



**Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"**

VINICIUS DE PAIVA DIONIZIO

**O USO DE BLOCKCHAIN E POTENCIAIS PRÁTICAS NO SETOR PÚBLICO
BRASILEIRO**

**Assis/SP
2022**



**Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"**

VINICIUS DE PAIVA DIONIZIO

**O USO DE BLOCKCHAIN E POTENCIAIS PRÁTICAS NO SETOR PÚBLICO
BRASILEIRO**

Projeto de Trabalho de Conclusão de Curso apresentado
no curso de Bacharelado em Ciência da Computação na
FEMA.

**Orientando: Vinicius de Paiva Dionizio
Orientador: Dr. Almir Rogério Camolesi**

**Assis/SP
2022**

FICHA CATALOGRÁFICA

D592u Dionizio, Vinicius de Paiva.

O uso de blockchain e potenciais práticas no setor público brasileiro / Vinicius de Paiva Dionizio – Assis, SP: FEMA, 2022.

45 f.

Trabalho de Conclusão de Curso (Graduação) – Fundação Educacional do Município de Assis – FEMA, curso de Ciência da Computação, Assis, 2022.

Orientador: Dr. Almir Rogério Camolesi.

1. Blockchain. 2. Smart Contract. 3. Solidity. 4. Setor público. I. Título.

CDD 005.74

Biblioteca da FEMA

O USO DE BLOCKCHAIN E POTENCIAIS PRÁTICAS NO SETOR PÚBLICO BRASILEIRO

VINICIUS DE PAIVA DIONIZIO

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____ Dr. Almir Rogério Camolesi

Examinador: _____ Me. Guilherme de Cleve Farto

**Assis/SP
2022**

DEDICATÓRIA

Dedico este trabalho à minha família que sempre acreditou na minha capacidade, principalmente pai, mãe e irmão que foram direta e indiretamente ativos na minha formação de caráter.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me guiado por toda a minha vida, mesmo que por vezes faltei com a fé, Ele me sustentou, me deu saúde e sabedoria para que eu pudesse enfrentar todos os desafios.

Ao meu orientador Prof. Almir Rogério Camolesi, que assim que o procurei demonstrou confiança e alegria ao me ver concluindo esse processo, e que me guiou por todo esse ano e fez com que eu confiasse mais em mim, enriquecendo o trabalho com seu conhecimento e tornando a pesquisa e apresentação mais fácil, e ao examinador Prof. Guilherme de Cleve Farto que igualmente se mostrou alegre pela minha decisão e que com seu olhar de examinador pôde me guiar nas limitações do projeto inicial.

Agradeço também toda a minha família e amigos, aos que me cobraram para que eu não desistisse na etapa final do percurso, em especial meus pais Valmir Dionizio e Vera Lucia de Paiva Dionizio, meu irmão Valmir Dionizio Junior, que por diversas vezes compreenderam minha ausência para focar nos estudos, meus amigos Felipe Pescada e Rafael Rocha que foram bem insistentes para que eu concluísse a minha formação, à Érica Pelegrin que disponibilizou seu tempo para me auxiliar.

Agradeço a todos que de forma direta ou indireta contribuíram para que este trabalho pudesse ser concluído.

RESUMO

O setor público é responsável por controlar boa parte dos recursos do Estado que estão disponíveis para a população, como transporte público, registro e autenticidade de documentos em cartório, saúde pública, entre outros. Além disso, é função de um estado democrático permitir sistemas de votação seguros e íntegros, que permitam à população escolher seus próximos representantes de forma justa e igualitária. Apesar disso, entende-se que existem falhas em vários desses setores, o que leva a problemas de fraude, corrupção em diversos setores do ente público, o que desencadeia uma falta de confiança nos serviços prestados. Para procurar resolver vários desses problemas, pode-se adotar a tecnologia blockchain, que permite que todos os dados fiquem armazenados de forma descentralizada e que todos os nós da cadeia tenham acesso às informações. Sendo assim, o objetivo geral deste trabalho é realizar um estudo de caso sobre o impacto da tecnologia Blockchain caso inseridas no âmbito dos Governos Federal, Estaduais e Municipais, por meio da proposta de exemplos de sua utilização e relevância em cada setor.

Palavras-chave: blockchain, contratos inteligentes, setor público.

ABSTRACT

The public sector is responsible for controlling a large part of the State resources that are available to the population, such as public transport, registration and authenticity of documents in a notary's office, public health, among others. Furthermore, it is the function of a democratic state to allow safe and fair voting systems, which allow the population to choose their next representatives in a fair and equitable manner. Despite this, it is understood that there are flaws in several of these sectors, which leads to problems of fraud, corruption in various sectors of the public entity, which triggers a lack of trust in the services provided. To try to solve several of these problems, blockchain technology can be adopted, which allows all data to be stored in a decentralized way and all nodes in the chain to have access to information. Therefore, the general objective of this work is to carry out a case study on the impact of Blockchain technology if inserted in the scope of Federal, State and Municipal Governments, through the proposal of examples of its use and relevance in each sector.

Keywords: blockchain, smart contracts, public sector.

LISTA DE ILUSTRAÇÕES

Figura 1: Comparativo entre uma transação tradicional e uma em rede distribuída.	16
Figura 2: Execução de uma transação em blockchain	16
Figura 3: Funcionamento da criptografia de chave pública.	17
Figura 4: Verificação de transações por redes públicas e privadas.	19
Figura 5: Hello Word em Solidity.	22
Figura 6: Fluxograma do WaveVote.	26
Figura 7: Processo licitatório simplificado.	28
Figura 8: Fluxograma do registro de marca e patente no Brasil.	29
Figura 9: Trecho de código Solidity declarando o contrato LicitacaoFactory	34
Figura 10: Trecho de código Solidity com as funções de LicitacaoFactory	35
Figura 11: Interface com dados de um novo contrato	36
Figura 12: Trecho de código Solidity declarando o contrato Licitacao	37
Figura 13: Trecho de código Solidity com as funções de Licitacao	38
Figura 14: Trecho de código Solidity com as funções de Licitacao	39
Figura 15: Trecho de código Solidity com as funções de Licitacao	40
Figura 16: Interface de exibição dos dados de um contrato	41

LISTA DE TABELAS

Tabela 1: Principais tipos de variáveis da linguagem Solidity.	21
Tabela 2: Serviços de um Cartório Segundo a Legislação Brasileira.	24
Tabela 3: Projetos que Exploram os Registros de Documentos por Blockchain.	24
Tabela 4: Projetos que o blockchain na rede elétrica.	31

LISTA DE ABREVIATURAS E SIGLAS

IDE	Ambiente de Desenvolvimento Integrado
API	Interface de Programação de Aplicação

SUMÁRIO

1. INTRODUÇÃO	12
1.1. JUSTIFICATIVA	13
1.2. OBJETIVOS	13
1.3. MOTIVAÇÃO	14
1.4. METODOLOGIA	14
2. REFERENCIAL TEÓRICO	15
2.1. BLOCKCHAIN	15
2.2. ARQUITETURA BLOCKCHAIN	18
2.3. CONTRATOS INTELIGENTES	19
2.4. SOLIDITY	20
3. BLOCKCHAIN NO SETOR PÚBLICO BRASILEIRO	22
3.1. CARTÓRIOS COMPROVAÇÃO DE DOCUMENTOS	23
3.2. SISTEMAS DE VOTAÇÃO	25
3.3. DADOS PÚBLICOS	27
3.4. LICITAÇÕES	27
3.5. PROPRIEDADE INTELECTUAL, MARCAS E PATENTES	29
3.6. GESTÃO DE SAÚDE	30
3.7. OUTROS	31
4. IMPLEMENTAÇÃO DE UM CONTRATO INTELIGENTE	33
5. CONCLUSÕES E TRABALHOS FUTUROS	42
REFERÊNCIAS	44

1. INTRODUÇÃO

De acordo com os dados transmitidos pelo TSE, no ano de 1996, eleitores de 57 cidades tiveram o primeiro contato com a urna eletrônica e seu uso se popularizou, pois foi considerado uma revolução no processo eleitoral brasileiro (TSE, 2021). Mesmo assim, a urna eletrônica vem sendo alvo de frequentes ataques de cidadãos que duvidam de sua confiabilidade apesar de nunca ter havido comprovação de fraude, uma vez que este não é o principal modelo utilizado em boa parte dos países democráticos que elegem seus representantes através do voto popular.

Foi nesta época também que a internet se fez mais presente entre a população brasileira, mas o maior crescimento foi com a popularização das redes sociais a partir de 2004. Em 2008 surgiu a primeira referência ao termo *Blockchain*, uma tecnologia utilizada para assegurar dados da moeda criptográfica Bitcoin, e apesar de surgirem no mesmo escopo e terem forte ligação, o *Blockchain* não se limita apenas a transações de moedas criptográficas (CURY, 2019).

O Blockchain é de certa forma uma revolução, algo similar à internet em sua origem, pois pela primeira vez na história, não se depende de um órgão mandatário para controlar a confiabilidade das transações, por isso alguns até se referem ao próprio blockchain como uma máquina confiável (BADR, HORROCKS, WU, 2018).

O grande diferencial do *Blockchain* é sua segurança, eficiência e transparência em suas transações, pois o processamento, armazenamento e visualização das informações podem ser de uso comum entre todos os usuários que tenham acesso a ele (CURY, 2019), desde que a rede que o mantém seja também confiável.

O *Blockchain* está sendo utilizado tanto por iniciativas públicas quanto privadas, que enxergam não só o grande potencial da tecnologia e o avanço tanto tecnológico, mas também a transparência que existe com sua implementação e aplicação. Com base nesses fatores, ao longo deste trabalho, serão abordadas situações como comprovação de documentos, sistema de voto, marcas, patentes e propriedades intelectuais.

1.1. JUSTIFICATIVA

Apesar de existir um portal da transparência do governo brasileiro e este ser informatizado, existem lacunas que prejudicam a fiscalização e obtenção de informações públicas, abrindo precedentes para a desconfiança da população. Desta forma, se algumas mudanças nas tecnologias atuais fossem realizadas, com a implementação do conceito de blockchains, haveria a possibilidade de que alcançássemos a verdadeira e total transparência no acesso aos documentos públicos, diminuindo as chances de corrupção e adulteração de documentos.

Alguns órgãos do governo já estão explorando essa nova tecnologia, que oficializaram o uso do blockchain para certificado em documentos, apesar de não ser utilizado para validar os documentos e sim para certificar a existência de um determinado documento em uma data e horário específico (SANTOS, 2021).

1.2. OBJETIVOS

O objetivo geral deste trabalho é realizar o estudo de caso sobre o impacto da tecnologia Blockchain caso sejam inseridas no âmbito dos Governos Federal, Estadual e Municipal, através da proposta de exemplos de sua utilização e realização de testes de confiabilidade e relevância em cada setor.

Para isso, levaremos em conta os seguintes objetivos específicos:

- A compreensão dos conceitos base do Blockchain;
- Estudar onde a tecnologia pode ser utilizada, como por exemplo, a comprovação de documentos, sistema de voto, marcas, patentes e propriedades intelectuais;
- E por fim, propor a utilização da tecnologia no âmbito dos Governos Federal, Estaduais e Municipais;

1.3. MOTIVAÇÃO

A partir da realização do estudo da praticidade e viabilidade de implementação em alguns setores do Governo, espera-se que a tecnologia de Blockchain se torne uma referência para que, futuramente exista uma avaliação da viabilidade dessa tecnologia para que possa ser implementada em larga escala, o que beneficiaria tanto a população quanto o Estado.

A popularidade em alta das criptomoedas e NFT e conseqüentemente dos blockchains, chamou a atenção de pessoas que não são da área técnica, e com a implementação em serviços do Governo, podem conquistar ainda mais curiosos e permitir que a população em geral tenha maior controle do país onde vive.

Além disso, contribuiria para maior eficiência, redução do tempo de espera de ações e maior transparência, de modo que o próprio contribuinte consiga perceber que seu imposto está sendo bem administrado.

1.4. METODOLOGIA

A metodologia de pesquisa utilizada consistirá no levantamento bibliográfico, onde será realizado um estudo exploratório com o propósito de fundamentar os conceitos que estarão presentes posteriormente nas implementações.

Assim, o levantamento bibliográfico será focado no estudo da estrutura do blockchain, sobre seus atuais utilizadores como por exemplo criptomoedas e NFT, estudo sobre os contratos inteligentes e da linguagem Solidity responsável pela programação de tais contratos. Após isso, e através do estudo exploratório será apresentado os setores em que a tecnologia poderá ser aplicada.

Por fim será demonstrado um exemplo de código desenvolvido com a finalidade de aproveitar os benefícios da tecnologia com a base no conceito das licitações públicas.

2. REFERENCIAL TEÓRICO

No referencial teórico apresenta-se o conteúdo base do trabalho, como o conceito de blockchain, o que são contratos inteligentes e para que eles são usados, e também uma breve descrição da linguagem Solidity, utilizada para programação desses contratos.

2.1. BLOCKCHAIN

De acordo com Andoni et al. (2019), o blockchain é uma estrutura de dados digital que possui uma base de dados distribuída e compartilhada, e as transações são mantidas através de um arquivo similar a um log, em ordem cronológica.

As transações são chamadas de blocos e representam um compilado de várias transações. Eles possuem registros de data e hora e são criptograficamente vinculados aos blocos anteriores, gerando dessa forma uma cadeia de registros, que determina o blockchain.

No modelo de dados tradicional, existe um servidor ou unidade centralizadora, que faz o intermédio entre as partes envolvidas e o armazenamento das informações e transações. A desvantagem desse modelo se dá no caso dessa unidade falhar, o que tornaria todos os demais serviços inacessíveis de acordo com Armbrust (2010).

Já no blockchain, não existe a necessidade desse intermediário, pois todos os pontos presentes na rede possuem a cópia de todos os dados, e todos os usuários trabalham para conferir se as transações estão íntegras e são reais, conforme Andoni et al. (2019), aumentando a transparência da rede.

Um comparativo entre os dois tipos de redes é apresentado na Figura 1, onde na direita temos uma rede tradicional, e na esquerda, uma rede distribuída.

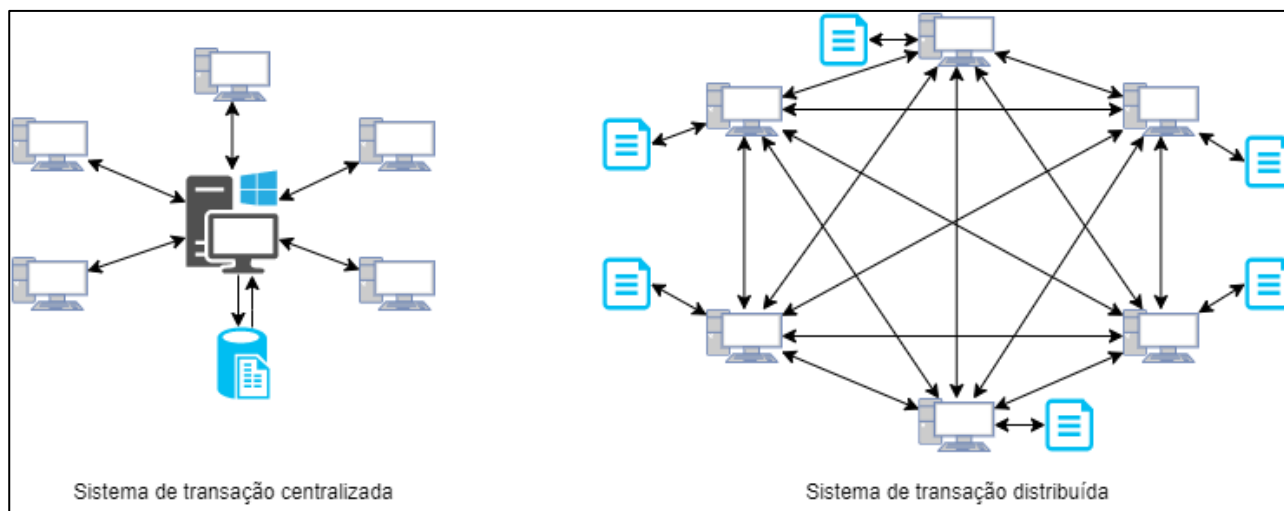


Figura 1: Comparativo entre uma transação tradicional e uma em rede distribuída.

Fonte: Elaborado pelo autor com base em Andoni et al. (2019).

Como o blockchain é totalmente digital, um de seus desafios é que os dados não sejam duplicados, pois sua transmissão de dados é o equivalente a copiar as informações de um local para outro. (Andoni, et al.,2019).

Já as transações blockchain são executadas conforme representadas na Figura 2: os usuários executam uma transação que é incluída em um bloco, tendo sua identidade confirmada pelos nós da rede, o bloco é adicionado a cadeia de blocos antes da transação ser confirmada e executada.

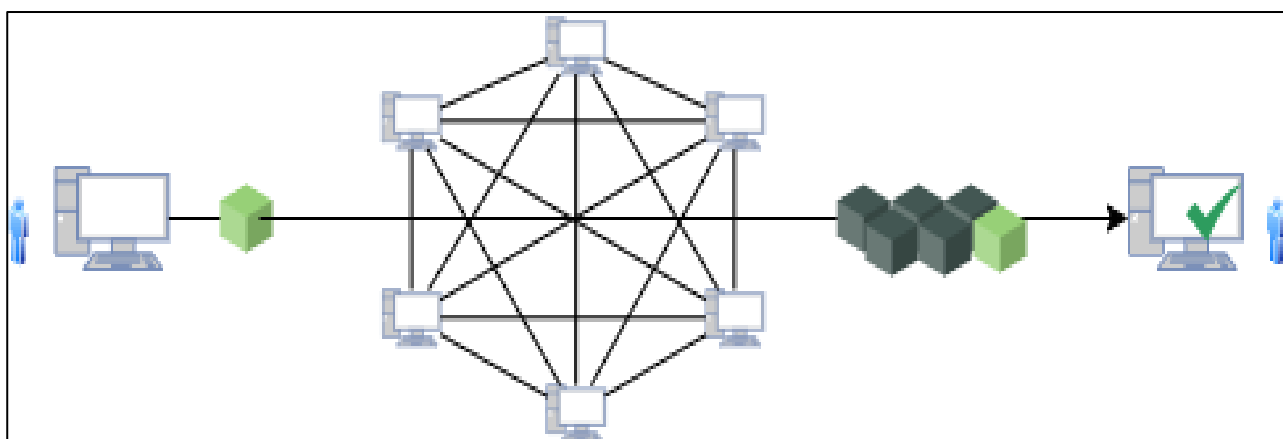


Figura 2: Execução de uma transação em blockchain

Fonte: Elaborado pelo autor com base em Andoni et al. (2019).

Um detalhe é que nas redes blockchain é necessário que ao menos 51% da rede seja considerada confiável, pois são os próprios membros que comparam as versões do

histórico de transações, e que algumas outras funções responsáveis pela segurança da rede são: funções hash e a criptografia de chave pública assimétrica (Andoni et al., 2019).

As funções hash são funções matemáticas que fazem a conversão de uma entrada para um tamanho específico, sendo usadas para verificar se os dados são idênticos, já que a adição de um simples caractere como um “espaço”, alteraria o hash.

A criptografia de chave pública funciona conforme demonstrado na Figura 3, onde cada usuário possui 2 chaves criptográficas, sendo 1 secreta e uma pública que é compartilhada com outros usuários através da rede, essas chaves se relacionam também de forma matemática sendo que somente a chave pública pode descriptografar as informações que foram encriptadas com a chave privada.

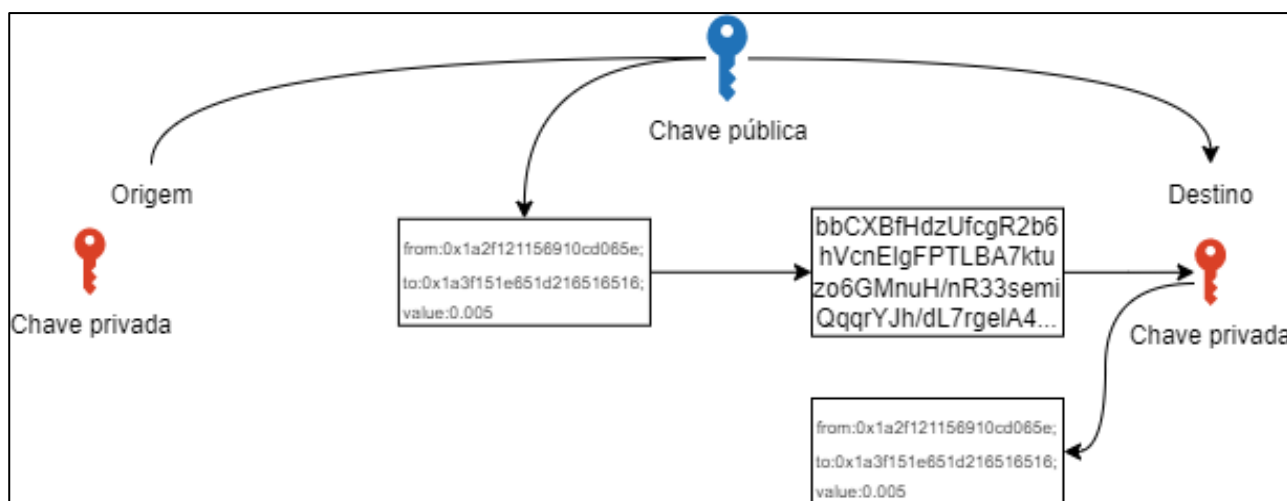


Figura 3: Funcionamento da criptografia de chave pública.

Fonte: Elaborado pelo autor com base em Sakurai, 2020.

Walport (2016) também cita que outra grande vantagem das redes blockchain é que elas podem ser combinadas com contratos inteligentes, que além de serem invioláveis, podem ter regras definidas pelos usuários com condições a serem executadas caso alguma ação pré-programada aconteça.

Uma das aplicações mais conhecidas implementada em blockchain sendo também a pioneira, é o Bitcoin, criado por Satoshi Nakamoto (2008). Já a primeira aplicação blockchain baseada em contratos inteligentes é a Ethereum, implementada por Vitalik Buterin (2013).

O Bitcoin é uma moeda digital que permite a realização de pagamentos eletrônicos e as moedas são mineradas conforme as transações vão sendo realizadas, fazendo com que sejam finitas na rede. Esse dinheiro virtual não é controlado por nenhum banco central e cada usuário possui uma carteira digital onde as moedas são armazenadas, sendo que ela só pode ser acessada pela chave privada do usuário e seu endereço é derivado de sua chave pública, de forma a promover o anonimato na rede.

Já o Ethereum, por permitir a implementação de regras, permite que seus clientes criem aplicações que vão ser executados na arquitetura blockchain, segundo Peyrott (2017), de forma que os conceitos da aplicação possam ser construídos.

Mattila et al. (2016) menciona ainda que o termo blockchain caracteriza diversas arquiteturas, algoritmos e domínios que são construídos com base nesse sistema de cadeias de registros.

2.2. ARQUITETURA BLOCKCHAIN

Cada aplicação que será desenvolvida em blockchain possui um uso específico, e regras e operações próprias, sendo que algumas de suas características padrão são:

- Cada nó mantém uma cópia de todo histórico de transações;
- Cada nó da rede pode receber uma ou mais transações;
- Qualquer usuário pode se juntar a rede, e sair quando quiser;
- Os nós da rede são os responsáveis pela aprovação das modificações e distribuem para a rede essas informações;
- Existe um sistema de incentivos ou “punições” de forma a coibir alguns comportamentos, como por exemplo ganhar moedas ao realizar mais rápido as transações;
- Registros são permissão não são aceitos na rede;
- Um usuário não precisa necessariamente conhecer o outro.

Baliga (2017) menciona que não existe um consenso sobre quais transações podem ou não ser aceitas pelo sistema, mas que os algoritmos costumam barrar as transações que

apresentam falhas de nós, atrasos nas mensagens, mensagens corrompidas ou nós maliciosos ou não confiáveis identificados.

As arquiteturas são classificadas então em: híbridas, públicas e privadas. Uma arquitetura é híbrida quando trabalha com blocos públicos e privados, pública quando qualquer um pode ingressar na rede, como ocorre com o Bitcoin e privada quando tem um uso projetado específico e não é qualquer um que pode se juntar a rede e aprovar as transações, conforme demonstrado na Figura 4, onde na rede da esquerda todos os usuários participam do processo de validação das transações, enquanto na da direita somente participam alguns usuários selecionados.

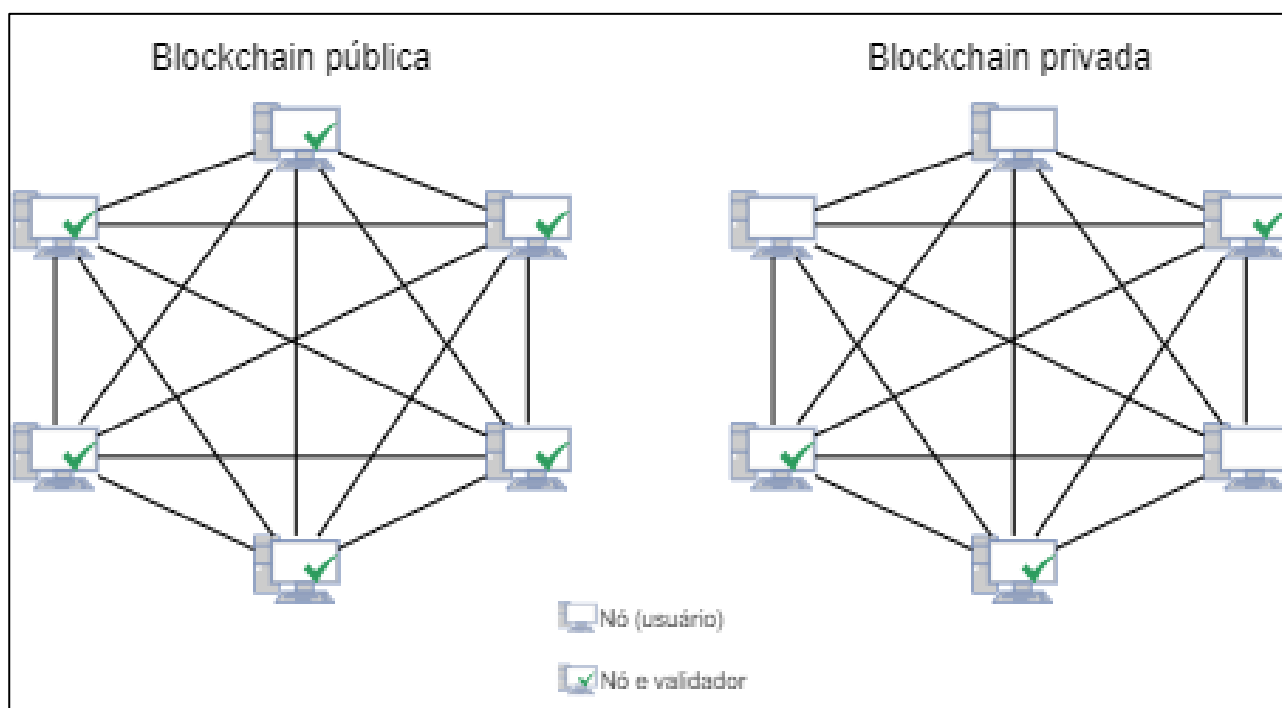


Figura 4: Verificação de transações por redes públicas e privadas.

Fonte: Elaborado pelo autor com base em Froystad, 2016.

2.3. CONTRATOS INTELIGENTES

Os contratos inteligentes, também conhecidos como *smart contracts*, funcionam como um mecanismo de controle descentralizado, e sua função é fazer o monitoramento constante de alguma atividade, ajustando os perfis e penalizando os consumidores que estiverem fora das regras e normas estipuladas.

Para isso, é necessário que a transação envolva duas ou mais partes do contrato e não precise de interferência humana ou externa, pois as regras estarão implementadas via linguagem de programação e serão executadas em algum dispositivo. Além das regras também se faz importante que sejam implementados benefícios, obrigações e penalidades, de forma que os contratos consigam tomar ações acertadas e com isso regular o nível da oferta e demanda de uma aplicação.

Eles foram introduzidos por Szabo (1994) em uma discussão em um site, como um protocolo de transação computadorizada que executa os termos de um contrato, fazendo a introdução das cláusulas contratuais em hardware ou software de forma que elas possam se auto aplicar e com isso, minimizar a quantidade de intermediários. A diferença entre eles e os do mundo real, é que são completamente digitais, Mattila et al. (2016) menciona que um contrato inteligente é um programa legível por máquina, escrito em um código que se executará quando um conjunto de atributos pré-definidos for atendido. Vale ressaltar que contratos inteligentes não precisam de inteligência artificial para funcionar, independentemente do que seu nome possa sugerir.

Dessa forma, seu funcionamento se dá com base em scripts que são armazenados em cadeia e possuem um endereço único, e para se adicionar um contrato inteligente a ela basta fazer o endereçamento da transação, sendo ele executado conforme o que já foi adicionado a transação, conforme Christidis e Devetsikiotis (2016).

Outro detalhe desses contratos é o mencionado por Porto et al. (2021), onde o mesmo não permite interrupção, reversão, suspensão, parada ou cessação, reforçando por si só o cumprimento das obrigações acordadas.

Coutinho et al. (2020) menciona que existem diferentes plataformas onde esses contratos podem ser desenvolvidos e executados, sendo a mais utilizada a Ethereum.

2.4. SOLIDITY

A linguagem Solidity foi criada para o desenvolvimento de contratos inteligentes, sendo orientada a contratos e de alto nível, segundo Ribeiro e Mendizabal (2021). Ela possui elementos e tipos parecidos com o C++ e o Javascript, e algumas de suas características

são: tipagem estática conforme demonstrado na Tabela 1, compilada para o formato EVM-Bytecode e suporte a herança múltipla e tipos complexos.

Tipo	Palavra-chave	Descrição
Booleanos	bool	Tipos booleanos, seu valor pode ser true ou false.
Inteiros	int, int8...int256	Números inteiros declarando o tamanho em bits em intervalos de 8 (de 8 até 256 bits). A palavra-chave int é um alias para int256.
Bytes, string	bytes, bytes1...bytes32 / string	Sequência de bytes de tamanho dinâmico.
Endereço	address	Variável que armazena o valor de um endereço Ethereum de tamanho 20 bytes

Tabela 1: Principais tipos de variáveis da linguagem Solidity.

Fonte: Ribeiro e Mendizabal (2021).

De acordo com Ribeiro e Mendizabal (2021) Solidity foi desenhado para se comunicar com aplicações desenvolvidas em Javascript. Devemos pensar na linguagem como um pouco mais complexa que **SQL**, onde estabelecemos condições aos dados e os armazenamos em um banco de dados caso as condições sejam atingidas. A diferença é que o banco de dados é a própria Blockchain, por isso não há funções de output como *printf*, *echo* ou *alert*, sendo assim uma alternativa para isso é criarmos funções **Getters** que serão utilizadas apenas para leitura, não gravando transação alguma. E para indicar à linguagem que a função é de apenas leitura é utilizada a palavra reservada **view**. Exemplo de um Hello World na Figura 5.

```
○ ○ ○  
  
// SPDX-License-Identifier: UNLICENSED  
  
pragma solidity ^0.8.17;  
  
contract HelloWorld {  
    string private message = "Hello world";  
  
    function getMessage() public view returns (string memory) {  
        return message;  
    }  
  
}
```

Figura 5: Hello Word em Solidity.

3. BLOCKCHAIN NO SETOR PÚBLICO BRASILEIRO

De acordo com Porto et al. (2021), as possibilidades de tratativas no universo digital ganharam novas formas de atuação, inclusive com o uso dos contratos inteligentes, que podem ser caracterizados como um contrato construído em uma plataforma digital e descentralizada, porém com alta segurança na execução das transações que forem ali combinadas.

Com base nisso ele pode ser utilizado para as mais diversas finalidades, incluindo o setor público que pode tirar proveito da tecnologia para comprovação de documentos, sistemas de voto, gerenciamento de marcas e patentes e demais propriedades intelectuais.

Assim, de acordo com Ribeiro e Mendizabal (2021), as aplicações blockchain são categorizadas por entusiastas em 4 versões, sendo:

- Blockchain 1.0: primeira versão e origem das blockchains, sendo categorizado pelas aplicações baseadas em criptomoedas e criptoativos, com destaque para o Bitcoin;
- Blockchain 2.0: criação dos contratos inteligentes e códigos que permitem a criação de outras aplicações além das criptomoedas;

- Blockchain 3.0: criação de outras aplicações descentralizadas que em geral tem sua execução em blockchain, mas uma interface amigável para interação com os usuários. Criação do algoritmo DAG (*Directed Acyclic Graphs*) para empilhamento de transações;
- Blockchain 4.0: evolução da versão 3.0 para a “Indústria 4.0”, com várias aplicações híbridas em uma rede blockchain responsável por registrar as transações de uma empresa, atuando de forma complementar a sistemas automatizados.

3.1. CARTÓRIOS COMPROVAÇÃO DE DOCUMENTOS

Uma das funções dos cartórios é, entre outras, o armazenamento de documentos, que acaba se tornando um problema com o passar do tempo, devido ao volume de dados físicos armazenados, poeira, traças, baratas e a própria questão de conservação do documento em si, sem falar em acidentes naturais como inundações e incêndios.

Com o uso de uma rede descentralizada como o blockchain, por mais que um dos nós fosse comprometido, os demais continuariam tendo a cópia do documento, mantendo sua integridade e autenticidade. Além disso, Ribeiro e Mendizabal (2021) também mencionam a questão da verificação das informações adicionadas por mais de 50% da rede, o que significa que um criminoso ou indivíduo mal intencionado teria que ter uma capacidade computacional maior que toda a rede para conseguir corromper os demais nós.

Esse fator é especialmente importante quando se trata de aplicações que exigem que os dados não possam ser alterados, como o caso da autenticidade de documentos públicos e privados, serviço garantido e desempenhado pelos cartórios e registros, conforme demonstrado na Tabela 2.

Serviço	Exemplos de Documentos
Tabelionato de Notas	Escrituras, Procuраções e outros.
Registro de Contratos Marítimos	Transações de Embarcações Marítimas.
Protesto de Títulos	Inadimplência e Descumprimento da Obrigação
Registro de Imóveis	Situação e Titularidade de Imóveis
Títulos de Pessoa Jurídica	Registro de Entidades e outros
Registro Civil das Pessoas Naturais	Nascimentos, Casamentos, Óbitos e outros
Registro de Distribuição	Centro de Informações Judiciais

Tabela 2: Serviços de um Cartório Segundo a Legislação Brasileira.

Fonte: Ribeiro e Mendizabal (2021).

O blockchain parece uma alternativa promissora para resolver os problemas citados no início, como a questão do armazenamento, cuidado e preservação dos documentos, porém, por a tecnologia ser recente ainda há muitos embates sendo travados entre o governo, cartórios e profissionais, de acordo com Ribeiro e Mendizabal (2021).

Com base nesses fatores, é provável que os cartórios passem, pouco a pouco, a adotar a tecnologia blockchain. No Brasil, inclusive, já existem alguns projetos sobre esse tema, conforme demonstrado na Tabela 3.

Projeto	Website
OriginalMy	originalmy.com
STAMPD	stampd.io
Blockusign	blockusign.co
Blocknotary	blocknotary.com
OriginStamp	originstamp.org/home

Tabela 3: Projetos que Exploram os Registros de Documentos por Blockchain.

Fonte: Ribeiro e Mendizabal (2021).

Um dos produtos do OriginalMy é o OMySign¹ que, através da Lei nº 14.063, permite que contratos sejam assinados através de assinaturas eletrônicas avançadas e certificados digitalmente através da emissão de certificados pela ICP-Brasil ou outro meio capaz de autenticar a autoria e integridade dos documentos. Assim, não existe mais um limite territorial na assinatura de contratos e as transações são verificadas por redes blockchain. A empresa também oferece outros serviços como uma identidade digital baseada em blockchain e uma API para integração com outros sistemas.

O Blocknotary² possui 3 produtos, sendo: entrevistas remotas com autenticação de usuário por blockchain, assinatura de documentos virtuais e habilitação de notas em jornal eletrônico. A aplicação foi reconhecida em Vermont, USA como uma tecnologia capaz de autenticar documentos com segurança.

3.2. SISTEMAS DE VOTAÇÃO

As urnas eletrônicas foram criadas em 1995 e passaram a ser utilizadas a partir de 1996, sendo também utilizadas em 32 outros países até o presente momento, porém, ainda existe muito debate acerca de sua real segurança e da dificuldade de saber se o voto foi realmente contabilizado para o candidato escolhido.

Conforme Ribeiro e Mendizabal (2021), em 2017 uma equipe de segurança da informação da UNICAMP realizou uma série de testes nas urnas e descobriu várias falhas, sendo capaz de alterar a mensagem para o usuário após registro do voto e também no desvio de votos.

Espera-se então que utilizando o blockchain a população tenha uma maior confiança no processo de votação democrática do país, e como projetos nesse quesito existem o Agora e WaveVote.

O WaveVote³ é baseado na rede Ethereum e inspirado no projeto Stonecoldpat⁴, seu funcionamento é descrito no fluxograma da Figura 6. Dessa maneira, primeiramente é feito o registro do usuário na aplicação através do envio de suas chaves públicas. quando essa chave for aceita pela rede é feito seu registro na rede e o usuário pode escolher seu voto.

¹<https://originalmy.com/omysign>

²<https://www.blocknotary.com/>

³<https://github.com/descampsk/wavevote>

⁴<https://github.com/stonecoldpat/>

A aplicação então envia os votos nulos para a rede, para que a aplicação calcule qual candidato foi escolhido e por fim faz a contagem dos votos.

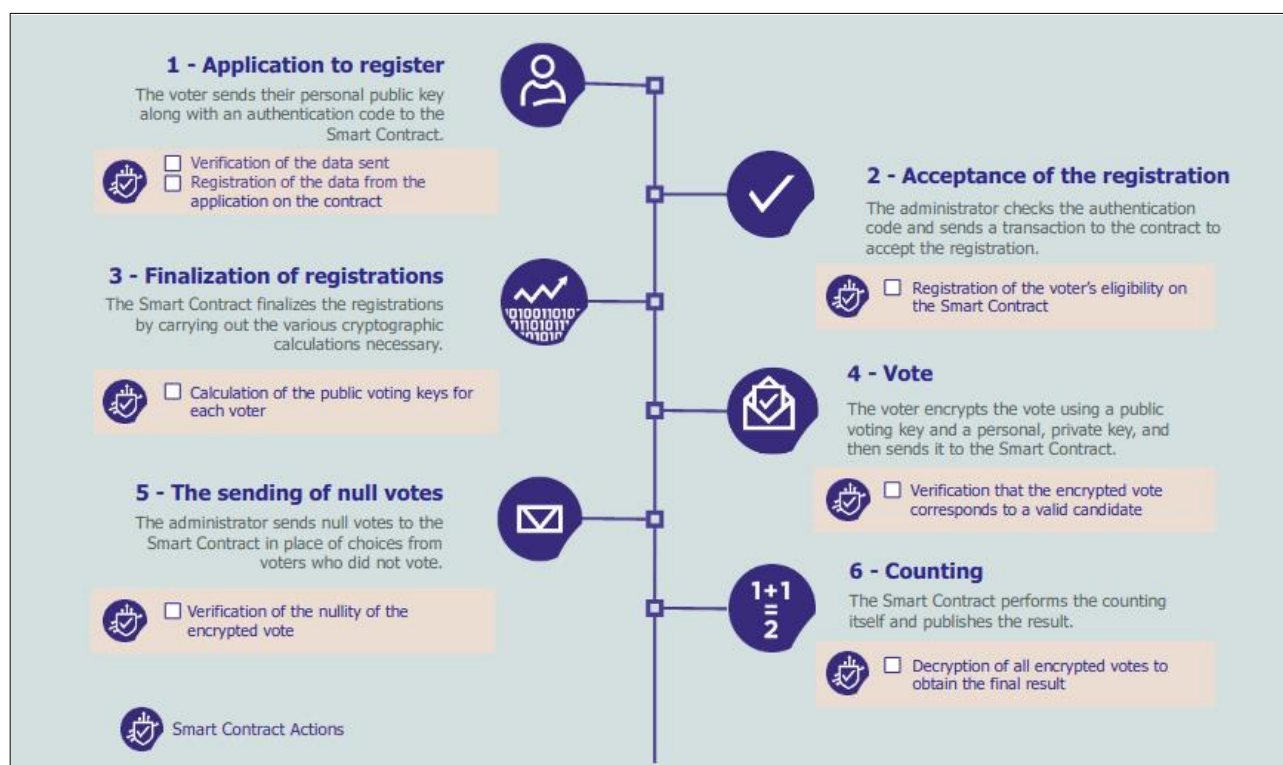


Figura 6: Fluxograma do WaveVote.

Fonte: Neimi e Mai, 2018.

O Agora⁵ é um sistema similar, permitindo a votação através de aplicativos, protocolos ou verificação de cadeia de suprimentos (*supply chain tracking system*) e sua proposta é:

- Possuir um ecossistema central com forte criptografia e uma rede distribuída para que os dados sejam protegidos contra intervenção;
- Transparência em todo processo de votação e o resultado é obtido logo após sua finalização;
- A escolha de cada candidato permanece oculta;
- O processo de votação se torna mais simples, já que pode ser feito de qualquer lugar, não precisando mais ir necessariamente até uma central de votação;
- Redução de custos com a diminuição de equipamentos físicos e pessoas para sua manutenção e operação;

⁵<https://www.agora.vote/>

- Eliminação de violência e desconfiança, já que os resultados podem ser apurados e são totalmente confiáveis.

3.3. DADOS PÚBLICOS

Um dos principais usos das redes blockchain poderia ser o armazenamento de dados públicos, pois a falsificação de documentos é algo que ainda se faz presente na sociedade. Com base nisso, essas redes poderiam evitar a fraude de documentos como CPF, carteira de habilitação, registros de posse de terras, entre outros, segundo Ribeiro e Mendizabal (2021), pois sendo salvos em uma Blockchain, a possibilidade de alteração de um dado exige uma capacidade computacional muito alta, o que hoje só pode ser alcançada por computadores quânticos.

Outro uso poderia ser na transparência e auditoria de dados do governo, permitindo que qualquer cidadão possa acessá-los, evitando a corrupção. Embora várias secretarias e estados tenham já um portal da transparência, nem sempre é uma tarefa fácil visualizar as informações ou ter a certeza de que realmente representam a realidade.

3.4. LICITAÇÕES

Segundo o Portal da Transparência da Controladoria-Geral da União⁶, a licitação é o processo por meio do qual a Administração Pública contrata obras, serviços, compras e alienações. Em outras palavras, licitação é a forma como a Administração Pública pode comprar e vender. Já o contrato é o ajuste entre órgãos ou entidades da Administração Pública e particulares, em que há um acordo para a formação de vínculo e a estipulação de obrigações recíprocas.

⁶ <https://www.portaltransparencia.gov.br/>

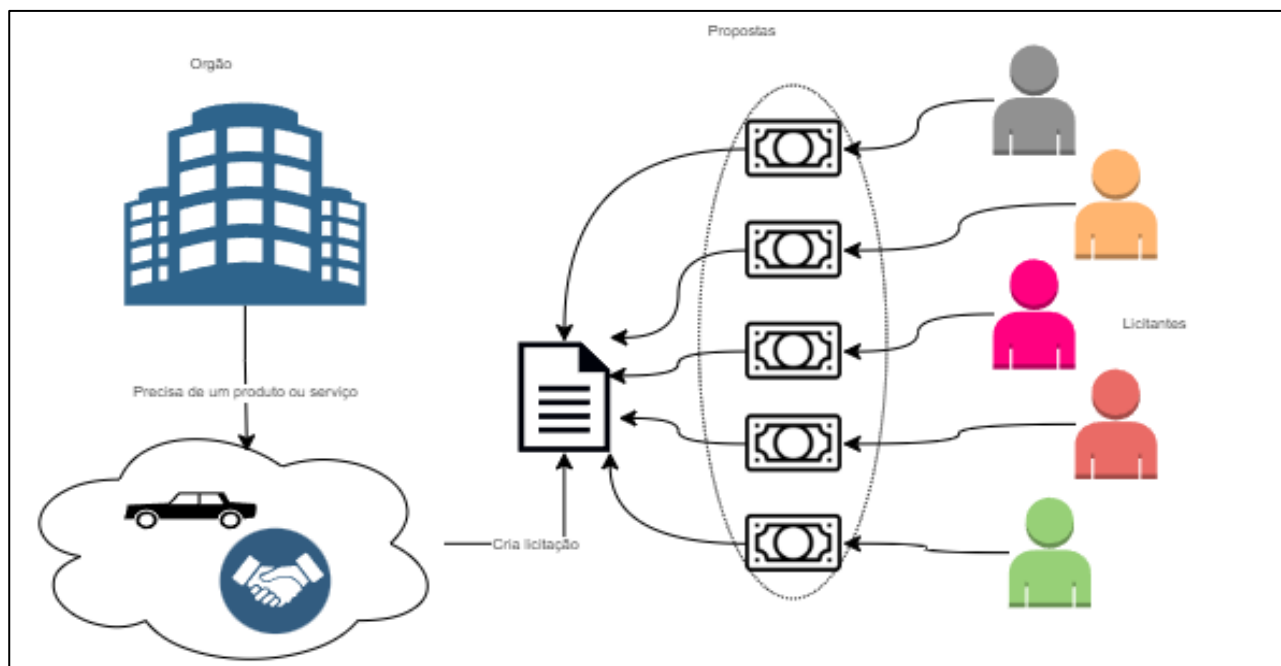


Figura 7: Processo licitatório simplificado.

Por ser um ato público, a licitação nunca deverá ser sigilosa. O público deve ter acesso aos procedimentos referentes a uma licitação, salvo quanto ao conteúdo das propostas, que só pode ser conhecido por ocasião da respectiva abertura (SOUZA, 1997).

O processo de licitação deve afastar qualquer suspeita de favorecimento e garantir que o dinheiro público seja utilizado com cautela e eficiência. A licitação é a forma mais clara de se atender aos princípios das atividades da Administração Pública (SOUZA, 1997).

Segundo Biancolini et al. (2018) o blockchain reduzirá o problema com o atraso de pagamentos pelo Orgão contratante, pois a partir do momento em que se destacar no orçamento a verba necessária para o contrato, todo o processo de pagamento poderá ser automatizado por meio dos *smart contracts*, garantindo que aquele numerário apenas seja utilizado no momento da entrega de determinado produto ou serviço.

Tal situação permite que o gestor não possa desviar tais recursos para outra finalidade, pois não poderá alterar a programação existente no Blockchain. Lembrando, ainda, que todas essas operações terão garantida uma transparência muito maior e em tempo real, facilitando fiscalização da própria Administração, órgãos de controle como Tribunais de Contas e da própria população, de acordo com Biancolini et al. (2018).

A redução de custos, capacidade de reduzir o tempo e disponibilidade das informações e gastos são valores importantes para a inserção do sistema Blockchain no sistema licitatório brasileiro, além de tornar as chances mais igualitárias, a transparência seria total.

3.5. PROPRIEDADE INTELECTUAL, MARCAS E PATENTES

Atualmente no Brasil, o processo de registro de marcas e patentes demora entre 1 e 1,5 anos, seguindo o passo a passo detalhado no fluxo da Figura 7, além dos custos a serem pagos em cada etapa.

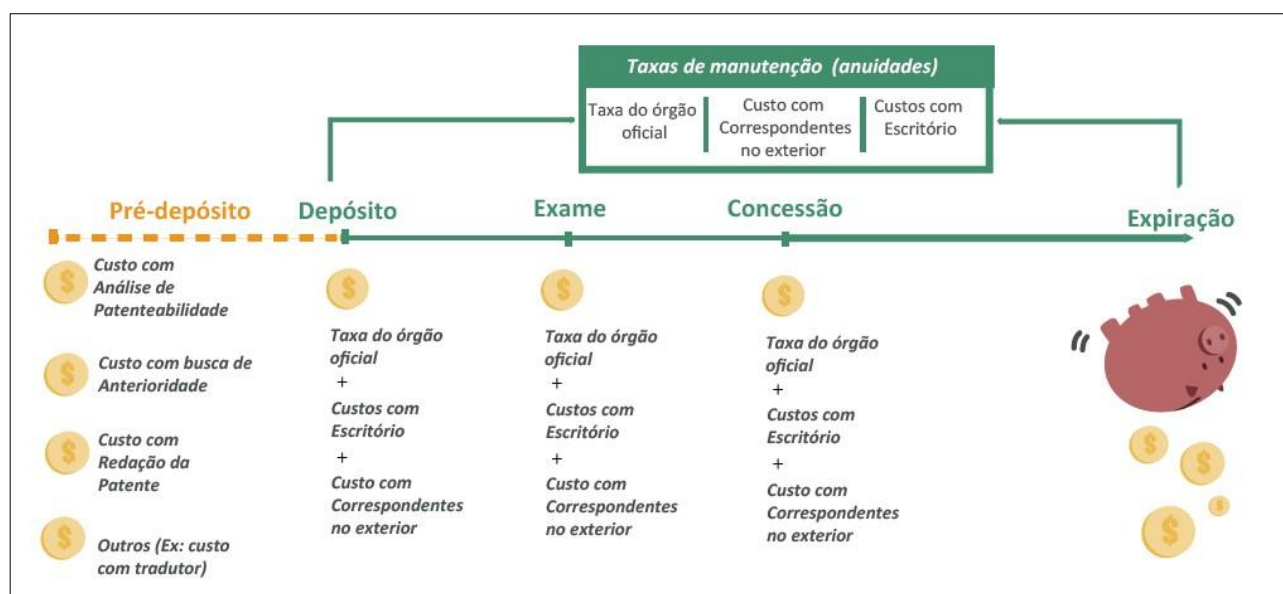


Figura 8: Fluxograma do registro de marca e patente no Brasil.

Fonte: Couto, 2022.

Esse registro é regulado pela Lei nº 9.610 que define as regras para o registro de marcas e patentes, englobando diversos itens da propriedade intelectual, como: obras textuais, software e aplicativos, composições musicais, ilustrações, fotografias, logos, desenhos, entre outros.

Assim, similar ao uso do blockchain para identificação de documentos, o mesmo também pode ser usado para propriedade intelectual, pois permite que todos os envolvidos tenham acesso ao que já está na rede, já em contrapartida, seria necessário a criação de um conjunto de normas acordadas internacionalmente, segundo WIPO (2020).

Outra vantagem seria a redução do tempo e custo para o processo, pois ao menos 51% da rede deveria concordar que aquele registro não apenas é válido, mas também não está vinculado a outro portador, o que seria mais ágil já que todas as informações estariam no mesmo local, e não haveria necessidade de se consultar diversas bases de dados, ou fazer buscas internacionais.

Um exemplo desse tipo de registro que já vem ocorrendo é o NFT, ou seja, um token não fungível, único e exclusivo que não pode ser copiado ou fraudado, de acordo com Conegundes e Calazans (2022). Ele é então caracterizado por ser um título digital transacionado através de redes blockchain, que asseguram sua autenticidade e unicidade.

A empresa IPwe já possui uma rede blockchain que armazena cerca de 80% da quantidade de patentes existentes e faz o licenciamento de outros serviços financeiros por meio de NFTs, com isso, o processo de valorização dos ativos poderia ser feito pelo mercado.

3.6. GESTÃO DE SAÚDE

Como pode ser observado durante a pandemia do Covid-19, a gestão da saúde é de grande interesse do setor público, de forma a se poder controlar surtos de forma ágil e eficaz e direcionar os atendimentos para os locais com maior necessidade, além de permitir que os dados de um usuário sejam acessados por toda a rede, sem necessidade de cadastros adicionais, o que apenas dificulta o atendimento.

Isso ocorre porque cada local utiliza sistemas diferentes, que muitas vezes não se conectam nem mesmo dentro do próprio centro de atendimento, porém, com o uso de uma rede blockchain todo o histórico de atendimentos e dados pessoais podem ficar disponíveis na mesma rede, podendo ser acessados por qualquer nó ligado à saúde.

Isso proporcionaria, dentre outros, alguns dos seguintes benefícios:

- Agilidade no atendimento e processamento de dados dos pacientes;
- Redução de erros humanos provocados por adição de dados errados ou duplicados;
- Maior controle sobre a distribuição de medicamentos e médicos.

Conforme Ribeiro e Mendizabal (2021), alguns dos projetos nessa área são: MedRec, MedicalChain, Pokitdok e GUARDTIME. O MedRec, sendo que alguns dos projetos estão sendo mantidos por grandes instituições como a Microsoft, MIT e IBM.

3.7. OUTROS

Além das aplicações mencionadas, existem diversas pesquisas em outros setores que também almejam tirar proveito dos benefícios oferecidos pelo blockchain, como, por exemplo, setor de consumo de energia, indústrias farmacêuticas e de alimentos, transporte urbano e gestão da saúde.

No consumo de energia, a implementação de uma rede blockchain poderia controlar picos de gastos, “penalizando” o consumidor por isso (com preços mais altos por exemplo), ou também permitir que uma fábrica compre créditos de emissão de carbono de outros países com consumo mais baixo, permitindo assim que a emissão dos gases fique em um nível abaixo do recomendado. Na Tabela 4 é apresentado alguns projetos em países que já estão sendo implementados, sendo que no Brasil tem-se as empresas GREENCHAIN, Enercred e FOHAT que estão trabalhando em projetos similares, conforme Ribeiro e Mendizabal (2021).

Projeto	Atividades	Plataforma	Região
Alliander	Troca de energia descentralizada	Ethereum	Países Baixos
Assetron Energy	Criptoativos e Investimentos	Waves	Austrália
CarbonX	Certificados e Créditos de Carbono	Etehereum	Canadá
Tennet & Sonnen	Gerencimanto de Redes (Grid)	Hyperledger Fabric	Países Baixos

Tabela 4: Projetos que o blockchain na rede elétrica.

Fonte: Ribeiro e Mendizabal (2021).

Atualmente, o país mais avançado na implementação do blockchain no setor público é a Estônia, de acordo com Ribeiro e Mendizabal (2021), onde estão procurando automatizar todos os serviços públicos através da adoção do e-Estonia. Outros países que já vem anunciando que também adotarão a tecnologia são: Singapura, China, Emirados Árabes, Japão e Canadá, conforme Ribeiro e Mendizabal (2021).

4. IMPLEMENTAÇÃO DE UM CONTRATO INTELIGENTE

Será tomado o tópico de licitações mencionado anteriormente para exemplificar o processo de desenvolvimento de um contrato inteligente.

O contrato seguirá um padrão de como funciona uma licitação pública, de forma mais clara com uma demonstração simples, não entraremos no âmbito da legislação brasileira e somente serão seguidos os passos para se licitar um objeto, seja produto ou serviço, para que seja de fácil entendimento à um cidadão comum.

Para isso, serão utilizadas algumas ferramentas para auxiliar e facilitar o processo do uso da blockchain na rede de testes pública Goerli⁷ com a API Infura⁸ que fará o trabalho de um nó, a comunicação em javascript se dará com a biblioteca Web3.js⁹ e utilizando uma carteira MetaMask¹⁰, uma carteira criada com o objetivo de armazenar os criptoativos de quem a possui e interagir com a rede Ethereum e toda transação efetuada utilização os ativos existentes na carteira.

A exibição dos códigos do smart contract desenvolvido se dará por meio da IDE Remix¹¹ com a versão do Solidity mais atual até o presente momento, e por mais que os testes possam ser realizados pelo próprio Remix, será utilizada uma interface para melhor exibição das informações.

Todo o código de implementação que está sendo apresentado na sequencia deste trabalho podem ser consultados no repositório do Github¹², em <https://github.com/viniciuspdionizio/brasilchain>, de forma a servir como base de estudos e contribuição.

⁷ <https://goerli.net/>

⁸ <https://infura.io/>

⁹ <https://web3js.readthedocs.io/>

¹⁰ <https://metamask.io/>

¹¹ <https://remix.ethereum.org/>

¹² <https://github.com/>

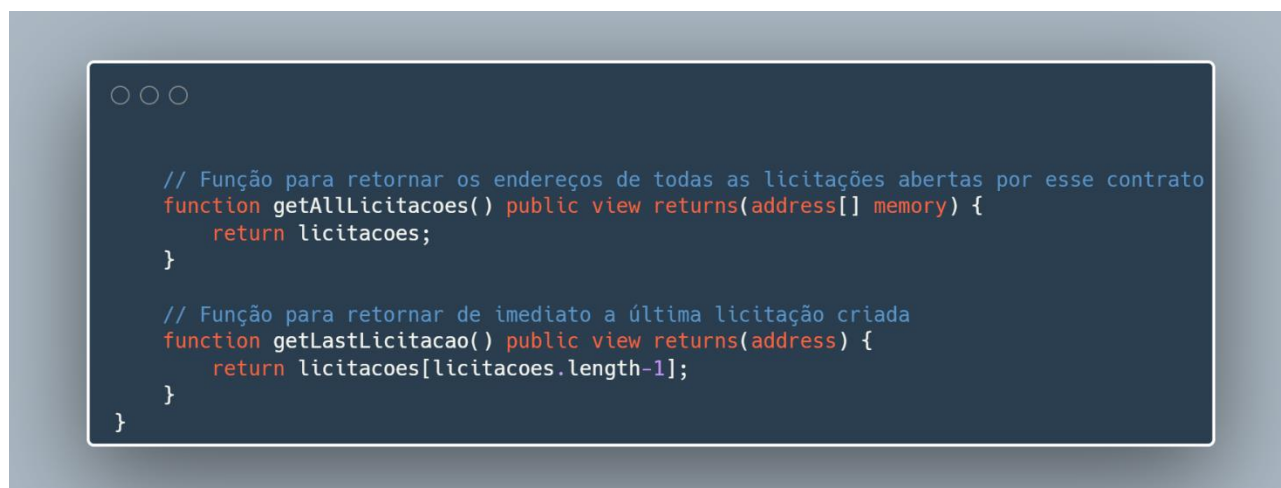
O contrato publicado será o **LicitacaoFactory**, *smart contract* com o objetivo de armazenar todos os contratos abertos pela mesma e proteção do *smart contract* **Licitacao**, pois assim o código fonte do contrato será inalterável.

O contrato **LicitacaoFactory** não necessita de informações informadas previamente, por este motivo a implementação de um construtor não é necessária, a única função que se faz necessário o consumo computacional, inserindo novos dados na Blockchain é a **abrirLicitacao**, que cria um novo registro do contrato **Licitacao**, onde os dados informados na chamada da função são repassados ao construtor do contrato, conforme mostrado na Figura 9.

```
○○○  
  
// SPDX-License-Identifier: UNLICENSED  
  
pragma solidity ^0.8.17;  
  
// Estrutura para descrever cada item requerido na licitação  
// Declarada fora da declaração dos contratos pois é utilizada pelos dois  
struct Item {  
    // Descrição do produto/servico  
    string descricao;  
    // Complemento da descrição  
    string compl;  
    // Quantidade  
    uint16 quantidade;  
}  
  
// Declaração do contrato  
contract LicitacaoFactory {  
    // Todas as licitações abertas por esse contrato  
    address[] public licitacoes;  
  
    // Função para abrir uma nova licitação, informando os dados iniciais necessários  
    function abrirLicitacao(uint dataEntregaPropostas,  
        uint dataAberturaPropostas,  
        string memory identificacao,  
        string memory processo,  
        Item memory item) public {  
        Licitacao novaLicitacao = new Licitacao(msg.sender,  
            dataEntregaPropostas,  
            dataAberturaPropostas,  
            identificacao,  
            processo,  
            item);  
        licitacoes.push(address(novaLicitacao));  
    }  
}
```

Figura 9: Trecho de código Solidity declarando o contrato LicitacaoFactory.

Dessa forma, serão obtidos a qualquer momento o endereço de todas as licitações abertas por este *smart contract*, com as funções mostradas no código da Figura 10.

A screenshot of a code editor with a dark background and light text. The code is Solidity and defines two public view functions. The first function, getAllLicitacoes(), returns an array of addresses. The second function, getLastLicitacao(), returns the address of the last bid in the array. The code is as follows:

```
function getAllLicitacoes() public view returns(address[] memory) {
    return licitacoes;
}

function getLastLicitacao() public view returns(address) {
    return licitacoes[licitacoes.length-1];
}
```

Figura 10: Trecho de código Solidity com as funções de LicitacaoFactory.

As funções em que não há a palavra-chave **view** em sua chamada, em Blockchains públicas normalmente há uma taxa cobrada que é revertida para o nó que executou a função, pois há o custo computacional calculado, sendo assim, quanto mais execução uma função tiver, maior o custo.

As demais funções com a palavra-chave **view** são funções para obtenção de informações que não realizam alterações na base de dados e que não realizam transações, por este motivo não há gasto computacional a ser cobrado.

Um exemplo prático com uma interface para abrir uma nova licitação é demonstrada na Figura 10, onde é informado a data de entrega das propostas e a data de abertura das propostas respectivamente, e que são convertidas em *timestamp* pois a linguagem Solidity não armazena tipos de datas, e também os demais dados necessários e ao realizar a ação no botão Publicar a carteira MetaMask instalada como extensão do navegador se encarregará de mostrar ao usuário que sua conta será utilizada para realizar uma transação e um valor aproximado de quanto será a taxa, conforme mencionado anteriormente.

The image shows a web interface for creating a new bid (NOVA LICITAÇÃO) with a MetaMask notification overlay. The interface is divided into two main sections: a form for creating a new bid and a summary of the bid details.

Formulário de criação (NOVA LICITAÇÃO):

- Data de entrega das propostas:** 01/10/2022
- Data de abertura das propostas:** 23/10/2022
- Número da licitação:** 1234/2022
- Processo:** 0105
- Item:** Enxada (Cabo de madeira guatambú)
- Quantidade:** 10

Licitação nº 1234/2022 (Summary):

- Processo:** 0105
- Data de entrega das propostas:** 1664651400
- Data de abertura das propostas:** 1666552500
- Item:** Enxada
- Quantidade:** 10

MetaMask Notification Overlay:

- Novo endereço detectado!** Clique aqui para adicionar à sua agenda de endereços.
- URL:** http://localhost:3000
- Conta:** Account 1 (0x5cA...cCb6)
- Interação:** INTERAÇÃO COM CONTRATO
- Taxa de gás estimada:** 0.01522105 GoerliETH
- Taxa máxima:** 0.02535185 GoerliETH
- Site sugerido:** provavelmente em < 15 segundos
- Botões:** Cancelar, Publicar

Figura 11: Interface com dados de um novo contrato.

O contrato **Licitacao** publicado está disponível para qualquer pessoa através do endereço gerado, sendo assim qualquer usuário pode acessar os atributos e funções declaradas públicas, que estão declaradas na Figura 12.

```
○ ○ ○  
  
// Declaração do contrato  
contract Licitacao {  
    struct Licitante {  
        address endereco;  
        uint valor;  
    }  
  
    // Propostas foram abertas  
    bool public propostasAbertas;  
    // Data de publicação  
    uint public dataPublicacao;  
    // Data de inicio de entrega das propostas  
    uint public dataEntregaPropostas;  
    // Data da abertura das propostas  
    // Fechamento licitação  
    uint public dataAberturaPropostas;  
    // Orgão requerente da licitação  
    address public orgao;  
    // Número da licitação  
    string public identificacao;  
    // Número do processo  
    string public processo;  
    // Item requerido na licitação  
    Item public item;  
    // Array de licitantes que propuseram seus valores  
    Licitante[] public licitantes;  
    // Index do vencedor da licitação  
    // Utilizado pela função vencedor()  
    uint private vencedorIndex;
```

Figura 12: Trecho de código em Solidity declarando o contrato Licitacao.

As variáveis e funções públicas são de acesso a qualquer pessoa que faça a chamada, porém regras podem ser impostas para evitar os acessos maliciosos, algumas regras são explanadas nas funções do trecho mostrado nos trechos de código das figuras.

```

// Construtor chamado ao criar o contrato
// Dados necessarios informar ao criar:
// Orgão requerente, modalidade, número da licitação e quantidade de dias
constructor(address _orgao,
             uint _dataEntregaPropostas,
             uint _dataAberturaPropostas,
             string memory _identificacao,
             string memory _processo,
             Item memory _item
            ) {
    orgao = _orgao;
    identificacao = _identificacao;
    processo = _processo;
    dataAberturaPropostas = _dataAberturaPropostas;
    dataEntregaPropostas = _dataEntregaPropostas;
    item = _item;
    dataPublicacao = block.timestamp;
}

// Função para que os interessados possam fazer sua oferta
// Parâmetros: _valor = Valor proposto
function propor(uint _valor) public isAceitandoPropostas {
    Licitante storage lic = licitantes.push();
    lic.endereco = msg.sender;
    lic.valor = _valor;
    if (_valor < licitantes[vencedorIndex].valor) {
        vencedorIndex = licitantes.length - 1;
    }
}

// Função para encerrar a fase de propostas da licitacao e abrir
function abrirPropostas() public isManager {
    require(dataAberturaPropostas < block.timestamp, "Data de abertura das propostas publicado ainda
    nao chegou");
    propostasAbertas = true;
}

```

Figura 13: Trecho de código Solidity com as funções do contrato Licitacao.

Os modificadores utilizados pelas funções do contrato **Licitacao** são explicados na Figura 15, onde são executados testes e caso seja aprovado a execução é continuada, caso contrário o código já é encerrado, evitando maiores gastos de taxa de modo que não precise executar a função até o fim.

Por exemplo, para se obter o vencedor da licitação publicada, duas regras são impostas na função, a primeira pelo modificador **isFinished** que autoriza a continuação do código caso a licitação tenha sido finalizada e a segunda pela função da própria linguagem Solidity **require** que no teste demonstrado no código da Figura 14, exige que existam licitantes para o contrato, caso não haja licitante, tecnicamente não há vencedor.


```
function vencedor() public view isFinished returns(Licitante memory) {
    require(licitantes.length != 0, "Nao ha nenhum licitante para esta licitacao");
    return licitantes[vencedorIndex];
}

function getInfo() public view returns(uint, uint,
    uint, address,
    string memory, string memory,
    Item memory, uint, address) {
    return (dataPublicacao, dataEntregaPropostas,
        dataAberturaPropostas, orgao,
        identificacao, processo, item,
        licitantes.length, propostasAbertas ? vencedor().endereco : address(0));
}
```

Figura 14: Trecho de código Solidity com as funções do contrato Licitacao.

Apesar da função **vencedor** ser apenas uma **view** e não terá cobrança de taxa, o modificador **isFinished** ainda se faz necessário, visto que o vencedor só é garantido quando a licitação em si tenha sido finalizada.

Os modificadores também utilizam das funções **require** e caso não haja falhas, o código é continuado, os nomes dos modificadores são utilizados ao declarar uma função que seu uso se faz necessário.



```

// Modificadores que são feitos exigencias para o prosseguir com o código
// São utilizados na declaração de uma função

modifier isManager() {
    require(msg.sender == orgao, "Apenas o orgao requerente pode chamar essa funcao");
    _;
}

modifier hasNotStarted() {
    require(dataPublicacao == 0, "Licitacao ja foi publicada");
    _;
}

modifier isAceitandoPropostas {
    require(dataAberturaPropostas > block.timestamp
        && dataEntregaPropostas < block.timestamp
        && !propostasAbertas
        && dataPublicacao != 0, "Licitacao nao esta aceitando propostas");
    _;
}

// Verifica se a licitacao ja foi encerrada
modifier isFinished {
    require(dataAberturaPropostas < block.timestamp || propostasAbertas, "Abertura das propostas
ainda nao realizada");
    _;
}
}

```


Figura 15: Trecho de código Solidity com as funções do contrato Licitacao.

Os quatro modificadores escritos na Figura 15 são autodescritivos, e a função `require` aceita um segundo parâmetro do texto que é retornado caso o teste do primeiro parâmetro falhe, caso o teste não falhe, a linha seguinte com caractere sublinhado (`_`) indica que será onde será executado a continuação do código escrito na função que declarou o modificador.

Por fim, a interface de exibição dos dados do contrato, assim qualquer pessoa com acesso ao endereço do contrato pode realizar a consulta e uma interface própria, respeitando apenas os parâmetros obrigatórios ao enviar uma transação.

Todas as transações enviadas ao blockchain, em que algum valor em seu armazenamento será alterado, se faz necessário informar o endereço da conta que fará a alteração, ao contrário das funções de apenas leitura.

A Figura 16 mostra os dados obtidos pela função **getInfo()** do *smart contract* Licitacao, para que as informações possam ser manipuladas de forma mais intuitiva.



The screenshot displays a user interface for a bidding process. At the top, it shows the title "Licitação nº 1234/2022" in bold. Below this, several key dates and times are listed: "Publicado em: 23/10/2022, 16:11:48", "Entrega das propostas: 01/10/2022, 16:10:00", and "Abertura das propostas: 23/10/2022, 16:15:00". The interface also identifies the "Orgão solicitante" with a long alphanumeric string, the "Processo" number "0105", and the "Item" as "Enxada Cabo de madeira guatambú 10". A "Vencedor" field contains another alphanumeric string. At the bottom, there are three interactive elements: a button labeled "2 Proposta(s)", a "Proposta" button with a paper plane icon, and a large grey button labeled "Obter vencedor".

Figura 16: Interface de exibição dos dados de um contrato.

5. CONCLUSÕES E TRABALHOS FUTUROS

O setor público brasileiro é responsável pela implementação de várias políticas de bem comum, como a gestão da saúde, emissão e autenticação de documentos, processo democrático de votação e registros de marcas e patentes. Devido à grande demanda, muitas vezes ele não consegue ser tão eficiente quanto deveria, além de muitas vezes exigir altos custos.

Já o blockchain é uma rede distribuída que permite que todos os participantes, ou nós da rede, tenham as mesmas informações, e para que essas sejam inseridas na rede é necessário que sejam aceitas por mais de 50% dos nós, garantindo assim que a informação esteja correta e não possa ser alterada.

Com base nesses fatores, entende-se que o blockchain pode ser uma alternativa para aplicação no setor público, permitindo uma maior confiança nos serviços prestados, redução de custos e uma melhor confiabilidade nos mesmos.

Para isso, foram apresentados alguns exemplos de uso do blockchain em sistemas de votação, autenticação de dados públicos, registro de marcas e patentes, saúde pública, entre outros, além de um exemplo mais prático no sistema de licitações. Mencionando projetos que já estão sendo desenvolvidos nesses setores não apenas no Brasil, mas também em outros países.

Sendo assim, pode-se concluir que essa tecnologia, embora recente se comparada com as demais, representa um grande benefício na otimização dos serviços públicos e deve ser cada vez mais utilizada ao longo dos anos.

Em trabalhos futuros é esperado que seja explorado com maior profundidade as soluções que outros países estão buscando com base no blockchain, suas vantagens e desafios de implementação, assim como o próprio Brasil busca avançar na tecnologia e já está em passos adiantados, segundo o próprio Tribunal de Contas da União¹³ (TCU), em maio de 2022 foi lançada a rede Blockchain Brasil, e segundo sua publicação¹⁴, a vantagem da Rede Blockchain Brasil é a possibilidade de tornar o governo federal hiper conectado. Segundo o secretário de Fiscalização, Integridade de Atos, Pagamentos de Pessoal e de

¹³ <https://portal.tcu.gov.br/inicio/>

¹⁴ <https://portal.tcu.gov.br/imprensa/noticias/tcu-e-bndes-lancam-rede-blockchain-brasil-e-definem-proximos-passos.htm>

Benefícios Sociais do TCU, Wesley Vaz, atuaria como uma camada comum e confiável para o compartilhamento de informações entre os atores do setor público.

REFERÊNCIAS

- ANDONI, Merlinda & ROBU, Valentin & FLYNN, David & ABRAM, Simone & GEACH, Dale & JENKINS, David & MCCALLUM, Peter & PEACOCK, Andrew. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. **Renewable and Sustainable Energy Reviews**. v.100, Fevereiro, 2019, p.143-174
- ARMBRUST, M & FOX, A & GRIFFITH, R, JOSEPH, AD & KATZ, R & KONWINSKI, A. **A view of cloud computing**. Commun ACM 2010;53(4):50–8.
- BADR, B.; HORROCKS, R.; WU, X. B.; **Blockchain By Example**. Birmingham: Packt Publishing Ltd, 2018.
- BALIGA, A. **Understanding blockchain consensus models**. Disponível em <<https://api.semanticscholar.org/CorpusID:36258295>>. Acesso em: 13 de junho de 2022.
- BIANCOLINI, A.; SILVA, F. C. D.; OSTI, J. R. **Como a tecnologia blockchain vem impactando, ou pode impactar, nas estruturas administrativas estatais**. Disponível em <http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2018/12/revista_esa_8_09.pdf>. Acesso em: 15 de abril de 2022.
- BUTERIN, V. **Ethereum white paper**. Ethereum. 2013.
- CHRISTIDIS, K. e DEVETSIKIOTIS, M. **Blockchains and smart contracts for the internet of things**. IEEE Access, 4:2292–2303. 2016.
- CONEGUNDES, Camila e CALAZANS, Guilherme. **Blockchain: uma solução possível para transações de patentes**. Disponível em <<https://www.daniel-ip.com/pt/artigos/blockchain-uma-solucao-possivel-para-transacoes-de-patentes/>>. Acesso em: 08 de julho de 2022.
- COUTINHO, Emanuel & MAIA, Delano & BRAGA, Wagner Bezerra & ABREU, Antonio. **Avaliando o Custo de Contratos Inteligentes em Aplicações Blockchain por meio de Ambientes de Simulação**. 10.5753/mssis.2020.12495.
- COUTO, Júlia. **Série Tipos de PI: Patentes**. Disponível em <<https://pris.com.br/blog/serie-tipos-de-propriedade-intelectual-patentes/>>. Acesso em: 2 de junho de 2022.
- CURY, M. E. **Blockchain: entenda o que é e quais são as principais aplicações**. Exame.com. Disponível em <<https://exame.com/tecnologia/blockchain-entenda-o-que-e-e-quais-sao-as-principais-aplicacoes>>. Acesso em: 12 de abril de 2022.
- FROYSTAD, P, Holm J. **Blockchain: powering the internet of value (White paper)**. Disponível em <<https://www.evry.com/globalassets/insight/bank2020/bank-2020-blockchain-powering-the-internet-of-value-whitepaper.pdf>>. Acesso em: 18 de junho de 2022.
- MATTILA, J & SEPPÄLÄ, T & NAUCLER, C & STAHL, R & TIKKANEN, M & BÅDENLID, A. **Industrial blockchain platforms: An exercise in use case development in the energy industry**. Disponível em <<https://www.etla.fi/julkaisut/industrial-blockchain-platforms-an-exercise-in-use-case-development-in-the-energy-industry/>>. Acesso em: 15 de junho de 2022.

NAKAMOTO, S. **Bitcoin: A peer-to-peer electronic cash system**. Disponível em <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 5 de junho de 2022.

NEIMI, Laurence AI & MAI, Nicolas. **Blockchain in practice what are the uses and limits of this new technology?** Disponível em <<https://www.wavestone.com/app/uploads/2018/04/blockchain-in-practice.pdf>>. Acesso em: 6 de junho de 2022.

PEYROTT, S. **An introduction to Ethereum and smart contracts: a programmable blockchain learn about verified. distributed computations in the cloud using Ethereum**. Disponível em <<https://auth0.com/blog/an-introduction-to-ethereum-and-smart-contracts-part-2>>. Acesso em: 22 de junho de 2022.

PORTO, Lucas Magno de Oliveira & GLÓRIA, Luciano Ribeiro Tambasco & BROCHADO, Mariah. **Contratos Inteligentes na Blockchain: Validade e Restrições**. Disponível em <<https://revistas.ufrj.br/index.php/rjur/article/download/44806/27459>>. Acesso em: 07 de julho de 2022.

RIBEIRO, Lucas e MENDIZABAL, Odorico. **Introdução à Blockchain e Contratos Inteligentes: Apostila para Iniciante**. Relatório Técnico INE 001/2021. Universidade Federal de Santa Catarina - Departamento de Informática e Estatística. 2021.

SAKURAI, Rafael G. **Criptografia de chave pública ou assimétrica**. Disponível em <<http://www.universidadejava.com.br/outros/criptografia-assimetrica/>>. Acesso em: 29 de abril de 2022.

SANTOS, J. P. **Governo federal oficializa uso de blockchain em documentos**. Disponível em <<https://investidor.estadao.com.br/criptomoedas/blockchain-governo-oficializa-uso-para-documentos>>. Acesso em: 20 de abril de 2022.

SOUZA, F. **Manual Básico de Licitação: Como agir diante de um procedimento licitatório**. Ed. 1. Nobel, 1997.

SZABO, N. **Smart Contracts**. Disponível em <<https://nakamotoinstitute.org/smart-contracts/>>. Acesso em: 20 de novembro de 2022.

TCU. **TCU e BNDES lançam Rede Blockchain Brasil e definem próximos passos**. Disponível em <<https://portal.tcu.gov.br/imprensa/noticias/tcu-e-bndes-lancam-rede-blockchain-brasil-e-definem-proximos-passos.htm>>. Acesso em: 12 de outubro de 2022.

TSE.JUS.BR. **Urna eletrônica 25 anos: lançado em 1996, equipamento é o protagonista da maior eleição informatizada do mundo**. Disponível em <<https://www.tse.jus.br/imprensa/noticias-tse/2021/Maio/urna-eletronica-25-anos-lancado-em-1996-equipamento-e-o-protagonista-da-maior-eleicao-informatizada-do-mundo>>. Acesso em: 12 de abril de 2022.

WALPORT, M. **Distributed ledger technology: beyond blockchain**. Disponível em <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>. Acesso em: 5 de junho de 2021.

WIPO. **Blockchain: Transformando o registro de direitos de PI e fortalecendo a proteção dos direitos de PI não registrada**. Disponível em <https://www.wipo.int/wipo_magazine_digital/pt/2020/article_0002.html>. Acesso em: 7 de junho de 2021.