ATEC - ÁREA DE ENGENHARIAS E TECNOLOGIAS
CIÊNCIA DA COMPUTAÇÃO
(BACHARELADO)

PROTÓTIPO DE SISTEMA BLOCKCHAIN PARA RASTREABILIDADE DA APLICAÇÃO DE DINHEIRO PÚBLICO NA ÁREA DA SAÚDE

WILLIAN BINDA

CHAPECÓ, JUNHO DE 2025

UNIVERSIDADE COMUNITÁRIA DA REGIÃO DE CHAPECÓ
ATEC - ÁREA DE ENGENHARIAS E TECNOLOGIAS
CURSO DE CIÊNCIA DA COMPUTAÇÃO
(BACHARELADO)

PROTÓTIPO DE SISTEMA BLOCKCHAIN PARA RASTREABILIDADE DA APLICAÇÃO DE DINHEIRO PÚBLICO NA ÁREA DA SAÚDE

Relatório Parcial do Trabalho de Conclusão de Curso submetido à Universidade Comunitária da Região de Chapecó para a disciplina de Ciência da Computação.

WILLIAN BINDA

Orientador: Prof. Radamés Pereira, M.Sc.

CHAPECÓ, JUNHO DE 2025

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ALGORITIMOS

LISTA DE SIGLAS

ACTs Acordos de Cooperação Técnica.

CGU Controladoria-Geral da União.

CIN Carteira de Identidade Nacional.

COFINS Contribuição para o Financiamento da Seguridade Social.

DAO Organização Autônoma Descentralizada.

DApps Aplicações Descentralizadas.

DREX Digital Real Eletrônico X.

Dnocs Departamento Nacional de Obras Contra as Secas.

EVM *Ethereum Virtual Machine*.

FCE Fundo de Compensação de Exportações.

FPE Fundo de Participação dos Estados.

FPM Fundo de Participação dos Municípios.

ICMS Imposto sobre Circulação de Mercadorias e Serviços.

INSS Instituto Nacional do Seguro Social.

IPI Imposto sobre Produtos Industrializados.

IPTU Imposto Predial e Territorial Urbano.

IPVA Imposto sobre a Propriedade de Veículos Automotores.

IR Imposto de Renda.

ISS Imposto sobre Serviços.

LAI Lei de Acesso à Informação.

LGPD Lei de Geral de Proteção de Dados.

MS Ministério da Saúde.

PBFT *Practical Byzantine Fault Tolerance*.

PIB Produto Interno Bruto.

PMEs Prontuários Médicos Eletrônicos.

PoS *Proof of Stake*.

SUS Sistema Único de Saúde.

SUMÁRIO

1 INTRODUÇÃO

A tecnologia *blockchain* (cadeia de blocos) tem se consolidado como uma ferramenta promissora para a transformação de diversos setores da sociedade, incluindo logística, meio ambiente, saúde e, especialmente, a administração pública. Sua estrutura descentralizada e imutável proporciona mecanismos eficazes para assegurar a integridade, rastreabilidade e transparência de dados e transações — características fundamentais para enfrentar desafios históricos, como a corrupção, a má gestão e a ineficiência na aplicação dos recursos públicos.

Apesar dos avanços institucionais em transparência, como o Portal da Transparência, a Lei de Acesso à Informação (LAI) e a Lei de Geral de Proteção de Dados (LGPD), ainda persistem obstáculos significativos no acesso da população às informações sobre a destinação e aplicação dos impostos arrecadados. Quando disponíveis, esses dados frequentemente estão fragmentados, desatualizados ou são apresentados de maneira pouco intuitiva, dificultando o exercício do controle social. Esse problema se torna ainda mais crítico em áreas sensíveis como a saúde, onde a ausência de mecanismos eficientes de rastreabilidade em tempo real favorece desvios de verbas, subutilização dos recursos e falta de responsabilização efetiva.

Diante desse contexto, este trabalho propõe o desenvolvimento de um protótipo de sistema *blockchain* com foco na rastreabilidade do dinheiro público aplicado na área da saúde. A solução utiliza *smart contracts* (contratos inteligentes) para registrar, de forma automatizada e imutável, o percurso do dinheiro desde sua arrecadação até sua destinação final, permitindo que qualquer cidadão ou órgão fiscalizador acompanhe essas transações em tempo real. Nesse cenário, o uso da *blockchain* representa não apenas uma inovação tecnológica, mas também uma proposta concreta para o fortalecimento da democracia e da governança pública.

Para fundamentar essa iniciativa, o trabalho apresenta uma revisão técnica e conceitual sobre os princípios da tecnologia *blockchain*, com ênfase em suas aplicações no setor público, seus benefícios e limitações. São abordadas as possibilidades de automação por meio de contratos inteligentes e realizadas comparações com soluções implementadas em diferentes países. Além disso, são analisadas experiências nacionais e internacionais que evidenciam o potencial dessa tecnologia para ampliar a eficiência e a transparência na gestão pública.

Ao final, é proposto um modelo funcional que ilustra, de forma prática, como a *blockchain* pode ser aplicada como instrumento de transparência, participação cidadã e controle social, especialmente em uma área tão sensível quanto a saúde.

Com isso, este trabalho visa contribuir para a reflexão sobre o uso de tecnologias emergentes na promoção da transparência pública, propondo uma solução eficiente e segura para o rastreamento do dinheiro público, com foco em um setor crítico e sensível como a saúde.

1.1 Delimitação do problema

Apesar das ferramentas de controle e transparência existentes, como o Portal da Transparência, o acesso da população às informações sobre a destinação do dinheiro público ainda é limitado, pouco intuitivo e, muitas vezes, desatualizado. Isso dificulta a fiscalização cidadã e favorece práticas de corrupção, principalmente em áreas sensíveis como a saúde. A ausência de mecanismos eficientes de rastreabilidade em tempo real impossibilita o acompanhamento completo do ciclo do dinheiro, desde sua arrecadação até sua aplicação final. O problema central, portanto, reside na falta de um sistema transparente, imutável e acessível que permita à sociedade acompanhar com precisão o uso do dinheiro público em saúde, especialmente em níveis federal, estadual e municipal.

1.2 Objetivos

1.2.1 *Objetivo geral*

Desenvolver um protótipo de sistema *blockchain* para a rastreabilidade da aplicação de dinheiro públicos na área da saúde.

1.2.2 *Objetivos específicos*

- Conceituar a tecnologia *blockchain*, destacando suas principais características e aplicações relacionadas à transparência e integridades das informações;
- Investigar soluções existentes que utilizam *blockchain* para rastreabilidade de recursos públicos, incluindo dinheiro público, documentos e registros oficiais;
- Apresentar a viabilidade do uso da tecnologia *blockchain* como ferramenta de transparência na administração pública;
- Mapear o fluxo da distribuição e aplicação do dinheiro público, com foco nas áreas de saúde nos níveis federal, estadual e municipal;

1.3 Justificativa

A transparência na gestão do dinheiro público é um dos pilares fundamentais da democracia, pois permite que cidadãos e órgãos de controle acompanhem como os recursos arrecadados estão sendo aplicados. No entanto, muitos países, incluindo o Brasil, ainda enfrentam sérias dificuldades na rastreabilidade e fiscalização dos gastos governamentais, especialmente em setores sensíveis como saúde, educação e infraestrutura.

Casos de corrupção envolvendo verbas públicas são recorrentes e comprometem a confiança nas instituições. Um exemplo recente ocorreu em dezembro de 2024, quando uma operação revelou o desvio de R$ 1,4 bilhão no Departamento Nacional de Obras Contra as Secas (Dnocs).

Nesse esquema, uma organização criminosa utilizava empresas de fachada para fraudar contratos e lavar dinheiro, evidenciando a ausência de mecanismos eficazes de controle e rastreamento em tempo real (Elijonas, 2024).

Diante desse cenário, a tecnologia *blockchain* surge como uma alternativa inovadora e viável, capaz de mitigar esses problemas por meio de registros descentralizados, imutáveis e auditáveis. Ao eliminar a necessidade de intermediários e permitir a verificação pública de todas as transações, a *blockchain* contribui significativamente para a prevenção de fraudes e o aumento da integridade na aplicação dos recursos públicos. Como destacam (Kshetri; Rogers, 2018), a utilização de sistemas baseados em *blockchain* no setor público pode transformar profundamente a governança ao oferecer rastreabilidade integral, reduzir disputas legais e permitir a responsabilização de agentes públicos.

Além disso, a implementação de contratos inteligentes possibilita a automação da gestão e da distribuição dos fundos, garantindo que as regras estabelecidas para a utilização do dinheiro público sejam executadas de forma transparente, sem interferência política ou administrativa. Assim, qualquer cidadão pode acompanhar, em tempo real, o percurso dos recursos desde sua arrecadação até a aplicação final.

1.4 Delimitação do Escopo

Este trabalho abordará exclusivamente o uso da tecnologia *blockchain* como ferramenta para rastreamento da aplicação de dinheiro públicos na área da saúde. A pesquisa se limitará a analisar e propor um modelo de sistema voltado para essa finalidade, sem abranger outras tecnologias de transparência digital, como portais eletrônicos, sistemas de controle internos ou inteligência artificial. Além disso, o estudo não tratará da aplicação de dinheiro em outras áreas como educação, infraestrutura ou segurança pública. O foco está restrito à análise da viabilidade e potencial da *blockchain* como solução para promover maior rastreabilidade e transparência na gestão de dinheiro público destinado à saúde.

2 BLOCKCHAIN E CONTRATOS INTELIGENTES: CONCEITOS, FUNCIONAMENTO E SEGURANÇA DOS DADOS

O avanço das tecnologias digitais tem impulsionado novas formas de registrar, processar e proteger informações. Nesse contexto, a tecnologia *blockchain* vem se destacando por oferecer um modelo inovador de armazenamento de dados baseado em redes distribuídas, que eliminam a necessidade de intermediários e garantem altos níveis de integridade, segurança e transparência. Inicialmente utilizada no contexto das criptomoedas, essa tecnologia passou a ser estudada e aplicada em diversos setores, incluindo o setor da saúde.

Este capítulo tem como objetivo apresentar os principais conceitos e fundamentos técnicos da *blockchain*, desde sua origem até sua aplicação em ambientes modernos como a *Web* 3.0. Serão abordados o funcionamento da estrutura de blocos encadeados, a lógica por trás da validação das transações, a importância das carteiras digitais e a arquitetura da *Ethereum Virtual Machine* (EVM). Além disso, serão exploradas as características e o papel dos contratos inteligentes no processo de automatização e verificação de regras dentro da *blockchain*, bem como o surgimento de soluções de segunda camada como resposta aos desafios de escalabilidade das redes mais utilizadas.

A compreensão desses aspectos técnicos é essencial para embasar o desenvolvimento do protótipo proposto neste trabalho, além de fornecer uma base sólida para a análise de sua aplicabilidade em contextos de rastreamento de dinheiro público.

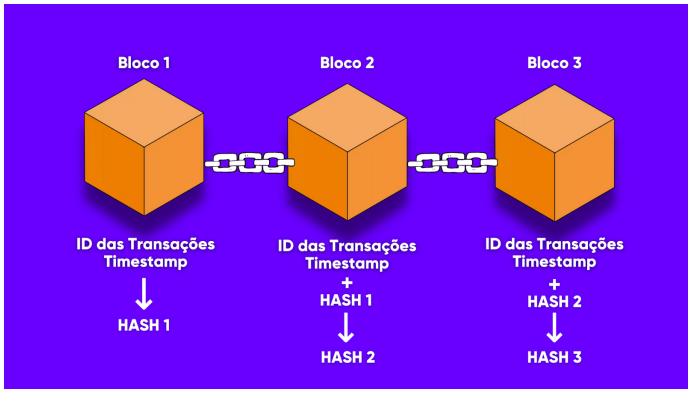
2.1 Histórico do Blockchain

A ideia de *blockchain* começou a ser desenvolvida entre as décadas de 1980 e 1990, sendo oficialmente apresentada em 1991 por Stuart Haber e W. Scott Stornetta no artigo *How to Time-Stamp a Digital Document* (Como marcar a data e hora em um documento digital). O objetivo inicial era criar um método para armazenar documentos digitais de forma que garantisse sua integridade, impedindo alterações e prevenindo fraudes. Para isso, os autores propuseram o uso de técnicas como o *hashing* (uma espécie de impressão digital dos dados) e o conceito de Árvore de Merkle, que possibilita o armazenamento eficiente de grandes volumes de dados dentro de um único bloco.

Nos primeiros dias da *blockchain*, os dados registrados nos blocos eram simples, contendo informações como a data e hora de geração do bloco, além das chaves públicas, como ilustrado na Figura 1.

Com o passar do tempo, o conceito de *blockchain* evoluiu para o que conhecemos atualmente como uma rede distribuída *peer-to-peer* (ponto a ponto), na qual múltiplos computadores denominados de nós se conectam e interagem diretamente, sem a necessidade de uma autoridade central. Essa característica fortalece a segurança e a descentralização da tecnologia. Em essência, a *blockchain* funciona como um livro contábil digital público e imutável, onde todas as transa-

Figura 1 – Funcionamento inicial da *blockchain*



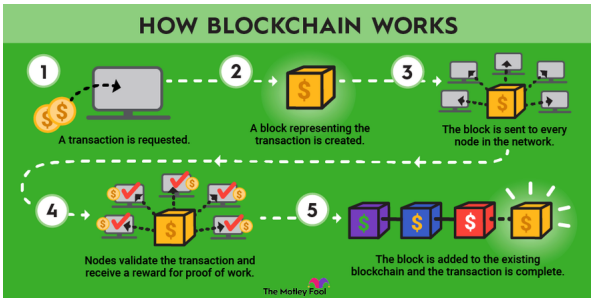
Fonte: (Souza, 2025).

ções são registradas de forma permanente, encadeadas em blocos e disponibilizadas de maneira transparente para consulta.

> Em uma blockchain típica, o cabeçalho de cada bloco é composto por uma string de 80 bytes, sendo 4 bytes destinados à sua identificação, 32 bytes para armazenar o *hash* do bloco anterior, 32 bytes para o *hash* do bloco atual, 4 bytes que registram a data e hora de sua criação, e 8 bytes usados no processo de mineração. Desses 8 bytes, 4 são dedicados à dificuldade da mineração, enquanto os outros 4 guardam o valor denominado Nonce, que representa o resultado do trabalho realizado pelo minerador (Kuntz, 2022, p. 25).

A *blockchain* é formada por uma sequência de blocos encadeados que armazenam registros de transações, como ilustrado na Figura 2. Cada computador conectado à rede recebe uma cópia completa da *blockchain*, contendo todos os blocos criados desde o início da rede. Cada bloco armazena informações sobre as transações realizadas até o momento da criação do próximo bloco, além de conter o *hash* do bloco anterior e o *hash* do bloco atual, garantindo a integridade dos dados.

Figura 2 – Funcionamento detalhado da *blockchain*



Fonte: (Bylund, 2025).

Esse formato de encadeamento torna a alteração de qualquer informação extremamente difícil, pois seria necessário modificar todos os blocos subsequentes em todas as cópias da rede simultaneamente. Para validar e adicionar novos blocos, é preciso resolver um problema matemático complexo, conhecido como *proof-of-work* (prova de trabalho), um processo que requer grande capacidade computacional, chamado de mineração (Kuntz, 2022).

Uma das principais características da *blockchain* é sua imutabilidade e segurança estrutural. Cada transação registrada em um bloco, uma vez validada e adicionada à cadeia, torna-se permanente e não pode ser alterada. Isso garante um alto nível de confiabilidade para o armazenamento de dados sensíveis e críticos. Além disso, como a rede é descentralizada e distribuída entre diversos nós, não há um ponto único de falha. Qualquer tentativa de modificação exigiria alterar todos os blocos subsequentes em todos os nós da rede, o que torna a fraude virtualmente inviável (Kuntz, 2022).

A tecnologia *blockchain* está sendo progressivamente aplicada em diversos setores, com um exemplo notável sendo a indústria da saúde. Os prontuários médicos podem ser armazenados de forma segura, permitindo que os dados dos pacientes sejam acessados de qualquer ponto da rede, mas sempre com a garantia de privacidade. Essa abordagem resolve um problema crítico, pois assegura que apenas indivíduos autorizados possam acessar ou modificar essas informações sensíveis (Kuntz, 2022).

Além disso, a tecnologia também se mostra útil na gestão de medicamentos controlados. Por exemplo, na dispensação de medicamentos, o uso de *blockchain* garante que esses produtos sejam entregues exclusivamente ao titular da transação, evitando fraudes e assegurando a rastreabilidade e segurança de todo o processo (Kuntz, 2022).

O funcionamento da *blockchain* pode ser comparado ao *BitTorrent* (protocolo de compartilhamento de arquivos ponto a ponto). Ambos operam em redes distribuídas, em que os dados não são centralizados em um único servidor, mas sim distribuídos entre os computadores da rede. No *BitTorrent*, os arquivos são compartilhados diretamente entre os usuários, enquanto na *blockchain*, os blocos de transações são compartilhados entre os nós da rede. A principal diferença reside na imutabilidade dos dados na *blockchain*, o que garante a segurança das transações registradas. Já o *BitTorrent* é projetado principalmente para a troca de arquivos, sem a preocupação com a integridade ou imutabilidade dos dados (Kuntz, 2022).

2.2 Carteiras Digitais

No ecossistema *blockchain*, as contas dos usuários são baseadas em um par de chaves criptográficas: uma chave pública e uma chave privada. A chave pública, também chamada de *address* (endereço), é compartilhada com outros usuários e funciona como um identificador único para o envio e recebimento de transações. Já a chave privada deve ser mantida em total sigilo, pois é responsável por autorizar movimentações e garantir a segurança da conta — funcionando de forma análoga a uma senha bancária (Kuntz, 2022).

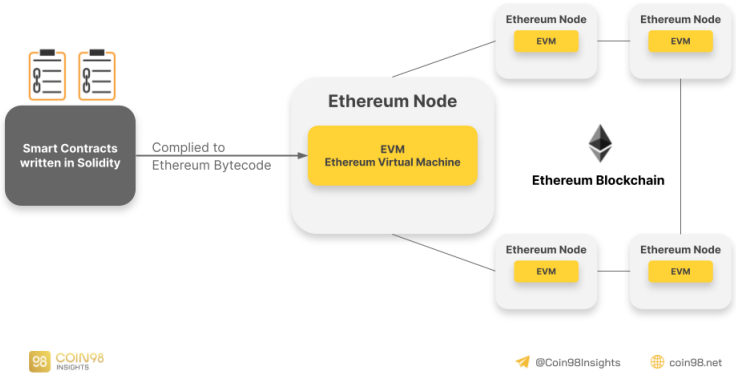
Essas contas podem ou não conter criptomoedas, mas são essenciais para interações com a rede *blockchain*, como a realização de transações ponto a ponto e a execução de contratos inteligentes. Além disso, as carteiras digitais exercem um papel importante na autenticação de usuários em aplicações descentralizadas, conhecidas como Aplicações Descentralizadas (DApps).

Os DApps operam sobre redes *blockchain* e implementam suas regras de negócio diretamente por meio de contratos inteligentes, sem necessidade de servidores centrais ou intermediários. Nesse contexto, a autenticação via carteira digital substitui os modelos tradicionais de login, permitindo que o usuário se conecte de forma segura, sem depender de senhas centralizadas ou do armazenamento de dados pessoais por terceiros (Kuntz, 2022).

2.3 Ethereum e Contratos Inteligentes: A Revolução da Web 3.0

O surgimento da rede *Ethereum* e dos contratos inteligentes trouxe uma inovação significativa ao universo da *blockchain*, ao permitir que regras de negócio sejam programadas diretamente na rede, substituindo a lógica centralizada da *Web* 2.0 por um modelo descentralizado característico da *Web* 3.0. Por meio dos contratos inteligentes, é possível registrar dados, automatizar processos e emitir eventos de forma transparente, sem necessidade de intermediários. A Figura 3 a seguir, demonstra a estrutura da EVM.

Figura 3 – Estrutura da *Ethereum Virtual Machine*



Fonte: (Dirgantara, 2023).

Criada por Vitalik Buterin no início da década de 2010 e lançada em 2015, a *Ethereum* revolucionou a *blockchain* ao introduzir o conceito de uma máquina de estados baseada em transações (Kuntz, 2022), na qual cada bloco armazena informações detalhadas como número do bloco, *timestamp* (marca temporal), lista de transações, dados do minerador, recompensas, dificuldade de mineração, limites de gás, entre outros elementos essenciais à segurança e integridade da rede.

Cada bloco da rede *Ethereum* contém três estruturas denominadas *Merkle-Patricia* — *stateRoot*, *transactionRoot* e *receiptsRoot* — responsáveis, respectivamente, por armazenar o estado atual da rede, o histórico de transações e os recibos correspondentes. A plataforma também utiliza uma unidade denominada *gas fee* (taxa de gás), que representa o esforço computacional necessário para a execução de operações. Toda transação demanda uma quantidade específica de gás, a qual deve ser paga pelo usuário. Em casos em que dois blocos são gerados simultaneamente, a rede prioriza aquele que possui maior dificuldade acumulada, enquanto o outro, denominado bloco órfão, pode ser incorporado à cadeia com uma recompensa reduzida (Kuntz, 2022).

Para superar limitações de escalabilidade, surgiram soluções de *Layer 2* (segunda camada), como *Arbitrum*, *Optimism* e *Polygon*. Essas redes complementam a *Ethereum*, permitindo transações mais rápidas e com menor custo, ao processar operações *off-chain* (fora da cadeia principal) e registrá-las posteriormente na rede principal *on-chain*.

A criação e execução de contratos inteligentes na *Ethereum* são feitas por meio da EVM — uma máquina virtual compatível com todos os nós da rede, capaz de executar qualquer função computacional *Turing Completeness*. Os contratos são escritos, em sua maioria, na linguagem *Solidity* exemplificada no Algoritimo 1, compilados para bytecode e processados pela EVM de forma descentralizada e segura (Kuntz, 2022).

Algoritmo 1 – Exemplo de contrato Solidity simples.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

contract Cofrinho {
    address public dono;
    constructor() {
        dono = msg.sender;
    }
    function depositar() public payable {
        // O valor enviado (msg.value)
    }
    function sacar() public {
        require(msg.sender == dono, "Apenas o dono pode sacar.");
        payable(dono).transfer(address(this).balance);
    }
    function saldo() public view returns (uint) {
        return address(this).balance;
    }
}
```

Fonte: Elaborado pelo autor.

2.4 Comparativo entre Ethereum e Subcamadas (Layer 2)

Embora a rede *Ethereum* tenha revolucionado o desenvolvimento de DApps, ainda enfrenta desafios significativos relacionados à escalabilidade e ao custo das transações. Com o aumento da demanda, sua camada principal *Layer 1* frequentemente atinge o limite de capacidade, resultando em altas taxas e lentidão no processamento. Para mitigar esses problemas, surgiram as chamadas soluções de *Layer 2*, que operam sobre a *Ethereum* com o objetivo de aumentar a capacidade de processamento, reduzir custos e melhorar a experiência do usuário, sem comprometer a segurança e a descentralização da camada principal. Essas soluções realizam transações fora da cadeia principal, registrando apenas os resultados consolidados na *Layer 1*, o que proporciona maior eficiência e desempenho à rede (Kuntz, 2022).

Entre as principais abordagens de segunda camada destacam-se os *Rollups*, que agrupam várias transações realizadas *off-chain* e as registram em lote na *Ethereum*. Essa estratégia permite que grandes volumes de dados sejam processados de forma eficiente e segura, com posterior validação na rede principal. *Rollups* como o Arbitrum e o Optimism utilizam o *Optimistic Rollups* (modelo otimista), em que se assume que as transações são válidas por padrão, permitindo contestações apenas quando necessário. Outra abordagem são as *Sidechains* (Cadeias laterais), que consistem em *blockchains* paralelas à *Ethereum*. Elas mantêm compatibilidade com a EVM, mas operam com suas próprias regras de consenso, o que lhes garante maior autonomia e desempenho, ainda que com menor segurança descentralizada. Um exemplo amplamente utilizado é a *Polygon Proof of Stake* (PoS) (prova de participação), conhecida por oferecer transações rápidas e de baixo custo. Por fim, há os *ZK-Rollups* e o *Validium*, que utilizam provas criptográficas — como as *zero-knowledge proofs* — para garantir a validade das transações realizadas fora da cadeia. Nos *ZK-Rollups*, essas provas são publicadas na *blockchain* junto com os dados das transações, assegurando máxima segurança e verificabilidade. Já no *Validium*, os dados permanecem fora da *blockchain*, aumentando ainda mais a escalabilidade, embora com sacrifício parcial da disponibilidade dos dados. Todas essas soluções são fundamentais para ampliar a adoção da tecnologia *blockchain*, permitindo a criação de aplicações descentralizadas escaláveis, acessíveis e economicamente viáveis (Kuntz, 2022).

A seguir na Tabela 1, apresenta-se uma comparação entre a *Ethereum Layer 1* e algumas das soluções de *Layer 2* mais utilizadas atualmente.

Tabela 1 – Comparação entre *Ethereum* e soluções de segunda camada

Característica	***Ethereum* (L1)**	***Polygon* (L2)**	***Arbitrum* (L2)**	***Optimism* (L2)**
Tipo de rede	Camada 1 pública	*Sidechain* (PoS)	*Rollup* otimista	*Rollup* otimista
Transações por segundo (TPS)	~30	~7.000	~4.500	~2.000
Custo médio por transação (Gás)	US$ 0,3–1,0	US$ 0,001	US$ 0,03	US$ 0,03
Tempo de confirmação	12–15 s	~2 s	~1 s	~1 s
Segurança	Muito alta	Moderada*	Alta	Alta
Compatível com EVM	Sim	Sim	Sim	Sim
Popularidade / adoção	Muito alta	Alta	Alta	Média

Fonte: (Ethereum et al., 2024).

2.5 Desafios e Limitações da Tecnologia Blockchain

Apesar das inúmeras vantagens da tecnologia *blockchain* e dos contratos inteligentes, seu uso ainda apresenta diversas desvantagens e desafios que precisam ser considerados, especialmente em projetos voltados ao setor público. Tais limitações dizem respeito não apenas à complexidade técnica envolvida, mas também aos riscos operacionais e de segurança inerentes à própria natureza descentralizada dessas tecnologias.

No caso específico dos contratos inteligentes, uma de suas principais limitações é a imutabilidade do código após a sua implantação. Uma vez publicado na rede, o contrato não pode mais ser alterado, o que exige extremo cuidado no planejamento e desenvolvimento, pois qualquer falha, mesmo que pequena, pode acarretar prejuízos significativos e irreversíveis. Um exemplo emblemático desse tipo de risco foi o ataque ao Organização Autônoma Descentralizada (DAO), ocorrido em 2016, que resultou na divisão da própria rede *Ethereum* em duas versões distintas: *Ethereum* e *Ethereum* Classic.

Além disso, a presença de vulnerabilidades no código dos contratos inteligentes é um problema recorrente, frequentemente decorrente de práticas inadequadas de desenvolvimento. Exemplos comuns incluem a falta de definição correta da visibilidade de funções e variáveis, o uso de versões instáveis ou inseguras de compiladores, conhecidas como *floating pragmas*, e a implementação de funções sensíveis sem os controles de acesso apropriados. Essas falhas expõem os contratos a ataques que, muitas vezes, não requerem técnicas avançadas, sendo explorados a partir de descuidos básicos dos desenvolvedores (Kuntz, 2022).

Essa realidade evidencia outra fragilidade dos contratos inteligentes: a responsabilidade

integral do desenvolvedor pela segurança da aplicação. Como a lógica de funcionamento permanece registrada de forma permanente na *blockchain*, qualquer brecha deixada no código pode ser explorada por agentes mal intencionados, que se aproveitam das regras legítimas da rede para causar danos, sem que seja necessário manipular diretamente a infraestrutura ou utilizar técnicas de invasão sofisticadas(Kuntz, 2022).

No entanto, apesar dessas limitações, é possível mitigar consideravelmente os riscos associados aos contratos inteligentes por meio de auditorias especializadas. Existem empresas reconhecidas internacionalmente, como *CertiK*, *OpenZeppelin* e *Trail of Bits*, que oferecem serviços de auditoria técnica de código-fonte para *smart contracts*, analisando falhas de segurança, vulnerabilidades lógicas e inconsistências de implementação. Essas auditorias, realizadas antes da publicação dos contratos na rede principal, tornam o ambiente mais seguro, aumentam a confiança dos usuários e fortalecem a credibilidade dos projetos baseados em *blockchain*. Portanto, embora a responsabilidade do desenvolvedor seja grande, há meios técnicos confiáveis para garantir maior robustez ao sistema, especialmente quando se busca transparência e confiança em aplicações públicas (Certik; Openzeppelin; Bits, 2024).

2.6 Conclusão do Capítulo: Fundamentos da Tecnologia Blockchain

A análise realizada ao longo deste capítulo permitiu compreender os principais fundamentos da tecnologia *blockchain* e sua evolução até os contratos inteligentes, com ênfase na rede *Ethereum* e suas soluções de escalabilidade. Observou-se que a *blockchain* oferece uma infraestrutura descentralizada, segura e transparente, cujas características técnicas — como imutabilidade, criptografia e validação distribuída — a tornam altamente adequada para contextos que demandam integridade e confiança nas informações.

A introdução dos contratos inteligentes ampliou ainda mais o potencial da tecnologia, possibilitando a automatização de regras e transações sem a necessidade de intermediários, o que reduz custos, aumenta a eficiência e elimina pontos vulneráveis à fraude. Além disso, as soluções de segunda camada foram discutidas como alternativas viáveis para superar as limitações de escalabilidade da *Ethereum*, mantendo a compatibilidade com sua estrutura e segurança.

Esses conhecimentos técnicos formam a base conceitual necessária para a proposta desenvolvida neste trabalho. No capítulo seguinte, serão abordadas as aplicações da *blockchain* na administração pública, com foco na viabilidade de sua adoção para promover a rastreabilidade do dinheiro público, especialmente no setor da saúde.

3 UTILIZAÇÃO DA BLOCKCHAIN PARA GOVERNOS

A aplicação da tecnologia *blockchain* vai muito além do universo das criptomoedas, alcançando setores como saúde, logística, meio ambiente e, em especial, a administração pública. Sua estrutura descentralizada e imutável oferece uma base robusta para promover maior transparência, rastreabilidade e segurança nos dados governamentais. Essa capacidade permite, por exemplo, implementar sistemas que acompanham em tempo real o fluxo de recursos públicos — desde a arrecadação até a aplicação final — reduzindo riscos de corrupção, desvios e má gestão.

Embora ainda seja desconhecida por grande parte da população brasileira e internacional, a *blockchain* já possui aplicações concretas no setor público nacional. Um exemplo notável é a nova Carteira de Identidade Nacional (CIN), cuja emissão utiliza *blockchain* para garantir maior rastreabilidade, segurança e consistência. Segundo o Ministério da Gestão e da Inovação em Serviços Públicos, o sistema permite, inclusive, a inscrição do CPF diretamente no balcão do órgão de identificação, trazendo benefícios diretos à cidadania (Govbr, 2023).

Internacionalmente, a Estônia é referência na adoção da tecnologia, com o sistema *e-Residency*, um registro digital descentralizado que armazena informações como identidade, escolaridade e histórico de trabalho desde o nascimento do cidadão (Vale, 2020). No Brasil, outro avanço importante é o Digital Real Eletrônico X (DREX) — a moeda digital do Banco Central — que utiliza *blockchain* para garantir transações mais seguras e transparentes. Além disso, bancos como o Itaú e o Banco do Brasil já exploram essa tecnologia para reforçar a segurança e rastreabilidade de suas operações financeiras.

Diante desse cenário, torna-se evidente o potencial transformador da *blockchain* na gestão pública. Este capítulo explora aplicações já adotadas por governos ao redor do mundo, analisa benefícios e desafios envolvidos e propõe uma abordagem de rastreabilidade do dinheiro público baseada em contratos inteligentes e registros descentralizados, com o objetivo de promover maior transparência, controle social e confiança nas instituições.

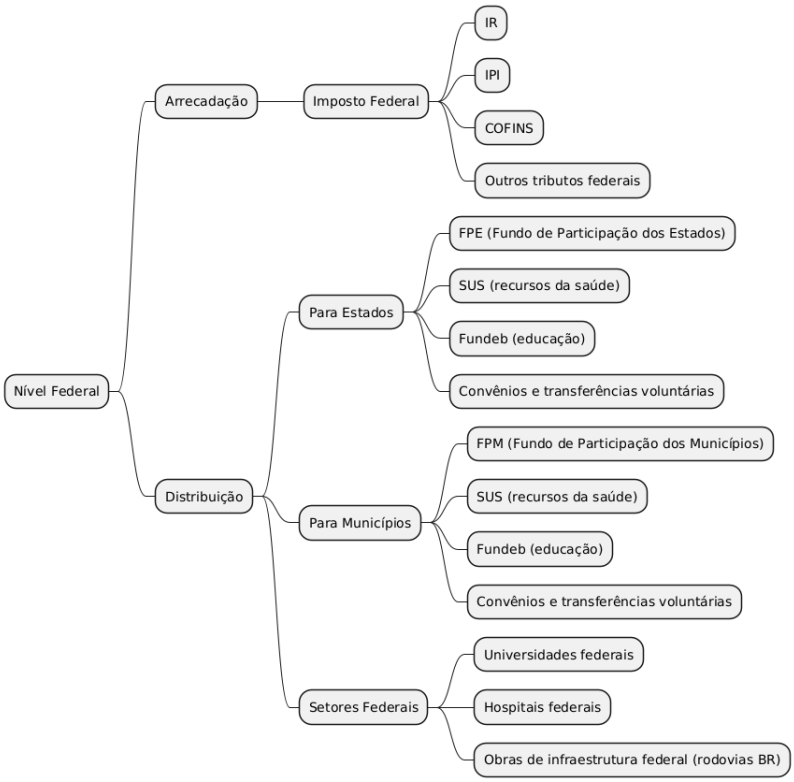
3.1 Arrecadação e Distribuição do Dinheiro Público no Brasil

No Brasil, a arrecadação e distribuição de recursos públicos são regidas por um conjunto de normas constitucionais e legais que estabelecem as competências tributárias e os mecanismos de repartição de receitas entre os entes federativos (Brasil, 1988).

A Constituição Federal de 1988 define as competências tributárias da União, dos Estados, do Distrito Federal e dos Municípios. A União é responsável pela arrecadação de tributos como o Imposto de Renda (IR), o Imposto sobre Produtos Industrializados (IPI) e a Contribuição para o Financiamento da Seguridade Social (COFINS) representado na Figura 4. Os Estados arrecadam tributos como o Imposto sobre Circulação de Mercadorias e Serviços (ICMS) e o Imposto sobre a Propriedade de Veículos Automotores (IPVA). Os Municípios, por sua vez, arrecadam tributos como o Imposto sobre Serviços (ISS) e o Imposto Predial e Territorial Urbano (IPTU) (Brasil,

1988).

Figura 4 – Fluxo de arrecadação e distribuição de nível federal

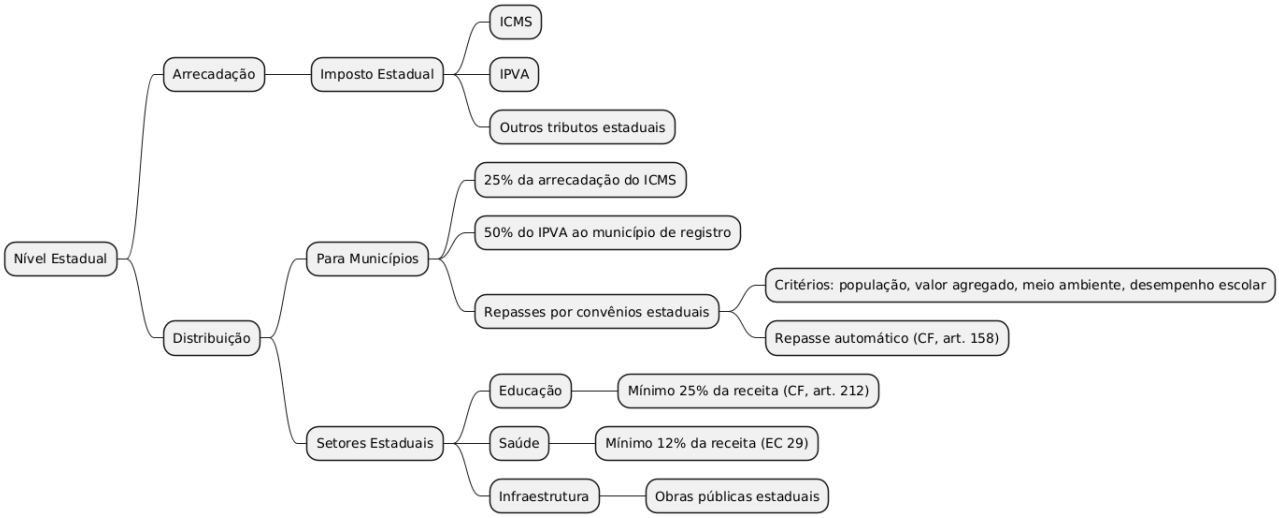


Fonte: Elaborado pelo autor.

A repartição de receitas entre os entes federativos é estabelecida nos artigos 158 e 159 da Constituição. O artigo 158 determina que pertencem aos Municípios: o produto da arrecadação do IPVA, 50% do IPVA arrecadado no território municipal; 25% do produto da arrecadação do ICMS; entre outros. O artigo 159 estabelece que a União deve entregar: 21,5% do produto da arrecadação do IR e do IPI ao Fundo de Participação dos Estados (FPE); 22,5% ao Fundo de Participação dos Municípios (FPM); 10% ao Fundo de Compensação de Exportações (FCE); entre outros (Brasil, 1988).

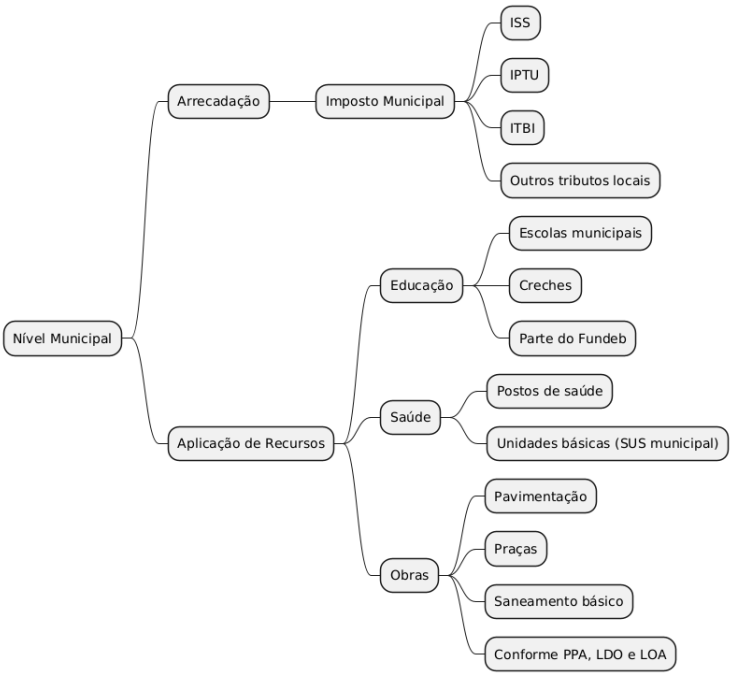
Além disso, a Constituição estabelece aplicações mínimas de recursos em setores essenciais. O artigo 212 determina que os Estados e os Municípios devem aplicar, anualmente, no mínimo 25% da receita resultante de impostos na manutenção e desenvolvimento do ensino (Brasil, 1988). O artigo 198, com a redação dada pela Emenda Constitucional nº 29/2000, estabelece que a União, os Estados, o Distrito Federal e os Municípios devem aplicar recursos mínimos em ações e serviços públicos de saúde evidenciado nas Figuras 5 e 6. A Emenda Constitucional nº 29/2000, promulgada em 13 de setembro de 2000, foi um passo fundamental para a garantia da efetivação do direito à saúde, ao vincular um aporte mínimo de recursos a serem gastos pelos entes federados obrigatoriamente em ações e serviços públicos de saúde (Brasil, 2000).

Figura 5 – Fluxo de arrecadação e distribuição de nível estadual



Fonte: Elaborado pelo autor.

Figura 6 – Fluxo de arrecadação e distribuição de nível municipal



Fonte: Elaborado pelo autor.

Essas normas visam assegurar uma distribuição equitativa do dinheiro públicos, promovendo o desenvolvimento regional equilibrado e garantindo o financiamento adequado das políticas públicas essenciais, como saúde, educação e infraestrutura conforme demonstrado no fluxo apresentado no Anexo.

3.2 Aplicabilidade e Viabilidade da Blockchain no Setor Público

A tecnologia *blockchain* tem se destacado como uma alternativa viável e promissora para enfrentar diversos desafios da administração pública, especialmente em países em desenvolvimento. Um de seus usos mais relevantes está na gestão de registros de propriedade de terras, um setor historicamente marcado por fragilidades, informalidade e ausência de sistemas confiáveis (Kshetri; Rogers, 2018).

Em regiões como o Haiti, o terremoto de 2010 destruiu todos os registros físicos municipais, deixando milhares de agricultores sem documentação que comprovasse a posse de suas terras. Essa vulnerabilidade compromete a segurança jurídica e impede o acesso a crédito e à proteção patrimonial. Segundo (Kshetri; Rogers, 2018), ativos sem documentação formal geram perdas econômicas globais da ordem de US$ 20 trilhões.

Diante desse cenário, a *blockchain* surge como uma alternativa segura, transparente e eficiente. Sistemas baseados nessa tecnologia permitem a criação de registros imutáveis com histórico completo de transações, contendo informações como autor, data e finalidade de cada modificação. Isso reduz drasticamente as chances de fraudes e disputas judiciais. No Brasil, municípios como Pelotas (RS) e Morro Redondo já utilizam a *blockchain* para registrar dados de zoneamento, identidade do proprietário e coordenadas geográficas (Kshetri; Rogers, 2018).

Além da segurança jurídica, a redução de custos é um benefício importante: na Geórgia, a migração do registro fundiário para a *blockchain* reduziu taxas de aproximadamente US$ 200 para apenas US$ 0,10 (Kshetri; Rogers, 2018). No entanto, é preciso reconhecer que a tecnologia, por si só, não soluciona todos os problemas. A qualidade e legitimidade dos dados inseridos ainda dependem de mecanismos institucionais confiáveis e, muitas vezes, enfrentam resistência política por parte de setores que enxergam a transparência como uma ameaça ao status quo.

Ainda assim, quando implementada com critérios de justiça e imparcialidade, a *blockchain* tem potencial para representar o primeiro acesso legal e efetivo à propriedade para populações marginalizadas, rompendo ciclos históricos de exclusão. Como destacam (Zia et al., 2022), sistemas públicos de registro baseados em *blockchain* fornecem logs de auditoria imutáveis com assinaturas criptográficas, permitindo a responsabilização de agentes públicos por alterações indevidas.

Além dos registros fundiários, a *blockchain* vem se mostrando viável também em sistemas de distribuição de benefícios sociais, promovendo maior eficiência, transparência e rastreabilidade. No Brasil, um exemplo prático é a moeda social Mumbuca, do município de Maricá (RJ). Através de uma criptomoeda local, os repasses são direcionados ao consumo regional, garantindo que os benefícios cheguem aos destinatários pretendidos e impulsionem a economia local (Zia et al., 2022).

A utilização de contratos inteligentes potencializa ainda mais esse tipo de sistema. Esses contratos permitem a programação automática de regras de uso dos recursos, como a limitação de gastos a determinados estabelecimentos ou a concessão de incentivos para comportamentos

sustentáveis. Essa abordagem amplia a eficiência das políticas públicas, promovendo uma governança digital orientada por dados e automatismos.

Exemplos internacionais reforçam essa tendência. Iniciativas como a *FairCoin* (Espanha), a *Moneda PAR* (Argentina) e a *Sarafu* (Quênia) mostram como moedas digitais locais baseadas em *blockchain* têm contribuído para a inclusão econômica, resiliência comunitária e desenvolvimento sustentável, sobretudo em momentos de crise.

Em resumo, a *blockchain* não apenas resolve gargalos técnicos da administração pública, como também possui viabilidade econômica, social e tecnológica, abrindo caminho para uma nova era de governança pública baseada em confiança, descentralização e transparência.

3.3 Casos Reais de Falta de Rastreabilidade e Ineficiência

A falta de mecanismos eficazes de rastreabilidade financeira no setor público brasileiro tem contribuído para práticas como corrupção, má gestão de recursos e desvios orçamentários. A ausência de transparência no controle de gastos públicos compromete a confiança da sociedade nas instituições e dificulta a fiscalização adequada por parte dos órgãos competentes, resultando em impactos negativos para a administração pública e para o desenvolvimento social.

Um caso emblemático ocorreu em 2024, quando uma operação da Polícia Federal revelou o desvio de R$ 1,4 bilhão no Departamento Nacional de Obras Contra as Secas (Dnocs). O esquema envolvia empresas de fachada utilizadas para fraudar contratos e lavar dinheiro público (Elijonas, 2024). A inexistência de um sistema de controle em tempo real permitiu que as transações ocorressem de forma opaca, dificultando a atuação dos órgãos fiscalizadores e retardando a responsabilização dos envolvidos.

Outro escândalo de grandes proporções atingiu o Instituto Nacional do Seguro Social (INSS) entre os anos de 2019 e 2024, quando um esquema fraudulento resultou em prejuízos estimados em R$ 6,3 bilhões. Nesse caso, entidades de classe firmavam Acordos de Cooperação Técnica (ACTs) com o INSS para realizar descontos mensais não autorizados nos benefícios de aposentados e pensionistas. A maior parte das vítimas sequer reconhecia os débitos. Uma investigação conduzida pela Controladoria-Geral da União (CGU) revelou que 97% dos beneficiários entrevistados negaram ter autorizado os descontos (Uol, 2025).

A Operação Sem Desconto, deflagrada em abril de 2025, resultou em mais de 200 mandados de busca e apreensão e levou ao afastamento do então presidente do INSS. O caso gerou forte repercussão política, com exigências de investigação mais profunda e a suspensão imediata de todos os convênios similares. Esse episódio deixou clara a necessidade de mecanismos de rastreabilidade robustos que permitam a verificação de autorizações, o monitoramento de transações e a identificação de irregularidades de forma preventiva (Uol, 2025).

Além dos escândalos de corrupção, a pandemia da COVID-19 expôs deficiências estruturais nos sistemas tradicionais de distribuição de benefícios sociais. Para mitigar os impactos da crise sanitária, o governo brasileiro implementou, com urgência, o Auxílio Emergencial,

beneficiando cerca de 66 milhões de pessoas com o repasse total de R$ 280 bilhões até o final de 2020 — o equivalente a aproximadamente 4% do Produto Interno Bruto (PIB) (Zia et al., 2022). Apesar da importância da iniciativa, o programa enfrentou diversos entraves operacionais: burocracia excessiva, cadastros desatualizados, exclusão de beneficiários legítimos e atrasos nos repasses comprometeram sua efetividade.

Outro problema recorrente foi o uso indevido dos recursos. Em muitos casos, o dinheiro destinado a regiões vulneráveis foi gasto em municípios mais ricos ou absorvido por grandes redes varejistas, reduzindo o impacto positivo esperado nas economias locais e falhando em atingir os públicos prioritários (Zia et al., 2022).

Esses exemplos concretos revelam não apenas a vulnerabilidade dos atuais sistemas de gestão pública, mas também a necessidade urgente de adotar soluções que garantam transparência, auditabilidade e rastreabilidade em tempo real.

3.4 Blockchain na Saúde Pública: Trabalhos Relacionados

Diversas pesquisas recentes têm investigado o uso da tecnologia *blockchain* na área da saúde, especialmente com foco na gestão de dados sensíveis, como prontuários médicos eletrônicos. No contexto brasileiro, destaca-se a proposta de Rodrigues (2021), que apresenta uma plataforma baseada em *blockchain* voltada ao gerenciamento dos Prontuários Médicos Eletrônicos (PMEs) de pacientes do Sistema Único de Saúde (SUS). A motivação reside no desafio enfrentado pelo sistema público de saúde, que atende uma população superior a 214 milhões de habitantes, distribuídos por um território de dimensões continentais. Atualmente, os dados clínicos encontram-se fragmentados entre diferentes unidades de saúde, sem integração eficiente e com limitações significativas em termos de segurança, escalabilidade e rastreabilidade.

O estudo reconhece que os prontuários em papel ainda são comuns, embora haja um esforço crescente de informatização. No entanto, mesmo os registros eletrônicos, quando existentes, permanecem isolados em sistemas locais, dificultando a construção de uma base nacional unificada. Esse cenário compromete tanto a eficiência no atendimento quanto a transparência no uso dos dados, dificultando auditorias e análises epidemiológicas em larga escala. Soma-se a isso a fragilidade na segurança das informações, que, em muitos casos, dependem apenas de senhas simples, sem proteção criptográfica robusta. Ademais, o paciente não possui controle efetivo sobre a divulgação de seus dados médicos, em desacordo com os princípios da LGPD Rodrigues (2021).

Para mitigar essas limitações, propõe-se uma arquitetura distribuída baseada em *blockchain*, composta por três componentes principais: unidades de saúde, uma rede de validadores ou mineradores e uma base global de dados externa. A proposta utiliza uma rede permissionada, adequada ao contexto institucional do SUS, em que a participação e o acesso são controlados por autoridades de saúde. O modelo contempla a criação, atualização, recuperação e auditoria dos prontuários, com todas as operações registradas em blocos imutáveis. O algoritmo de consenso

adotado é o *Practical Byzantine Fault Tolerance* (PBFT), escolhido por seu equilíbrio entre segurança e desempenho, especialmente em redes com até 200 nós — número compatível com as unidades federativas brasileiras (Rodrigues, 2021).

A avaliação teórica foi realizada por meio de modelagem analítica, utilizando teoria das filas para simular o tempo de resposta das transações e o impacto de diferentes topologias de rede. Os resultados indicam que, mesmo em cenários com falhas parciais nos validadores, o sistema mantém desempenho satisfatório. Em termos de escalabilidade, estimou-se que a plataforma poderia suportar mais de 1,4 bilhão de visitas anuais ao SUS sem comprometer sua estabilidade. Quanto ao custo, mesmo considerando o crescimento exponencial da base de dados até 2030, o impacto financeiro seria inferior a 1% do orçamento anual do Ministério da Saúde (MS), reforçando a viabilidade econômica da proposta (Rodrigues, 2021).

Do ponto de vista da transparência, a plataforma representa um avanço significativo. Todas as ações realizadas sobre os prontuários ficam registradas de forma imutável, permitindo o rastreamento completo do ciclo de vida das informações. Isso facilita auditorias e investigações, além de fortalecer o controle social sobre a gestão pública da saúde. A confidencialidade é assegurada por criptografia de chave pública, e o acesso aos dados só é possível mediante autorização do paciente, em conformidade com a LGPD, garantindo maior proteção aos direitos individuais (Rodrigues, 2021).

Essa proposta se destaca no estado da arte por ser uma das poucas voltadas especificamente à realidade do SUS. Enquanto a maioria dos estudos se concentra em ambientes hospitalares privados ou sistemas internacionais, a plataforma de Rodrigues busca integrar diferentes unidades do sistema público brasileiro, considerando suas particularidades operacionais e institucionais. Embora ainda conceitual, a pesquisa oferece uma base sólida de conhecimento técnico e experimental, capaz de orientar o desenvolvimento de soluções reais nos próximos anos. Fica evidente, portanto, que a tecnologia *blockchain* possui grande potencial para modernizar a gestão da saúde pública no Brasil, promovendo eficiência, integridade e, sobretudo, maior transparência no uso dos dados dos cidadãos (Rodrigues, 2021).

A pandemia de COVID-19 também evidenciou limitações dos sistemas públicos de saúde, especialmente no gerenciamento de vacinas. Um caso emblemático é o sistema VAMS, dos Estados Unidos, que, mesmo com um investimento de US$ 44 milhões, apresentou falhas como previsão incorreta de estoques, vulnerabilidades de segurança e ineficiências nos agendamentos (Zia et al., 2022).

De modo geral, os dados de saúde pública continuam fragmentados entre diversas instituições e expostos a riscos de manipulação, o que dificulta a rastreabilidade e a resposta eficiente a crises sanitárias.

A tecnologia *blockchain* surge como uma alternativa segura e descentralizada, com registros imutáveis e auditáveis, acessíveis apenas por profissionais autorizados. Isso facilita a rastreabilidade da cadeia de suprimentos da produção à aplicação da vacina garantindo maior segurança e eficiência.

Exemplos de iniciativas bem-sucedidas incluem a Estônia, que desde 2008 utiliza a infraestrutura KSI *blockchain*, com validações criptográficas para proteger dados públicos; o Reino Unido, que empregou sensores conectados à *blockchain* para monitorar, em tempo real, a temperatura de armazenamento das vacinas; e a Coreia do Sul, especificamente na Ilha de Jeju, que adotou um sistema baseado em *blockchain* para rastrear contatos de turistas, com foco na privacidade e no controle epidemiológico (Zia et al., 2022).

3.5 Potenciais Impactos da Blockchain na Gestão Pública

A adoção de tecnologias baseadas em *blockchain* na administração pública pode gerar impactos relevantes tanto do ponto de vista social quanto econômico.

Socialmente, a transparência na gestão dos recursos públicos fortalece a democracia ao permitir o controle social efetivo, promovendo maior confiança da população nas instituições. A rastreabilidade pública também pode inibir a corrupção, já que qualquer cidadão pode acompanhar a destinação e o uso das verbas públicas.

No aspecto econômico, a automatização e a imutabilidade proporcionadas pelos contratos inteligentes podem reduzir significativamente os custos com auditorias, fraudes e retrabalho administrativo. Além disso, o redirecionamento mais eficiente dos recursos tende a gerar ganhos em setores essenciais como saúde, educação e infraestrutura (Rodrigues, 2021).

Quando aplicada de forma estruturada, a *blockchain* pode atuar como um elemento catalisador para a melhoria da eficiência estatal, o empoderamento cidadão e a construção de uma cultura de governança orientada por dados.

3.6 Considerações Finais

A análise das aplicações da *blockchain* no setor público evidencia seu potencial como ferramenta estratégica para transformar a forma como os governos gerenciam, distribuem e prestam contas dos recursos públicos. A transparência, a rastreabilidade e a segurança proporcionadas por essa tecnologia oferecem as bases necessárias para uma gestão mais eficiente e democrática.

A implementação de sistemas baseados em *blockchain*, como o protótipo proposto neste trabalho, representa um passo relevante rumo à modernização da administração pública, especialmente em setores sensíveis como a saúde, onde a confiança da população depende diretamente da lisura e da eficácia na aplicação dos recursos.

4 MODELAGEM

Este capítulo apresenta uma modelagem preliminar do protótipo proposto para a rastreabilidade da aplicação do dinheiro público no setor da saúde, utilizando *smart contracts* em uma rede *blockchain*. Trata-se de uma etapa inicial que visa representar, de forma sistemática e visual, a estrutura lógica, os fluxos operacionais e a interação entre os principais componentes do sistema, servindo como base para uma implementação futura em código.

Para isso, são utilizados diversos diagramas, como *mind maps* (mapas mentais), casos de uso, atividades, classes, arquitetura e interfaces visuais. Esses elementos têm o objetivo de traduzir o funcionamento do protótipo em representações compreensíveis e alinhadas às boas práticas da engenharia de software. A modelagem contribui para a compreensão do comportamento esperado dos *smart contracts* em diferentes esferas de governo — federal, estadual e municipal — evidenciando a separação de responsabilidades, os processos de distribuição e aplicação dos recursos, a transparência dos dados públicos e os mecanismos de controle de acesso.

Além disso, este capítulo discute a escolha por uma arquitetura escalável e modular, com foco na possibilidade de expansão futura para outros setores além da saúde, como educação e infraestrutura. O conjunto de diagramas aqui apresentados constitui um alicerce conceitual que orientará a construção do protótipo funcional, assegurando os princípios de rastreabilidade, transparência e segurança na gestão de recursos públicos.

4.1 Mapa Mental sobre o Fluxo de Aplicação

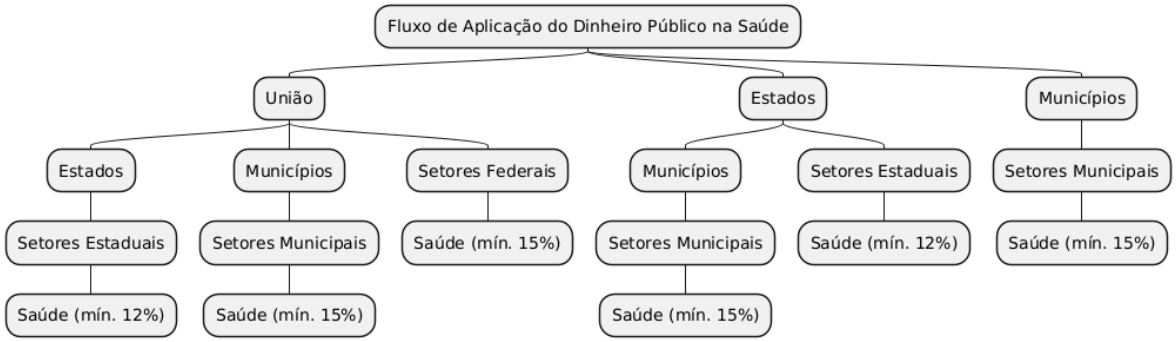
Para facilitar a compreensão da lógica e da estrutura dos contratos inteligentes que compõem o protótipo proposto, elaborou-se um diagrama do tipo *mind map* que representa, de forma visual e hierárquica, o fluxo de execução dos contratos nos três níveis de governo. Esse diagrama foi desenvolvido com o objetivo de complementar os diagramas tradicionais da UML — como os de casos de uso e de classes — oferecendo uma visão mais intuitiva e exploratória da automação dos processos de distribuição e aplicação do dinheiro público na área da saúde.

Nos mapas mentais, observa-se como os contratos inteligentes foram organizados de maneira modular, respeitando a divisão federativa e mantendo uma lógica central padronizada para rastreabilidade e validação. Na Figura 7, é apresentado o diagrama do tipo *mind map*, que representa a modelagem desses contratos inteligentes.

Cada nível governamental possui seu próprio *smart contract*, responsável por ações como o recebimento de recursos, a definição de destino, a execução dos gastos e o registro para auditoria pública. Além disso, o diagrama destaca as obrigações constitucionais mínimas de investimento na área da saúde, conforme estabelecido pela Emenda Constitucional nº 29/2000 e regulamentações posteriores: a União deve aplicar, no mínimo, 15% da Receita Corrente Líquida; os Estados, 12% da receita de impostos; e os Municípios, 15% da mesma base (Brasil, 2000).

A separação por níveis de governo reflete a realidade da arrecadação e da aplicação

Figura 7 – Fluxo detalhado do dinheiro público nos contratos inteligentes



Fonte: Elaborado pelo autor.

do dinheiro público, permitindo uma simulação mais fiel e educativa do funcionamento do modelo brasileiro de financiamento da saúde. Essa abordagem também reforça a importância da rastreabilidade em cada etapa do processo, promovendo a transparência e facilitando o controle social.

4.2 Arquitetura

A arquitetura proposta para o protótipo foi concebida com foco na possibilidade de escalabilidade e modularidade, considerando cenários em que a aplicação venha a ser estendida para outros setores além da saúde, como educação e infraestrutura — os quais possuem regras próprias para a alocação de recursos públicos entre os níveis federal, estadual e municipal. A estrutura modular tem o potencial de facilitar o reaproveitamento da lógica dos contratos inteligentes e a adição de novos módulos com menor impacto sobre a estrutura existente. No entanto, por se tratar de uma modelagem preliminar, tais características ainda carecem de validação prática, a ser realizada em uma futura etapa de implementação do protótipo.

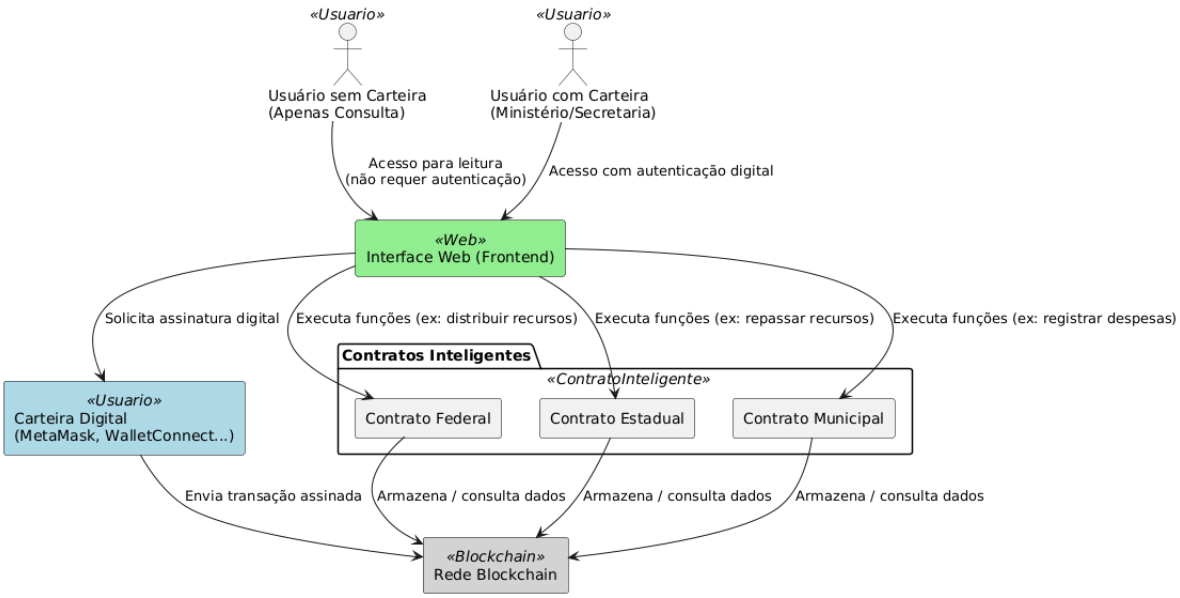
O acesso à aplicação será através de uma interface *web*, que permite tanto a consulta pública de dados quanto a interação transacional com os *smart contracts*. Usuários que desejam apenas visualizar informações — como o percentual mínimo constitucional aplicado à saúde, valores distribuídos e o histórico de transações — não precisam autenticar sua identidade digital, podendo navegar livremente sem conexão com uma carteira digital.

Por outro lado, usuários autorizados, como ministérios e secretarias que precisam executar ações ativas — como o registro de despesas ou a distribuição de dinheiro público — devem se conectar à aplicação utilizando uma carteira digital. Essa autenticação é necessária para que a assinatura digital seja validada e a transação seja efetivamente enviada e registrada na *blockchain*.

Dessa forma, a arquitetura promove segurança, descentralização e transparência, ao mesmo tempo em que assegura uma experiência acessível para o controle social da população. A

Figura 8 ilustra essa arquitetura, evidenciando os atores, a interface web, os contratos inteligentes e a interação com a *blockchain*.

Figura 8 – Arquitetura do protótipo

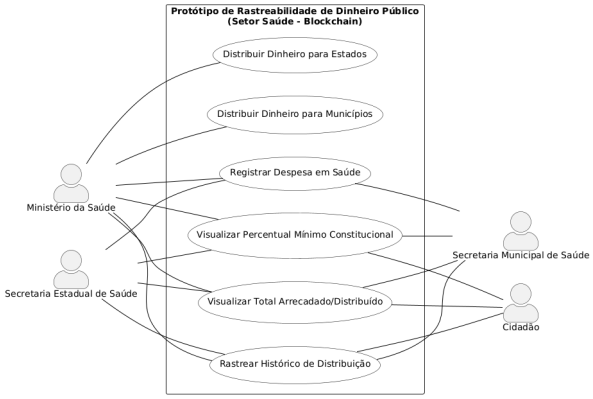


Fonte: Elaborado pelo autor.

4.3 Casos de uso

O diagrama de casos de uso apresentado na Figura 9 descreve as funcionalidades do protótipo de rastreabilidade conforme os diferentes papéis dos atores no modelo federativo. Cada ator executa ações específicas de acordo com suas competências legais na distribuição e aplicação do dinheiro público destinado à saúde.

Figura 9 – Diagrama de casos de uso



Fonte: Elaborado pelo autor.

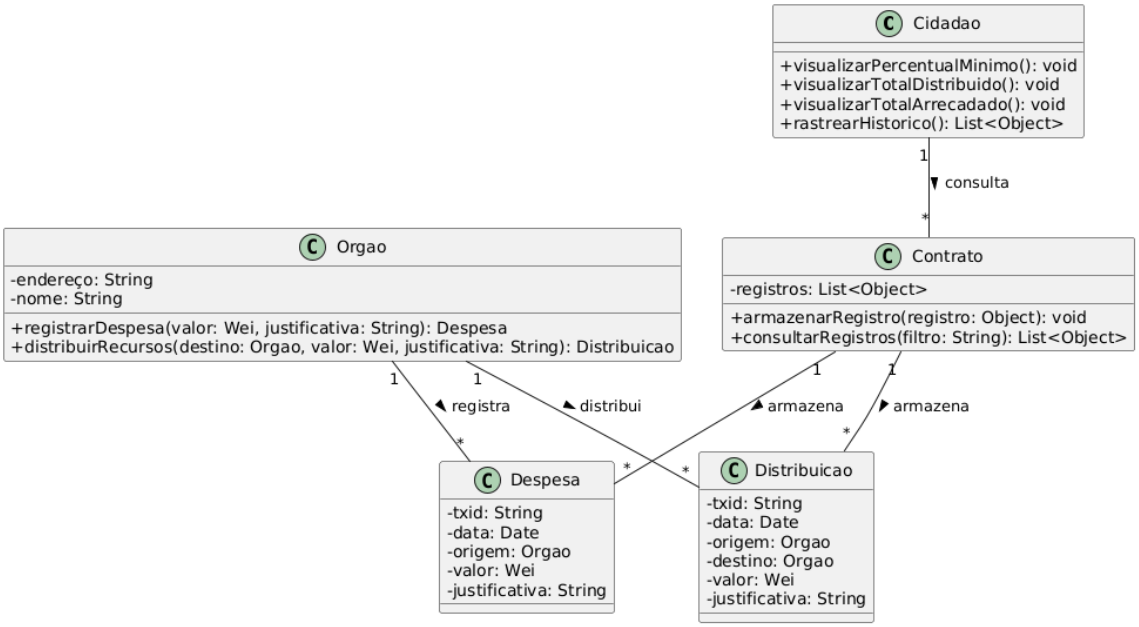
Órgãos públicos — como o Ministério da Saúde e as Secretarias Estaduais e Municipais — podem realizar a transferência de valores entre entes federativos ou registrar despesas diretamente, conforme sua esfera de atuação. Além disso, esses órgãos têm acesso às funcionalidades de rastreamento das informações registradas na *blockchain*, incluindo os percentuais constitucionais mínimos, valores arrecadados e distribuídos, bem como o histórico de movimentações.

Já os cidadãos contam com acesso restrito à visualização desses dados, assegurando a transparência pública e fortalecendo o controle social.

4.4 Diagrama de Classes

A Figura 10 apresenta o diagrama de classes do protótipo, modelando os principais atores e objetos envolvidos na rastreabilidade do dinheiro público aplicado na saúde. Cada classe representa uma entidade relevante no contexto da aplicação, com seus respectivos atributos e métodos.

Figura 10 – Diagrama de classes



Fonte: Elaborado pelo autor.

A classe Orgao representa os entes públicos — federais, estaduais ou municipais — e encapsula a lógica de registro de despesas e de distribuição de valores entre os níveis de governo. Um órgão pode efetuar gastos dentro de sua própria esfera ou transferir valores para outros entes subordinados. Essas ações originam instâncias das classes Despesa e Distribuicao, que armazenam os dados das transações registradas na *blockchain*.

A classe Contrato representa o contrato inteligente implantado na *blockchain*, sendo responsável por armazenar e consultar os registros de forma imutável. Todas as despesas e

distribuições são persistidas por meio dessa classe, simulando a lógica de um contrato inteligente real.

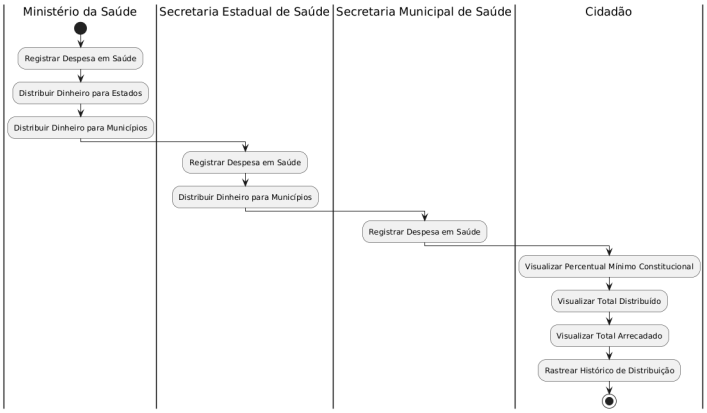
Já a classe Cidadao fornece funcionalidades de visualização pública, permitindo o acesso a informações como os percentuais constitucionais mínimos exigidos, os valores totais arrecadados e distribuídos, bem como o histórico completo das movimentações. Como os órgãos também acessam esses dados, a modelagem pressupõe que a classe Orgao herda os métodos da classe Cidadao, promovendo reutilização e clareza no desenho do protótipo.

Esse modelo favorece uma estrutura organizada, extensível e coerente com os princípios de rastreabilidade, representando fielmente o comportamento esperado do protótipo proposto.

4.5 Diagrama de Atividades

A Figura 11 apresenta o diagrama de atividades que ilustra o fluxo sequencial de execução no protótipo, representando as ações realizadas por cada ator conforme seu nível de governo.

Figura 11 – Diagrama de atividades



Fonte: Elaborado pelo autor.

O fluxo inicia-se no Ministério da Saúde, que, por ocupar a instância mais elevada da hierarquia federativa, pode tanto registrar despesas diretas no setor da saúde quanto realizar a distribuição de dinheiro público para os estados e municípios.

Na etapa seguinte, a Secretaria Estadual de Saúde recebe os valores transferidos da esfera federal, podendo registrar suas próprias despesas ou redistribuir os montantes para as secretarias municipais. Já no nível municipal, a Secretaria Municipal de Saúde é responsável exclusivamente pelo registro dos gastos diretos com saúde, utilizando os valores recebidos das instâncias superiores.

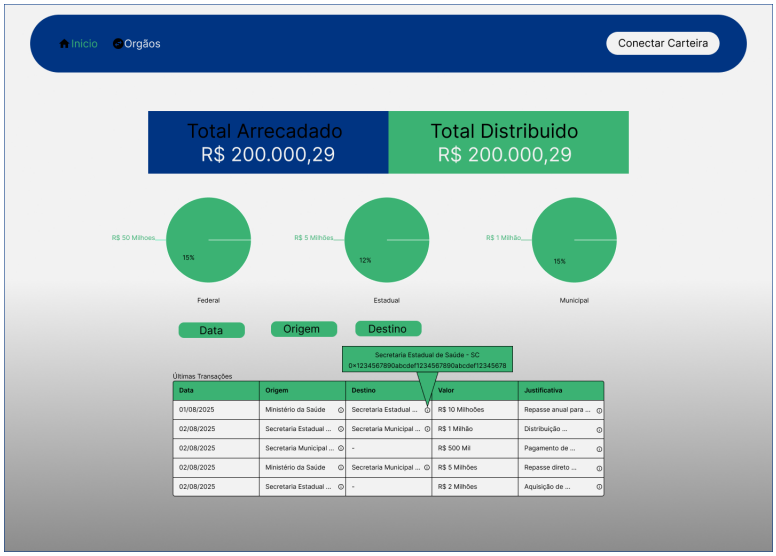
Por fim, o cidadão exerce seu papel de controle social utilizando o protótipo para visualizar os percentuais constitucionais mínimos exigidos, os montantes arrecadados e distribuídos, bem como rastrear o histórico completo das transferências e despesas.

Esse fluxo demonstra como os contratos inteligentes modelam a lógica hierárquica da gestão do dinheiro público, promovendo transparência, automação e rastreabilidade em todas as etapas do processo.

4.6 Interface do Protótipo: Visualização e Registro

A Figura 12 apresenta a interface inicial do protótipo, que funciona como a página principal acessível a qualquer usuário. Nessa tela, são exibidas informações consolidadas sobre o total arrecadado e distribuído, com ênfase nos dados do ano vigente. Um gráfico em formato de pizza ilustra a distribuição do dinheiro público entre os níveis federal, estadual e municipal. Logo abaixo, uma tabela dinâmica apresenta as transações registradas na *blockchain*, sejam elas referentes à distribuição de valores ou despesas diretas.

Figura 12 – Tela inicial de visualização dos dados



Fonte: Elaborado pelo autor.

Cada linha da tabela exibe a data da transação, o órgão responsável, o destinatário, o valor movimentado e a justificativa correspondente. Além disso, essa página centraliza a funcionalidade de rastreabilidade, permitindo ao usuário aplicar filtros por período, origem ou destino. Dessa forma, torna-se possível acompanhar de forma detalhada e segmentada o percurso do dinheiro público em cada esfera de governo.

A Figura 13 apresenta a interface de movimentação de valores, acessível apenas a usuários autenticados que representem órgãos públicos devidamente autorizados. Nessa tela, é possível registrar transações financeiras, como o repasse de valores para outro ente federativo ou o lançamento de uma despesa.

O formulário exige autenticação por meio de uma carteira digital, garantindo a validade da operação e a rastreabilidade do autor da transação. Os campos obrigatórios incluem o tipo de

Figura 13 – Tela de registros e distribuições

Fonte: Elaborado pelo autor.

movimentação, o endereço de destino, o valor a ser transferido e a justificativa da ação. Após o envio, os dados são transmitidos diretamente ao contrato inteligente correspondente, sendo armazenados na *blockchain* de forma imutável e auditável.

4.7 Considerações Finais da Modelagem

A modelagem apresentada neste capítulo permite compreender com clareza a estrutura e o funcionamento do protótipo de rastreabilidade proposto, destacando-se pela utilização de contratos inteligentes em uma arquitetura orientada à transparência e à automação das movimentações financeiras públicas.

Por meio dos diagramas desenvolvidos, foi possível ilustrar tanto os fluxos operacionais — como a distribuição de recursos, o registro de despesas e o rastreamento de transações — quanto a organização lógica do sistema em níveis federativos distintos. A utilização de filtros e permissões também foi cuidadosamente representada, garantindo flexibilidade de acesso e segurança no controle das ações realizadas pelos diferentes entes públicos.

A modelagem das interfaces reforça o caráter didático e acessível do protótipo, ao mesmo tempo em que sustenta a rastreabilidade técnica das informações.

Entretanto, é importante reconhecer que a modelagem apresentada possui algumas limitações, inerentes ao seu caráter conceitual. O protótipo foi projetado para fins ilustrativos e simulados, não estando integrado a sistemas oficiais de arrecadação, repasse ou auditoria de dados governamentais. Além disso, o uso de uma rede local e a ausência de dados reais de execução orçamentária limitam a representação de complexidades jurídicas, fiscais e operacionais envolvidas na aplicação de recursos públicos em larga escala. Essas restrições, no entanto,

não invalidam o valor do modelo, que cumpre o papel de demonstrar o potencial da tecnologia *blockchain* como ferramenta de transparência e controle social.

5 PROCEDIMENTOS METODOLÓGICOS

Este trabalho caracteriza-se como uma pesquisa aplicada, com abordagem qualitativa e desenvolvimento experimental, cujo objetivo principal é a construção de um protótipo funcional para rastrear a aplicação de dinheiro público utilizando tecnologia *blockchain*. O desenvolvimento do sistema será baseado em um conjunto de tecnologias consolidadas no ecossistema de aplicações descentralizadas.

Para a criação da interface do sistema, será utilizada a biblioteca *React*, escolhida por sua flexibilidade e ampla adoção no desenvolvimento de interfaces *web* modernas. A exibição de dados financeiros será complementada pela biblioteca *ECharts*, que possibilita a geração de gráficos interativos e responsivos.

A lógica dos contratos inteligentes será implementada em Solidity, linguagem padrão para plataformas compatíveis com a EVM. O ambiente *Remix IDE* será utilizado para a escrita, teste e implantação inicial desses contratos. Além disso, a biblioteca *OpenZeppelin* poderá ser empregada para garantir padrões seguros e auditados no desenvolvimento dos contratos.

Para simular uma rede *blockchain* local e validar o comportamento do sistema em um ambiente controlado, será utilizado o *Ganache*, ferramenta que permite testar transações e interações com contratos inteligentes de forma prática.

A integração entre a interface web e os contratos inteligentes será feita por meio da biblioteca *Ethers.js*, que facilita a comunicação com a *blockchain* e permite a execução de chamadas, transações e captura de eventos.

O controle de versionamento do projeto será realizado por meio da plataforma *GitHub*, possibilitando rastreamento das alterações, colaboração e organização durante todas as etapas do desenvolvimento.

A adoção dessa combinação de ferramentas visa garantir um ambiente de desenvolvimento eficiente, seguro e alinhado às boas práticas da engenharia de software aplicada a sistemas descentralizados.

CRONOGRAMA

QUADRO 1 – Cronograma de 02/2025 a 06/2025

Atividades	**Fev/2025**	**Mar/2025**	**Abr/2025**	**Mai/2025**	**Jun/2025**
Escolha do Tema e Orientador	X				
Elaboração do Pré-projeto	X				
Elaboração do Primeiro Capítulo		X	X		
Elaboração do Segundo Capítulo			X	X	
Elaboração do Terceiro Capítulo				X	
Modelagem do Protótipo de Pesquisa				X	
Entrega do Projeto de Pesquisa					X
Apresentação do Projeto de Pesquisa 1					X

Fonte: Elaborado pelo Autor (2025).

QUADRO 2 – Cronograma de 07/2025 a 12/2025

Atividades	**Jul/2025**	**Ago/2025**	**Set/2025**	**Out/2025**	**Nov/2025**	**Dez/2025**
Desenvolvimento do Contrato Inteligente	X	X	X	X		
Implementação da Interface Web	X	X	X	X		
Integração entre Web e Blockchain			X	X	X	
Testes Funcionais e Ajustes			X	X	X	
Documentação Técnica do Protótipo					X	X
Redação do TCC 2	X	X	X	X	X	X
Apresentação Final e Defesa						X

Fonte: Elaborado pelo autor.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 24 maio 2025.

____. **Emenda Constitucional nº 29, de 13 de setembro de 2000**. 2000. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc29.htm>. Acesso em: 24 maio 2025.

BYLUND, A. **What Is Blockchain?** 2025. Imagem retirada do site The Motley Fool. Disponível em: <https://www.fool.com/terms/b/blockchain/>. Acesso em: 30 mar. 2025.

CERTIK; OPENZEPPELIN; BITS, T. of. **Serviços e Auditorias de Smart Contract**. 2024. Disponível em: <https://www.certik.com/products/smart-contract-audit,https://milkroad.com/security/audit,https://security.blaize.tech/blog/top-smart-contracts-auditor>. Acesso em: 25 maio 2025.

DIRGANTARA, H. **What is Ethereum Virtual Machine?** 2023. Imagem retirada do site pintu. Disponível em: <https://pintu.co.id/en/academy/post/what-is-ethereum-virtual-machine#what-is-ethereum-virtual-machine>. Acesso em: 24 maio 2025.

ELIJONAS, M. **Operação investiga desvio de 1,4 bilhão no Dnocs da Bahia**. 2024. Disponível em: <https://www.cnnbrasil.com.br/nacional/operacao-investiga-desvio-de-r-14-bilhao-no-dnocs-da-bahia/>. Acesso em: 30 mar. 2025.

ETHEREUM; POLYGON; ARBITRUM; OPTIMISM; BUTERIN, V. **Documentação oficial das redes Ethereum, Polygon, Arbitrum, Optimism e artigo de Buterin**. 2024. Disponível em: <https://ethereum.org/en/layer-2/,https://wiki.polygon.technology/docs/overview/what-is-polygon/,https://docs.arbitrum.io/,https://community.optimism.io/docs/,https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698>. Acesso em: 17 maio 2025.

GOVBR. **Governo começa a utilizar o blockchain na emissão da Carteira de Identidade Nacional**. 2023. Disponível em: <https://www.gov.br/governodigital/pt-br/noticias/governo-comeca-a-utilizar-o-blockchain-na-emissao-da-carteira-de-identidade-nacional>. Acesso em: 30 mar. 2025.

KSHETRI, N.; ROGERS, R. **Blockchain-based property registries may help lift poor people out of poverty**. 2018. Disponível em: <https://theconversation.com/blockchain-based-property-registries-may-help-lift-poor-people-out-of-poverty-98796>. Acesso em: 31 maio 2025.

KUNTZ, J. **Blockchain Ethereum: fundamentos de arquitetura, desenvolvimento de contratos e aplicações**. Casa do Código, 2022. Disponível em: <https://www.casadocodigo.com.br/products/livro-blockchain-ethereum>. Acesso em: 30 abr. 2025.

RODRIGUES, C. K. d. S. Blockchain-based platform for managing patients' data in the public healthcare system of brazil. **Revista de Sistemas e Computação**, v. 11, n. 3, p. 63–72, 2021. Disponível em: <https://revistas.unifacs.br/index.php/rsc/article/view/7541>. Acesso em: 17 maio 2025.

SOUZA, C. **Blockchain: entenda de forma fácil o que é e como funciona**. 2025. Imagem retirada do site AreaBitcoin. Disponível em: <https://blog.areabitcoin.com.br/o-que-e-blockchain-e-como-funciona/>. Acesso em: 30 mar. 2025.

UOL. **Como funcionava o esquema bilionário de fraude no INSS**. 2025. Disponível em: <https://noticias.uol.com.br/ultimas-noticias/deutschewelle/2025/04/24/como-funcionava-o-esquema-bilionario-de-fraude-no-inss.htm>. Acesso em: 24 mai. 2025.

VALE, S. **Blockchain e Governos? Descubra como essa relação funciona!** 2020. Disponível em: <https://voitto.com.br/blog/artigo/aplicacao-blockchain-em-governos>. Acesso em: 30 mar. 2025.

ZIA, M.; WINTHER-TAMAKI, M.; KOVACS-GOODMAN, J.; SANCHES, B. H.; HARMALKAR, K. **Introdução à Blockchain para Governos Municipais**. ITS Rio – Instituto de Tecnologia e Sociedade, 2022. Disponível em: <https://itsrio.org/wp-content/uploads/2022/08/Introdu%C3%A7%C3%A3o-%C3%A0-Blockchain-para-Governos-Municipais.pdf>. Acesso em: 11 maio 2025.