações criptograficamente assinadas, que são agrupados em blocos. Cada bloco está criptograficamente ligado ao anterior (tornando-o resistente à adulteração) após validação e passar por uma decisão de consenso. Com a adição de novos blocos, blocos mais antigos tornam-se mais difíceis de modificar (criando os resistentes à adulteração). Novos blocos são replicados em cópias do livro-razão dentro da rede, e quaisquer conflitos são resolvido automaticamente usando regras estabelecidas."

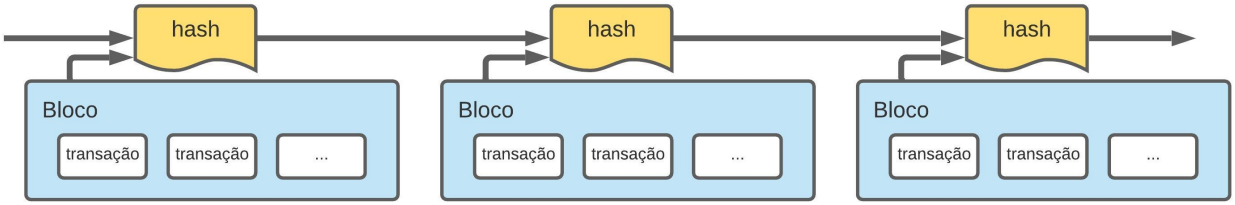

Figura 2.2 – Linha do Tempo
Fonte: Adaptado de Nakamoto [25].

A cadeia de blocos proposta por Nakamoto [25] se limitou a transferência de recursos e originou o que conhecemos como *Bitcoin*, a primeira moeda digital (Cong [9] Zheng [44]). Cada titular de um valor em *Bitcoin* pode transferir recursos a terceiros, em uma transação *peer to peer*, acrescentando sua transação em um bloco da cadeia *blockchain*. Cada bloco pode conter diversas transações.

As transações são efetuadas utilizando-se uma criptografia assimétrica com uma das partes assinando a transação com sua chave privada e a outra parte da transação confirmando com a chave pública do remetente (Zheng [44]).

No encadeamento do blockchain Bitcoin, cada bloco mantém em seu *header* um *hash* calculado sobre os dados do *header* do bloco anterior, além das seguintes informações: i) hora da construção (*timestamp*);ii) *nonce*; iii) *hash* das árvore *Merkel Tree* formada pelas transações do bloco.

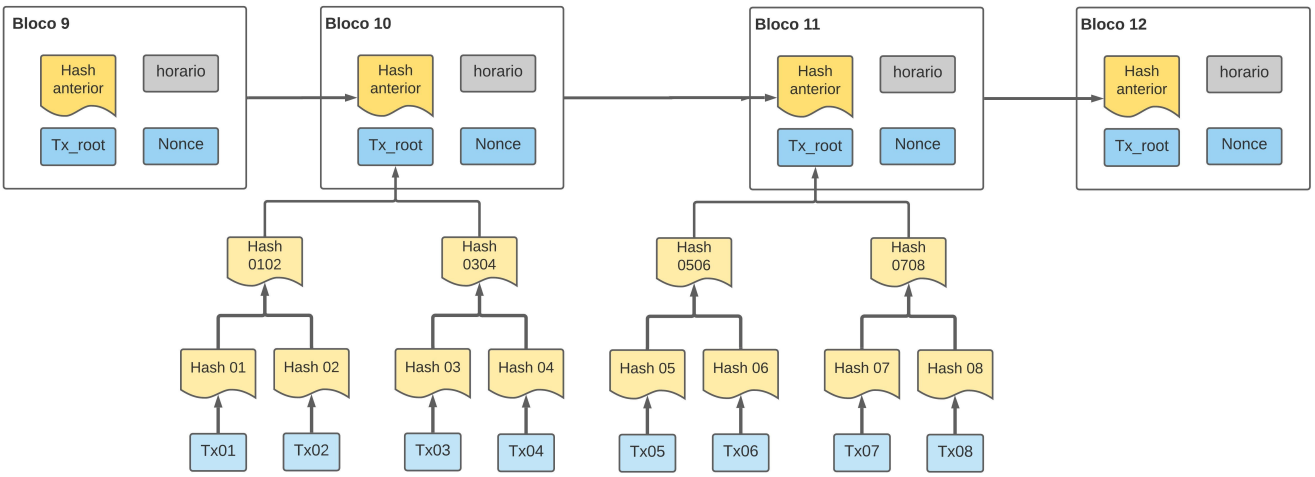

Figura 2.3 – Estrutura Bloco *blockchain Bitcoin*.
Fonte: Adaptado de Yermack [10].

Para que este mecanismo funcione é necessário que se confirme que não houve nenhuma outra transação realizada pelo cliente que transferiu os recursos, isso para impedir um duplo repasse dos mesmos recursos. A solução apresentada passa pelo anúncio público da transação e a concordância da maioria dos nós mineradores com o histórico das transações. Detalhes sobre ataques de duplo repasse podem ser vistos em Zhang [42].

Para que o histórico de transações seja de concordância majoritária, foi concebido por Nakamoto [25], um servidor próprio que anuncia publicamente o último *hash* do bloco de transações. Este servidor foi chamado de servidor da linha de tempo. O desafio, então, seria fazer com que esta linha de tempo pudesse ser implementada de forma única por todos que interagissem com o *blockchain*. Para isso, Nakamoto [25] propõe um protocolo de criptografia para estabelecer um consenso entre os participantes do *blockchain*. O protocolo utilizado no *Bitcoin* é denominado *proof of work* (prova de trabalho).

O protocolo *proof of work* consiste na realização de uma tarefa, previamente definida, para que o bloco possa ser inserido na cadeia. A tarefa proposta deve ser de difícil execução, mas de fácil comprovação de sua realização (Yaga [41]). Na proposta do *bitcoin*, a tarefa consiste na produção de um *nonce* que faça com que um determinado número de *bits* do *hash* tenha valor igual a zero. A comprovação da tarefa é imediata pois basta certificar o número de zeros do *hash* e o esforço computacional não é impossível. Introduzido este *nonce*, a transação proposta é adicionada ao *blockchain* e um novo *hash* do bloco é criado aguardando que outros mineradores realizem a tarefa proposta para validação de novos blocos.

O trabalho computacional para validação dos blocos inseridos na cadeia *blockchain* é recompensado com uma transferência de recursos aos que realizam essa tarefa (mineradores). Toda transação do Bitcoin envolve a transferência de uma parte dos recursos para os que participam da validação dos blocos. Tal procedimento torna atrativo utilizar os recursos computacionais disponíveis para participar da validação dos blocos, e não para promover ataques à cadeia. Detalhes

sobre a mitigação de ataques *Distributed Denial of Service - DDoS* pelo protocolo *proof of work* podem ser vistos em Saad [33].

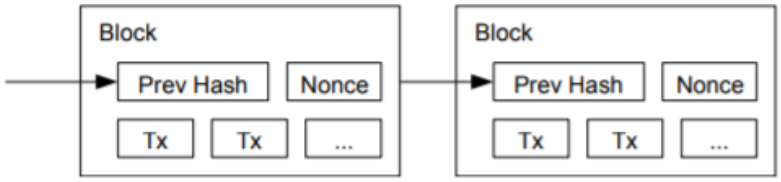

Figura 2.4 – Protocolo *proof of work*.
Fonte: Nakamoto [25].

A rede do *blockchain* proposta por Nakamoto [25] tem os seguintes passos:

- 1) uma nova transação é publicada em *broadcast* para todos os nós da rede;
- 2) cada nó coloca esta nova transação no bloco;
- 3) os nós iniciam o trabalho computacional para realizar a prova de trabalho;
- 4) quando algum nó realiza a tarefa ele coloca o novo bloco em *broadcast*;
- 5) a nova transação é aceita se todas as tarefas são comprovadas e se não são repetidas;
- 6) os nós manifestam a aceitação da nova transação e passam a utilizar o *hash* criado na última transação para uma nova tarefa.

O consenso exigido para a cadeia *blockchain Bitcoin* poderia ser fraudado caso algum dos validadores da cadeia (mineradores) controlasse mais da metade dos recursos computacionais do total da rede (ataque de 51%.). Este ataque deve ser considerado apesar de sua pouca probabilidade de ocorrer justamente em razão do oferecimento de recompensa pelo trabalho de validação dos blocos (mineração). Estudos sugerem a troca do protocolo de consenso para a escolha randômica de mineradores (Bae [6]), abandonando-se o *proof of work*, a punição para mineradores suspeitos, dentre outras medidas para manter o *blockchain Bitcoin* seguro (Shanaev [35]).

Para o bom funcionamento da entrega dos incentivos, o *blockchain* permite que transações sejam divididas e, em regra, as transferências de recursos são feitas considerando a transferência principal, diminuída do valor a ser pago pela tarefa de validação da transação, valor este que é direcionado, na mesma transação, para remunerar o trabalho dos mineradores.

Com o passar dos anos, uma cadeia *blockchain* poderia ter tamanho incomensurável e de difícil armazenamento em todos os nós da cadeia. Para evitar o problema de espaço de armazenamento na cadeia do *blockchain*, foi proposto uma simplificação para a validação das transações. Não é necessário que os nós possuam todas as transações arquivadas, mas apenas os *headers* (cabeçalhos) dos blocos. Cada *header* tem tamanho muito pequeno (cerca de 80 bytes) que podem ser facilmente

armazenadas em computadores caseiros. Para isso utiliza-se a estrutura denominada *Merkle tree* que nada mais é que uma árvore de informações resumidas.

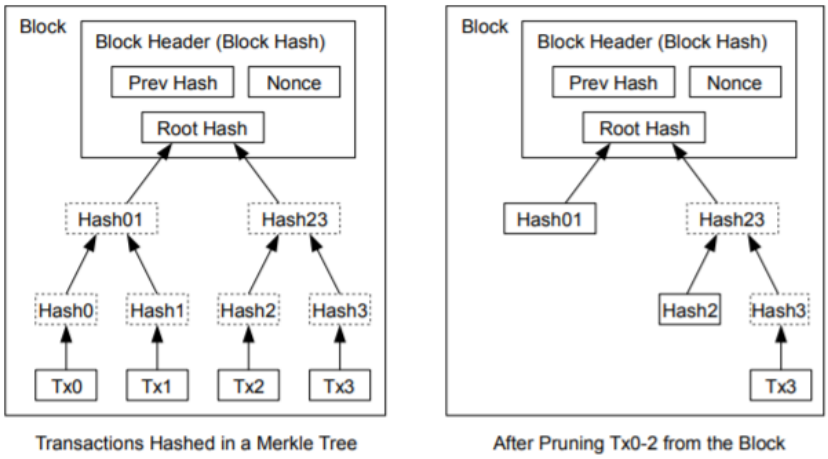

Figura 2.5 – Árvore de Merkle
Fonte: Nakamoto [25]

A proposta de Nakamoto transformou-se em realidade e o que fora proposto em seu texto *"Bitcoin: a Peer to Peer Eletronic Cash System"* [25], quando em aplicação, se mostrou bastante sólido. Em 2016 houve uma movimentação de cerca de 10 bilhões de dólares com bitcoins (Zheng [44]). As virtudes vislumbradas do processo hoje se fazem presentes na moeda virtual criada e a transferência de recursos sem intermediário, utilizando um sistema distribuído de computação, está em operação.

A idéia do *blockchain* para a transferência de recursos foi desdobrada, levando o conceito para outras atividades. Hoje há cadeias de *blockchain* não somente para moedas virtuais, mas para qualquer contrato que pode ser formatado em uma transação de um *blockchain*. Esses contratos, desde que bem formulados, são registrados e podem ser exigidos (executados) quando suas condições ocorrerem. Tudo isso sem a necessidade de qualquer intermediário.

O *blockchain Ethereum* é o mais conhecido sistema que possibilita a formatação de *smartcontracts*, concedendo às cadeias *blockchain* um alcance extraordinário. Esta característica do *Ethereum* é que o torna o sistema mais indicado para a construção de um *smartcontracts* específico para a migração da base de dados de um cartório imobiliário para uma cadeia de *blockchain*.

2.2.1.1 *Coloured Coins*.

Antes da concepção da cadeia de *blockchain Ethereum*, estudos foram feitos para a utilização da cadeia do *Bitcoin* para outras finalidades além da troca de criptomoedas. Ao resolver a questão da computação descentralizada e a formação de um consenso para o encadeamento de blocos, o *Bitcoin* se tornou objeto de intensos estudos para sua utilização em outros fins. Desta forma, inúmeros estudos foram produzidos que apresentavam protocolos de utilização do *Bitcoin* que serviriam para outras finalidade.

Uma das alternativas para utilização do *Bitcoin* foi denominada *coloured coins*. Por este protocolo metadados são incluídos na cadeia de *blockchain* e, assim, informações podem ser preservadas nos blocos encadeados, ampliando a utilização do *Bitcoin* para outros fins. Rosenfeld, em artigo publicado em 2012 [32], apresenta uma visão geral deste protocolo.

A virtude da utilização do protocolo *coloured coins* é poder utilizar a cadeia de *blockchain Bitcoin* para armazenar dados. O grande problema, entretanto, é que a quantidade de dados armazenáveis é muito pequena. Os metadados são incluídos em campo próprio (*OP RETURN*) que possui tamanho de apenas 80 *bytes*.

A limitação de dados dificulta a ampla utilização do *blockchain Bitcoin*, mas é suficiente para o armazenamento de *hash* de documentos e, assim, possibilitar a utilização do *Bitcoin* como coadjuvante na preservação de dados como se faz necessário nos registros públicos.

A inclusão de *hash* de documentos na cadeia de *blockchain Bitcoin* também permite que se formatem, de forma limitada, *smartcontracts*. Para tal é necessário que o processamento se dê fora da cadeia de *blockchain* e neste aspecto a cadeia *Ethereum*, que possibilita um processamento na própria cadeia, tem larga vantagem em relação ao *Bitcoin*.

Uma melhor abordagem sobre as características do protocolo *coloured coins* pode ser vista em [3].

2.2.2 *Blockchain Ethereum*.

Após o advento da cadeia do *Bitcoin*, em 2013, Buterin nos apresenta um novo modelo de cadeia de *blockchain* denominada *Ethereum*. A descrição se deu no artigo "*Ethereum White Paper*" [13] e introduz a possibilidade de novas aplicações para cadeias de *blockchain*. O novo modelo de *blockchain* aumenta a aplicação das cadeias de processamento descentralizadas para muito além da troca de valores de criptomoedas. Neste novo cenário uma cadeia de *blockchain* funcionaria como um Ciclo Completo de Turing, permitindo programações para um número indefinido de aplicações.

A primeira diferença entre as cadeias *blockchain Bitcoin e Ethereum* diz respeito ao protocolo de consenso utilizado pelas cadeias. O *Bitcoin* utiliza o protocolo *proof of work* e o *Ethereum* se vale do protocolo GHOST (*Greedy Heaviest Observed Subtree*). Os protocolos de consenso se prestam para a solução de problemas relacionadas à *forks* (criação de ramos na cadeia de *blockchain*), definindo qual ramo da cadeia *blockchain* seguirá e qual será abandonado. No protocolo *proof of work* do *Bitcoin* a cadeia maior é a que prossegue e as menores são abandonadas. No protocolo *GHOST*, a mineração permite a criação de ramos e o peso desses ramos é que definirá a cadeia que será preservada no *blockchain*. A descrição do protocolo *GHOST* pode ser vista em Sompolinsky [38].

Sompolinsky [38] também reporta que a utilização do protocolo GHOST pode evitar o ataque 51%. Em tal ataque, os fraudadores buscam construir uma cadeia maior para se sobrepor à cadeia original do blockchain. Como o protocolo GHOST nem sempre aproveita a cadeia maior, esse ataque fica menos efetivo. A figura representa um comparativo de um ataque 51% em uma cadeia de *blockchain* com os protocolos proof of work e *GHOST*.

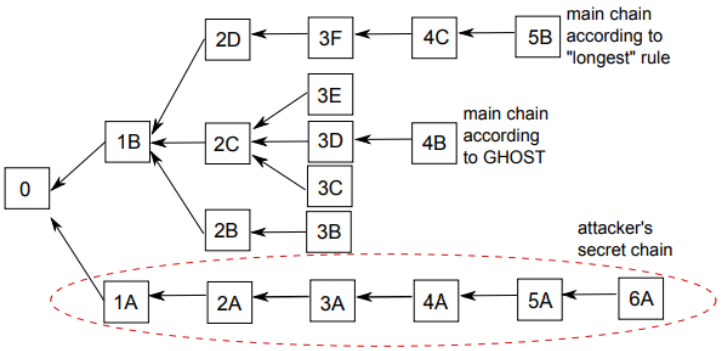

Figura 2.6 – Comparativo ataque 51%.
Fonte: Sompolinsky [38].

Outra inovação apresentada pelo *Blockchain Ethereum* diz respeito às contas que interagem com o *blockchain*. No *Ethereum* além das contas externas, controladas por usuários; contas internas, controladas por contratos, também interagem com o *blockchain* Vujičić [39].

Vitalik [13] aponta a existência de mensagens (*messages* e transações (*transactions*) no *Blockchain Ethereum*. Vujičić [39] define transação como "uma instrução criptograficamente assinada"e informa a existência de dois tipos de transações: i) uma que dá origem a uma mensagens; e ii) outra que cria uma nova conta. A transação seria um pacote de dados assinado e despachado por uma conta externa.

O estado de transição da cadeia *Ethereum* se mostra mais sofisticado que o do *Bitcoin*. A primeira constatação que se deve fazer, em ambas as cadeias, é se a transação está formatada da forma correta, após esta análise preliminar as diferenças se apresentam. Enquanto no cenário da cadeia do *Bitcoin* a transição dos blocos necessita confirmar apenas se a conta que envia recursos tem valores suficientes para o envio e para o processamento descentralizado (mineração), confirmando a transação em caso positivo e não o fazendo em caso negativo, o cenário da cadeia *Ethereum* necessita de novos dados. Para a execução do processamento dos *smartcontracts* torna-se necessário um novo cálculo de recursos para o processamento, que pode variar de contrato para contrato. Os novos valores que devem ser checados da conta daquele que inicia a transação no *blockchain* são denominados de de *STARTGAS* e *GASPRICE* (Vujičić [39]).

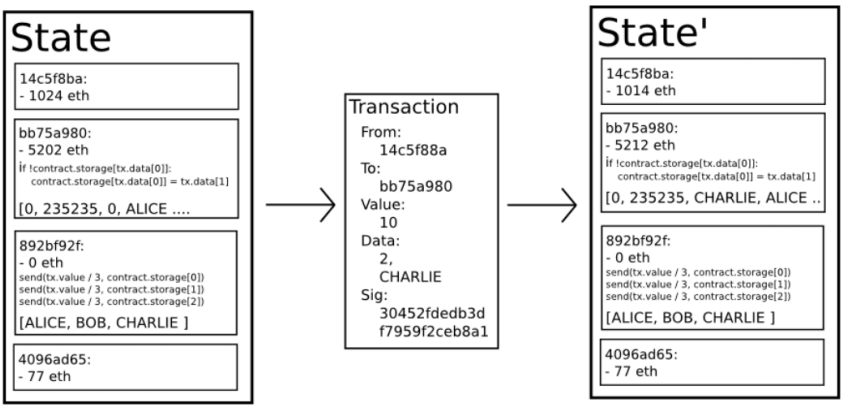

Figura 2.7 – Transação Ethereum.
Fonte: Vitalik [13].

Na figura observamos uma transição de estágios onde se verifica a disponibilidade de recursos para o processamento exigido na transação. Na transição é verificado se os valores para o processamento (*startgas e gasprice*) estão presentes na conta que acessa o *blockchain*. Existindo valores suficientes, é criado um segundo estágio (*state'*) com esses valores já debitados.

O *STARTGAS* pode ser entendido como o limite de gastos fixado para o processamento descentralizado e o *GASPRICE* é o valor fixado para cada passo do processamento do *smartcontracts*. A fixação desses valores serve para evitar a execução em erro de eventuais *loops* infinitos de algum *smartcontracts*. Tais valores inibem, igualmente, ataques de negação de serviços pois cada requisição no sistema é tarifada.

Os códigos dos *smartcontracts* do *blockchain Ethereum* são processado em uma máquina virtual - *Ethereum Virtual Machine (EVM)*. A programação dos contratos é compilada para a linguagem da EVM.

Com a implementação de uma cadeia de *blockchain* que oferta operações de um Ciclo Completo de Turing as possibilidades para utilização de *blockchain* romperam as barreiras da mera formatação de um livro caixa como no *Bitcoin*.

2.2.2.1 *Smartcontracts*.

O conceito de *Smartcontracts* foi apresentado por Szabo que o definiu, em tradução livre, como "um conjunto de promessas, especificado em formato digital, incluindo protocolos dentro dos quais as partes cumprem essas promessas"(Magazzeni [22]). Szabo [14], quando tratou dos *smartcontracts*, não se afastou dos conceitos jurídicos relativos aos contratos e apresentava o que a tecnologia poderia trazer para inovar neste ramo do direito (Szabo [14]). Este conceito foi apresentado em 1996, muito antes da concepção das cadeias de *blockchain*.

Vimos que a cadeia de *blockchain Ethereum* se aproveita da solução de consenso de transações processadas de forma distribuída e acrescenta a possibilidade de que programas inseridos no *blockchain* demandem a construção de novos blocos. Tal possibilidade é que torna viável a concepção

e execução dos denominados *smartcontracts* (Cong [9]).

Os contratos inteligentes, na verdade, são codificações implantadas em uma cadeia de *blockchain* e que, como toda codificação, realiza as operações pré-determinadas quando as condições previstas ocorrem. Não há muita diferença entre um *smartcontracts* e outro programa computacional. A grande diferença é que a codificação inicialmente fixada não pode ser alterada pois os comandos foram implementados em uma cadeia de *blockchain* que é praticamente imutável. Assim, torna-se possível estabelecer obrigações e compromissos com caráter de irretratabilidade quando as condições pré-fixadas ocorrerem (Shermin [36]). Essas características identificam um *smartcontracts* .

Os *smartcontracts* interagem na cadeia de *blockchain Ethereum* como qualquer outro cliente da cadeia. A atuação na cadeia se dá por meio de contas, que identificam o usuário da cadeia, assim, cada *smartcontract* possui uma conta interna que o habilita a interagir na cadeia. Os *smartcontracts* podem ser referidos em transações e realizar transações definidas em seu código.

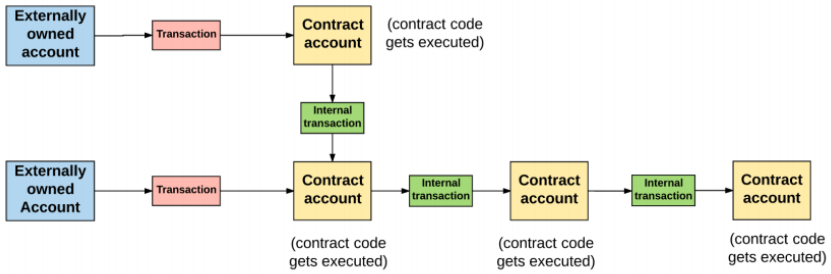

Figura 2.8 – Transações de *Smartcontracts*
Fonte: Preethi Kasireddy [17].

Um *smartcontract* tem, pois, a virtude de ser autoexecutável, o que traz uma maior segurança para as transações neles fixadas. Não há espaço para um inadimplemento contratual nas relações entabuladas por um *smartcontract*. A programação dessas relações deve ser cuidadosa para prever todas as condições futuras e evitar alguma fragilidade de inexecução quando as condições se implementarem. A cuidadosa programação é que permitirá uma efetiva 'autoexecutoriedade'.

Narder, na obra "Curso de Direito Civil" [24] conceitua contrato da seguinte forma:

> "Contrato é modalidade de fato jurídico, mais especificamente, de negócio jurídico bilateral ou plurilateral, pelo qual duas ou mais vontades se harmonizam a fim de produzirem resultados jurídicos obrigacionais, de acordo com o permissivo e limites da lei."

Os *smartcontracts* não são contratos na ótica do direito brasileiro, pois se tratam de uma codificação que pode expressar um pacto entre pessoas, com a definição de direitos e obrigações tal como nos contratos jurídicos. A codificação de um *smartcontract* poderia ser comparada ao texto formal, o instrumento jurídico adotado para um contrato. O contrato jurídico expressaria os direitos e obrigações assumidas e a sua formalização se daria na codificação dos *smartcontracts*. O direito prevê diversas formas de se contratar, inclusive contratos verbais. Ninguém formaliza um

contrato escrito para a compra e venda de pão e leite em uma padaria, mas existe um contrato formalizado de forma verbal. Com os *smartcontracts* temos mais uma forma de expressar um contrato jurídico, a codificação de direitos e obrigações. Agora, com os *smartcontracts* temos não mais um texto formal, mas uma codificação que reporta os direitos e obrigações assumidas contratualmente.

Há limitações legais para a formalização de contratos na legislação brasileira. A regra é que os contratos possam se estabelecer de qualquer forma, salvo quando a legislação imponha uma forma determinada. Assim, a codificação (*smartcontracts*) pode, em regra, servir como instrumento de um contrato. Como exemplo das limitações legais, trazemos a compra e venda de imóveis, que deve ser realizada por instrumento público (escritura pública lavrada em um cartório de notas). Deste modo, para a validade de um *smartcontracts* que regulasse a compra e venda de imóvel, seria necessária a devida escritura pública onde obrigações e direitos fossem estipuladas entre os contratantes e os *smartcontracts* poderiam ser formatados como opção de execução de parte desse contrato como, por exemplo, o pagamento parcelado do valor em criptomoedas.

Rodrigues [31] ao tratar dos *smartcontracs* afasta a possibilidade de sua apreciação pelo Poder Judiciário eis que o mesmo teria sua autoexecutoriedade sempre que as condições estabelecidas na programação ocorressem. Em nossa realidade jurídica, qualquer discussão em razão de relações jurídicas podem ser levadas ao Poder Judiciário, mesmo que tais relações tenham sua origem em um *smartcontrac*.

2.2.2.2 A Linguagem *Solidity* e a *IDE Remix*.

Para a codificação dos *smartcontracts* foi concebida uma linguagem de alto nível, orientada a contratos, denominada *Solidity*. Com síntese semelhante à linguagem *JavaScript* foi desenhada para facilitar a programação de contratos a serem executados na Máquina Virtual *Ethereum - EVM (Ethereum Virtual Machine)* (Grishchenko [2].

A linguagem *Solidity* se apresenta de forma muito semelhante às linguagens orientadas a objetos e os *smartcontracts* corresponderiam às classes. Nos *smartcontracts* é possível formatar declarações de variáveis de estado, funções, modificadores de funções, eventos, tipos de estruturas e tipos de Enum. Os conceitos de herança também estão presentes na linguagem.

A *IDE Remix* é recomendada para a programação *Solidity*. Apresenta grande facilidade de trabalho pois é baseada em *Browser* e possui um compilador integrado. Permite a execução simulada de cadeias de *blockchain*, fato que foi determinante para a sua escolha em nosso projeto.

A documentação da linguagem está disponível na internet [4].

2.2.3 Criptografia e Descriptografia.

A criptografia, palavra de origem grega, que une *kruptós* (secreto ou oculto) e *graphía* (escrita), é um mecanismo que podemos utilizar para a transmissão e armazenamento de dados e tem por objetivo principal evitar que terceiros não autorizados tenham acesso à informação transmitida ou guardada.

No passado teve enorme importância nos cenários da diplomacia e guerra. Atualmente é instrumento essencial para as relações privadas no ambiente da rede mundial de computadores. Atividades como *home bank* e transações bancárias *on line* seriam inimagináveis sem a utilização de uma criptografia confiável.

Resumidamente, a criptografia consiste em codificar uma mensagem ou dado para que somente pessoas autorizadas, e que saibam como decodificar a mensagem, possam acessar os dados. Inúmeras técnicas surgiram para a construção desses códigos e, basicamente, encontramos dois modelos de criptografia:

- i) a de uso de chave simétrica e
- ii) a de uso de chave assimétrica.

Ao utilizar o procedimento de chave simétrica, emissor e destinatário da mensagem possuem uma única e idêntica chave para codificação e decodificação. Assim, a confiança entre as duas partes é essencial e o bom funcionamento dessa técnica pressupões a prévia transmissão e guarda da chave comum de forma segura. Sinteticamente funciona da seguinte forma:

- a) as partes compartilham a chave comum;
- b) o emissor ou guardião da mensagem utiliza a chave criptográfica para codificar a mensagem;
- c) após a transmissão ou guarda da mensagem cifrada, o destinatário da mensagem pode desvendar o real conteúdo utilizando a chave criptográfica previamente compartilhada para descriptografar a mensagem.

A criptografia simétrica também é conhecida como criptografia de chave privada ou criptografia de chave única.

Este é o modelo mais antigo da criptografia e a complexidade das chaves evoluiu de forma acentuada com o advento da computação. Nas reminiscências da utilização da criptografia o código alfabético foi utilizado como forma de cifrar mensagens (chave criptográfica) e o mecanismo funcionava como uma mera troca de letras segundo uma regra previamente definida e compartilhada entre os emissores e destinatários da mensagem.

A criptografia assimétrica, conhecida também como criptografia de chave pública funciona com a utilização de duas chaves criptográficas. Uma chave é utilizada para codificar a mensagem e a outra chave diversa é utilizada para decodificar a mensagem. Uma chave é denominada chave pública e a outra chave privada . A chave pública é de conhecimento geral, não sendo necessário qualquer medida para resguardar o seu conteúdo. A chave privada, ao contrário, deve ser armazenada com segurança pelo seu titular. Este modelo pressupõe a divulgação e armazenamento de chaves públicas de emissor, guardião e destinatário das mensagens. Assim, as chaves públicas são divulgadas abertamente e qualquer pessoa que deseje encaminhar ou guardar uma mensagem

para determinado destinatário utilizaria a chave pública do destinatário para cifra a mensagem e, assim, somente o destinatário, detentor da chave privada correspondente, é que poderia decodificar a mensagem. (Szabo [14])

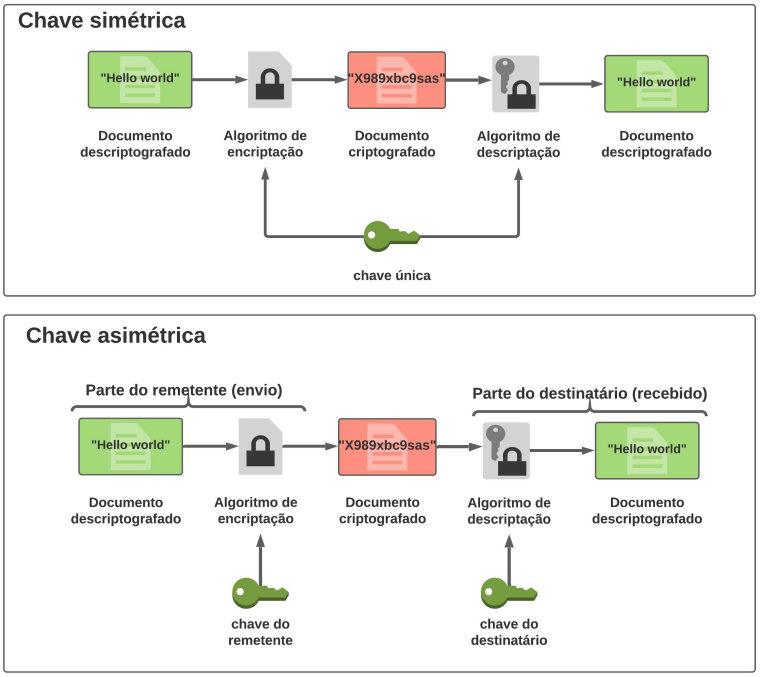

Figura 2.9 – Criptografia Simétrica e Assimétrica
Fonte: Autores.

A evolução da criptografia sempre estará ligada à capacidade de se descobrir os códigos criptográficos e, consequentemente, quebrar a mensagem cifrada e obter a real informação. No passado a simplória chave alfabética apresentava segurança satisfatória, hoje complexos modelos criptográficos que utilizam combinação de chaves de até 512 bits podem se sentir ameaçadas diante da computação quântica que se avizinha.

2.2.3.1 *Hash*.

Podemos definir *hash* como uma função criptográfica unidirecional que codifica uma mensagem de tamanho indeterminado em uma mensagem de mesmo tamanho.

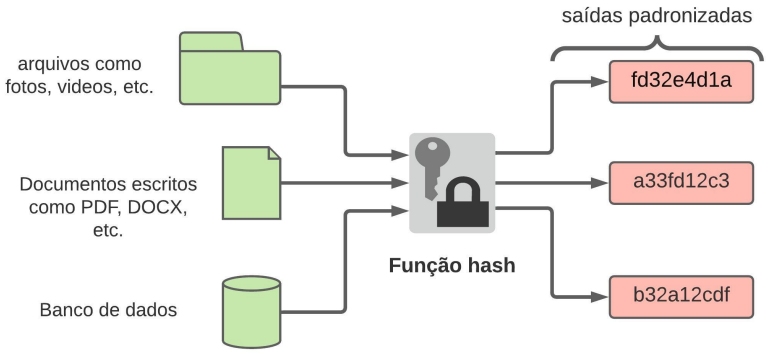

Figura 2.10 – Função *Hash*.
Fonte: Autores.

A característica unidirecional da função *hash* torna impossível a sua utilização como chave criptográfica mas a sua importância está na fixação de um tamanho pré-determinado para a mensagem cifrada. Em razão dessas característica, a função *hash* é chamada de função resumo. Ou seja, qualquer mensagem pode ter o seu *hash* calculado e ser resumida ao tamanho desse *hash*.

Para a boa utilização da função *hash* temos que buscar os seguintes predicados na função:

- i) inicialmente o cálculo do *hash* deve ser fácil e rápido;
- ii)a reversão do *hash* para a mensagem original deve ser difícil;
- iii) qualquer alteração da mensagem original deve gerar alteração no *hash*;
- iv) a mesma mensagem deve gerar, sempre, o mesmo *hash* e
- v) mensagens diversas não podem gerar *hash* iguais.

Uma boa função *hash* tem ampla utilização para a certificação da integridade de uma mensagem ou dado. A menor alteração que se faça em uma mensagem pressupõe uma alteração em seu *hash* e, portanto, é facilmente constatável qualquer alteração da mensagem original.

Essas duas características da função *hash*, quais sejam, a boa utilização para constatar a integridade de dados e a capacidade de resumir qualquer mensagem a um tamanho pré determinado podem ser bastante exploradas em projetos de armazenamento de dados como os utilizados em cartórios de imóveis.

As cadeias de *blockchain* encontram nas funções *hash* um elemento essencial para sua segurança e aspectos relacionados a possíveis ataques são objeto de estudos frequentes. As características das funções *hash* e estudos sobre sua vulnerabilidade são reportados em Wang [30].

2.2.3.2 *MD5 – Message Digest Algorithm 5.*

Existem várias formas de se calcular um *hash* de arquivos. Uma das funções que executa essa tarefa é a denominada *MD5* (*Mensage Digest 5*). Essa função, atualmente, já não é muito utilizada em razão de sua fragilidade na questão de colisão, ou seja, de que duas mensagens possam produzir um mesmo *hash*. Apesar dessa fragilidade, sua utilização ainda é segura para casos de verificação de integridade de documentos.

A função foi desenvolvida no *MIT*, por Ron Rivest, no início da década de 1990, e converte todo arquivo em uma sequencia de 32 caracteres hexadecimais (128 bits).

Uma das fragilidades do *MD5* para o arquivamento de senhas é que seu algoritmo é muito leve e rápido, assim, com facilidade é possível fazer uma ataque de combinações para identificar a senha que deu origem ao *hash MD5*. Essa fragilidade, entretanto, não interfere na função do *hash* para a prova de integralidade de documentos e se torna uma virtude em razão da rapidez com que se calcula o *hash* para o texto ou documento que se quer testar a integridade. Importante ressaltar o MD5 é bastante referenciado e de fácil implementação.

Apresentamos exemplos de códigos para implementação do MD5.

```
--> Criacao de um hash MD5 em java script <--
    <script type="text/javascript">
         var hashMD5 = CryptoJS.MD5([documento PDF]);
    </script>


--> Criacao de um hash MD5 em PHP <--
    <?php
         $hashMD5 = md5([documento PDF]);
     ?>
```

Outro aspecto positivo para o uso do *MD5* nos propósitos de nosso trabalho é que apesar de sua fragilidade de colisão, ou seja, que dois documentos possam gerar um mesmo número de *hash*, não é possível a adulteração de um documento e fazer com que o documento adulterado tenha o mesmo *hash*, assim, as fragilidades apontadas, não interferem no resultado esperado em nosso trabalho.

Detalhes sobre como se processa a função *MD5* podem ser consultadas na RFC1321 (*RFC – Request For Comments da IETF (Internet Enginnering Task Force)* [1].

2.2.4 Critérios Para Utilização da Tecnologia *Blockchain*.

As cadeias de *blockchain*, como vimos, reúnem diversas tecnologias que já se apresentavam há vários anos. A criptologia assimétrica é narrada por Szabo [14], em 1997, como uma nova perspectiva para a transmissão de dados. O mesmo Szabo apresentou o conceito de *smartcontract* em 1994. Assim, os mesmos instrumentos utilizados pelo *blockchain* podem ser utilizados por outras tecnologias (Halaburda [16]) e surge, então, a discussão sobre o porque utilizar *blockchain*.

Inicialmente é importante apresentar os diversos tipos de cadeia *blockchain*. Yaga [41] e Wust

[40] reportam 2 (dois) tipos de cadeias de *blockchain*: i) uma em que qualquer pessoa pode ingressar e interagir com a rede (*permissionedless*, também chamada de *blockchain* público); ii) outra em que apenas pessoas autorizadas podem interagir com a rede (*permissioned*, também conhecida como *blockchain* privada). Zhnag [34] introduz uma terceira classificação denominada *blockchain consortium* em que somente pessoas pré-determinadas podem validar nós mas o acesso aos dados seria público.

Wust [40] apresenta interessante fluxo para a tomada de decisão sobre a conveniência ou não para a utilização das cadeias de *blockchain*.

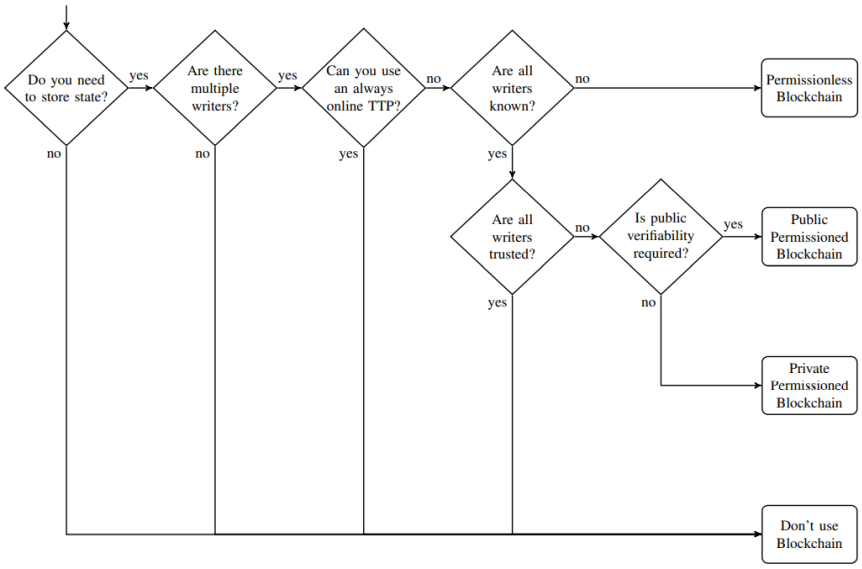

Figura 2.11 – Fluxo Para Decidir Sobre Utilização do *Blockchain*.
Fonte: Wust [40]

De forma semelhante, Yaga [41] apresenta um outro fluxo, elaborado pelo *The United States Department of Homeland Security (DHS) Science Technology Directorate* para orientar sobre a utilização do *blockchain* ou outras tecnologias.

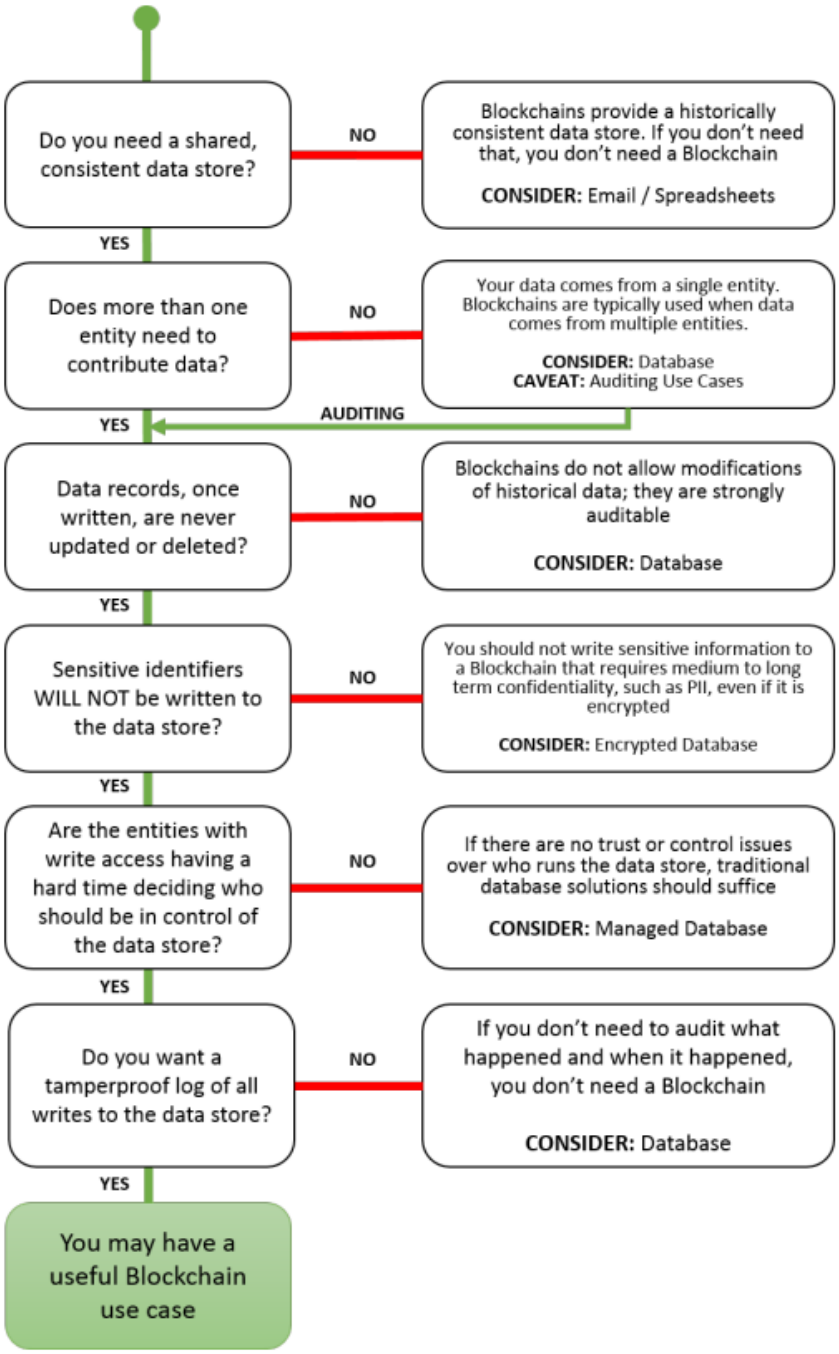

Figura 2.12 – Fluxo Para Decidir Sobre Utilização do *Blockchain* - DHS.
Fonte: Yaga [41].

Observando os dois fluxos apresentados podemos afirmar que os serviços de registros de imóveis são compatíveis para a utilização de cadeias *blockchain*. As seis perguntas trazidas no fluxo da DHS são respondidas de forma afirmativa para as atividades de registros públicos.

Diversos autores também atestam a compatibilidade da utilização de cadeias *blockchain* para as atividades de registro de imóveis (Nofer [27], Zheng [44], Crosby [11], Wust [40][]).

2.2.5 *Blockchain as a Service - BaaS.*

Blockchain as a Service - BaaS se traduz pela utilização da tecnologia *blockchain* para a realização de serviços. *BaaS* tem se mostrado como uma tecnologia emergente e na visão de Singh [37] é similar à computação em nuvem, ofertando benefícios semelhantes.

Zheng [43] afirma que o *blockchain as a service* seria uma combinação da computação em nuvem com a tecnologia *blockchain*.

A computação em nuvem, ao seu tempo, na definição trazida pelo *NIST (National Institute of Standards and Tecnologia)*, órgão do Departamento de Comércio dos Estados Unidos, é um modelo que permite acesso difuso, e sob demanda, a uma rede compartilhada de recursos de computação configuráveis de forma rápida e fácil gerenciamento [23].

A mesma *NIST* apresenta cinco características principais para a computação em nuvem: i) serviço *on demand* e *self service*; ii) capacidade de disponibilização de serviços em diversas plataformas; iii) provisão de recursos computacionais em diferentes localidades e disponíveis aos clientes de forma onipresente; iv) facilidade para ampliação dos recursos exigidos pelos clientes (elasticidade); v) recursos podem ser monitorados e disponibilizados de forma transparente aos clientes e provedores.[23]

Por fim o órgão de padronização americano apresenta três modalidade de serviços que podem ser ofertados pela computação em nuvem: i) *Software as a Service* onde provedores podem oferecer aplicações diretamente a seus clientes utilizando infraestrutura da nuvem. ii) *Planform as a Service* onde os consumidores podem implantar seus softwares na nuvem utilizando programas de linguagem, bibliotecas, serviços e ferramentas fornecidos pelo provedor da computação em nuvem. iii) *Infrastruture as a Service* aqui o consumidor não tem o controle da infraestrutura da nuvem, mas controla todos os sistemas operacionais, espaços de armazenamento e estruturas para implantar softwares, possibilitando,inclusive, a gestão de componentes de rede.

Zheng [43] entende que o *blockchain as a service* funcionaria de forma semelhante aos serviços *Platform as a Service*.

Por fim, Singh conclui que a utilização do *blockchain* como serviço (*BaaS*) dependerá das peculiaridades da aplicação e a sua operacionalização, em seus aspectos de segurança, privacidade e governança também podem ser definidos pelos provedores [37].

Atualmente diversas empresas como a IBM e Microsoft anunciam plataformas para utilização do *blockchain as a Service* [43].

Para a implantação da tecnologia do *blockchain* em aplicações diversas em uma *smart city*, Biswas [7] apresenta o esquema de uma *framework*, com cinco camadas que, em uma visão *top down* teríamos:i) camada de interface *interface layer*; ii) camada de dados *database layer*; iii) camada de comunicação *communication layer* e iv) camada física *physical layer*.

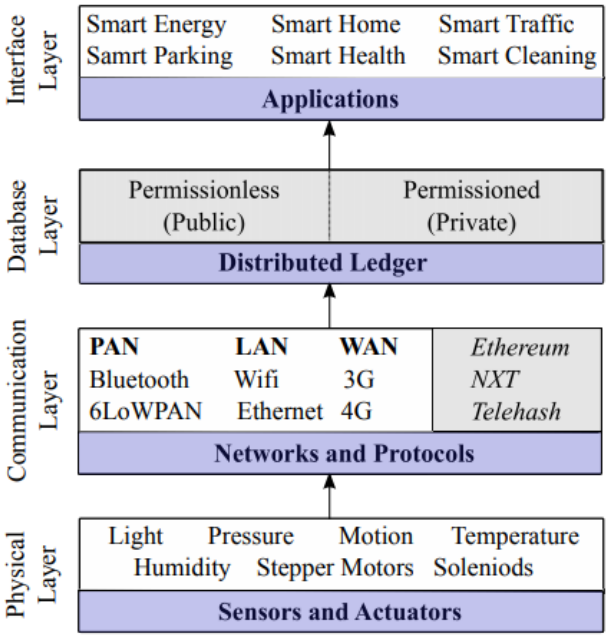

Figura 2.13 – *Framework* para *Blockchain as a Service - Baas* em uma *Smart City*
.

Fonte: Biswas [7].

Nos serviços de registros públicos a camada física proposta por Biswas poderia ser representada pelos computadores presentes nos cartórios que alimentariam a cadeia *blockchain* disponível. Na camada de aplicação teríamos um 'Cartório Inteligente'.

2.3 Registro de Imóveis.

A atividade de registro de imóveis em nosso país é delegada pelo Poder Público a pessoas que, por meio de concurso público, passam a exercer a função de Oficial de Registro de Imóveis. A atividade pública, exercida por particulares, é fiscalizada pelos Tribunais de Justiça e Ministérios Públicos Estaduais.

Existe uma legislação federal que impões as condições e requisitos para a escrituração dos registros públicos. A importância desta atividade se evidencia em uma sociedade capitalista onde a propriedade privada é eixo dos sistemas econômicos.

Assim, os registros de imóveis se mostram como instrumentos essenciais em nosso país para a preservação do direito de propriedade e para a garantia das relações jurídicas que se vinculam à propriedade privada.

No anexo I de nosso trabalho discorremos com mais detalhes sobre os registros públicos e o direito de propriedade na legislação brasileira.

A seguir abordaremos apenas os elementos essenciais dos conceitos de propriedade e da realidade dos registros públicos para a compreensão dos sistema de *blockchain* proposto.

2.3.1 Propriedade.

O direito de propriedade estabelece um vínculo de um objeto ou imóvel a uma pessoa, seja ela física ou jurídica (pessoas jurídicas são as empresas e sociedades).Este vínculo, em uma sociedade capitalista, precisa ser reconhecido pela sociedade para que o proprietário possa reivindicar os direitos sobre o bem contra qualquer outra pessoa.

Para a garantia do direito de propriedade de bens imóveis é necessário que o Estado afirme quem é o legítimo titular desse direito para todas as demais pessoas da sociedade, somente assim é que o legítimo proprietário poderá exercer o seu direito contra terceiros.

Aspecto interessante do direito de propriedade é a faculdade que o proprietário tem de ceder parte desse direito a terceiros, mantendo, entretanto, a própria propriedade. Assim, o direito de posse, por exemplo, pode ser repassado a título oneroso em um contrato de locação de imóveis. Essa faculdade também permite a entrega dos bens imóveis como garantia de empréstimos e tal fato é instrumento essencial para o incremento de toda a economia.

Para todos as relações que se estabelecem com os imóveis, a publicidade é essencial, pois o direito à propriedade pode ser invocado, indistintamente, contra qualquer pessoa caracterizando-se, na linguagem jurídica, como oponível *erga omnes*.

A publicidade das relações que envolvem os imóveis é dada pelos Ofícios de Registros de Imóveis, também conhecidos como cartórios de imóveis.

2.3.2 Ofícios de Registros de Imóveis.

Como já afirmamos a principal função dos cartórios de imóveis é dar a devida publicidade do direito de propriedade. Assim, informações sobre a localidade do imóvel, suas especificações, o seu titular, as restrições eventualmente existentes sobre o direito de propriedade, dentre outras, devem estar inscritas de forma transparente e de fácil acesso a qualquer interessado.

A manutenção desses dados e a sua constante atualização, quando relações jurídicas alterem os direitos de propriedade, devem ser objeto de preocupação do Poder Público, pois somente assim é que se pode garantir o livre exercício desse direito.

No país, os cartórios de registros de imóveis tem essa função. Para que tais registros possam ser confiáveis, a legislação definiu que cada imóvel somente pode ser escriturado em um único cartório de imóveis. A concentração desses dados em apenas um cartório serve para evitar conflitos de informações. Assim, os cartórios de imóveis são distribuídos em localidades definidas pelos Tribunais de Justiça Estaduais e promovem a inscrição de todos os imóveis da região definida pelo tribunal.

A escrituração dos registros é disciplinada por legislação federal que gera uma uniformidade em todo o país para as inscrições de registros nos cartórios de imóveis. Todos os cartórios de registros de imóveis do país devem seguir a Lei nº 6.015/73 e suas alterações.

A norma federal estabelece a obrigatoriedade de manutenção de 5 (cinco) livros nos cartórios de registro de imóveis: Livro 1 - Protocolo; Livro 2 - Registro Geral; Livro 3 - Registro Auxiliar;

Livro 4 - Indicador Real e Livro 5 - Indicador Pessoal.

É no Livro 2 - Registro Geral - que as principais informações sobre os imóveis devem ser escrituradas. A identificação do imóvel, com suas características, a indicação do proprietário e dos ex-proprietários e referências sobre os ônus atribuídos aos imóveis são anotados nesse livro.

2.3.3 Procedimentos para o Registro de Imóveis.

Os cartórios de imóveis, como vimos, servem para a manutenção de uma base de dados confiável sobre a situação dos imóveis e devem seguir um padrão de escrituração fixado em lei. Na gestão desses serviços, os cartórios recebem, principalmente, dois tipos de demandas. A primeira uma demanda por informações que armazena. A segunda referente à alteração do banco de dados que administra.

Par melhor entendimento, apresentamos nas figuras 2.9 e 2.10, os fluxos dessas atividades dos ofícios de registro de imóveis.

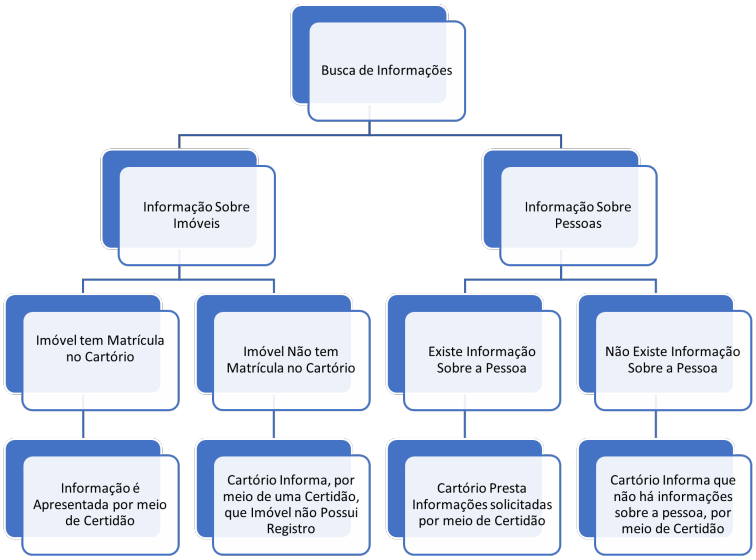

Figura 2.14 – Fluxo de Busca de Informações
. Fonte: Autores.

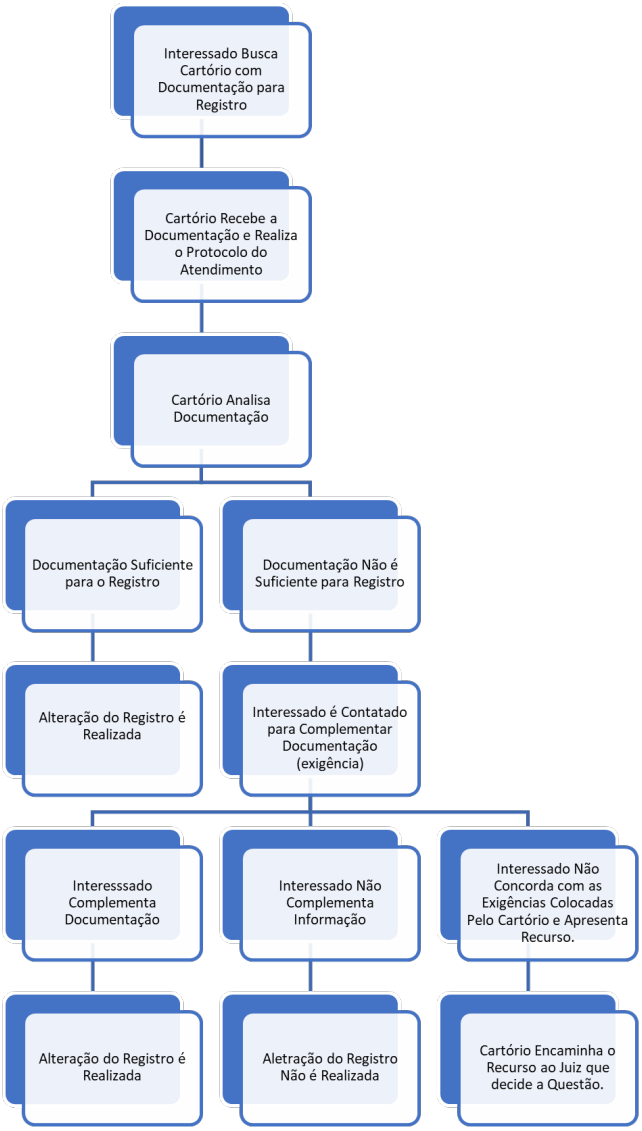

Figura 2.15 – Fluxo de Alteração de Registros
. Fonte: Autores.

Nosso trabalho apresentará uma alternativa de transição para a adoção de cadeia de *Blockchain* que possa auxiliar a atividade de registros de imóveis, especialmente nos aspectos relacionados à segurança referente à imutabilidade dos dados registrários.

3 Arquitetura Proposta.

3.1 Protótipos dos Sistemas.

Para a formalização de um protótipo de sistemas que possa introduzir o *blockchain* nas rotinas de um cartório de registro de imóveis, realizamos visita ao 7º Ofício de Registro de Imóveis do Distrito Federal e acompanhamos, integralmente, os processos adotados pelo cartório para uma averbação em um registro de imóveis.

Apresentaremos os atuais fluxos de processos do ofício de registro de imóveis para alteração de registros, indicaremos uma proposta para os novos fluxos advindos da inclusão do *blockchain* no sistema e, em seguida, abordaremos os protótipos do sistema de *blockchain* e do sistema *WEB*.

3.1.1 Processos de Um Ofício de Registro de Imóveis.

As duas principais demandas de um ofício de registro de imóveis são os de busca de informações (figura 2.14) e o de alteração de registros (figura 2.15). Tais fluxos são definidos pela Lei de Registros Públicos e devem ser observados por todos os cartórios de registro de imóveis. O fluxo de pedidos de informação (figura 2.14) não é escopo do presente trabalho pois não há alteração de registros, mas uma mera recuperação de dados já registrados.

Os pedidos de alterações de registro (descrito na figura 2.15), quando se torna possível a realização dessas alterações, geram um fluxo de processos nos cartório que pode ser representado pela figura 3.1

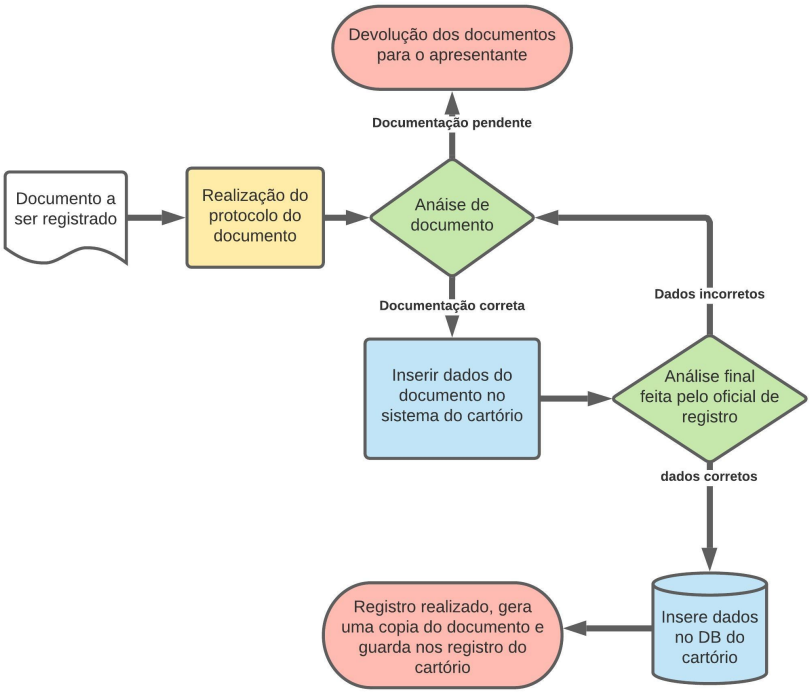

Figura 3.1 – Fluxo de Processos do Cartório.
Fonte: Autores.

Os atuais processos não contemplam registros em plataformas diversas da existente nos cartórios. Em visita às instalações do 7º Ofício de Registro de Imóveis do Distrito Federal pudemos constatar a utilização de um software específico que auxilia na formalização dos registros e é responsável pelo armazenamento das informações registradas em banco de dados local. Informações colhidas indicam a obrigatoriedade de manutenção de um *backup* dos dados registrados em localidade diversa da sede do cartório.

A proposta de nosso trabalho indica a alteração dos fluxos de processos praticados pelos cartórios, onde se acrescentam atividades para a inclusão de dados na cadeia de *blockchain* privada. Assim, os processos para a alteração de registros ficariam, sinteticamente, como indicado na figura 3.2.

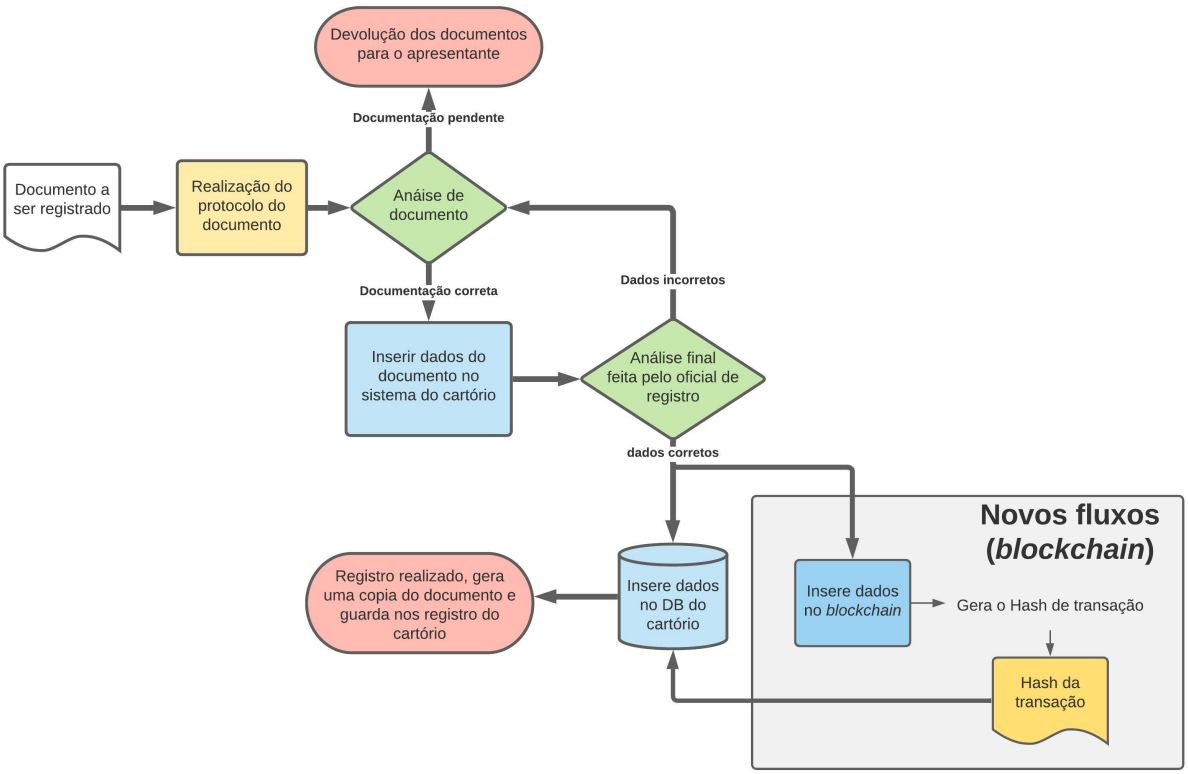

Figura 3.2 – Proposta de Fluxo de Processos do Cartório.
Fonte: Autores.

Os itens apontados em destaque são etapas incluídas e dizem respeito à alimentação de dados na cadeia de *blockchain Ethereum*.

Para validar a hipótese de que as cadeias de *blockchain* podem auxiliar na segurança dos registros imobiliários, formulamos um *smartcontract* para os registros do Livro nº 2 dos Ofícios de Registro de Imóveis.

3.1.2 Protótipo Cadeia Blockchain Ethereum

3.1.2.1 Arquitertura do *Blockchain*.

Zhang [34] apresenta uma arquitetura do *blockchain* em 6 (seis) camadas: i) camada de aplicação; ii) camada de contratos; iii) camada de incentivo; iv) camada de consenso; v) camada de rede e vi) camada de dados.

A figura 3.3 representa as camadas propostas.

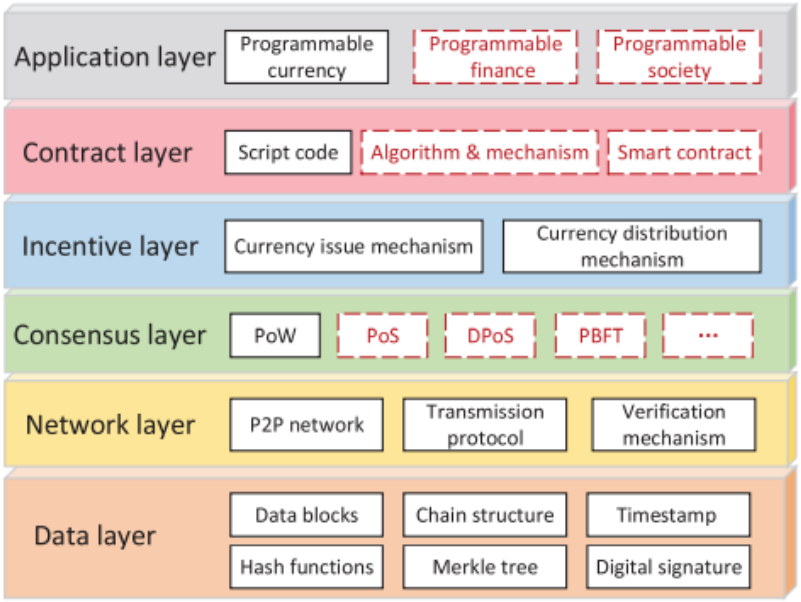

Figura 3.3 – Arquitetura do *Blockchain*.
Fonte: Zhang [34].

As camadas de incentivo, consenso, e dados apontadas por Zhang dependem da cadeia de *blockchain* escolhida. Em nosso trabalho apresentamos uma proposta de cadeia *Ethereum*, que tem definidas as formas de incentivo (mineração), consenso (GHOST) e dados (bloco *Ethereum*).

A camada de contrato de nosso trabalho apresenta um *smartcontract* que se destina ao armazenamento de dados de registros imobiliários na cadeia de *blockchain*. Detalharemos sua arquitetura em tópico próprio.

Serviços de governamentais, que podem ser uma espécie de *programable society*, são os destinatários de nosso *smartcontract* na camada de aplicação.

3.1.2.2 Arquitetura da Cadeia Privada *Ethereum*.

Propomos uma cadeia privada de *blockchain Ethereum* com 12 (doze) nós certificadores que corresponderiam aos diversos ofícios de registros de imóveis do Distrito Federal além de nós certificadores disponibilizados a órgãos gestores da cadeia de *blockchain* e fiscalizadores da atividade pública delegada, assim distribuídos:

- i) 9 (nove), sendo um para cada ofício de registro de imóveis;
- ii) 1 (um) para o Ministério Público e
- iii) 2 (dois) para o Tribunal de Justiça, sendo um para a Corregedoria Geral e outro para a Vara de Registros Públicos.

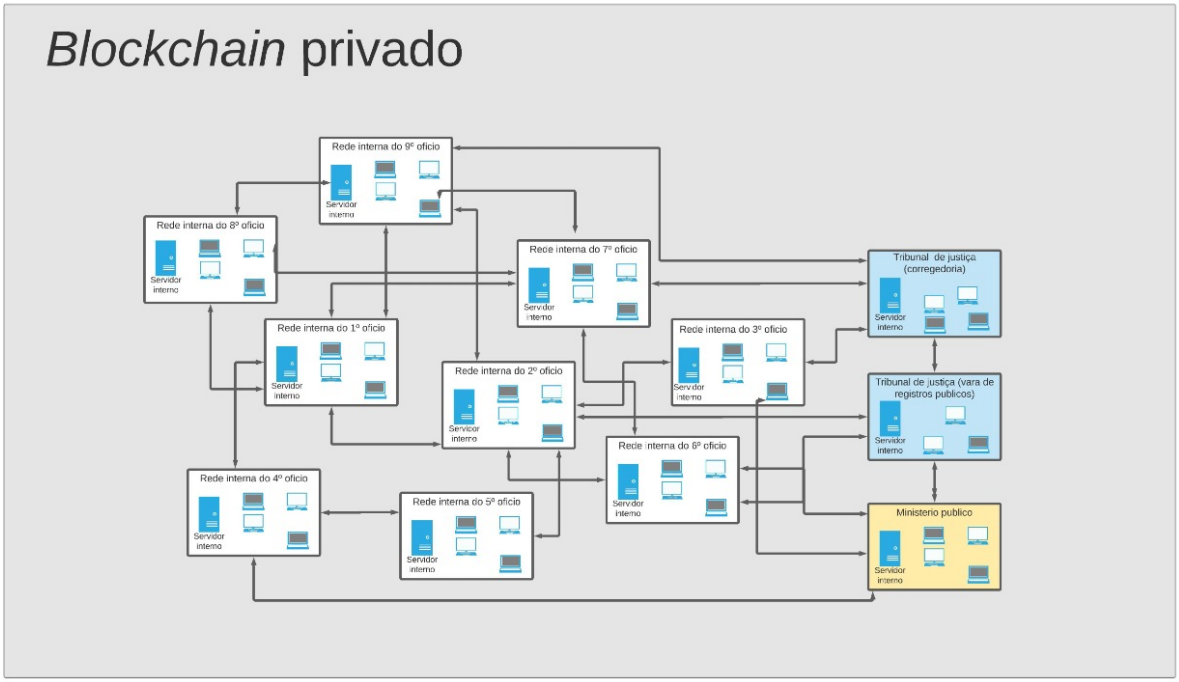

Figura 3.4 – Proposta de Nós Certificadores.
Fonte: Autores.

Ressalte-se que a alteração do número de nós certificadores pode ser facilmente implementada mesmo quando o bloco já estiver em funcionamento. Isto torna possível a fixação de outros certificadores caso ocorra o desmembramento de algum cartório atual.

A escrituração dos registros, como vimos, deve se dar nos 5 livros obrigatórios dos Cartórios de Imóveis. Na prática, em regra, não há livros físicos, mas fichas enumeradas que reportam a situação de cada imóvel. As fichas físicas são armazenadas em arquivo próprio e há, em regra, igualmente, um banco de dados que contém as mesmas informações digitalizadas.

Concebemos a formalização de uma cadeia de *blockchain* em que funções específicas farão os registros dos livros 1, 2 e 3. As funções para os livros 1 e 3 são semelhantes pois os referidos livros são repositórios de documentos, de tamanho infinito. O *blockchain* traria apenas o encadeamento dos *hashs* desses documentos. Tais livros, entretanto, não fazem parte do escopo dessa pesquisa.

O Livro nº 1, Protocolo, é na verdade a porta de entrada dos registros de um cartório. Trata-se de um repositório dos atos apresentados para registro e sua importância está relacionada ao direito de preferência para determinados registros.

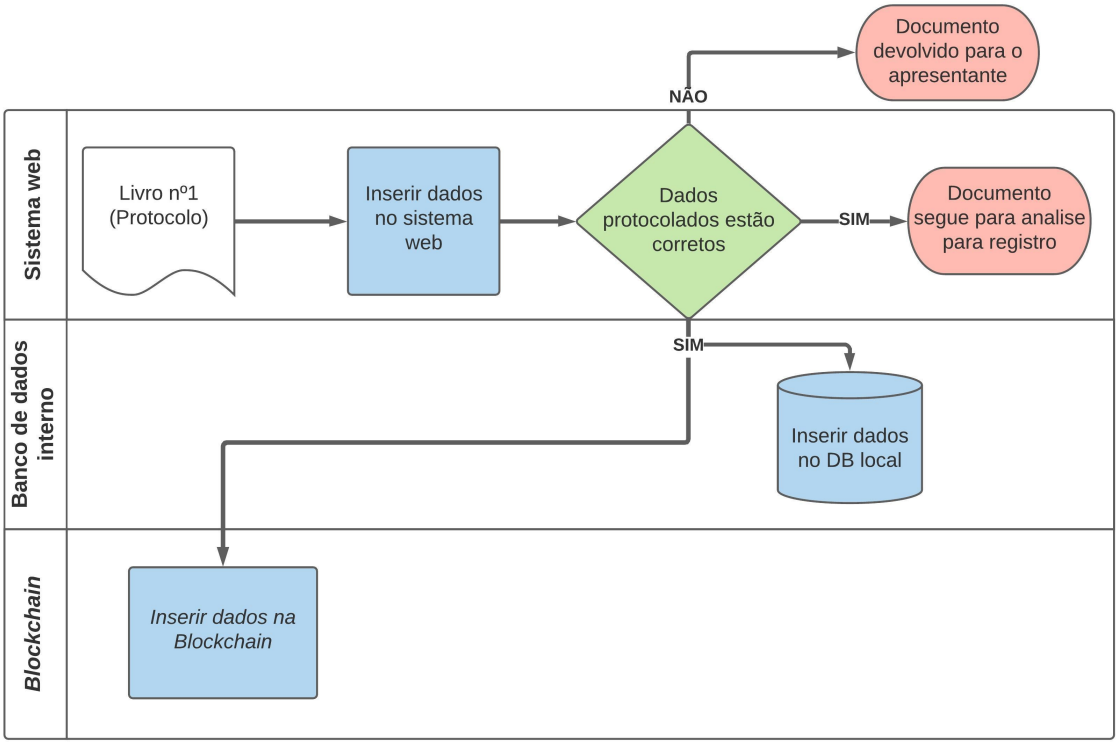

Figura 3.5 – Esquema do Livro nº 1.
Fonte: Autores.

O Livro nº 3, Registro Auxiliar, é um repositório de documentos que, referidos no Registro Geral, ficam depositados no Cartório para eventual consulta de interessados.

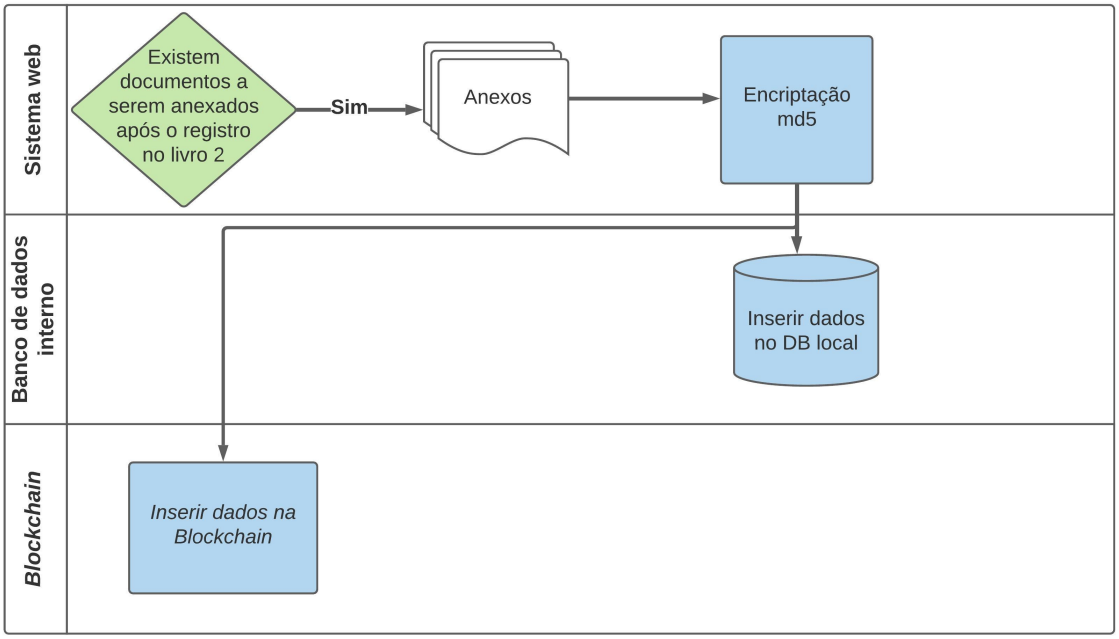

Figura 3.6 – Esquema do Livro nº 3.
Fonte: Autores.

O Livro nº 2, Registro Geral, é onde, de fato, são armazenadas as informações de cada um dos imóveis. Aqui a cadeia dominial (cadeia dos proprietário e ex-proprietários) deve ser preservada e os dados relevantes do imóvel devem estar disponíveis para que a situação presente do mesmo possa ser consultada por qualquer interessado. Os registros e averbações contidos nesse livro tem o objetivo de dar transparência a esses dados.

Para os registros públicos, documentos são apresentados nos cartórios, tais como: escritura pública de compra e venda; escritura de penhora de imóveis, etc.. Em nosso modelo, também criamos coluna própria no banco de dados para o armazenamento do *hashs MD5* da digitalização dos documentos apresentados para registro.

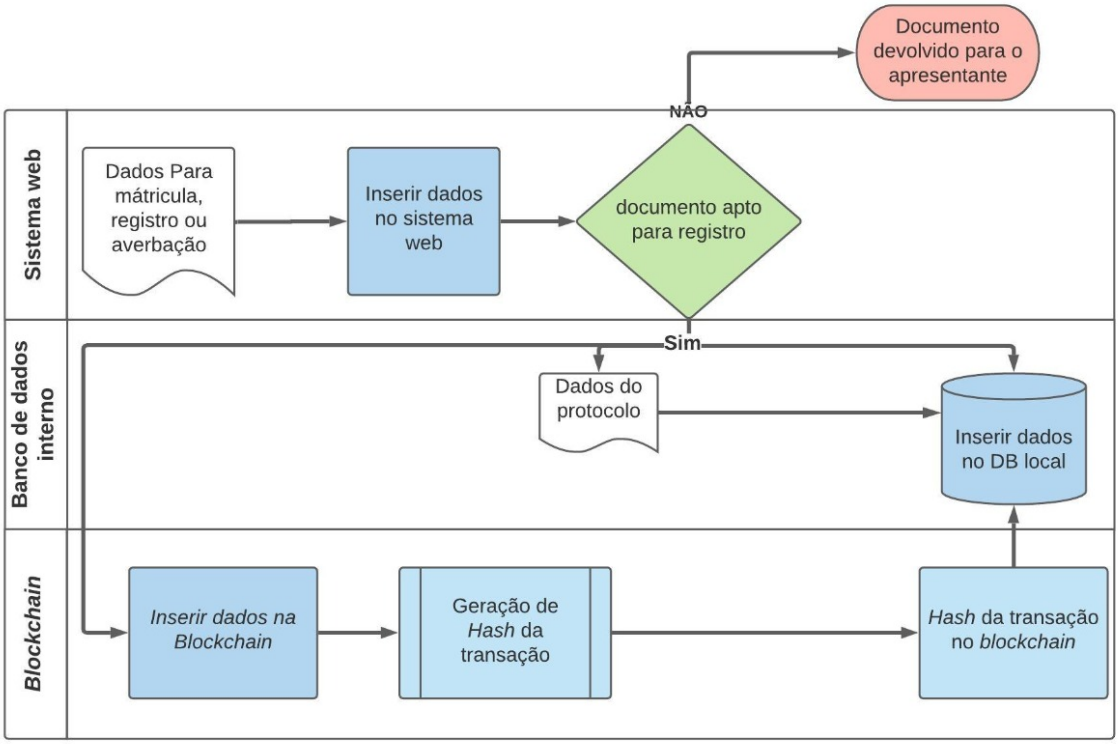

Figura 3.7 – Esquema do Livro nº 2.
Fonte: Autores.

Os Livros nº 4 e nº 5, Indicador Real e Indicador Pessoal, respectivamente, são na verdade repositórios de todos imóveis (Indicador Real) ou pessoas (Indicador Pessoal) que tenham sido referidos nos diversos registros ou averbações. Tais livros são, na verdade, índices de pessoas e imóveis referidos nos registros do cartório. Tal função entendemos serem subsidiárias e, portanto, deixamos apenas no sistema WEB que pode entregar de forma mais efetiva e rápida o resultado de buscas sobre pessoas ou imóveis referidos. Todo o trabalho desenvolvido teve por objetivo criar uma cadeia de *blockchain Ethereum* privada que pudesse resguardar de forma mais segura informações as inscrições nos registros de imóveis no Distrito Federal. O modelo teria escalabilidade nacional eis que as normas de regência são de competência federal e apenas pequenas adequações são formalizadas pelos diversos Tribunais de Justiça Estaduais, assim, sua aplicação em outros Estados Federados seria de fácil adaptação.

Os registros passariam a ter dois controles independentes, um no próprio cartório (em seu sistema próprio e nos arquivos de documentos) e outro na cadeia de *blockchain* que serviria para identificar eventuais alterações nos sistemas de registros ou nos documentos armazenados fisicamente no cartório.

3.1.2.3 Camada de Contrato do *Blockchain Ethereum*.

O *smartcontratc* sugerido em nosso trabalho tem sua arquitetura apresentada no seguinte fluxo.

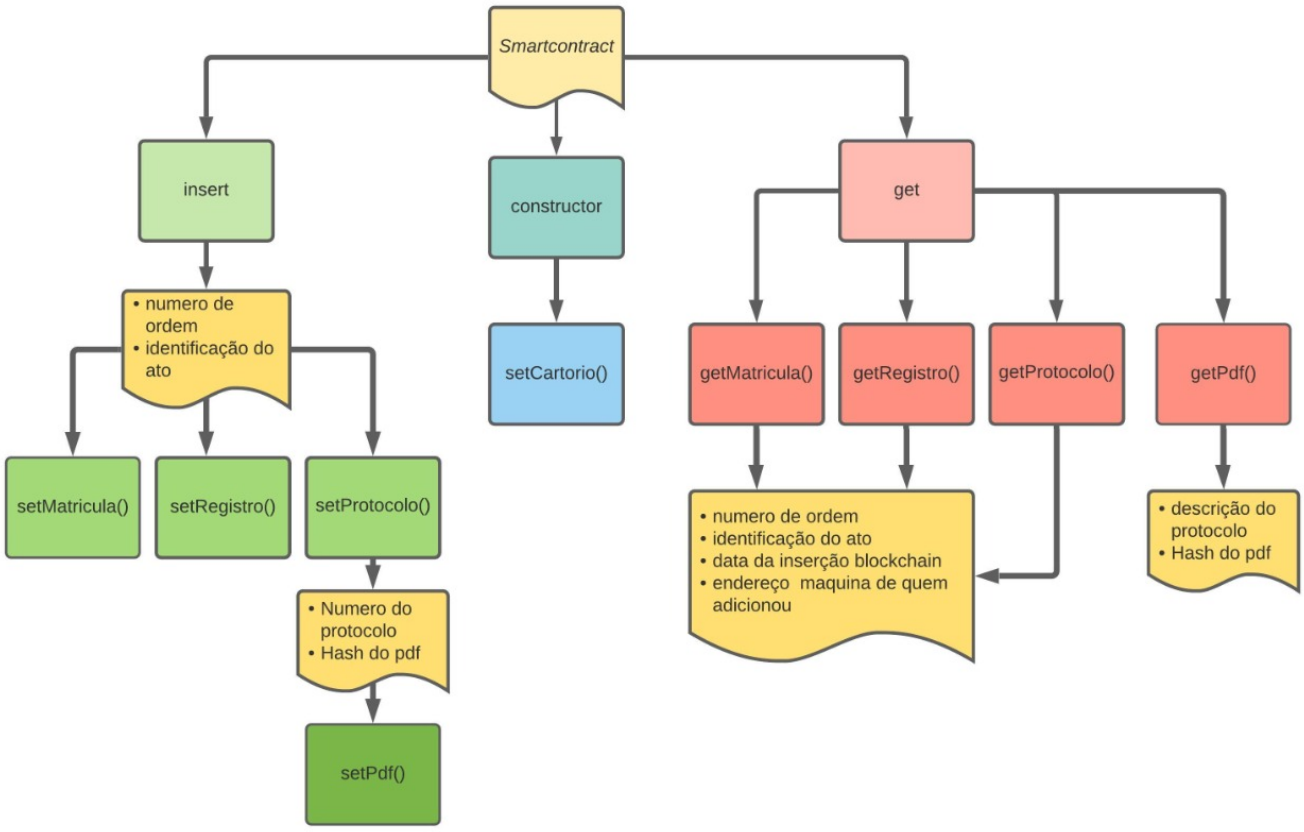

Figura 3.8 – Arquitetura do *Smartcontract*.
Fonte: Autores.

Nos sistemas de *blockchain*, não encontramos as típicas funções *CRUD* (*create, read, update and delete*) as cadeias permitem a inserção de dados (*create*) e a leitura dos dados (*read*), modificação e retirada de dados não ocorrem no *blockchain*. Assim, apenas funções *get* (para leitura) e *set* (para inserções) são possíveis.

Formatamos um sistema de *blockchain Ethereum* com um *smartcontratc* em que são definidas *structs* para as matrículas, registros e documentos anexos (pdf). As *structs* das matrículas e registros contam com os dados exigidos por lei. Já a *struct* dos documentos anexos foi denominada de "Pdf"e conta com o número de ordem do protocolo, o *hash* da digitalização em formato .pdf dos documentos apresentados no registro e a data do registro. Utilizamos a encriptação MD5 para cálculo do *hash* que servirá para funções de fiscalização (checagem de eventual alteração dos documentos armazenados nos cartórios).

O *smartcontract* foi desenvolvido na *IDE REMIX* na linguagem *Solidity*. As simulações foram realizadas na própria *IDE REMIX*, utilizando uma conta diversa para cada um dos 12 nós certificadores.

As *structs* das matrículas, registros e documentos anexos (Pdf) são apresentadas na figura 3.9.

Figura 3.9 – *Structs* Matrícula, Registro e Documentos (Pdf).
Fonte: Autores.

Após definir os dados essenciais que deveriam ser armazenados no *blockchain* para as matrículas e registros, passamos a definir as funções que permitem esse armazenamento e a recuperação desses dados.

Para o armazenamento dos dados formalizamos três funções, sendo uma para cada tipo de inscrição: matrícula (*setMatricula*), registro e averbação (*setRegistro*) e documentos anexos (*setPdf*). Vejamos cada uma delas.

A função de definição de matrícula recebe o número de ordem da matrícula e a identificação do imóvel. Esta função será executada sempre que o Ofício de Registro de Imóveis concluir a realização do registro de matrículas novas. A função executa a tarefa de inserção de dados no *blockchain* do fluxo proposto para atividades do cartório (figura 3.2). A codificação da função está descria abaixo.

```
1   function setMatricula (
2         uint numeroOrdem,
3         string identificacaoImovel
4         ) public {
5             Matricula matricula1;
6
7             matricula1.data = now;
8             matricula1.numeroOrdem = numeroOrdem;
9             matricula1.identificacaoImovel = identificacaoImovel;
10            dono = msg.sender;
11
12            if (Matriculas[numeroOrdem].numeroOrdem == 0) {
13                Matriculas[numeroOrdem] = matricula1;
14            }
15            else {
16                require (Matriculas[numeroOrdem].numeroOrdem == 0,"Ja Existe
                      Matricula Cadastrada com o Numero");
17            }
```

```
18          }
```

A função de definição de registros é semelhante à de definição das matrículas e, igualmente, recebe o número de ordem da matrícula a que se refere; o número de ordem do registro (ou averbação) e a descrição do registro (ou averbação). Esta função também será executada quando do término de um novo registro (ou averbação) pelo Oficial do Registro de Imóveis. A função executa a tarefa de inserção de dados no *blockchain* do fluxo proposto para atividades do cartório (figura 3.2).

```
1     function setRegistro (
2             string registro_tipo, //para dizer se    averbacao ou registro
3             uint registro_numeroRegistro,
4             uint registro_numeroMatricula,
5             string registro_descricao
6             ) public {
7             Registro registro1;
8
9             registro1.data = now;
10            registro1.registro_tipo = registro_tipo;
11            registro1.registro_numeroRegistro = registro_numeroRegistro;
12            registro1.registro_numeroMatricula = registro_numeroMatricula;
13            registro1.registro_descricao = registro_descricao;
14            dono = msg.sender;
15
16            if (Registros[registro_numeroMatricula] [registro_numeroRegistro].
                  registro_numeroRegistro == 0) {
17                Registros[registro_numeroMatricula] [registro_numeroRegistro] =
                      registro1;
18            }
19            else {
20                require (Registros[registro_numeroMatricula] [
                      registro_numeroRegistro].registro_numeroRegistro == 0, "J
                      Existe Registro Cadastrado com o Numero");
21                }
22            }
```

Para armazenar dados dos documentos apresentados, optamos por inserir o *hash* desses documentos na cadeia *blockchain*. Assim, a função que armazena esses *hashs* ficou assim codificada:

```
1  function setPdf(
2         uint _numeroProtocolo,
3         string _hash
4         ) public {
5             require(msg.sender == dono, "Somente o Cart rio responsavel pelos
                  registros    autorizado a inserir novos dados");
6             Pdf pdf1;
7
8             pdf1.data = now;
9             pdf1.pdf_numeroProtocolo = _numeroProtocolo;
10            pdf1.pdf_hash = _hash;
11            dono = msg.sender;
12
```

```
13              if (Pdfs[_numeroProtocolo].pdf_numeroProtocolo == 0) {
14                  Pdfs[_numeroProtocolo] = pdf1;
15              }
16              else {
17                  require (Pdfs[_numeroProtocolo].pdf_numeroProtocolo == 0, " J
                        Existe anexo Cadastrada com o Numero");
18              }
19          }
```

Para a recuperação dos dados utilizamos outras três funções, uma para recuperar dados da matrícula, outra para recuperar dados dos registros (ou averbações) e a última para recuperar *hashs* dos documentos apresentados.

A codificação da função que recupera dados das matrículas no *blockchain* é a seguinte:

```
1     function getMatricula (uint _numeroOrdemMatricula) public view returns (
2         uint _numeroOrdem,
3         string _identificacaoImovel,
4         uint _data,
5         address _endereco_operador) {
6         return (Matriculas[_numeroOrdemMatricula].numeroOrdem,
7             Matriculas[_numeroOrdemMatricula].identificacaoImovel,
8             Matriculas[_numeroOrdemMatricula].data,
9             Matriculas[_numeroOrdemMatricula].endereco_operador);
10    }
```

A codificação da função que recupera dados dos registros no *blockchain* está descrita abaixo.

```
1     function getRegistro (uint _numeroRegistro, uint _numeroMatricula) public
          view
2         returns (uint _data,
3         string _registro_tipo,
4         uint _registro_numeroRegistro,
5         uint _registro_numeroMatricula,
6         string _registro_descricao) {
7
8         return (Registros[_numeroMatricula] [_numeroRegistro].data,
9             Registros[_numeroMatricula] [_numeroRegistro].registro_tipo,
10            Registros[_numeroMatricula] [_numeroRegistro].registro_numeroRegistro
                  ,
11            Registros[_numeroMatricula] [_numeroRegistro].
                  registro_numeroMatricula,
12            Registros[_numeroMatricula] [_numeroRegistro].registro_descricao);
13    }
```

Por fim, apresentamos a função de recuperação dos documentos anexos.

```
1     function getPdf (uint _numeroProtocolo) public view returns (
2         uint _numeroProtocolo1,
3         string _hash,
4         uint _data) {
5         return (Pdfs[_numeroProtocolo].pdf_numeroProtocolo,
6             Pdfs[_numeroProtocolo].pdf_hash,
```

```
7               Pdfs[_numeroProtocolo].data);
8     }
```

As funções de recuperação de dados de matrícula, registro e documentos servem para as atividades de fiscalização. Aqui é possível acessar os dados obrigatórios das matrículas e registros, por meio de seus números de ordem ou pelo *hash* da transação (que consta do sistema WEB).

3.1.3 Protótipo Sistema WEB.

Na pesquisa de campo que fizemos junto ao 7º Ofício de Registro de Imóveis do Distrito Federal observamos a utilização de um software para a gestão dos procedimentos do cartório. A plataforma utilizada atende de forma satisfatória as necessidades do Ofício de Imóveis. Observamos a existência de diversos módulos compatíveis com as atividades do cartório. Há módulos para expedição de certidões, para a inscrição de matrículas, registros e averbações, bem como para as buscas pessoais e de imóveis. As informações lançadas na plataforma são armazenadas localmente, em servidor próprio do cartório, e a manutenção de *backups* são obrigatórias, devendo um deles estar situado em localidade diversa da sede do cartório.

Na atividade diária do cartório observamos um fluxo de processos que se assemelha ao descrito na figura 3.1.

Formalizamos um sistema WEB simplificado para os registros imobiliários com a finalidade de demonstrar que os atuais sistemas dos cartórios de imóveis podem, após pequenas adaptações, se adequar à cadeia de *blockchain* proposta em nosso trabalho.

O sistema *WEB* tem a seguinte arquitetura.

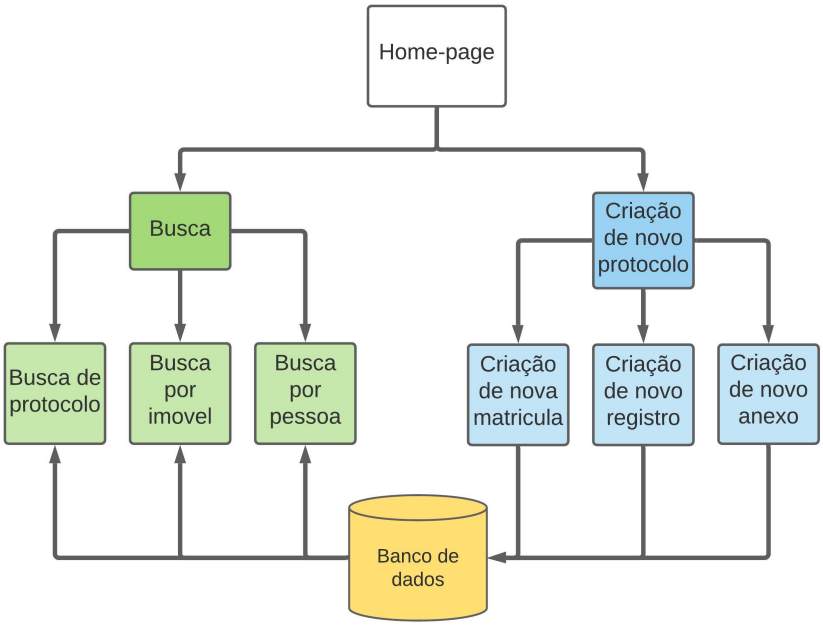

Figura 3.10 – Arquitetura do sistema *WEB*.
Fonte: Autores.

Nosso sistema apresenta um *front end* com três páginas principais.

A página inicial, *index* do sistema, permite a criação de novos protocolos e a pesquisa de protocolos em aberto, matrículas e registros

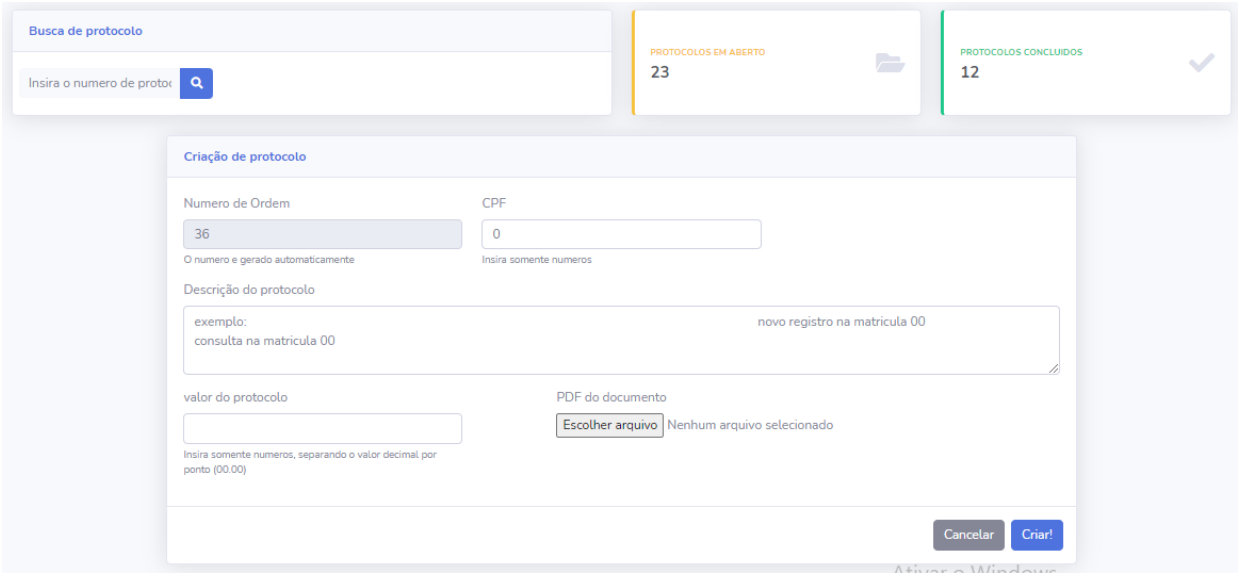

Figura 3.11 – Página para Busca e Criação de Protocolos.
Fonte: Autores.

A página das matrículas apresenta dados obrigatórios das matrículas além dos registros e averbações de cada matrícula.

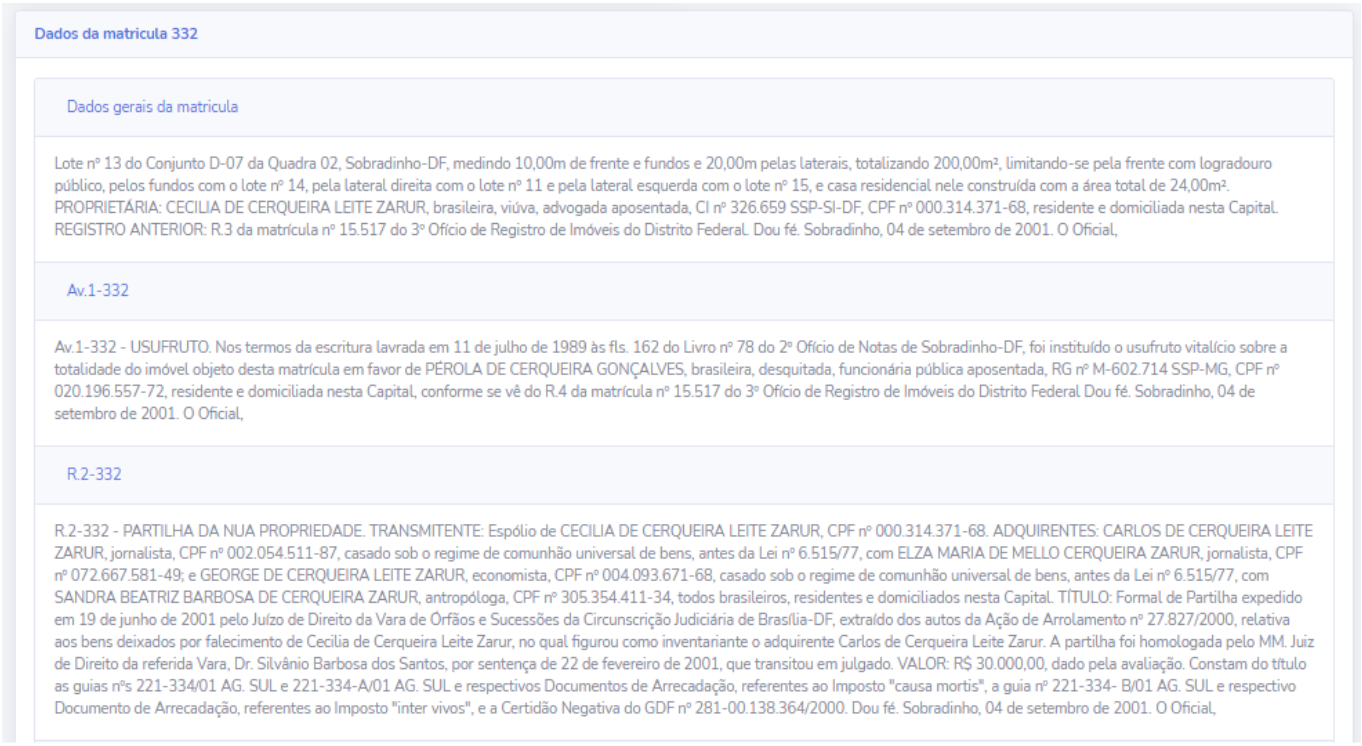

Figura 3.12 – Página com Dados da Matrícula com Todos seus Registros e Averbações.
Fonte: Autores.

Há ainda uma página para que possam ser criados registros ou averbações associadas a suas respectivas matrículas.

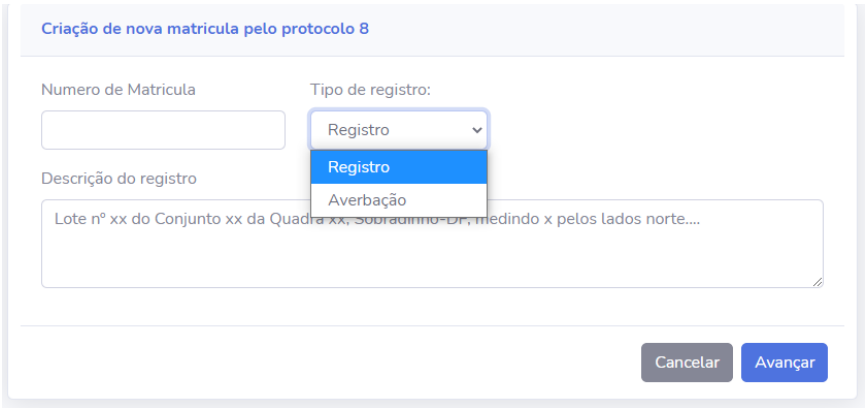

Figura 3.13 – Página para Criação de Registros ou Averbações.
Fonte: Autores.

Além dessas três páginas principais há outras para os seguintes fins: i) criação de matrícula nova; ii) busca de matrículas e iii) busca por pessoas (CPF).

A página de criação de matrícula nova somente será utilizada para uma inscrição de um novo imóvel no Cartório. A figura 3.14 traz a tela onde este procedimento é realizado.

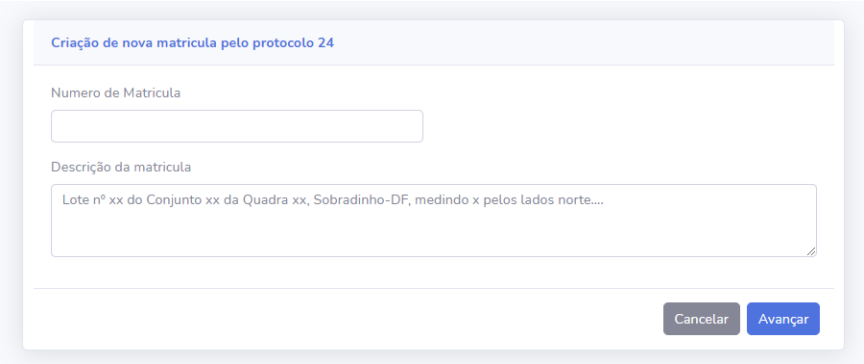

Figura 3.14 – Página para criação de matrícula
Fonte: Autores.

O banco de dados do sistema apresenta 4 tabelas, assim definidas: i)protocolo; ii) matrícula; iii) registros e iv) anexos.

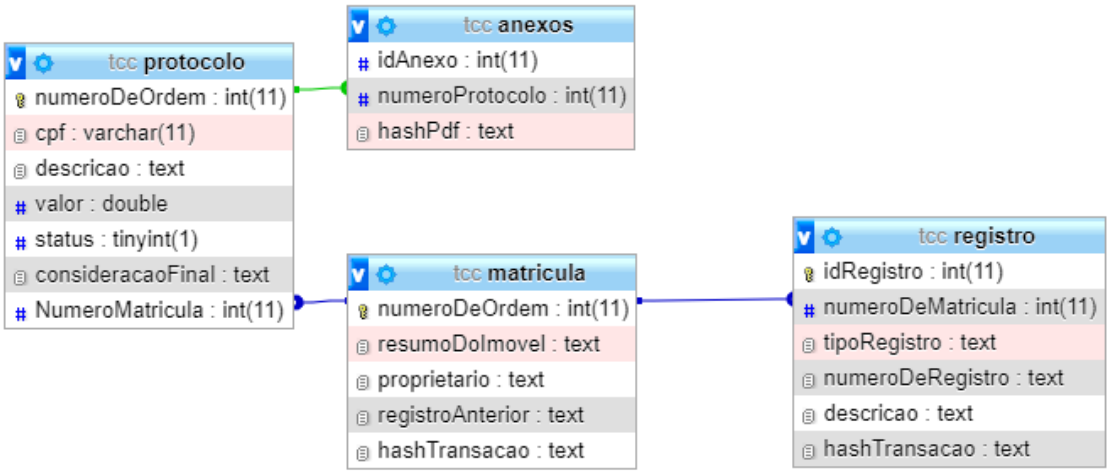

Figura 3.15 – Arquitetura do banco de dados.
Fonte: Autores.

O sistema *WEB* foi desenvolvido com o objetivo de indicar a possibilidade de coexistência dos atuais sistemas utilizados pelos cartórios com a cadeia de *blockchain* proposta. Concentramos os esforços para desenvolver um sistema simplificado, mas que realiza as principais funções que foram observadas no sistema do 7º Ofício de Registro de Imóveis, objeto de nossa pesquisa de campo.

3.2 *Blockchain Ethereum* e a Segurança dos Registros.

3.2.1 Modelo de Transição para Utilização de *Blockchain* nos Registros Públicos.

3.2.1.1 Registros de Imóveis no Distrito Federal.

Atualmente o Distrito Federal conta com 9 (nove) Ofícios de Registros de Imóveis que, juntos, mantêm inscrições de cerca de 825.000 (oitocentos e vinte e cinco mil) matrículas de imóveis urbanos.

A administração dos cartório e, consequentemente, armazenamento das informações sobre os imóveis do Distrito Federal é descentralizada.

A criação de uma cadeia de *blockchain* que reúna todas as informações dos cartórios de imóveis do Distrito Federal e distribua o processamento de ingresso de dados para diversos nós certificadores trará uma maior confiabilidade dos dados armazenados e dotará as instâncias de fiscalização de um instrumento mais eficaz para detectar de irregularidades.

Detalhes das áreas de abrangência dos cartórios do Distrito Federal foram descritos no anexo I.

3.2.1.2 Requisitos para Implantação de *Blockchain* nos Serviços de Registro de Imóveis.

Antes da efetiva implantação de uma cadeia de *blockchain* que aumente a segurança dos registros imobiliários é importante avaliar os requisitos para esta implantação.

Em estudo sobre a utilização de cadeias de *blockchain* para registros imobiliários, Graglia [15] apresenta 7 (sete) pré requisitos para a integração das cadeias de *blockchain* aos registros imobiliários, a saber:

- i) solução de identificação;
- ii) digitalização de dados;
- iii) sistema para assinaturas múltiplas;
- iv) uso de cadeia privada ou híbrida;
- v) certeza e precisão dos dados;
- vi) disseminação de conectividade e conhecimento para a população e
- vii) treinamento para profissionais envolvidos.

O estudo de Graglia é de 2017 e as condições ali colocadas ainda se mostram indispensáveis para um projeto de modernização de registros imobiliários. O Distrito Federal apresenta situação favorável a implantação de um modelo de transição eis que diversos pontos referidos no estudo estão presentes em nossa cidade.

A denominada solução de identificação, apontada por Graglia, exige que todo aquele que possa realizar transações imobiliários tenha condição de ser identificado de forma única.

Atualmente, todo cidadão nacional ou empresa que tenha capacidade jurídica, aqui entendida como a capacidade para assumir e contrair obrigações, tem a inscrição no CPF (Cadastro de Pessoas Físicas) ou CNPJ (Cadastro Nacional de Pessoas Jurídicas). Tais cadastros se apresentam com uma numeração única para cada cidadão ou empresa, fato que atenderia ao requisito da solução de identidade.

Para a implantação de uma solução de *blockchain* na realidade dos cartórios de imóveis é imprescindível a digitalização de dados. Tal exigência apontada nos estudos de Graglia resultam da necessidade de dotar os documentos registrados de um caráter de imutabilidade. Assim o estudo sugere a digitalização dos documentos de registro e, posteriormente, a formatação de um *hash* desse documento digitalizado. Assim, qualquer alteração desse documento levaria a alteração desse *hash*, o que seria facilmente detectado. Segundo o estudo de Graglia, esta solução foi a implementada na Suécia e Geórgia.

A utilização de assinaturas múltiplas para os registros é também uma preocupação de Graglia. Assim, para a efetivação dos registros é importante que se exija a assinatura digital de mais de uma autoridade. Em nossa realidade entendemos que tal preocupação deve ser de responsabilidade de cada titular do Ofício de Imóveis que, usualmente contam com Oficiais Titulares e Substitutos dos Ofícios que poderiam, internamente, formatar um procedimento próprio de multi assinaturas.

A adoção de múltiplas assinaturas poderia seguir as diretrizes apresentadas no artigo *"Decentralized document version control using ethereum blockchain and IPFS"* [26]. No referido artigo os autores apresentam uma solução de arquivamento em repositório público, de documentos redigidos por diversas pessoas. Os autores apresentam solução em que *smartcontracts* atualizariam no repositório público, de forma automática, novas versões de documentos, podendo ser exigida a aprovação desta nova versão por um número pré definido entre os diversos autores.

A proposta de Graglia passa pela utilização de uma cadeia privada ou híbrida para registros públicos imobiliários dada a preocupação do autor com o direito de propriedade. Entendemos da mesma forma e em nossa realidade propomos a utilização de uma cadeia privada com a presença de 12 (doze) nós certificadores, um para cada Ofício de Registro de Imóveis, 2 (dois) para o Tribunal de Justiça e 1 (um) para o Ministério Público.

Os registros imobiliários do Brasil encontram-se em um estágio em que há relativa certeza sobre os dados armazenados. Disputas sobre imóveis são comuns e um quadro de certeza absoluta sobre os dados armazenados, apesar de recomendável, são inatingíveis. O certo é que nossa legislação dá presunção de validade aos dados registrados e tal fato torna verossímil a base de dados presente nos Cartórios.

Nos estudos de Graglia a existência de uma rede de internet e de conhecimentos da população para a sua utilização também é fundamental e este fato é incontroverso pois a ausência dessas condições e habilidades trariam uma restrição ao exercício do direito de propriedade.

Outro ponto favorável ao Distrito Federal é a sua alta taxa de conectividade à rede mundial de computadores e uma sociedade com conhecimentos e experiências relativamente grande na utilização de serviços pela internet. Dados do Instituto Brasileiro de Geografia e Estatística –

IBGE – indicam que, em 2017, na Região Centro Oeste, 81,7 % da população acima de 10 anos utilizou a internet. O mesmo estudo indica que o aumento da utilização da internet nos domicílios brasileiros é uma tendência nacional.[18]

O último requisito apresentado por Graglia diz respeito ao treinamento de um corpo técnico capaz de gerir e dar suporte à nova tecnologia. Aqui, também, não há como divergir do autor. Os administradores da cadeia de *blockchain* deverão mantê-la em funcionamento de forma satisfatória, adaptando sua realidade para eventuais modificações da legislação específica referente aos registros públicos.

A proposta trazida é de uma cadeia privada que seria de responsabilidade do Tribunal de Justiça do Distrito Federal e Territórios, que conta com equipe de funcionários concursados que atuam na área da tecnologia da informação, operando, desenvolvendo e dando suporte aos sistemas do Tribunal de Justiça. No endereço eletrônico do TJDFT [19], identificamos cerca de 221 (duzentos e vinte e um) servidores lotados em áreas relacionadas ao atendimento de usuários, desenvolvimento e manutenção de sistemas. Tais servidores possuem conhecimentos na área de tecnologia da informação e que poderiam, com o devido treinamento, dar o devido suporte à cadeia de *blockchain*.

Após abordar os pré-requisitos que entende necessários à implantação do *blockchain* para os registros imobiliários, Graglia prossegue indicando 9 (nove) níveis de implementação da cadeia de *blockchain* para os serviços de registros de imóveis, assim identificados:

- i) Nenhuma integração;
- ii) Armazenamento de dados no *blockchain*;
- iii) Utilização de *Smartcontracts* para Processos de Registros e Averbações;
- iv) Utilização de *Smartcontracts* para transações imobiliárias a serem registradas;
- v) Registro Imobiliário de Propriedade totalmente formatado em cadeia *blockchain*;
- vi) Utilização do *blockchain* para transações de outros direitos reais ligados à propriedade;
- vii) Utilização do *blockchain* para transações que envolvem copropriedade;
- viii) Transações Imobiliárias realizadas e registradas de forma autônoma no *blockchain* e
- ix) Integração de diversas cadeias de *blockchain* de registros de imóveis, em seus diversos níveis de jurisdição.

O mesmo estudo aponta que o Brasil contaria com um caso de utilização do *blockchain* para armazenamento de dados de registro imobiliário, que corresponderia ao nível 'ii' de implementação. O caso referido foi tratado no documento "Registro de transações imobiliárias em *Blockchain* no Brasil (RCPLAC-01) - Estudo de Caso 1. 10.13140/RG.2.2.16022.45123.", [20]. No referido estudo de casos podemos identificar que a iniciativa pioneira se deu no Cartório de Imóveis de Pelotas-RS e que utilizaram a cadeia de *blockchain do Bitcoin*, com o protocolo de *colour coins*.

Nosso estudo segue em outra linha, apresentando uma solução de *blockchain Ethereum* privada. A utilização do protocolo *colour coins* tem limitações que não se apresentam na cadeia de *blockchain Ethereum*. O protocolo *colour coins* foi concebido para adaptar o *blockchain Bitcoin* para a realização de outras atividades diversas da troca de criptomoedas. Já a cadeia de *blockchain Ethereum* foi idealizada para a execução de tarefas computacionais por meio dos *smartcontracts*.

Outro ponto que julgamos favorável à utilização da cadeia *Ethereum* é a facilidade de programação na linguagem *Solidity* e a possibilidade da realização de simulações confiáveis na *IDE Remix*.

Nosso modelo não ultrapassa o estágio 'ii' definido no estudo de Graglia, mas amplia a sua utilização para a totalidade de cartórios de uma região, incorporando o Poder Público na adoção da cadeia de *blockchain*.

4 Resultados e Análise

4.1 Validação dos Resultados.

Para a validação dos resultados contamos com a colaboração do Cartório do 7º Ofício de Registros de Imóveis do Distrito Federal que nos forneceu cópia de 50 matrículas de seus arquivos. Os dados dos registros de imóveis são públicos, mas o acesso é sempre oneroso daí a dificuldade de se ampliar a base para a validação dos resultados.

De posse desses documentos, alimentamos nosso banco de dados do sistema *WEB* com as informações constantes dos arquivos fornecidos e, partindo dessa base de dados inicial, simulamos algumas operações mais comuns dos cartórios de imóveis.

Após a inserção dos dados no sistema *WEB*, simulamos uma alteração não desejada nos bancos de dados do cartório para validar a proposta de utilização da cadeia de *blockchain* como ferramenta para aferir a integridade de dados e documentos.

Nas simulações realizadas na *IDE REMIX*, cada cartório recebeu uma conta *Ethereum* conforme a tabela abaixo.

Nome	Endereço
1º ofício	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
2º ofício	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
3º ofício	0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
4º ofício	0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB
5º ofício	0x617F2E2fD72FD9D5503197092aC168c91465E7f2
6º ofício	0x5c6B0f7Bf3E7ce046039Bd8FABdfD3f9F5021678
7º ofício	0x03C6FcED478cBbC9a4FAB34eF9f40767739D1Ff7
8º ofício	0x1aE0EA34a72D944a8C7603FfB3eC30a6669E454C
9º ofício	0x0A098Eda01Ce92ff4A4CCb7A4fFFb5A43EBC70DC
Corregedoria	0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c
Vara de registros públicos	0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C
MPDFT	0x4B0897b0513fdC7C541B6d9D7E929C4e5364D2dB

Figura 4.1 – Tabela de Endereços dos Cartórios no *Blockchain*.
Fonte: Autores.

Apresentamos abaixo, a tabela do banco de dados do nosso sistema *WEB* com a inserção dos dados do 7º Ofício de Registro de Imóveis.

numeroDeOrdem	resumoDoImovel	proprietario	registroAnterior	hashTransacao
7	Lote nº 47 do Conjunto C da Quadra 12, Sobradinho-...	COMPANHIA URBANIZADORA DA NOVA CAPITAL DO BRASIL...	Inscrição nº 38, fls. 100, do antigo Livro 8-F d...	
14	Lote nº 17 do Conjunto G da Quadra 07, Sobradinho-...	JOSÉ ALVES DE CARVALHO, bancário, RG nº 1.134.05...	R.6 da Matrícula nº 73.402 do 3º Ofício de Regis...	
37	Lote nº 16 do Conjunto C-03 da Quadra 02, Sobradin...	SEZER DE ROMA ALVES DE OLIVEIRA, brasileiro, do ...	R.3 da Matrícula nº 145.104 do 3º Ofício de Regis...	
50	Apartamento nº 101 da Projeção 01 do Conjunto B-06...	ACYR MAURO PAIVA DA SILVA, brasileiro, solteiro,...	R.6 da Matrícula nº 86.387 do 3º Ofício de Regis...	
77	Apartamento nº 204 da Projeção 02, Edifício Flávia...	OSVALDO PEREIRA DE ARAÚJO, brasileiro, solteiro, ...	R.4 da matrícula nº 51.044 do 3º Ofício de Regist...	
332	Lote nº 13 do Conjunto D-07 da Quadra 02, Sobradin...	CECILIA DE CERQUEIRA LEITE ZARUR, brasileira, viú...	R.3 da matrícula nº 15.517 do 3º Ofício de Regist...	
589	Lote nº 28 do Conjunto B da Quadra 08, Sobradinho...	QUINTILIANO FERREIRA PANIAGO, RG nº 531.670 SSP-G...	R.6 e Av.7 da matrícula nº 79.963 do 3º Ofício de...	
899	Loja nº 68 do prédio comercial/residencial edifica...	NAZA CONSTRUÇÃO E INCORPORAÇÃO LTDA., com sede n...	Av.2 da matrícula nº 154.996 do 3º Ofício de Reg...	
988	Lote nº 49 do Conjunto F da Quadra 08, Sobradinho-...	RAIMUNDA CONCEIÇÃO RODRIGUES MECENAS, brasileira...	R.2 da matrícula nº 136.094 do 3º Ofício de Regi...	
1455	Lote nº 41 do Conjunto 08 da Quadra AR-11, Expansã...	COMPANHIA IMOBILIÁRIA DE BRASÍLIA - TERRACAP, co...	Av.1 da matrícula nº 184.542 do 3º Ofício de Reg...	
2100	Apartamento nº 301 do Bloco C2, a ser edificado no...	DISTRITO FEDERAL, pessoa jurídica de direito públ...	R.2 e R.6 da matrícula nº 19.299 desta Serventia....	

Figura 4.2 – Banco de Dados do Sistema *WEB*.
Fonte: Autores.

4.1.1 Inclusão de Dados

.

Os dados repassados pelo Cartório foram adicionados, inicialmente ao sistema *WEB*, assim, como exemplo, apresentamos a Matrícula 50 do 7º Ofício de Registro de Imóveis, na primeira figura observamos o arquivo físico do cartório e na figura seguinte, os mesmos dados em nosso sistema *web*.

MATRÍCULA Nº 50

IMÓVEL: Apartamento nº 101 da Projeção 01 do Conjunto B-06 da Quadra 14, Sobradinho-DF, com área privativa de 57,51m² e área comum de 31,49m², totalizando 89,00m², e a respectiva fração ideal do terreno de 0,01526. **PROPRIETÁRIO:** ACYR MAURO PAIVA DA SILVA, brasileiro, solteiro, maior, funcionário público, RG nº 362.082 SSP-DF, CPF nº 253.036.277-72, residente e domiciliado nesta Capital. **REGISTRO ANTERIOR:** R.6 da Matrícula nº 86.387 do 3º Ofício de Registro de Imóveis do Distrito Federal.
Dou fé. Sobradinho, 20 de junho de 2001. O Oficial,

Av.1-50 - HIPOTECA. O imóvel objeto desta matrícula acha-se hipotecado em 1º lugar e sem concorrência à CAIXA ECONÔMICA FEDERAL - CEF, filial de Brasília, CNPJ nº 00.360.305/0002-95, no valor de Cr$ 45.204.572,00, a ser pago em 252 prestações mensais e sucessivas, vencendo-se a primeira 30 dias após a data da escritura, aos juros efetivos de 10,25238% ao ano, conforme se vê do R.7 da matrícula nº 86.387 do 3º Ofício de Registro de Imóveis do Distrito Federal.
Dou fé. Sobradinho, 20 de junho de 2001. O Oficial,

Av.2-50 - PENHORA. O imóvel objeto da presente matrícula encontra-se PENHORADO por ordem do MM. Juiz de Direito da 2ª Vara Cível da Circunscrição Judiciária de Brasília, Dr. Alfeu Gonzaga Machado, nos termos de certidões extraídas dos autos da Ação de Execução nº 28.549/92, movida por PAULO OCTÁVIO INVESTIMENTOS IMOBILIÁRIOS LTDA contra ACYR MAURO PAIVA DA SILVA, proprietário do imóvel, e JOSÉ FRANCISCO DE ASSIS, para garantia de uma dívida no valor de R$ 77.826,40, conforme se vê do R.8 da matrícula nº 86.387 do 3º Ofício de Registro de Imóveis do Distrito Federal.
Dou fé. Sobradinho, 20 de junho de 2001. O Oficial,

Figura 4.3 – Matrícula 50 - Arquivo do Cartório.
Fonte: Autores.

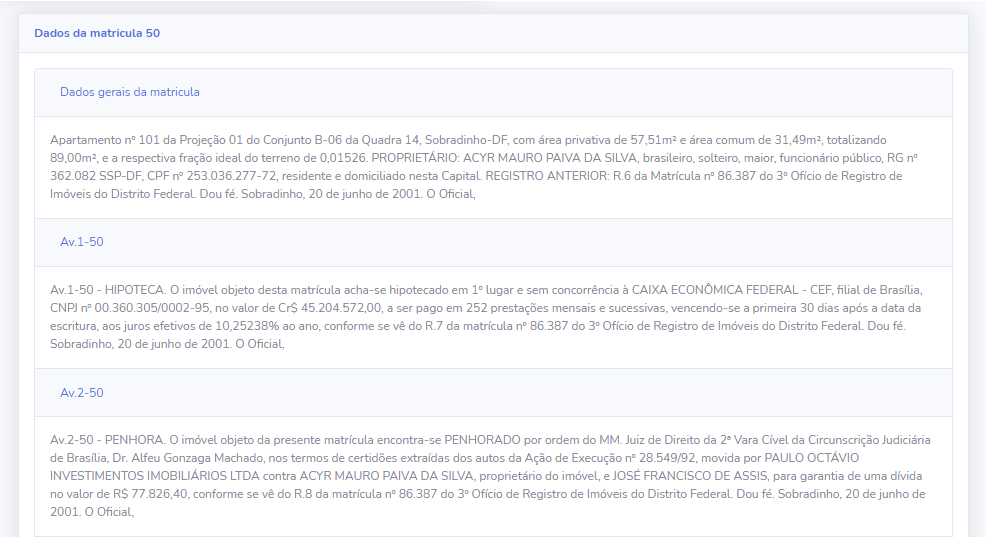

Figura 4.4 – Matrícula 50 - Sistema *WEB*.
Fonte: Autores.

A inserção de dados no *blockchain* deve respeitar as competências de cada cartório. Somente pode inserir dados na cadeia aquele que possui a matrícula em sua área de competência. No anexo de nosso trabalho indicamos as competências de cada cartório do Distrito Federal. No exemplo que trouxemos para a validação, as matrículas são todas do 7º Ofício de Registro de Imóveis.

Vara validar a inclusão de dados referentes à matrícula fizemos uma simulação de inserção pela conta do 7º Ofício e pelos demais cartórios. A figura abaixo demonstra o sucesso na inserção realizada pelo cartório de competência da matrícula (7º Ofício - endereço '0x03c...') e insucesso de

inclusão pelo 1º Ofício (endereço "0x5b3..."), 2º Ofício (endereço "0xAb8...") e 3º Ofício (endereço "0x4B2...").

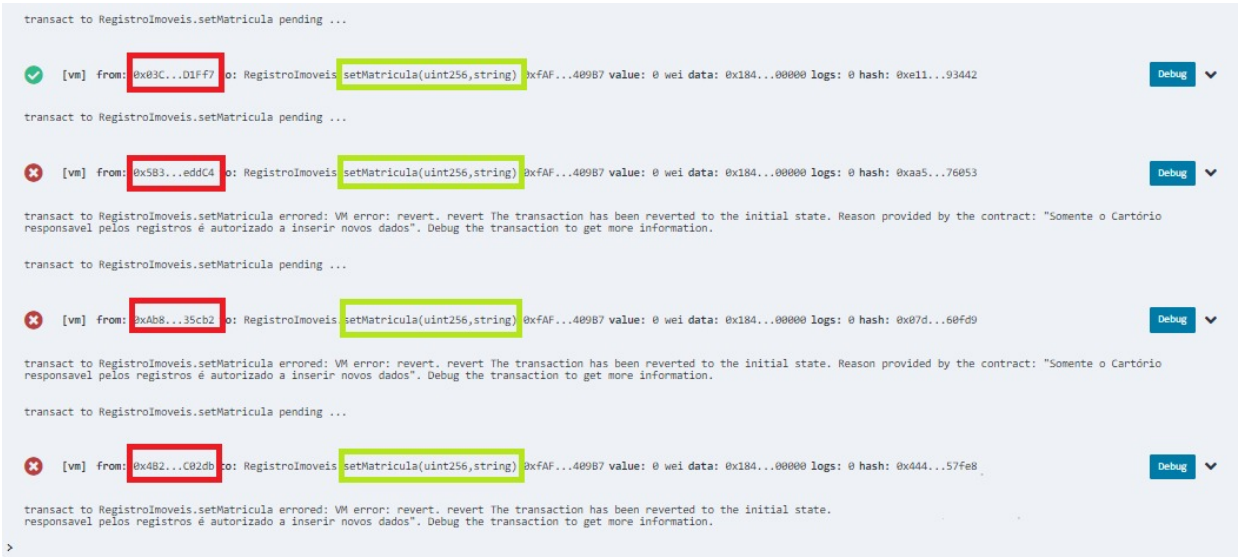

Figura 4.5 – Função *setMatricula*.
Fonte: Autores.

O sistema *blockchain*, portanto, permite o compartilhamento das bases de dados de todos os cartórios, preservando as respectivas atribuições de cada cartório ao vedar criações de matrículas, registros e averbações por cartórios diversos do titular da matrícula do imóvel.

A função *setRegistro* é a que permite a inclusão de registros e averbações. Nessa simulação realizamos a inserção de dados pela conta do cartório do 1º Ofício (endereço "0x5b3..."), pressupondo que a matrícula seria de sua atribuição e tentamos fazer novas inserções pelo cartório do 2º (endereço "0xAb8..."), corregedoria (endereço "0x03C...") e pelo 7º Ofício (endereço "0x03C...").

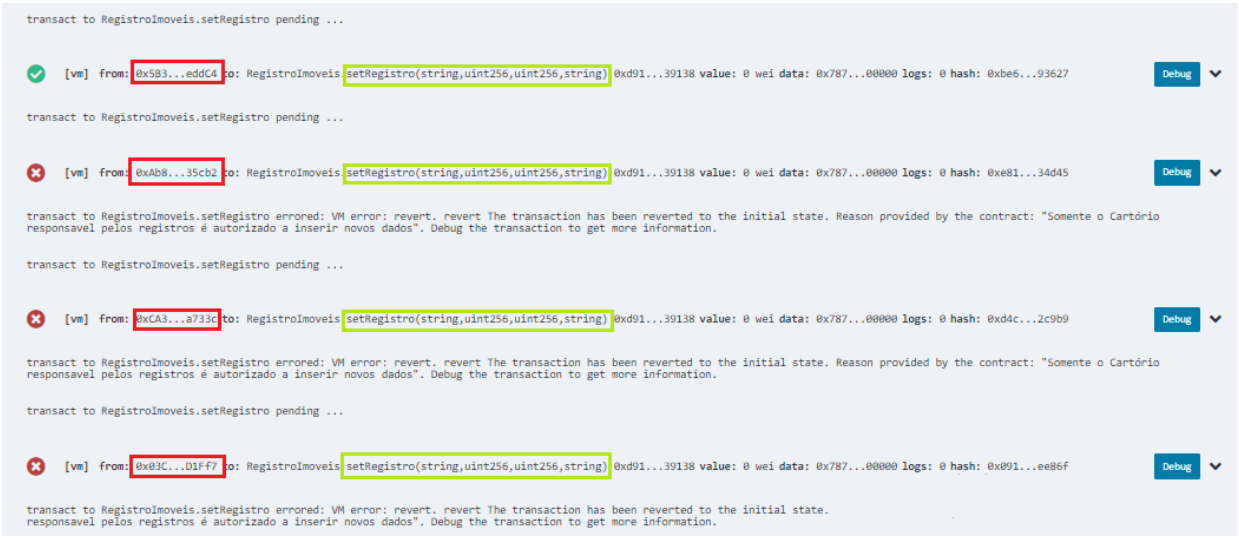

Figura 4.6 – Função *setRegistro*.
Fonte: Autores.

Mais uma vez verificamos que somente tem sucesso na inclusão de dados o cartório que criou a matrícula, no caso do exemplo, o cartório do 1º Ofício de Registro de Imóveis (endereço "0x5b3...").

4.1.2 Simulação de Mudança Indevida do Banco de Dados do Sistema *WEB*.

Simulamos uma mudança indevida no banco de dados do sistema *WEB* do cartório (banco de dados local), tal como ocorre em ataques do tipo *SQL injection*. Este tipo de ataque é muito comum e pode ter consequências graves em relação à integridade dos dados. Um ataque bem sucedido pode não somente dar acesso de leitura ao atacante, como permitir a modificação dos dados [5]. Informações colhidas no site *Exploit-DB* [28] indica a existência de mais de 8.000 (oito mil) vulnerabilidades do tipo *SQL injection*.

Deixamos de simular ataques na cadeia de *blockchain* pois os ataques comuns às cadeias de *blockchain* tem como alvo os usuários da cadeia e objetivam a obtenção de dados para roubo de criptoativos [29].

A simulação foi feita com uma mudança no banco de dados do cartório, com a alteração do nome do proprietário.

A figura abaixo mostra o banco de dados correto, em momento antes do ataque, constando o *hash* da transação que incluiu os mesmos dados na cadeia *blockchain* quando da realização do registro.

numeroDeOrdem	resumoDoImovel	proprietario	registroAnterior	hashTransacao
50	Apartamento nº 101 da Projeção 01 do Conjunto B-06...	ACYR MAURO PAIVA DA SILVA, brasileiro, solteiro,...	R.6 da Matrícula nº 86.387 do 3º Ofício de Regis...	0xfc1ad74d06d77617ed49909d6c4614e2c25cf7a01aad3fc5...

Figura 4.7 – Tabela do Banco de Dados do Sistema *WEB* em Momento Anterior ao Ataque *SQL Injection*.
Fonte: Autores.

Após o ataque, o banco de dados do sistema *WEB* tem os dados referentes ao nome do proprietário alterado conforme a figura abaixo.

```
UPDATE `matricula` SET `proprietario` = ' [Atacante do Sistema], brasileiro,\r\nsolteiro, maior, funcionário público, RG nº 362.082 SSP-DF, CPF nº 253.036.277-72, residente e\r\ndomiciliado nesta Capital.' WHERE `matricula`.`numeroDeOrdem` =
50;
```

[Editar em linha] [Edita] [Criar código PHP]

numeroDeOrdem	resumoDoImovel	proprietario	registroAnterior	hashTransacao
50	Apartamento nº 101 da Projeção 01 do Conjunto B-06...	[Atacante do Sistema], brasileiro, solteiro, mai...	R.6 da Matrícula nº 86.387 do 3º Ofício de Regis...	0xfc1ad74d06d77617ed49909d6c4614e2c25cf7a01aad3fc5...

Figura 4.8 – Tabela do Banco de Dados do Sistema *WEB* em Momento Posterior ao Ataque *SQL Injection*.
Fonte: Autores.

A violação do banco de dados local não afeta os dados da cadeia *blockchain* e a cadeia pode servir de instrumento para certificar se os dados do banco de dados local estão corretos.

Com a implementação do sistema de *blockchain*, os órgãos de fiscalização da atividade dos cartórios terão mais um instrumento para identificar eventuais alterações fraudulentas de registros. Propomos, a título exemplificativo, um fluxo para esta atividade de fiscalização conforme a figura 4.7.

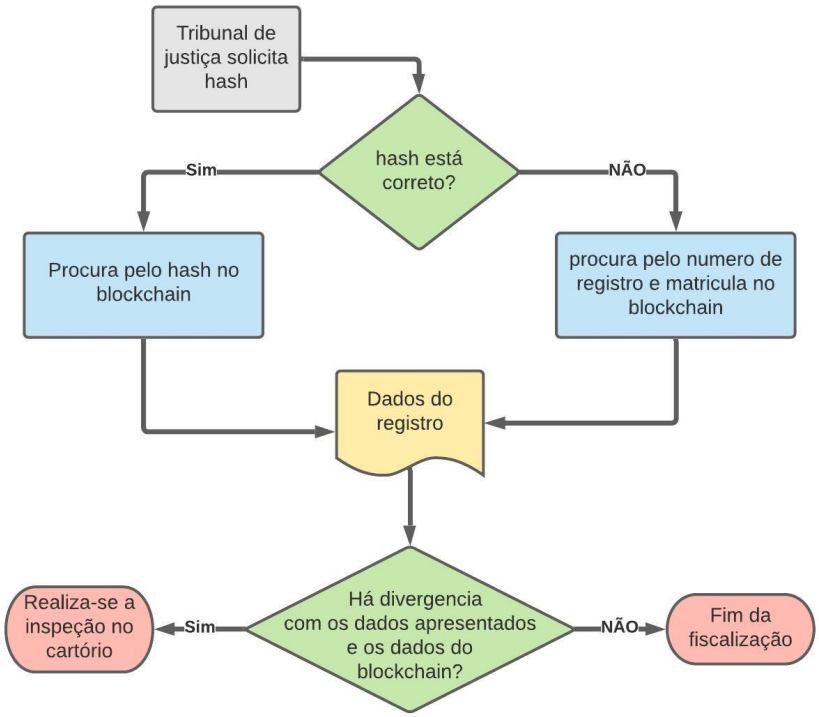

Figura 4.9 – Proposta de Fluxo de Fiscalização
Fonte: Autores.

Com a inclusão dos dados de todos os cartórios em uma cadeia de *blockchain* a tarefa de fiscalização exercida pelo Tribunal de Justiça em relação à atuação dos cartórios de imóveis poderá se valer de um novo instrumento.

Caso o real proprietário do imóvel seja surpreendido com a alteração dos dados, poderia formular uma reclamação junto ao Tribunal de Justiça para que fosse feita uma fiscalização em relação a esses dados. O órgão fiscalizador poderia acessar a cadeia *blockchain* para certificar quais dados foram incluídos quando da realização do registro (momento anterior ao ataque). A figura abaixo mostra a recuperação, pelo *hash* da transação, dos dados corretos mantidos na cadeia *blockchain*.

Figura 4.10 – Recuperação Dados Corretos pelo Blockchain.
Fonte: Autores.

Observamos que a busca da transação do registro na cadeia *blockchain* traz as informações corretas que deveriam constar do banco de dados local (antes do ataque). A cadeia de *blockchain* preserva os dados do momento do registro, mesmo após ataques aos sistemas locais e se mostra como um instrumento de segurança em relação à preservação dos dados.

4.1.3 Recuperação de Dados

.

A recuperação de dados deve ser livre a todos os que interagem com a cadeia de *blockchain*. Inicialmente demonstramos a coleta de dados do próprio cartório que realiza a inserção dos dados.

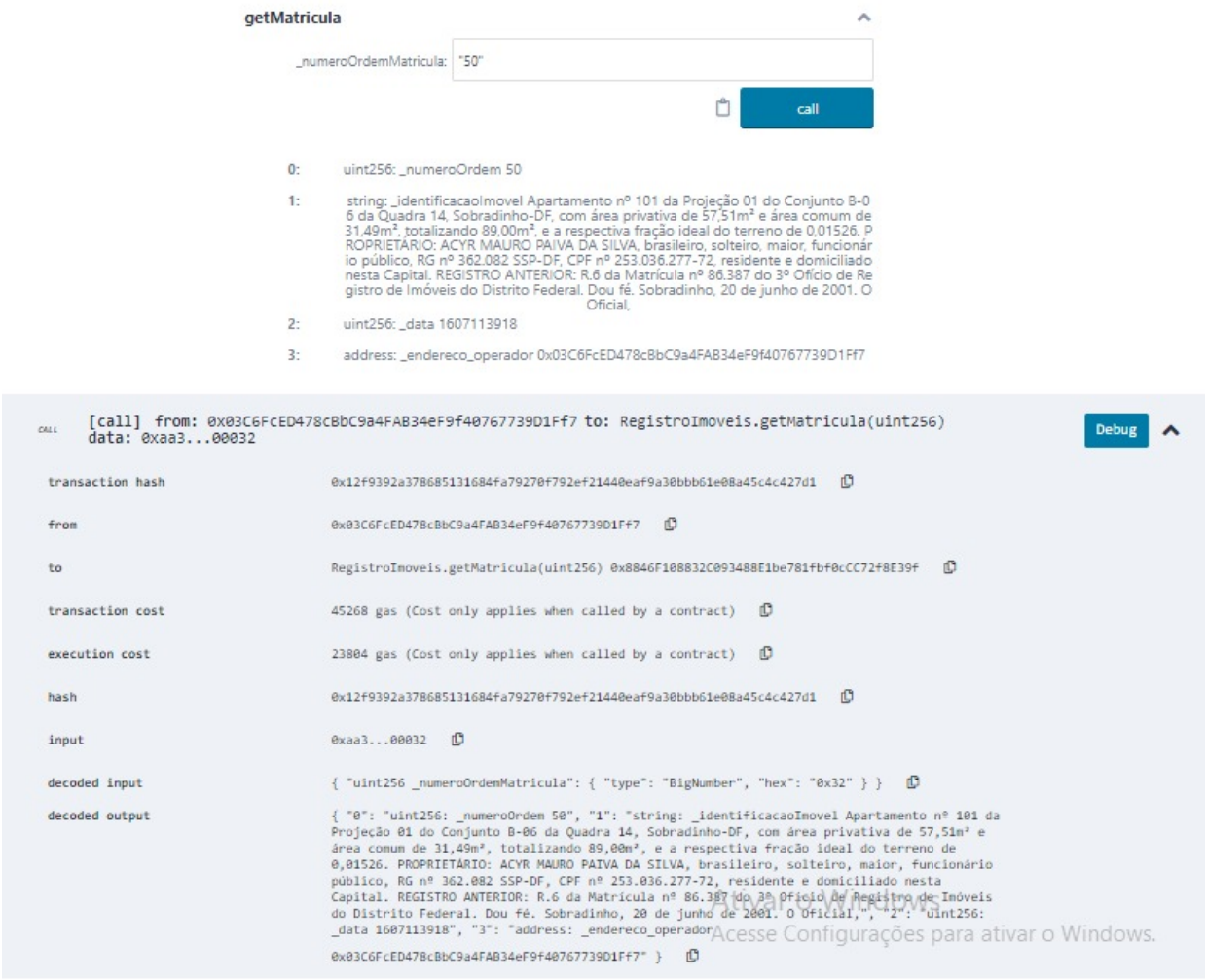

Figura 4.11 – Recuperação de Dados da Matrícula 50 pelo 7º Ofício de Registro de Imóveis. Fonte: Autores.

Observamos no campo *from* da parte inferior da imagem que a transação teve sucesso e que o endereço do demandante da informação é o 7º Ofício de Registro de Imóveis ("0x03C...").

Agora simulamos o acesso à Matrícula 50 do 7º Ofício de Registro de Imóveis pelo 1º Ofício de Registro de Imóveis (Ox5b3...).

Figura 4.12 – Recuperação de Dados da Matrícula 50 pelo 1º Ofício de Registro de Imóveis.
Fonte: Autores.

Observamos o sucesso da requisição de informação e, no campo *from*, o endereço "Ox5b3..."do 1º Ofício de Registro de Imóveis.

Agora demonstramos diversas requisições de informações, de diversos cartórios, todos com sucesso.

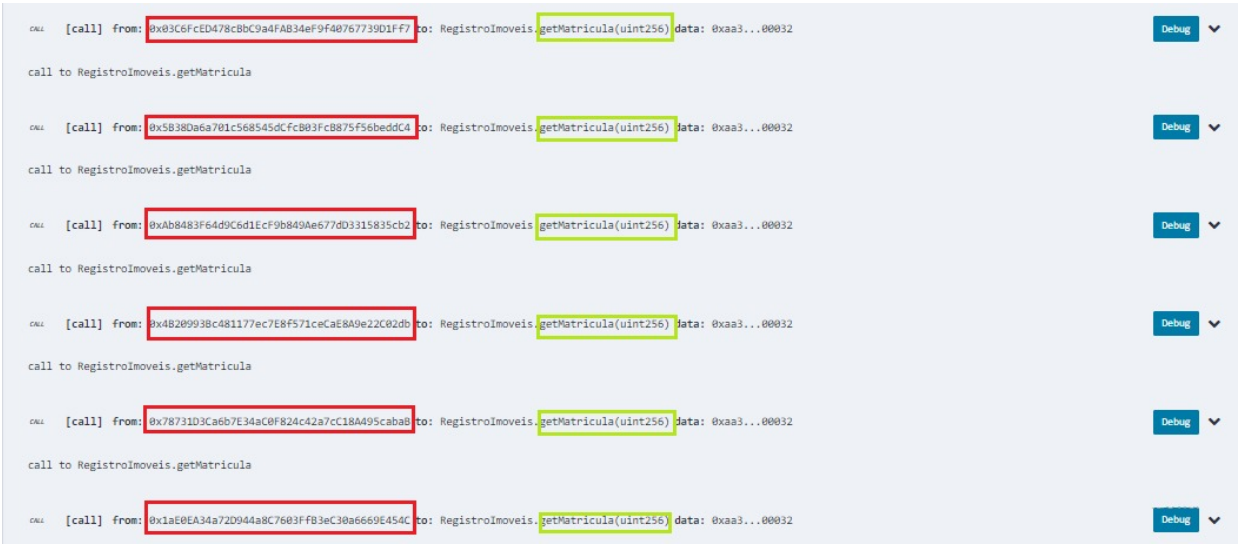

Figura 4.13 – Consulta ao *Blockchain* por Diversos Cartórios.
Fonte: Autores.

As simulações apresentadas indicam o funcionamento correto das funções de inserção e de recuperação de dados no *blockchain*. A inserção somente ocorre pelo cartório titular da matrícula e as consultas por qualquer integrante da cadeia *blockchain*.

5 Conclusões e Trabalhos Futuros.

5.1 Conclusões.

Constatamos que o registro de imóveis no Brasil tem uma legislação de regência que permite a transição do atual modelo para um modelo em que as cadeias de *blockchain* possam auxiliar e conferir uma maior confiabilidade dos dados armazenados nos diversos cartórios brasileiros.

Observamos, igualmente, que os *smartcontracts* da cadeia *Ethereum* podem ser utilizados para assumir determinadas funções dos cartórios de registros de imóveis, sendo compatíveis com as atuais exigências legais, podendo ser formatados nos moldes das exigências dos livros obrigatórios previstos em lei.

Nas simulações realizadas em ambiente da *IDE REMIX*, pudemos constatar que a inclusão das cadeias de *blockchain* nos serviços dos Ofícios de Registros de Imóveis não afetaria as atuais atribuições dos diversos cartórios, pois a gerência da cadeia privada de *blockchain Ethereum* e a codificação dos *smartcontracts* permitem estabelecer limitações às funções de inserção *(set)* e de recuperação de dados *(get)*.

Observamos que as cadeias de *blockchain* podem se comportar como um banco de dados distribuído que congrega informações de todos os cartórios de determinada região, introduzindo um novo instrumento de segurança para os dados registrados.

A realidade do Distrito Federal, que conta com uma boa oferta de serviços de internet; uma população que, quase em sua totalidade, possui acesso a internet móvel disponível em telefones celulares; um Tribunal de Justiça com servidores concursados na área de TI em número expressivo e que possui apenas 9 (nove) cartórios de registros de imóveis, apresenta condições satisfatórias para adotar, de forma pioneira, um modelo de transição com a utilização de cadeias de *blockchain* como coadjuvante aos serviços de registros de imóveis.

Para a adoção de um modelo de transição será necessário que os atuais dados referentes a matrículas, registros e averbações sejam digitalizados, sendo recomendável a digitalização dos registros auxiliares existentes. O serviço de protocolo não necessitaria da digitalização de dados anteriores, mas apenas a adoção da digitalização após implementação do armazenamento nas cadeias de *blockchain*.

Alternativa possível seria a manutenção dos atuais registros tais como se encontram e adotar a digitalização e o armazenamento nas cadeias de *blockchain* de novas matrículas, registros, averbações e registros auxiliares após a sua implementação, formalizando referências dos novos registros digitais aos registros até então existentes.

Por fim, o trabalho traz dados sobre vulnerabilidades de sistemas de *WEB* e de cadeias de *blockchain* que indicam a existência de maiores vulnerabilidades em bancos de dados do tipo *SQL* que em cadeias de *blockchain* e que os ataques às cadeias de *blockchain* se voltam, em regra, na

tentativa de obter dados de carteiras de criptoativos e não na tentativa de alterar dados incluídos na cadeia. Tal fato sugere que a introdução dos dados dos registros públicos em um *blockchain* trará ganhos nos aspectos de segurança dos bancos de dados dos registros imobiliários.

5.2 Trabalhos Futuros.

O trabalho apresentou uma proposta para a utilização de cadeia de *blockchain* para auxiliar na segurança dos registros imobiliários, limitou-se, entretanto, a simular a realidade de um *smart-contract* referente ao principal livro do registro imobiliário. Contribuição interessante e útil seria estender a presente pesquisa para simular o funcionamento dos demais livros cartorários.

Outra contribuição importante será a formatação de uma cadeia de *blockchain* privada para que o que foi objeto de simulação pudesse ser testada em ambiente de produção.

O presente projeto também pode ter desdobramento interessante no tocante à integração de sistemas hoje existentes nos Ofícios de Registros de Imóveis com as cadeias de *blockchain*, fato que permitiria a utilização transparente aos usuários dos dois sistemas propostos em nosso trabalho.

Bibliografia

[1] URL: <https://www.ietf.org/rfc/rfc1321.txt> (acesso em 07/12/2020).

[2] *A Semantic Framework for the Security Analysis of Ethereum Smart Contracts | SpringerLink*. URL: <https://link.springer.com/chapter/10.1007/978-3-319-89722-6_10> (acesso em 06/12/2020).

[3] *acessado em 28 de outubro de 2020*. URL: <https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Introduction>.

[4] *acessado em 29 de outubro de 2020*. URL: <https://solidity-portuguese.readthedocs.io/pt/latest/index.html>.

[5] Zainab Alwan e Manal Younis. "Detection and Prevention of SQL Injection Attack: A Survey". Em: *International Journal of Computer Science and Mobile Computing* 68 (ago. de 2017), pp. 5–17.

[6] J. Bae e H. Lim. "Random Mining Group Selection to Prevent 51% Attacks on Bitcoin". Em: *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. ISSN: 2325-6664. Jun. de 2018, pp. 81–82. DOI: <10.1109/DSN-W.2018.00040>.

[7] Kamanashis Biswas e Vallipuram Muthukkumarasamy. "Securing Smart Cities Using Blockchain Technology". Em: dez. de 2016. DOI: <10.1109/HPCC-SmartCity-DSS.2016.0198>.

[8] Raphael Bruce et al. "Blockchain Para Operações Interbancárias". Em: (dez. de 2019).

[9] Lin William Cong e Zhiguo He. "Blockchain Disruption and Smart Contracts". en. Em: *The Review of Financial Studies* 32.5 (mai. de 2019). Publisher: Oxford Academic, pp. 1754–1797. ISSN: 0893-9454. DOI: <10.1093/rfs/hhz007>. URL: <https://academic.oup.com/rfs/article/32/5/1754/5427778> (acesso em 02/12/2020).

[10] *Corporate Governance and Blockchains* | Review of Finance | Oxford Academic*. URL: <https://academic.oup.com/rof/article/21/1/7/2888422> (acesso em 02/12/2020).

[11] Michael Crosby. "BlockChain Technology: Beyond Bitcoin". en. Em: 2 (2016), p. 16.

[12] Maria Helena Diniz. *Sistemas de Registros de Imóveis*. São Paulo: Saraiva, 2009.

[13] *Ethereum Whitepaper*. en. URL: <https://ethereum.org> (acesso em 02/12/2020).

[14] *Formalizing and Securing Relationships on Public Networks | First Monday*. URL: <https://firstmonday.org/ojs/index.php/fm/article/view/548> (acesso em 02/12/2020).

[15] J. Michael Graglia e Christopher Mellon. "Blockchain and Property in 2018: At the End of the Beginning". Em: *Innovations: Technology, Governance, Globalization* 12.1-2 (jul. de 2018). Publisher: MIT Press, pp. 90–116. ISSN: 1558-2477. DOI: <10.1162/inov_a_00270>. URL: <https://doi.org/10.1162/inov_a_00270> (acesso em 02/12/2020).

[16] Hanna Halaburda. “Blockchain revolution without the blockchain?” Em: *Communications of the ACM* 61.7 (jun. de 2018), pp. 27–29. ISSN: 0001-0782. DOI: <10.1145/3225619>. URL: <https://doi.org/10.1145/3225619> (acesso em 02/12/2020).

[17] *How does Ethereum work, anyway?* URL: <https://www.preethikasireddy.com/post/how-does-ethereum-work-anyway> (acesso em 07/12/2020).

[18] IBGE. *Pesquisa Nacional por Amostragem de Domicílio Contínua: Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2018 - acessado em 20 de novembro de 2020*. URL: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101705_informativo.pdf>.

[19] Tribunal de Justiça do Distrito Federal. *Portal Transparência - acessado em 20 de novembro de 2020*. URL: <https://rh.tjdft.jus.br/transparencia/tlp/relatorio.asp#tlp3>.

[20] Victoria Lemieux, Daniel Flores e Claudia Lacombe. *Registro de transações imobiliárias em Blockchain no Brasil (RCPLAC-01) - Estudo de Caso 1*. Jan. de 2018. DOI: <10.13140/RG.2.2.16022.45123>.

[21] Luiz Guilherme Loureiro. *Registros Públicos: Teoria e Prática*. Salvador: Juspodium, 2017.

[22] D. Magazzeni, P. McBurney e W. Nash. “Validation and Verification of Smart Contracts: A Research Agenda”. Em: *Computer* 50.9 (2017). Conference Name: Computer, pp. 50–57. ISSN: 1558-0814. DOI: <10.1109/MC.2017.3571045>.

[23] Peter Mell e Timothy Grance. “The NIST Definition of Cloud Computing”. en. Em: (), p. 7.

[24] Paulo Nader. *Curso de Direito Civil, Volume 3: Contratos*. São Paulo: Saraiva, 2013.

[25] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Rel. técn. Publication Title: Manubot. Manubot, nov. de 2019. URL: <https://git.dhimmel.com/bitcoin-whitepaper/> (acesso em 02/12/2020).

[26] N. Nizamuddin et al. “Decentralized document version control using ethereum blockchain and IPFS”. en. Em: *Computers & Electrical Engineering* 76 (jun. de 2019), pp. 183–197. ISSN: 0045-7906. DOI: <10.1016/j.compeleceng.2019.03.014>. URL: <http://www.sciencedirect.com/science/article/pii/S0045790618333093> (acesso em 04/12/2020).

[27] Michael Nofer et al. “Blockchain”. en. Em: *Business & Information Systems Engineering* 59.3 (jun. de 2017), pp. 183–187. ISSN: 1867-0202. DOI: <10.1007/s12599-017-0467-3>. URL: <https://doi.org/10.1007/s12599-017-0467-3> (acesso em 02/12/2020).

[28] *Offensive Security’s Exploit Database Archive*. en. URL: <https://www.exploit-db.com/> (acesso em 07/12/2020).

[29] *Relatório sobre ameaças na blockchain*. pt. URL: <https://www.mcafee.com/enterprise/pt-br/assets/reports/rp-blockchain-security-risks.pdf> (acesso em 07/12/2020).

[30] *Research on the Security Criteria of Hash Functions in the Blockchain | Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*. URL: <https://dl.acm.org/doi/abs/10.1145/3205230.3205238> (acesso em 02/12/2020).

[31] Usha R. Rodrigues. “Law and the Blockchain”. Em: *Iowa Law Review* 104 (2018), p. 679. URL: <https://heinonline.org/HOL/Page?handle=hein.journals/ilr104&id=693&div=&collection=>.

[32] Meni Rosenfeld. “Overview of Colored Coins”. en. Em: (), p. 13.

[33] M. Saad et al. “Mempool optimization for Defending Against DDoS Attacks in PoW-based Blockchain Systems”. Em: *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. Mai. de 2019, pp. 285–292. DOI: <10.1109/BLOC.2019.8751476>.

[34] *Security and Privacy on Blockchain | ACM Computing Surveys*. URL: <https://dl.acm.org/doi/abs/10.1145/3316481> (acesso em 02/12/2020).

[35] Savva Shanaev et al. “Cryptocurrency Value and 51% Attacks: Evidence from Event Studies”. en. Em: *The Journal of Alternative Investments* 22.3 (dez. de 2019). Publisher: Institutional Investor Journals Umbrella, pp. 65–77. ISSN: 1520-3255, 2168-8435. DOI: <10.3905/jai.2019.1.081>. URL: <https://jai.pm-research.com/content/22/3/65> (acesso em 02/12/2020).

[36] Voshmgir Shermin. “Disrupting governance with blockchains and smart contracts”. en. Em: *Strategic Change* 26.5 (2017). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/jsc.2150, pp. 499–509. ISSN: 1099-1697. DOI: <https://doi.org/10.1002/jsc.2150>. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/jsc.2150> (acesso em 02/12/2020).

[37] J. Singh e J. D. Michels. “Blockchain as a Service (BaaS): Providers and Trust”. Em: *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. Abr. de 2018, pp. 67–74. DOI: <10.1109/EuroSPW.2018.00015>.

[38] Yonatan Sompolinsky e Aviv Zohar. “Secure High-Rate Transaction Processing in Bitcoin”. en. Em: *Financial Cryptography and Data Security*. Ed. por Rainer Böhme e Tatsuaki Okamoto. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2015, pp. 507–527. ISBN: 978-3-662-47854-7. DOI: <10.1007/978-3-662-47854-7_32>.

[39] D. Vujičić, D. Jagodić e S. Ranđić. “Blockchain technology, bitcoin, and Ethereum: A brief overview”. Em: *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*. Mar. de 2018, pp. 1–6. DOI: <10.1109/INFOTEH.2018.8345547>.

[40] K. Wüst e A. Gervais. “Do you Need a Blockchain?” Em: *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. Jun. de 2018, pp. 45–54. DOI: <10.1109/CVCBT.2018.00011>.

[41] Dylan Yaga et al. “Blockchain Technology Overview”. Em: *arXiv:1906.11078 [cs]* (out. de 2018). arXiv: 1906.11078, NIST IR 8202. DOI: <10.6028/NIST.IR.8202>. URL: <http://arxiv.org/abs/1906.11078> (acesso em 02/12/2020).

[42] S. Zhang e J. Lee. “Double-Spending With a Sybil Attack in the Bitcoin Decentralized Network”. Em: *IEEE Transactions on Industrial Informatics* 15.10 (out. de 2019). Conference Name: IEEE Transactions on Industrial Informatics, pp. 5715–5722. ISSN: 1941-0050. DOI: <10.1109/TII.2019.2921566>.

[43] W. Zheng et al. “NutBaaS: A Blockchain-as-a-Service Platform”. Em: *IEEE Access* 7 (2019). Conference Name: IEEE Access, pp. 134422–134433. ISSN: 2169-3536. DOI: <10.1109/ACCESS.2019.2941905>.

[44] Zibin Zheng et al. “Blockchain challenges and opportunities: a survey”. Em: *International Journal of Web and Grid Services* 14.4 (jan. de 2018). Publisher: Inderscience Publishers, pp. 352–375. ISSN: 1741-1106. DOI: <10.1504/IJWGS.2018.095647>. URL: <https://www.inderscienceonline.com/doi/abs/10.1504/IJWGS.2018.095647> (acesso em 02/12/2020).

ANEXO A – Registros de Imóveis

A.0.1 Propriedade.

O Brasil é uma República Federativa que se constitui como um Estado Democrático de Direito e que encontra na livre iniciativa um de seus fundamentos (art. 1º, inciso IV, Constituição Federal). Nossa Ordem Econômica e Financeira adota, dentre outros, os princípios da propriedade privada, da função social da propriedade, da livre concorrência e da defesa do consumidor, sendo assegurado a todos o livre exercício de qualquer atividade econômica (art. 170 da Constituição Federal). Tais dispositivos constitucionais apenas demonstram a importância data à propriedade privada nas sociedades que adotam o sistema capitalista, como a brasileira.

No âmbito do direito, a propriedade gera o denominado direito real (chamado assim pois não se fundamenta em contrato ou em qualquer outra relação, mas em razão da própria coisa) que se revela na possibilidade de usar, fruir e dispor de um bem próprio sem que qualquer outra pessoa possa intervir. As únicas limitações desse direito adviriam de concessões voluntárias de seu titular, de limitações naturais ou fixadas em lei (Ex: princípio da função social da propriedade).

Existem outros direitos reais que decorrem da propriedade, mas não se referem a bens próprios e sim a bens de terceiros. Quando um bem é hipotecado, o credor adquire um direito real de garantia mas tal direito do credor está fixado em bem de terceiro e não em bem próprio. A propriedade é, portanto, o principal direito real e apresenta uma característica que os doutrinadores germânicos chamam de elasticidade da propriedade pois, quando o direito real de terceiros cessa, a propriedade adquire novamente todas as suas características. No exemplo da hipoteca, quando o devedor paga sua dívida, a garantia (hipoteca) deve ser retirada, ou seja, o credor perde o direito real de garantia (hipoteca) e o proprietário adquire a plenitude de seu direito real de propriedade.

A propriedade liga um objeto a uma pessoa (física ou jurídica) e tal vínculo gera direitos que devem ser respeitados por todos (*erga omnes*). Para que tal direito possa ser resguardado é imprescindível que a propriedade seja bem estabelecida pois o proprietário pode reivindicar o seu bem de qualquer outro que indevidamente o detenha ou reivindique. Para melhor definir a propriedade de bens imóveis, o legislador concebeu um sistema que possibilita a todos o prévio conhecimento do titular do bem e de eventuais restrições que tal bem possa possuir. Este sistema tem seu sustentáculo nos Cartórios de Registro de Imóveis que mantém o cadastro de todos os bens imóveis urbanos, seus proprietários e anota todas as restrições que eventualmente possam existir para esse imóvel ou para seus titulares.

O Registro de Imóveis, portanto, na lição de Maria Helena Diniz [12], "assegura a possibilidade da identificação da coisa e de seu atual titular". Para a doutrinadora, tal fato se dá, pois o registro imobiliário, dentre outras consequências, garante a "continuidade registrária". Tal garantia se dá com um contínuo e permanente registro de ocorrências havidas em relação ao próprio imóvel ou das pessoas que com ele se relacionem. Este registro contínuo atualmente é expresso por anotações em livros previstos na legislação e, em nosso estudo, proporemos que tais registros e anotações

sejam armazenados em uma cadeia de *blockchain*.

A.0.2 Ofícios de Registros de Imóveis.

Os cartórios de imóveis são os responsáveis pelo registro dos imóveis urbanos e recebem as suas atribuições para o registro de todos os imóveis urbanos de determinada localidade. Em cidades grandes há uma grande quantidade de cartórios de imóveis, que são fiscalizados pelos Tribunais de Justiça dos Estados. A definição de uma área de competência dos cartórios serve para facilitar e ampliar a publicidade na divulgação das informações referentes aos imóveis. Em qualquer negociação o comprador pode se dirigir ao cartório da respectiva localidade do imóvel e lá obter informações sobre a natureza do imóvel, seus proprietários, suas confrontações, eventual existência de ônus sobre o imóvel, enfim, todos os dados relevantes para a tomada de decisão.

Importante lembrar que em nosso sistema legal, a propriedade imóvel somente se adquire mediante o registro no cartório de imóveis. Os atos que antecedem o registro, como o contrato de compra e venda, apenas geram direitos pessoais, não operando a transmissão da propriedade. Este fato dá ao registro de imóveis uma importância impar. O registro imobiliário se apresenta com três finalidades principais:

- i) traz a devida garantia de autenticidade das negociações imobiliárias;
- ii) dá segurança jurídica aos negócios que envolvem imóveis e
- iii) gera a eficácia dessas negociações para terceiros.

O registro usual de imóveis em nosso país é o registro imobiliário de bens urbanos. Este é o que conhecemos de forma ordinária e está a cargo dos diversos Cartórios de Registro de Imóveis de nossas cidades. Há outros bens imóveis que também são registrados mas em outras repartições públicas. Como exemplo apontamos o registro de imóveis rurais que é realizado pelo INCRA conforme previsão da Lei 4.504/64. O trabalho que faremos está limitado ao registro de bens imóveis previsto pela Lei 6.015/73.

As questões referentes ao registro imobiliário estão disciplinadas nos artigos 167 a 216 da lei nº 6.015/1973. Os Cartórios de Registro de Imóveis devem possuir 5 livros para os registros e averbações (art. 173 da Lei 6.015/73). São eles:

- i) Livro nº 1 – Protocolo;
- ii) Livro nº 2 – Registro Geral;
- iii) Livro nº 3 – Registro Auxiliar;
- iv) Livro nº 4 – Indicador Real;
- v) Livro nº 5 – Indicador Pessoal.

O Livro nº 1, Protocolo, "servira para apontamento de todos os títulos apresentados diariamente". A escrituração no protocolo exige as seguintes informações:

- i) número de ordem;
- ii) data da apresentação;
- iii) nome do apresentante;
- iv) natureza formal do título e
- v) os atos que formalizar de forma resumida.

O Livro nº 2, Registro Geral, se destina à matrícula do imóvel e ao registro ou averbação dos atos relacionados no artigo 167 da Lei nº 6.015/1973 que não sejam atribuídos ao Livro nº 3.

Cada imóvel terá uma matrícula própria que deve ser aberta por ocasião do primeiro registro feito. A escrituração da matrícula deve conter o seguinte:

- i) número de ordem, que segue indefinidamente;
- ii) data;
- iii) identificação do imóvel;
- iv) nome, domicílio e nacionalidade do proprietário;
- v) número do registro anterior e
- vi) em caso de multipropriedade em *time sharing* a indicação de eventuais matrículas da divisão de tempo.

A matrícula do imóvel pode ser equiparada ao nascimento desse imóvel. Após essa inscrição primitiva, as alterações posteriores desse imóvel devem ser anotadas no registro de imóveis por meio dos registros e averbações.

Os registros do livro nº 2 devem conter as seguintes informações:

- i) data;
- ii) nome, domicílio e nacionalidade do transmitente, ou devedor, e do adquirente ou credor;
- iii) título da transmissão ou do ônus;
- iv) forma do título, sua procedência e caracterização;
- v) o valor do contrato, da coisa, ou da dívida, prazo desta, condições e mais especificações, inclusive juros, se houver.

As averbações do livro nª 2 não contam com informações obrigatórias e, como exemplo, se destinam a anotações que indiquem alterações do estado das pessoas que se relacionam com o imóvel.

O Livro nº 3, Registro Auxiliar, se destina ao registro de:

- i) emissão de debêntures e as hipotecas, anticrese ou penhor que abonarem essas emissões;
- ii) as cédulas de crédito rural e de cré-dito industrial;
- iii) as convenções do condomínio edilício, condomínio geral voluntário e condomínio em multipropriedade;
- iv) penhor de máquinas e aparelhos utilizados na indústria, instalados ou em funcionamento;
- v) convenções antenupciais;
- vi) contratos de penhor rural e
- vii) outros títulos que interessados queiram registrar seu inteiro teor.

O Livro nº 4, Indicador Real, é um repositório de todos os imóveis que são referidos nos demais livros, devendo conter sua identificação, referências aos números de ordem dos outros livros e outras anotações que se façam necessárias. Cada registro deve receber um número que segue indefinidamente.

O Livro nº 5, Indicador Pessoal, é o repositório dos nomes de todas as pessoas que, individualmente ou coletivamente, ativa ou passivamente, direta ou indiretamente, figurem nos demais livros, fazendo referência aos respectivos números de ordem.

Após a definição dos diversos livros que devem existir em um cartório de imóveis, a legislação trata da forma como devem ser feitas as respectivas escriturações.

Todo título apresentado ao cartório deve ser escriturado no livro nº 1 – Protocolo – recebendo um número próprio seguindo a rigorosa ordem de sua apresentação. Tal ordem é importante pois a prenotação de títulos (protocolo) estabelece prioridade para o registro, e esta prioridade gera a preferência para aquisição de direitos reais (ex: prioridade entre hipoteca de um mesmo imóvel). Assim os títulos apresentados são inscritos no Protocolo, recebem um número e a data de sua pre-notação. O protocolo deve ser encerrado diariamente.

Permuta de imóveis são tratadas de forma singular no livro de protocolo. As permutas de imóveis, quando de uma mesma circunscrição, serão registradas em cada matrícula dos imóveis, mas sob um único número de protocolo.

O título que foi apresentado no protocolo tem prioridade para registro no prazo de 30 dias. Há situações específicas tratadas na lei de registros públicos:

- i) a apresentação de um título indicando tratar-se de 'segunda hipoteca' de um imóvel, aguardará o prazo de 30 dias para que seja registrada a hipoteca anterior, caso o título da primeira hipoteca não seja apresentada, será inscrita e terá prioridade sobre ela;
- ii) títulos que apresentem direitos contraditórios sobre imóveis não serão registrados no mesmo dia;
- iii) títulos prenotados no mesmo dia deverão ser registrados em dias subsequentes, uma a cada dia útil, obedecendo a ordem de sua apresentação e

- iv) escrituras públicas, lavradas no mesmo dia, que constem o horário de sua lavratura, seguirão a ordem de sua lavratura, independentemente do protocolo, caso sejam apresentadas no mesmo dia.

Apresentado o título, o oficial do cartório pode efetuar o registro ou indicar suas exigências para o registro. Tais exigências devem ser atendidas pelo apresentante sob pena do registro não ocorrer. Caso o apresentante do título não concorde ou não tenha condições de cumprir as exigências, poderá recorrer e a questão será decidida pelo Juiz de Registros Públicos. Instalado este processo, o oficial do cartório deve anotar tal fato à margem da prenotação do livro de Protocolo. Após o processo encerrar, o oficial do cartório devolverá os documentos apresentados ou fará o registro com a sentença que deverá ser mantida em cartório.

Há hipóteses previstas na legislação de retificação de registros e averbações. Tais retificações podem ser realizadas *de ofício* ou a requerimento de interessados e seguem procedimentos administrativos próprios. Importante ressaltar que, salvo erros materiais na lavratura de registros, qualquer outra alteração, em regra, dependerá de processo judicial.

A.0.3 Procedimentos para o Registro de Imóveis.

Passemos, agora a descrever como se dá o procedimento de registro de imóveis para que reste claro a transição que propomos com a utilização da cadeia de *blockchain*.

Como dissemos, o cartório de imóveis é, na verdade, um repositório de informações relevantes sobre imóveis de uma determinada região para que qualquer interessado possa ter acesso a essas informações. O funcionamento de um cartório de imóveis se dá, portanto, em duas tarefas principais. A primeira a de manutenção de um cadastro dos imóveis e suas restrições para que todos os dados sejam acessíveis aos interessados. A segunda a de promover as devidas alterações desse cadastro quando instado a fazê-lo.

Neste cenário, quem se dirige a um Cartório de Imóveis tem um, de dois possíveis objetivos:

- a) deseja informações sobre imóveis ou
- b) deseja alterar informações sobre imóveis.

Assim, podemos construir dois fluxos diversos para as atividades de um Cartório de Imóveis. O primeiro para os que desejam informações sobre imóveis (figura 2.1):

- i) interessado procura o Cartório de Imóveis e solicita informações;
- ii) o Cartório de Imóveis apresenta as informações solicitadas.

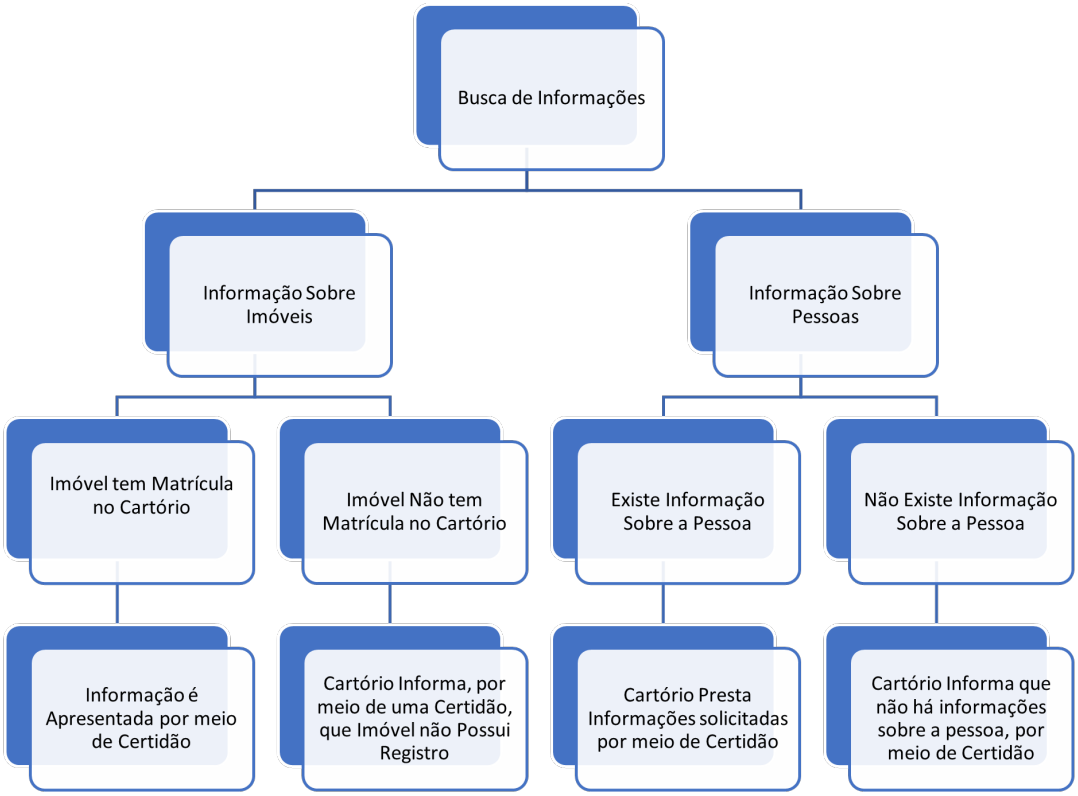

Figura A.1 – Fluxo de Busca de Informações
Fonte: Autores.

O segundo para quem deseja promover alterações de dados registrados no Cartório:

- i) interessado busca o Cartório de Imóveis, solicita as alterações munido da devida documentação;
- ii) Cartório de Imóveis recebe a documentação;
- iii) Após análise da documentação Cartório adota uma das seguintes ações:
  - a) promove a alteração (fim do processo) ou
  - b) indica os motivos para não fazê-lo.
- iv) Interessado é notificado dos motivos da não realização do registro e:
  - a) a) nada faz (fim do processo)
  - b) atende às exigências do cartório para a efetivação do registro.
    - i) cartório promove a alteração solicitada (fim do processo)
    - ii) cartório coloca novas exigências (volta ao item iv);
    - iii) cartório pede ao Poder Judiciário que decida sobre a alteração (processo de dúvida registrária).
- v) Cartório cumpre o decidido no processo de dúvida registrária

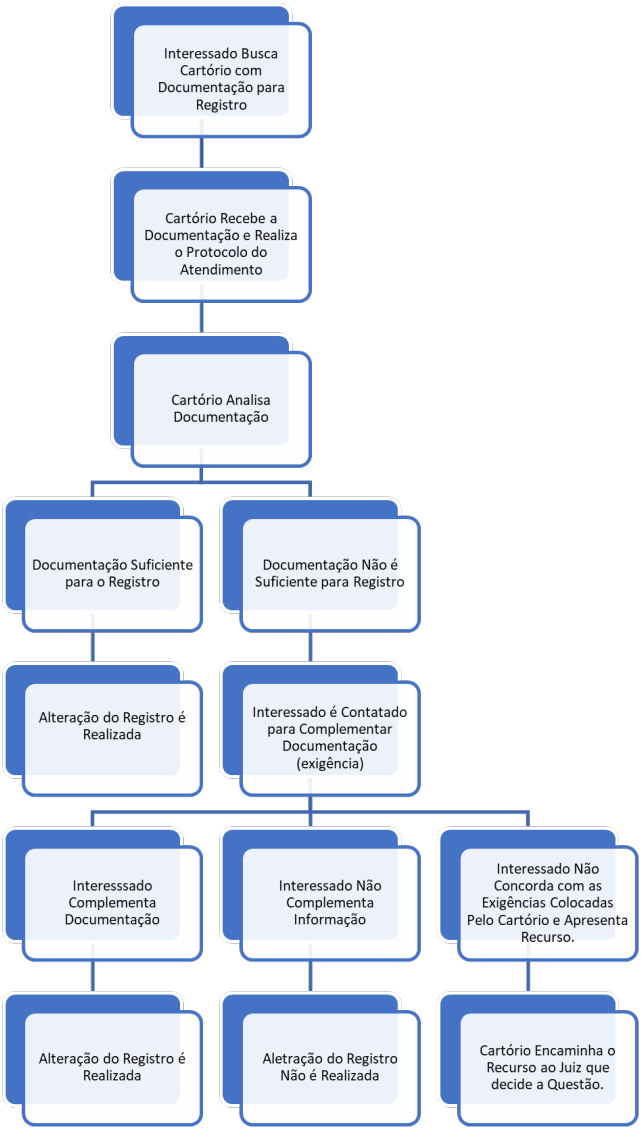

Figura A.2 – Fluxo de Alteração de Registros
Fonte: Autores.

Há ainda um terceiro fluxo, não ordinário, e de pouca interação que é a retificação de registros feitas pelo próprio cartorário (Ex: quando ocorrer algum erro material no registro) ou por ordem Judicial. Neste fluxo, no caso de retificação 'de ofício' (feita pelo próprio cartorário), simplesmente ocorre a retificação quando identificado o erro e, no caso de retificação por ordem judicial, simplesmente ocorre a retificação apontando a decisão judicial responsável.

A.0.4 Registros de Imóveis no Distrito Federal.

Com apenas 60 anos, o Distrito Federal conta hoje nesses 9 (nove) Ofícios de Registros Públicos com cerca de 825.565 (oitocentos e vinte e cinco mil, quinhentos e sessenta e cinco) Matrículas de imóveis urbanos, segundo informações obtidas junto à ANOREG/DF. Isto significa uma grande quantidade de dados que estão armazenados de forma difusa, não necessariamente de forma digital.

Os diversos Cartórios de Registro de Imóveis abrangem todas as regiões administrativas e suas competências territoriais estão assim definidas:

- - 1º Ofício de Registro de Imóveis (126.400 matrículas):
  - Asa Sul;
  - Lago Sul;
  - Sudoeste;
  - Cruzeiro;
  - Octogonal e
  - Setor Gráfico.
- - 2º Ofício de Registro de Imóveis (165.975 matrículas):
  - Parte Norte do Plano Piloto, incluindo áreas adjacentes de outras regiões administrativas;
  - Paranoá e
  - São Sebastião.
- - 3º Ofício de Registro de Imóveis (259.294 matrículas):
  - Taguatinga;
  - Águas Claras;
  - Samambaia e
  - Recanto das Emas.
  -
- - 4º Ofício de Registro de Imóveis (104.323 matrículas):
  - Guará e
  - Santa Maria.
- - 5º Ofício de Registro de Imóveis (49.596 matrículas):
  - Gama e
  - Santa Maria.
- - 6º Ofício de Registro de Imóveis (63.294 matrículas):
  - Ceilândia.
- - 7º Ofício de Registro de Imóveis (24.084 matrículas):
  - Sobradinho.

- - 8º Ofício de Registro de Imóveis (22.130 matrículas):
  - Planaltina.
- - 9º Ofício de Registro de Imóveis (10.469 matrículas):
  - Brazlândia.

O trabalho de fiscalização dos cartórios está ligado à Corregedoria do Tribunal de Justiça e o Ministério Público atua, igualmente, nos procedimentos registrários.