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 ALGORITIMOS

LISTA DE QUADROS

LISTA DE SIGLAS

EVM Ethereum Virtual Machine.

LAI Lei de Acesso à Informação.

LGPD Lei de Geral de Proteção de Dados.

dApp Aplicações Descentralizadas.

SUMÁRIO

1 INTRODUÇÃO

A tecnologia blockchain tem se consolidado como uma ferramenta promissora para transformar diferentes setores da sociedade, incluindo saúde, logística, meio ambiente e, especialmente, a administração pública. Sua estrutura descentralizada e imutável oferece mecanismos eficazes para garantir a integridade, a rastreabilidade e a transparência de dados e transações, características fundamentais para enfrentar os desafios históricos de corrupção, má gestão e ineficiência no uso dos recursos públicos.

Apesar dos avanços institucionais em transparência, como o Portal da Transparência, Lei de Acesso à Informação (LAI) e a Lei de Geral de Proteção de Dados (LGPD), ainda existem obstáculos significativos para o acesso da população aos dados sobre a destinação e aplicação dos impostos arrecadados. A informação, quando disponível, muitas vezes é fragmentada, desatualizada ou apresentada de forma pouco intuitiva, dificultando o exercício do controle social. O problema se agrava em áreas críticas como a saúde, onde a falta de mecanismos de rastreabilidade em tempo real permite brechas para desvios de verbas, subutilização de recursos e ausência de responsabilização efetiva.

Diante desse cenário, será proposto o desenvolvimento de um protótipo de sistema blockchain com foco na rastreabilidade do dinheiro público aplicado na área da saúde. A solução utiliza contratos inteligentes para registrar, de forma automatizada e imutável, o caminho percorrido pelos recursos desde sua arrecadação até sua destinação final, permitindo que qualquer cidadão ou órgão de fiscalização acompanhe essas transações em tempo real. O uso de blockchain, nesse contexto, representa não apenas uma inovação tecnológica, mas uma proposta concreta de fortalecimento da democracia e da governança pública.

Para demonstrar a viabilidade dessa proposta, foi realizada uma revisão técnica e conceitual sobre o funcionamento da blockchain, suas aplicações no setor público e os benefícios e limitações da sua implementação. São discutidas as potencialidades dos contratos inteligentes na automação de regras de uso de recursos, bem como a comparação entre soluções baseadas na rede Ethereum e suas subcamadas. O trabalho também apresenta exemplos de uso da blockchain em governos ao redor do mundo e no Brasil, com destaque para experiências que evidenciam ganhos em transparência e eficiência.

Na etapa seguinte, é detalhado o processo de modelagem e desenvolvimento do protótipo proposto. São apresentados os elementos da arquitetura do sistema, as ferramentas utilizadas, as regras estabelecidas nos contratos inteligentes e as funcionalidades da interface web desenvolvida para permitir a visualização e o acompanhamento das movimentações financeiras simuladas. O protótipo busca ilustrar, de forma prática, como a tecnologia pode ser empregada para oferecer maior controle social sobre a aplicação de recursos públicos na saúde.

Com isso, este trabalho busca contribuir para a reflexão sobre o uso de tecnologias emergentes na promoção da transparência pública, propondo uma solução acessível, segura e auditável para o rastreamento do dinheiro público, com foco em uma área crítica 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 recurso, 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, permitindo que cidadãos e órgãos de controle acompanhem como os recursos arrecadados estão sendo aplicados. No entanto, muitos países ainda enfrentam dificuldades na rastreabilidade e fiscalização dos gastos governamentais.

Casos de corrupção envolvendo dinheiro público são recorrentes, afetando áreas cruciais como saúde, educação e infraestrutura. Em dezembro de 2024, uma operação revelou o desvio de

1,4 bilhão no Departamento Nacional de Obras Contra as Secas (Dnocs), onde uma organização criminosa utilizava empresas de fachada para fraudar contratos e lavar dinheiro (ELIJONAS, 2024). Este é apenas um exemplo de como a falta de rastreabilidade e de controle pode abrir espaço para esquemas fraudulentos.

A tecnologia blockchain surge como uma solução inovadora para esse problema, permitindo o registro descentralizado, transparente e imutável de todas as transações financeiras. Ao eliminar a necessidade de intermediários e possibilitar a auditoria pública de todas as transações, a blockchain contribui significativamente para reduzir os riscos de fraudes e corrupção, pois seus dados são inalteráveis e acessíveis de forma pública e segura.

Através de contratos inteligentes, o sistema automatiza a gestão e a distribuição dos fundos, garantindo que as regras estabelecidas para a utilização do dinheiro público sejam cumpridas sem interferências externas. Dessa forma, qualquer cidadão poderá acompanhar, em tempo real, a arrecadação e o destino dos recursos.

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 recursos 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 públicos.

2.1 Histórico do Blockchain

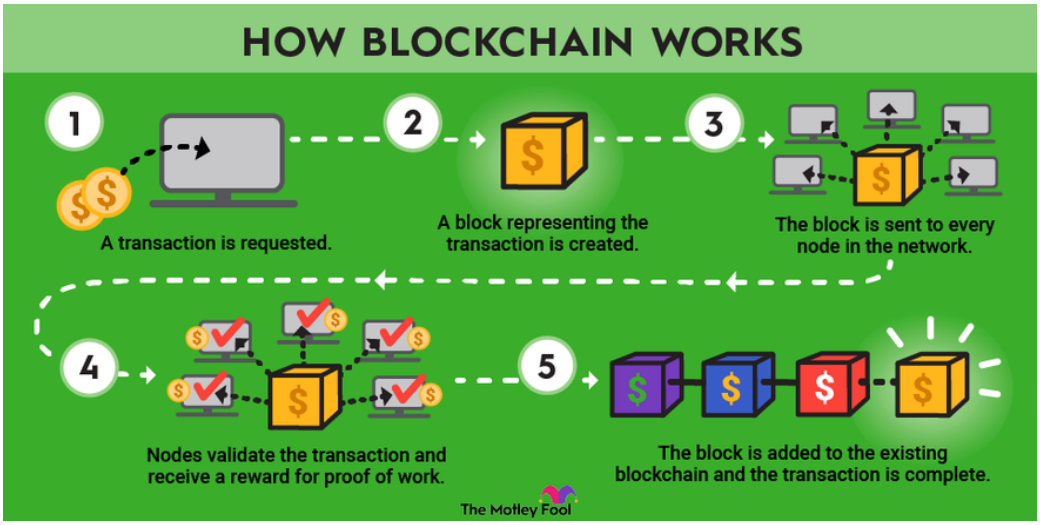
A ideia de blockchain começou a ser desenvolvida entre as décadas de 1980 e 1990, sendo oficialmente apresentada em 1991 por Stuart Haber e W. Scott Stornetta no artigo *How to Time-Stamp a Digital Document* (Como marcar a data e hora em um documento digital). O objetivo inicial era criar um método para 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.

Com o passar do tempo, o conceito de blockchain evoluiu para o que conhecemos atualmente como uma rede distribuída ponto a ponto (*peer-to-peer*), na qual múltiplos computadores (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 transações são registradas de forma permanente, encadeadas em blocos e disponibilizadas de maneira transparente para consulta.

A blockchain é formada por uma sequência de blocos encadeados que armazenam registros de transações, como ilustrado na Figura 1. 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 1 – Funcionamento da Blockchain



Fonte: (Fool, 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 prova de trabalho *proof-of-work*, um processo que requer grande capacidade computacional, chamado de mineração.

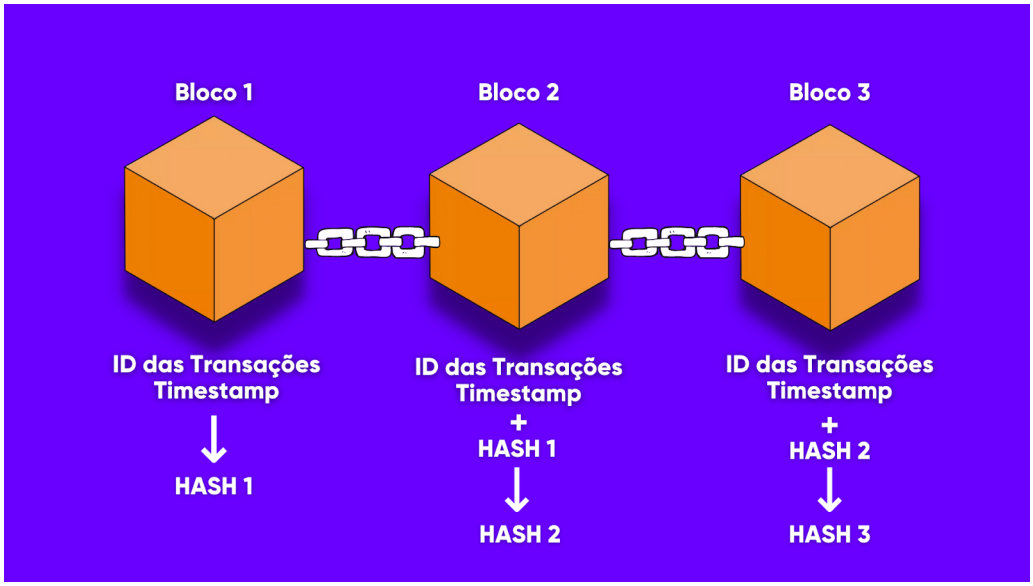
A segurança da blockchain aumenta à medida que mais nós (computadores) ingressam na rede, pois os dados ficam distribuídos de forma descentralizada, eliminando a existência de um ponto único de falha. Alterar qualquer informação em um bloco exigiria alterar todos os blocos subsequentes em todos os nós participantes, o que, na prática, torna a fraude praticamente inviável.

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 e privadas, como ilustrado na Figura 2. Com o tempo, a tecnologia se sofisticou e passou a ser utilizada para diversas aplicações, além das transações de criptomoedas, como o Bitcoin.

> 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).

Figura 2 – Funcionamento inicial da Blockchain



Fonte: (AreaBitcoin, 2025).

Uma das principais características da blockchain é sua imutabilidade. Uma vez que uma transação é registrada em um bloco e esse bloco é adicionado à cadeia, ela não pode ser alterada. Essa característica torna a blockchain uma tecnologia extremamente confiável para o armazenamento de dados importantes e críticos, uma vez que qualquer tentativa de modificação seria facilmente detectada.

A tecnologia blockchain está sendo progressivamente aplicada em diversos setores, com um exemplo notável sendo a indústria da saúde. Com o uso da blockchain, 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.

Além disso, a blockchain 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.

O funcionamento da blockchain pode ser comparado ao *BitTorrent* (protocolo de compartilhamento de arquivos ponto a ponto). Ambos operam em redes distribuídas ponto a ponto (*peer-to-peer*), 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.

2.2 Carteiras Digitais

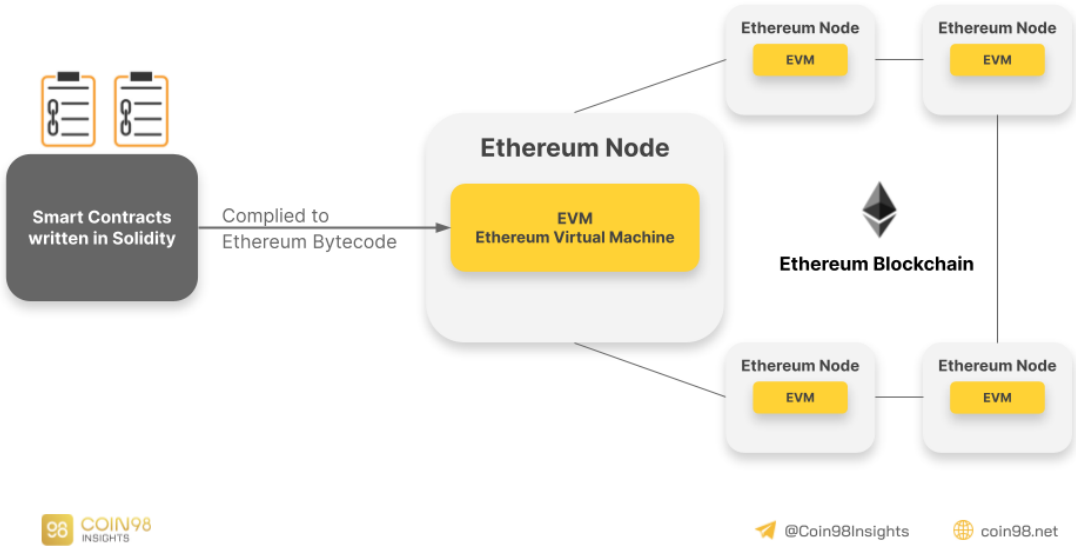
As contas na blockchain são associadas a uma chave pública e uma chave privada. A chave pública, muitas vezes chamada de *address* (endereço), é compartilhada com outros usuários e funciona como um identificador para a realização de transações. Já a chave privada, que deve ser mantida em segredo, funciona como uma senha que garante a segurança da conta, de maneira similar a uma senha bancária. Essas contas podem ou não conter criptomoedas, mas funcionam de forma análoga a uma conta bancária tradicional. A chave pública é essencial para realizar transações ponto a ponto (P2P) ou para interagir com contratos inteligentes (KUNTZ, 2022).

As contas na blockchain são associadas a um par de chaves criptográficas, uma chave pública e uma chave privada. A chave pública, frequentemente chamada de *address* (endereço), é compartilhada com outros usuários e funciona como um identificador único para a realização de transações. Já a chave privada deve ser mantida em sigilo absoluto, pois funciona como uma senha de acesso que permite autorizar movimentações e garantir a segurança da conta, de forma semelhante ao funcionamento de uma conta bancária tradicional. Essas contas podem ou não conter criptomoedas, mas são fundamentais para interagir com o ecossistema blockchain. Além de permitir transações ponto a ponto (P2P) e a execução de contratos inteligentes, as carteiras digitais também desempenham um papel importante na autenticação de usuários em aplicações descentralizadas, conhecidas como Aplicações Descentralizadas (dApp). Um dApp é um tipo de aplicação que opera sobre uma rede blockchain, onde a lógica de funcionamento geralmente implementada por meio de contratos inteligentes é descentralizada, transparente e imutável, eliminando a necessidade de servidores centrais ou intermediários. Dessa forma, a autenticação via carteira substitui modelos tradicionais de login, permitindo que o usuário se conecte diretamente ao dApp de forma segura e sem a necessidade de senhas centralizadas ou armazenamento de dados pessoais por terceiros

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 mundo da blockchain, permitindo a implementação das regras de negócios diretamente na blockchain, ao invés de serem centralizadas nos servidores da Web 2.0. Esse novo modelo descentralizado, característico da Web 3.0, faz com que as regras de negócios sejam programadas nos contratos inteligentes, que, além de salvar dados na blockchain, permitem consultas e a emissão de eventos de forma automatizada e sem a necessidade de intermediários. A seguir na Figura 3 é demostrado a estrutura da EVM.

Figura 3 – Estrutura da EVM



Fonte: (pintu, 2023).

Criada por Vitalik Buterin no início da década de 2010 e lançada em 2015, a Ethereum revolucionou o conceito de blockchain, introduzindo aspectos diferenciados no processo de geração de blocos. A blockchain da Ethereum pode ser vista como uma "máquina de estados baseada em transações"(KUNTZ, 2022), onde os blocos armazenam informações detalhadas, como: número do bloco, *timestamp* (marcação de tempo), lista de transações, minerador do bloco, recompensas, dificuldade de mineração, limites de gás e mais. Essas informações são fundamentais para garantir a integridade e a segurança da rede.

Cada bloco na Ethereum também contém três árvores de Merkle chamadas Merkle-Patricia Trees: stateRoot, transactionRoot e receiptsRoot. Essas estruturas são responsáveis por armazenar o estado atual da blockchain, as transações realizadas e os recibos das transações, garantindo tanto a eficiência quanto a integridade na verificação das transações.

A Ethereum utiliza uma unidade chamada *gas fee* (Taxa de Gás) para medir o esforço computacional necessário para realizar operações na rede. Cada transação ou execução de contrato inteligente exige uma quantidade específica de Gás, e os usuários pagam uma taxa para que suas operações sejam processadas. Quando dois blocos são gerados simultaneamente, o bloco com maior dificuldade acumulada é preferido pela cadeia, enquanto o bloco de menor número, chamado de "órfão", pode ser adicionado à cadeia com uma recompensa menor.

Além disso, a Ethereum deu origem a redes de segunda camada, como o Lightning Network, que oferecem transações mais rápidas e de baixo custo, solucionando algumas das limitações de escalabilidade da blockchain original.

Para criar contratos inteligentes, utiliza-se a EVM, uma máquina virtual que permite

a execução de contratos inteligentes. A EVM garante a *Turing Completeness* (completude de Turing), ou seja, sua capacidade de executar qualquer função computacional programável. Os contratos inteligentes são geralmente escritos em Solidity, uma linguagem específica para contratos inteligentes, que é compilada para bytecode e executada pela EVM, disponível em todos os nós da rede Ethereum.

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;
    }

    // Funcao para depositar Ether no contrato
    function depositar() public payable {
        // Qualquer pessoa pode depositar
        // Nenhuma logica adicional e necessaria aqui
    }

    // Funcao para sacar todo o saldo (apenas o dono)
    function sacar() public {
        require(msg.sender == dono, "Apenas o dono pode sacar.");
        payable(dono).transfer(address(this).balance);
    }

    // Funcao para consultar o saldo do contrato
    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 aplicações descentralizadas (dApps), ela ainda enfrenta desafios significativos relacionados à escalabilidade e ao custo das transações. Com o aumento da demanda, a camada principal da rede (Layer 1) frequentemente atinge sua capacidade máxima, o que resulta em altas taxas de transação (gas fees) e lentidão no processamento. Para mitigar esses problemas, surgiram as chamadas soluções de segunda camada (Layer 2), que são construídas sobre a Ethereum com o objetivo de aumentar a capacidade de processamento de transações, reduzir custos e melhorar a experiência do usuário, sem comprometer a segurança e a descentralização proporcionadas pela camada principal. Essas

soluções operam majoritariamente com transações fora da cadeia principal (off-chain), ou seja, são executadas em ambientes externos à blockchain principal e apenas registram o resultado final de forma resumida na rede principal (on-chain), o que proporciona maior eficiência. No contexto da blockchain, as operações on-chain são aquelas realizadas diretamente na rede, com registro permanente, imutável e público das transações, enquanto as operações off-chain ocorrem fora da blockchain e são posteriormente consolidadas ou referenciadas na cadeia principal, otimizando desempenho e reduzindo custos.

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 modelo otimista (Optimistic Rollups), em que se assume que as transações são válidas por padrão, permitindo contestações apenas quando necessário. Outra abordagem são as Sidechains, que consistem em blockchains paralelas à Ethereum. Elas mantêm compatibilidade com a Ethereum Virtual Machine (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 PoS, 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 – Comparativo entre Ethereum e Soluções de Segunda Camada (Layer 2)

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 (Gas)	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 DAO, ocorrido em 2016, que resultou na divisão da própria rede Ethereum em duas versões distintas: Ethereum e Ethereum Classic.

Além disso, a existência de vulnerabilidades no código dos contratos inteligentes é um problema recorrente, frequentemente decorrente de más práticas de desenvolvimento. Entre os exemplos mais comuns estão a ausência de definição adequada de visibilidade em funções e variáveis (SWC-100), o uso de compiladores com versões instáveis ou inseguras (conhecidos como floating pragmas), e a implementação de funções sensíveis, como selfdestruct(), sem os devidos controles de acesso. Tais falhas abrem espaço para ataques que, em muitos casos, não exigem técnicas complexas, sendo exploradas a partir de descuidos elementares por parte dos desenvolvedores.

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 e TRAIL OF BITS, 2024).

2.6 Considerações Finais

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 (Layer 2) 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 (SAVIO, 2020). No Brasil, outro avanço importante é o 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.

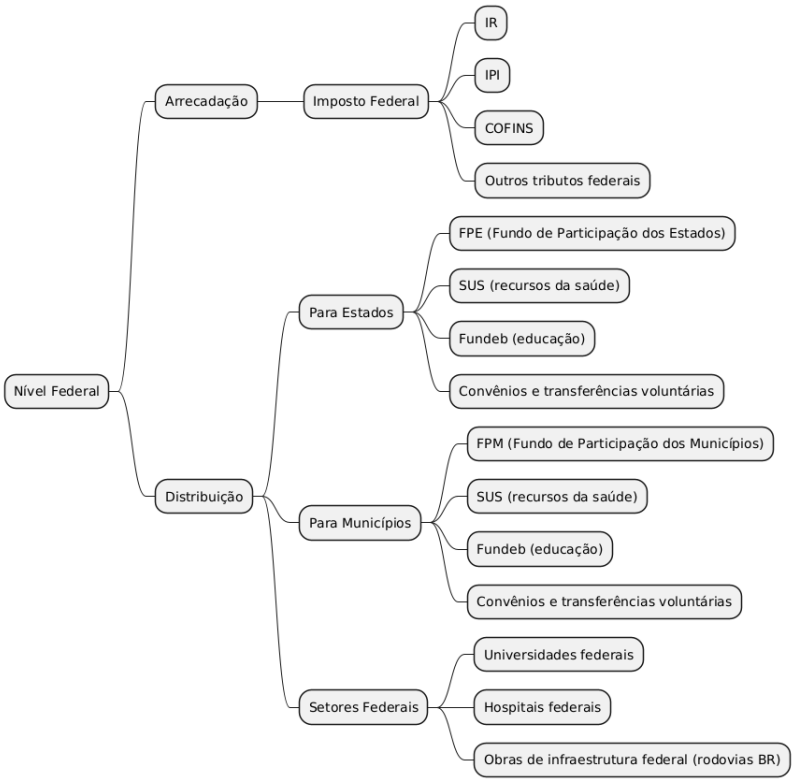
3.1 Arrecadação e Distribuição do Dinheiro Público no Brasil

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 de Qualquer Natureza (ISS) e o Imposto Predial e Territorial

Urbano (IPTU) (Brasil, 1988).

Figura 4 – Fluxo de arrecadação e distribuição de nível Federal

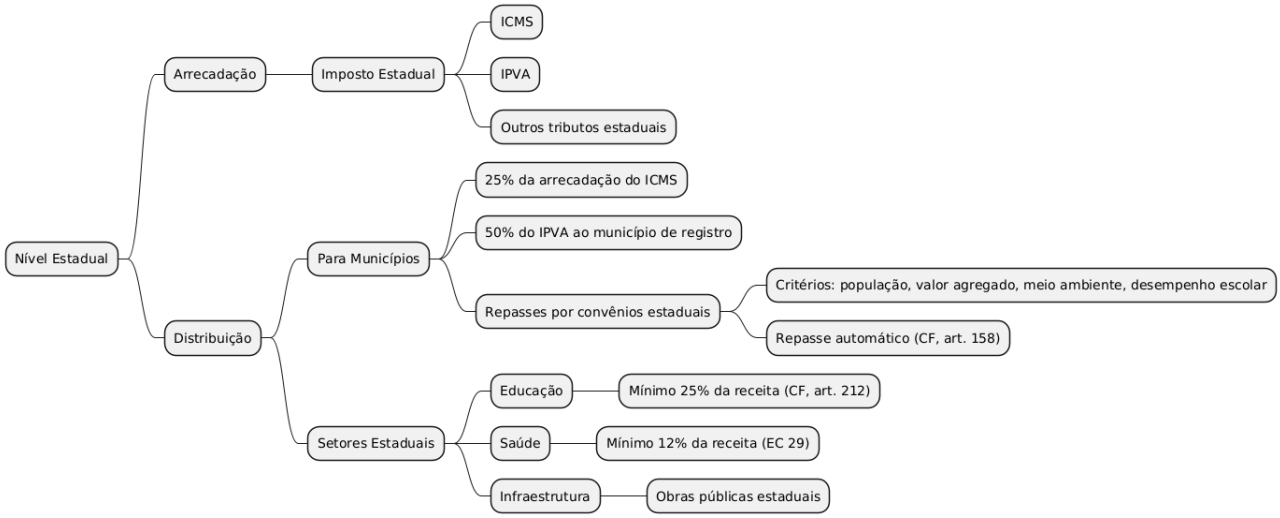


Fonte: Elaborado pelo autor.

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; entre outros (Brasil, 1988).

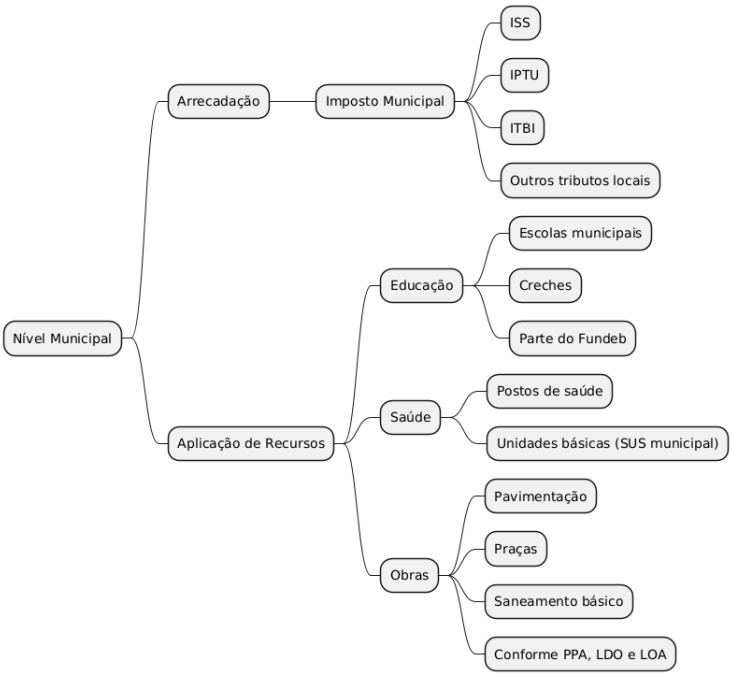
Além disso, a Constituição estabelece aplicações mínimas de recursos em setores essenciais. O artigo 212 determina que os Estados e os Municípios devem aplicar, anualmente, no mínimo 25% da receita resultante de impostos na manutenção e desenvolvimento do ensino (Brasil, 1988). O artigo 198, com a redação 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 Potencial de Aplicação da Blockchain na Gestão Pública

Um dos usos mais promissores da blockchain no setor público é na gestão de registros de propriedade de terras. Em muitos países em desenvolvimento, os sistemas existentes são frágeis, incompletos ou mesmo inexistentes, o que impede a comprovação legal da posse e prejudica o acesso a crédito e à proteção patrimonial (Kshetri; Rogers, 2018).

No Haiti, por exemplo, o terremoto de 2010 destruiu todos os registros físicos municipais, deixando milhares de agricultores sem documentação que comprovasse a posse das terras. Esse tipo de vulnerabilidade se repete em diversos contextos e compromete a segurança jurídica de milhões de famílias.

Estima-se que ativos sem documentação formal causem perdas econômicas globais da ordem de US$ 20 trilhões (Kshetri; Rogers, 2018). Diante disso, a blockchain surge como alternativa segura e transparente para registros de propriedade, já testada em países como Bermudas, Brasil, Geórgia, Gana, Honduras, Índia, Rússia e Ruanda.

Sistemas baseados em blockchain permitem a criação de registros imutáveis com histórico completo de transações, identificando autor, data e propósito de cada modificação. Isso reduz a possibilidade de fraudes e disputas judiciais. No Brasil, municípios como Pelotas (RS) e Morro Redondo vêm adotando a tecnologia para registrar dados como endereço, zoneamento, identidade do proprietário e coordenadas geográficas.

Além da segurança, a economia de custos também é significativa. Na Geórgia, a migração do registro fundiário para a blockchain reduziu taxas de até US$ 200 para valores tão baixos quanto US$ 0,10 (Kshetri; Rogers, 2018).

No entanto, a tecnologia não resolve, sozinha, todos os desafios. É necessário garantir a qualidade e legitimidade dos dados inseridos, além de enfrentar resistências políticas por parte de agentes que veem a transparência como uma ameaça (Kshetri; Rogers, 2018).

Quando implementada com critérios de justiça e imparcialidade, a blockchain pode representar o primeiro acesso real e legal à propriedade para populações marginalizadas, rompendo ciclos históricos de exclusão e vulnerabilidade.

Conforme destacam Zia et al. (2022), sistemas públicos de registro baseados em blockchain geram um log de auditoria imutável, com assinaturas criptográficas que permitem identificar e responsabilizar funcionários por alterações fraudulentas.

3.3 Exemplos Reais de Falta de Rastreabilidade no Brasil

A ausência de sistemas eficientes de rastreabilidade financeira no setor público brasileiro tem contribuído para diversos casos de corrupção. Um exemplo emblemático ocorreu em 2024, quando uma operação revelou o desvio de R$ 1,4 bilhão no Departamento Nacional de Obras Contra as Secas (Dnocs). Empresas de fachada foram utilizadas para fraudar contratos e lavar dinheiro público (ELIJONAS, 2024).

Casos como esse evidenciam a importância de soluções que possibilitem o acompanhamento detalhado da movimentação dos recursos desde sua origem. Um sistema baseado em blockchain permitiria que essas transações fossem registradas de forma transparente, dificultando a ocultação de irregularidades e facilitando a atuação de órgãos fiscalizadores e da própria sociedade civil.

Entre 2019 e 2024, o Instituto Nacional do Seguro Social (INSS) foi alvo de um esquema fraudulento que resultou em prejuízos estimados em R$ 6,3 bilhões. O esquema envolvia entidades de classe, como associações e sindicatos, que realizavam descontos mensais nos benefícios de aposentados e pensionistas sem a devida autorização.

Essas entidades alegavam oferecer serviços como assessoria jurídica, convênios com academias e planos de saúde. No entanto, a maioria dos beneficiários não reconhecia ou autorizava tais descontos. Uma pesquisa realizada pela Controladoria-Geral da União (CGU) revelou que 97% dos aposentados e pensionistas entrevistados afirmaram não ter autorizado os descontos em seus benefícios.

Para viabilizar os descontos, as entidades firmavam Acordos de Cooperação Técnica (ACT) com o INSS, permitindo que os valores fossem debitados diretamente na folha de pagamento dos beneficiários. Entretanto, muitas dessas entidades não possuíam a estrutura necessária para oferecer os serviços prometidos e, em alguns casos, utilizavam documentos falsificados para simular autorizações.

A Operação Sem Desconto, deflagrada pela Polícia Federal em abril de 2025, cumpriu 211 mandados de busca e apreensão e seis de prisão temporária em 13 estados e no Distrito Federal. Durante a operação, foram apreendidos veículos de luxo, joias e dinheiro em espécie. O então presidente do INSS, Alessandro Stefanutto, foi afastado do cargo em meio às investigações.

O escândalo levou o governo federal a suspender todos os convênios do tipo e a implementar medidas para ressarcir os beneficiários afetados. Além disso, o caso gerou repercussões políticas, com pedidos de investigação e a criação de comissões parlamentares para apurar as responsabilidades (UOL, 2025).

3.4 Desafios na Distribuição de Recursos Durante a Pandemia da COVID-19

A pandemia da COVID-19 evidenciou fragilidades nos mecanismos tradicionais de distribuição de recursos públicos. Governos em todo o mundo tiveram que implementar, com urgência, programas de transferência de renda para mitigar os impactos sociais e econômicos da crise sanitária.

No Brasil, o Auxílio Emergencial contemplou cerca de 66 milhões de pessoas, com um total de R$ 280 bilhões pagos até o final de 2020 — equivalente a aproximadamente 4% do PIB (Zia et al., 2022). Apesar da magnitude da operação, o programa enfrentou entraves operacionais devido à burocracia e à ausência de cadastros atualizados, o que resultou na exclusão de beneficiários legítimos e em atrasos nos repasses.

Além disso, recursos destinados a regiões vulneráveis muitas vezes foram gastos em municípios mais ricos ou em grandes redes varejistas, o que reduziu o impacto positivo nas economias locais.

3.5 Blockchain como Solução Tecnológica Viável

Frente a esses desafios, a blockchain desponta como solução para sistemas de benefícios mais eficientes, auditáveis e transparentes. Por meio de registros públicos imutáveis, os governos podem rastrear em tempo real como, onde e por quem os recursos estão sendo utilizados.

Uma aplicação prática no Brasil é a moeda social Mumbuca, do município de Maricá (RJ). Por meio de uma criptomoeda local, os repasses são controlados para incentivar o consumo regional e garantir que o benefício chegue ao seu destino previsto (Zia et al., 2022).

Tais sistemas podem ser otimizados com contratos inteligentes (smart contracts), que automatizam regras de uso. Por exemplo, uma moeda digital pode ser programada para ser utilizada apenas em estabelecimentos locais ou para recompensar práticas sustentáveis, integrando políticas públicas de maneira eficaz.

Exemplos internacionais reforçam esse movimento: a FairCoin (Espanha), a Moneda PAR (Argentina) e a Sarafu (Quênia) demonstram como moedas digitais locais promovem inclusão econômica, resiliência e desenvolvimento sustentável, sobretudo em cenários de crise.

3.6 Aplicações da Blockchain na Saúde Pública: Trabalhos Relacionados e Transparência nos Dados

Diversas pesquisas recentes têm se dedicado a investigar 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 desenvolvida por (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 da proposta reside no desafio enfrentado pelo sistema público de saúde brasileiro, que precisa atender uma população de mais de 214 milhões de habitantes distribuídos por um território continental. Atualmente, os dados clínicos estão fragmentados entre diferentes unidades de saúde, sem uma integração eficiente e com sérias limitações quanto à segurança, escalabilidade e rastreabilidade.

O trabalho reconhece que os prontuários em papel ainda são comuns, embora exista um esforço crescente de informatização. Contudo, mesmo os registros eletrônicos, quando utilizados, permanecem isolados em sistemas locais, o que impede a construção de uma base de dados 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 atualmente dependem, em muitos casos, apenas de senhas simples para controle de acesso, sem proteção criptográfica

avançada. Além disso, o paciente não possui controle efetivo sobre a divulgação de seus dados médicos, o que viola princípios estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD).

Para enfrentar essas limitações, (Rodrigues, 2021) propõe uma arquitetura distribuída baseada em blockchain, composta por três componentes principais: as unidades de saúde, uma rede de 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 aos dados são controlados por autoridades de saúde. O modelo contempla não apenas a criação e atualização dos prontuários, mas também sua recuperação e auditoria, com operações todas registradas em blocos imutáveis. O uso do algoritmo de consenso PBFT (Practical Byzantine Fault Tolerance) foi escolhido por seu equilíbrio entre segurança e desempenho, especialmente em redes com até 200 nós — número compatível com as unidades federativas do Brasil.

A avaliação teórica da proposta foi feita por meio de modelagem analítica, com o uso de teoria de filas para simular o tempo de resposta das transações e o impacto de diferentes topologias de rede. Os resultados indicam que, mesmo em cenários de falha parcial dos mineradores, o sistema mantém níveis aceitáveis de desempenho. Do ponto de vista da escalabilidade, estimou-se que a plataforma poderia absorver mais de 1,4 bilhão de visitas anuais ao SUS sem comprometer sua estabilidade. Em relação ao custo, mesmo considerando o crescimento exponencial da base de dados até 2030, o impacto financeiro da implementação da plataforma seria inferior a 1% do orçamento anual do Ministério da Saúde, o que reforça a viabilidade econômica do projeto.

Do ponto de vista da transparência, a plataforma proposta representa um avanço significativo. Todas as ações realizadas sobre os prontuários ficam registradas de forma imutável, permitindo o rastreamento completo do ciclo de vida de cada informação. Isso não apenas facilita auditorias e investigações, como também fortalece o controle social sobre a gestão pública da saúde. A confidencialidade dos dados é assegurada por criptografia de chave pública, e o acesso só é permitido mediante autorização do paciente, respeitando os princípios da LGPD e ampliando a proteção dos direitos individuais.

Essa proposta se destaca no estado da arte justamente por ser uma das poucas voltadas especificamente à realidade do SUS. Enquanto a maior parte dos estudos se refere a ambientes hospitalares privados ou a sistemas internacionais, a plataforma de Rodrigues visa integrar diferentes unidades de saúde do sistema público brasileiro, considerando suas particularidades operacionais e institucionais. Ainda que se trate de um modelo conceitual, a pesquisa oferece uma base sólida de conhecimento técnico e experimental que pode orientar o desenvolvimento de soluções reais nos próximos anos. Assim, fica evidente 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.

A COVID-19 também evidenciou limitações dos sistemas públicos de saúde, especialmente no gerenciamento de vacinas. Um caso emblemático é o sistema VAMS, dos EUA, que mesmo com investimento de US$ 44 milhões, apresentou falhas como previsão incorreta de

estoques, vulnerabilidades de segurança e ineficiência nos agendamentos (Zia et al., 2022).

Em geral, os dados de saúde pública são fragmentados entre diversas instituições e expostos a riscos de manipulação, dificultando a rastreabilidade e a resposta eficiente a crises sanitárias.

A blockchain oferece uma alternativa segura e descentralizada, com registros imutáveis e auditáveis, que podem ser acessados 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:

- Estônia: desde 2008 utiliza a infraestrutura KSI Blockchain, com validações criptográficas para proteger dados públicos;
- Reino Unido: utilizou sensores conectados à blockchain para monitorar, em tempo real, a temperatura de armazenamento das vacinas;
- Coreia do Sul (Ilha de Jeju): adotou um sistema baseado em blockchain para rastrear contatos de turistas, com foco na privacidade e no controle epidemiológico;

3.7 Impactos Sociais e Econômicos da Blockchain na Administração 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.

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.

3.8 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 a modelagem do protótipo proposto para rastreabilidade da aplicação de dinheiro públicos no setor da saúde, utilizando contratos inteligentes em uma rede blockchain. A modelagem visa representar, de forma sistemática e visual, a estrutura lógica, os fluxos de operação e a interação entre os principais componentes do sistema.

Para isso, foram utilizados diversos diagramas, como mindmaps, casos de uso, atividades, classes, arquitetura e interfaces visuais, com o objetivo de traduzir o funcionamento do protótipo em representações compreensíveis e alinhadas aos padrões de engenharia de software. Esses modelos auxiliam na compreensão do comportamento dos contratos inteligentes em cada nível de governo (federal, estadual e municipal), além de evidenciar a separação de responsabilidades, os processos de distribuição e gasto dos recursos, a visualização pública dos dados e o controle de permissões.

A escolha por uma arquitetura escalável e modular também é apresentada neste capítulo, com foco na possibilidade de expansão futura para outros setores além da saúde, como educação e infraestrutura. O conjunto de diagramas modelados fornece as bases para a implementação funcional do sistema e garante a rastreabilidade, transparência e segurança no uso do dinheiro públicos.

4.1 Mapa Mental sobre o Fluxo de Aplicação

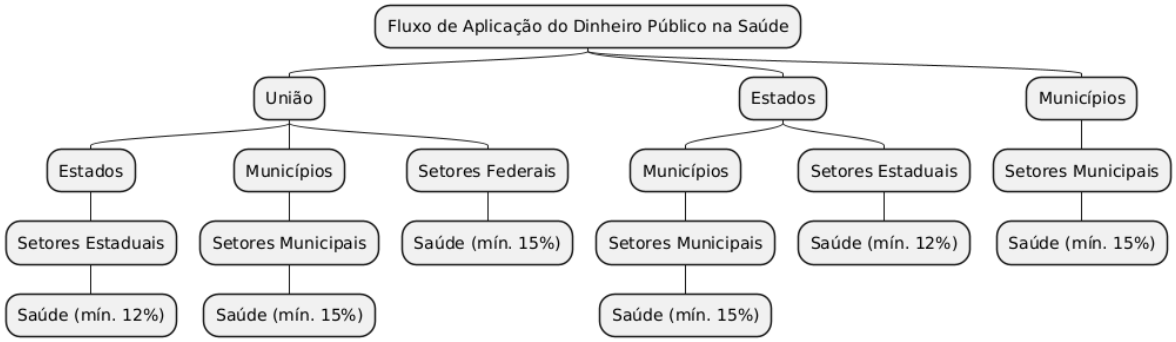
Para facilitar a compreensão da lógica e da estrutura dos contratos inteligentes que compõem o protótipo proposto, elaborou-se um diagrama de mindmap (mapa mental) que representa, de forma visual e hierárquica, o fluxo de execução dos contratos nos três níveis de governo: federal, estadual e municipal. Esse diagrama foi desenvolvido com o objetivo de complementar os diagramas tradicionais da UML — como os de casos de uso e classes — oferecendo uma visão mais intuitiva e exploratória da automação dos processos de distribuição e aplicação do dinheiro público na 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. Referente à Figura 7, observa-se o diagrama de mindmap representando a modelagem desses contratos inteligentes nos três níveis de governo.

Cada nível governamental possui seu próprio contrato inteligente, responsável por ações como recebimento de recursos, definição do destino, execução dos gastos e 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.

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

Figura 7 – Fluxo detalhado do dinehiro público nos contratos inteligentes



Fonte: Elaborado pelo autor.

recursos públicos, permitindo uma simulação mais fiel e educativa do funcionamento do sistema 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

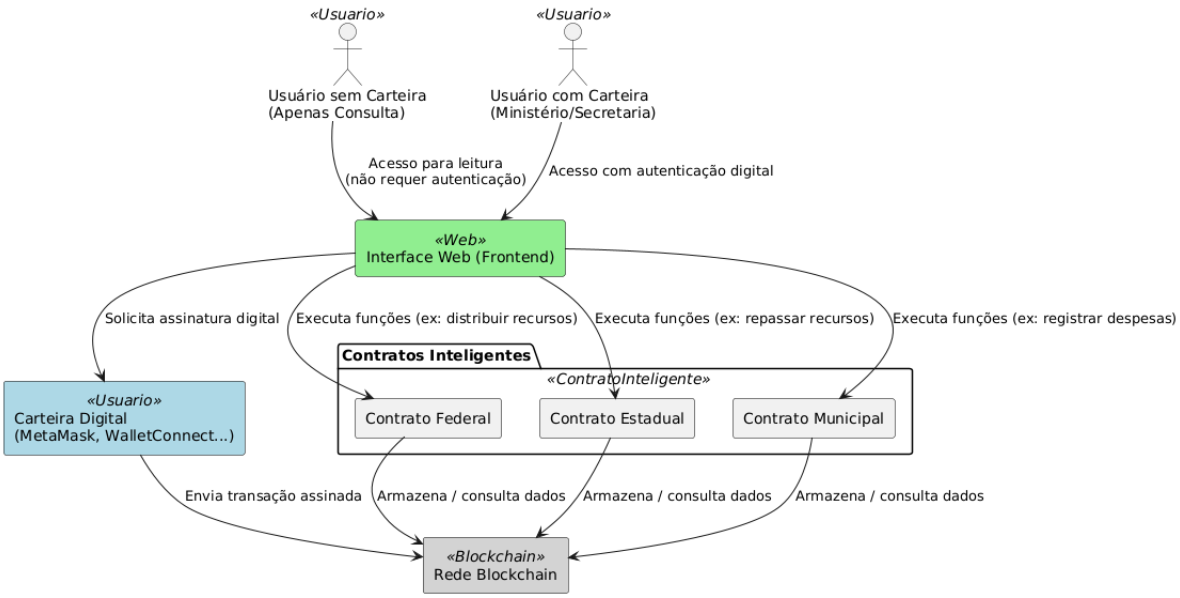
A arquitetura do protótipo foi concebida com foco em escalabilidade e modularidade, permitindo a futura expansão para outros setores além da saúde, como educação e infraestrutura, que possuem regras específicas de distribuição de recursos entre os níveis federal, estadual e municipal. A estrutura modular facilita o reaproveitamento da lógica de contratos inteligentes e a adição de novos módulos sem impacto significativo no sistema existente.

O acesso à aplicação é feito por meio de uma interface web, que permite tanto a consulta pública de dados, quanto a interação transacional com os contratos inteligentes. 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 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 recursos, devem se conectar à aplicação utilizando uma carteira digital compatível com a blockchain, como MetaMask ou WalletConnect. 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.

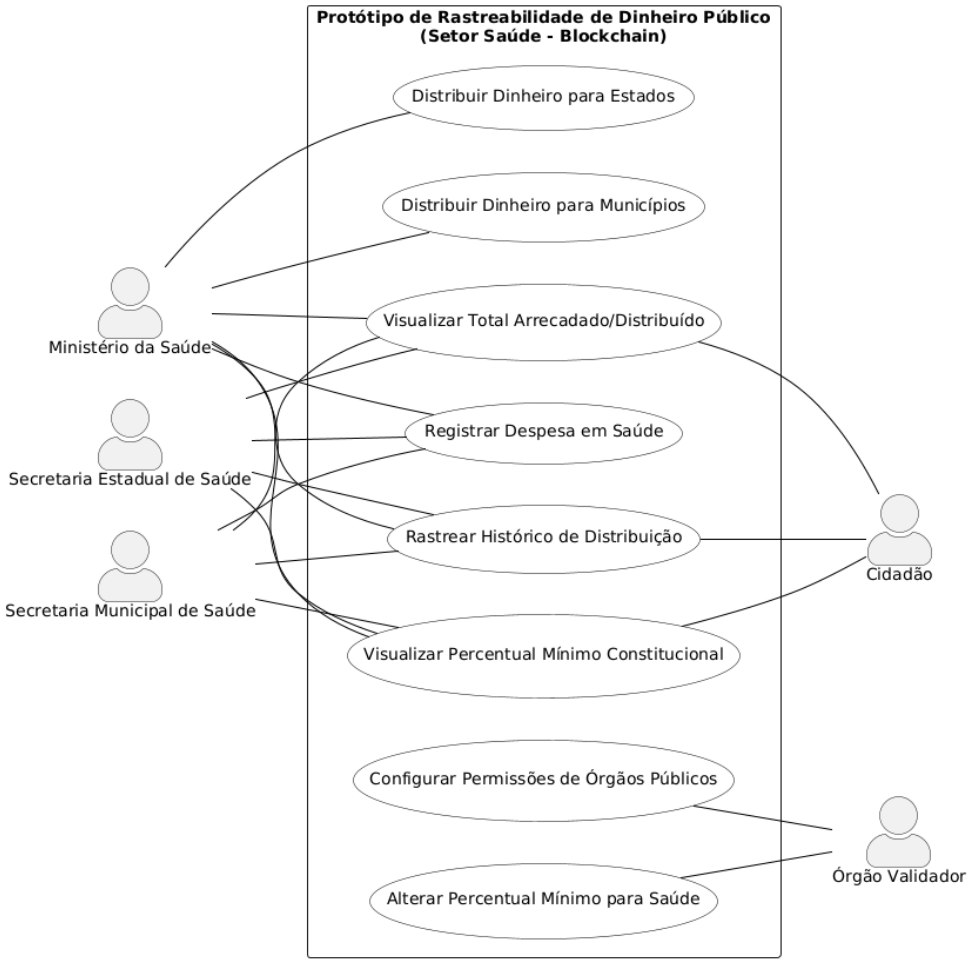
4.3 Casos de uso

O diagrama de casos de uso apresentado na Figura 9 descreve as funcionalidades disponíveis no protótipo de rastreabilidade para os diferentes atores do protótipo, conforme o seu papel no modelo federativo. Cada ator interage com o sistema por meio de ações específicas que refletem sua competência legal na distribuição e aplicação de dinheiro públicos voltados à saúde.

Órgãos públicos, como o Ministério da Saúde, as Secretarias Estaduais e Municipais, podem realizar distribuições de recursos para entes subordinados ou registrar despesas diretamente, conforme seu nível de atuação. Esses órgãos também possuem acesso às funcionalidades de rastreamento e visualização das informações armazenadas na blockchain, como os percentuais mínimos constitucionais exigidos, o total arrecadado e distribuído, e o histórico de movimentações. Cidadãos, por sua vez, têm acesso restrito à consulta desses dados, promovendo o controle social e a transparência pública.

Além dessas funcionalidades, o diagrama também contempla dois casos de uso essenciais para a operação segura e configurável do sistema: a configuração de permissões para os ministérios e secretarias autorizadas a operar com os contratos inteligentes; e a possibilidade de alterar os percentuais mínimos de destinação de recursos à saúde, garantindo aderência às legislações vigentes ou a novas normativas, quando necessário. Essas ações estão reservadas a um órgão validador responsável por credenciar os demais agentes públicos e parametrizar o comportamento do sistema.

Figura 9 – Diagrama de Casos de Uso



Fonte: Elaborado pelo autor.

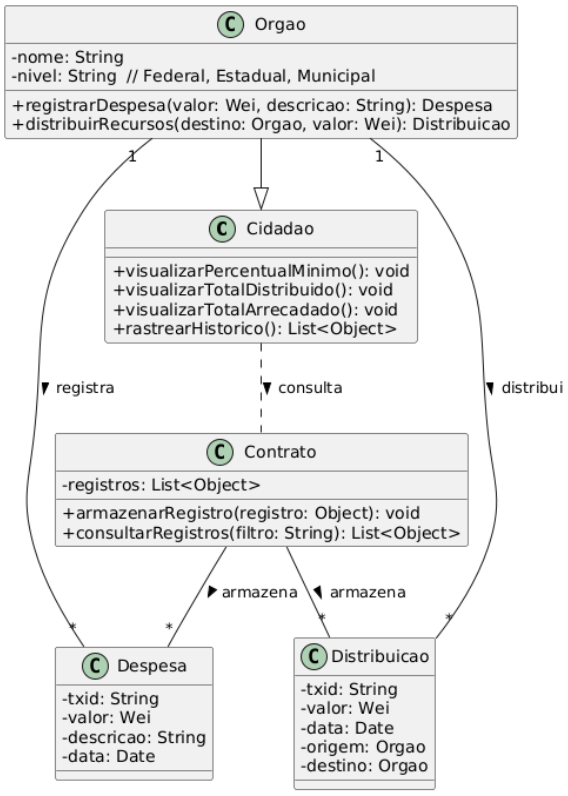
4.4 Diagrama de Classes

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

A classe Orgao representa os entes públicos (federal, estadual ou municipal) e encapsula a lógica de registro de despesas e distribuição de recursos entre os níveis de governo. Um órgão pode realizar várias despesas dentro do seu próprio nível, ou repassar recursos para outros órgãos subordinados. Essas ações geram instâncias das classes Despesa e Distribuicao, que armazenam os dados das transações registradas na blockchain, incluindo valores, datas, identificadores e descrições.

A classe Contrato representa o contrato inteligente implantado na blockchain, responsável por armazenar e consultar os registros de forma imutável. Todas as despesas e distribuições são persistidas por meio dessa classe, que simula a lógica de um smart contract real. A classe

Figura 10 – Diagrama de Classes



Fonte: Elaborado pelo autor.

Cidadao, por sua vez, oferece funcionalidades de visualização pública, permitindo acessar os dados registrados, como percentuais mínimos constitucionais, totais arrecadados e distribuídos, além do histórico completo das movimentações. Como os órgãos também têm acesso a essas informações, a modelagem pressupõe que Orgao herda os métodos de Cidadao, promovendo o reuso e a clareza sem redundância.

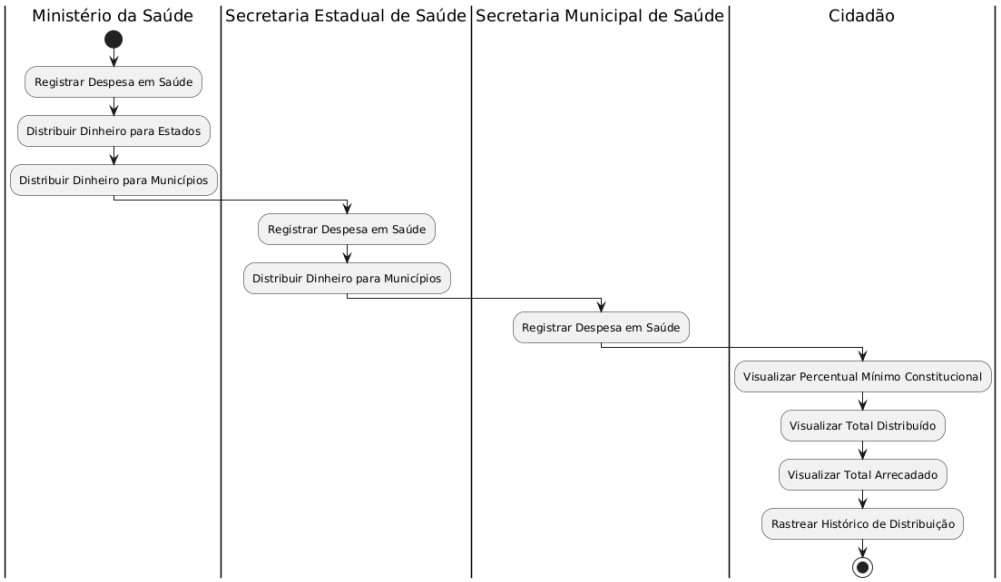
Esse modelo permite uma estrutura clara, extensível e alinhada aos princípios da rastreabilidade, refletindo fielmente o comportamento esperado do protótipo proposto.

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 governamental. O fluxo inicia-se no Ministério da Saúde, que, por deter a instância mais alta na hierarquia federativa, pode tanto registrar despesas diretas no setor da saúde quanto realizar distribuições de recursos para estados e municípios.

Na sequência, a Secretaria Estadual de Saúde recebe os recursos transferidos da esfera federal, podendo também registrar suas próprias despesas em saúde ou redistribuir os valores para as secretarias municipais. Já no nível municipal, a Secretaria Municipal de Saúde é responsável

Figura 11 – Diagrama de Atividades



Fonte: Elaborado pelo autor.

exclusivamente por registrar os gastos diretos com saúde, aplicando os recursos recebidos dos níveis superiores.

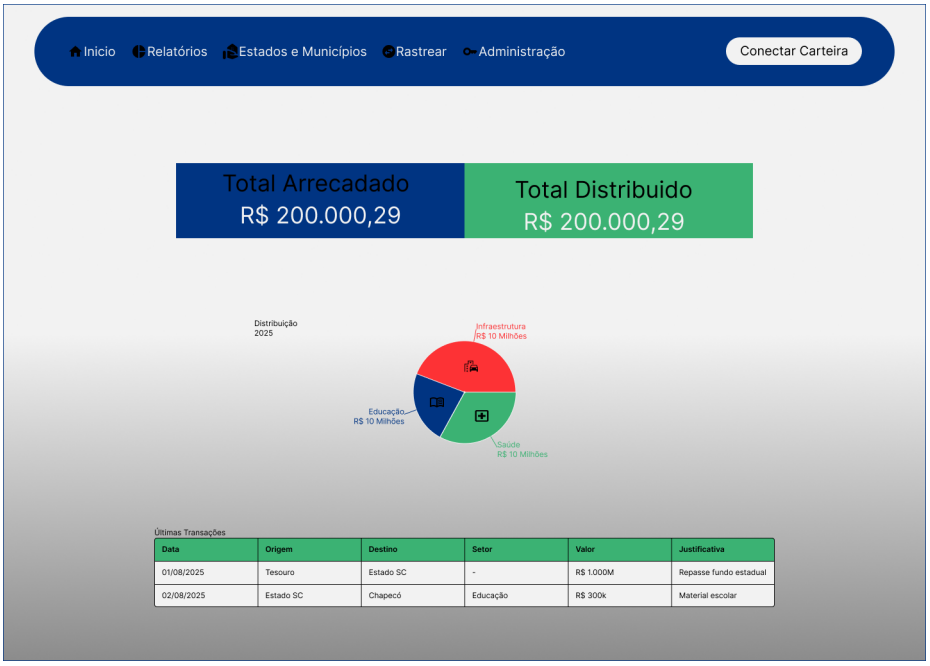
Por fim, o cidadão exerce um papel de controle social, utilizando o sistema para visualizar os percentuais mínimos constitucionais, os valores arrecadados e distribuídos, além de rastrear o histórico completo das transferências e gastos. Esse fluxo demonstra como os contratos inteligentes modelam a lógica hierárquica da gestão pública de recursos, promovendo transparência, automação e rastreabilidade em todas as etapas.

4.6 Telas do prototipo

A Figura 12 apresenta a interface inicial do protótipo, que atua como a página principal acessível a qualquer usuário, inclusive sem autenticação. Nessa tela, são exibidas informações consolidadas sobre o total arrecadado e distribuído no setor da saúde, com destaque para o ano vigente. Um gráfico em formato de pizza demonstra a proporção dos recursos já distribuídos entre os níveis federal, estadual e municipal, enquanto uma tabela exibe as últimas cinco transações registradas, sejam elas distribuições ou gastos. Cada linha da tabela inclui o órgão que realizou a ação, o destino, o valor movimentado, a justificativa e a data da transação. Além disso, essa página também permite realizar o rastreamento completo dos dados por meio de filtros dinâmicos, possibilitando a seleção por órgão específico, nível de governo, data de transação, origem ou destino, facilitando a visualização das informações conforme a necessidade do usuário.

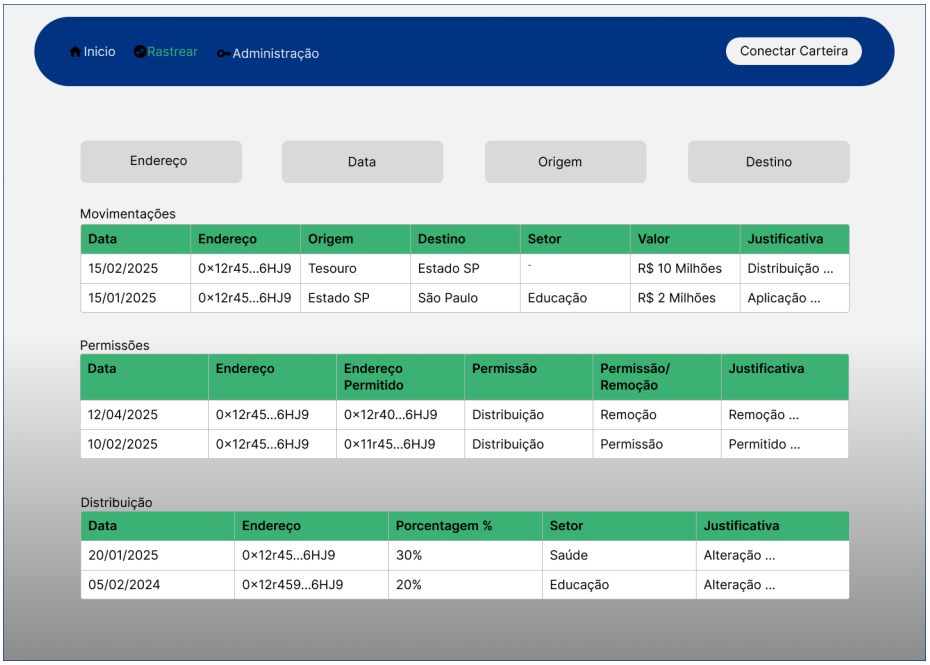
Na Figura é modelada a interface de movimentação de recursos, voltada exclusivamente para usuários autenticados que representam órgãos públicos autorizados. Nessa tela, é possível

Figura 12 – Página inicial



Fonte: Elaborado pelo autor.

Figura 13 – Página de rastreamento



Fonte: Elaborado pelo autor.

registrar novas transações, como o repasse de recursos para outro nível de governo ou o registro de uma despesa em saúde. O formulário de movimentação exige a autenticação via carteira digital, garantindo a integridade da ação e a rastreabilidade da origem da transação. Os campos

obrigatórios incluem o endereço de destino, valor, tipo de movimentação (gasto ou repasse), justificativa e data. Essa interface é responsável por acionar os contratos inteligentes correspondentes e registrar os dados diretamente na blockchain.

A Figura 14 apresenta a tela de configuração de permissões do sistema, destinada ao órgão validador responsável pela governança e controle de acesso dos demais órgãos públicos. Nessa tela, é possível gerenciar as permissões de distribuição de recursos e registro de despesas para cada ente federativo, permitindo aprovar, revogar ou modificar acessos. A interface inclui uma tabela com os registros de permissões concedidas ou revogadas, indicando o endereço do órgão, o nível de governo, a justificativa da alteração, a data da modificação e o agente responsável pela mudança. Além disso, essa tela também permite configurar ou alterar os percentuais mínimos constitucionais de aplicação na saúde, conforme previsto por lei. Essas configurações são registradas na blockchain e respeitam os critérios legais de cada nível federativo.

4.7 Conseiderações finais

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. Com base nesse conjunto de representações, o próximo capítulo apresenta a implementação prática do protótipo, transformando os modelos conceituais aqui descritos em funcionalidades reais, testáveis e auditáveis.

5 PROCEDIMENTOS METODOLÓGICOS

Além da fundamentação teórica e da modelagem proposta, o desenvolvimento do protótipo será realizado com base em um conjunto de tecnologias específicas adequadas ao ecossistema blockchain e à construção de aplicações descentralizadas. Para a criação da interface do sistema, será utilizada a biblioteca React, devido à sua flexibilidade e ampla adoção no desenvolvimento de interfaces web modernas. A lógica dos contratos inteligentes será programada em Solidity, linguagem padrão para a EVM, com apoio do ambiente de desenvolvimento Remix IDE, que permitirá a escrita, testes e implantação dos contratos em ambiente de desenvolvimento. Para a simulação de uma blockchain local e validação do comportamento do sistema em um ambiente controlado, será utilizado o Ganache, ferramenta que simula uma rede Ethereum local com suporte a múltiplas contas e transações. A integração entre a interface em React e os contratos inteligentes será realizada por meio da biblioteca ethers.js, que facilita a comunicação com a blockchain e permite a realização de chamadas, transações e eventos. O uso de bibliotecas auxiliares como a OpenZeppelin também será considerado, especialmente para a implementação de contratos seguros e auditáveis, uma vez que ela fornece padrões amplamente aceitos e testados para contratos Solidity. Para a visualização de informações financeiras de forma clara e interativa, a biblioteca ECharts será utilizada na geração de gráficos dinâmicos e responsivos dentro da interface. O controle de versionamento e colaboração do código será gerenciado por meio da plataforma GitHub, permitindo a rastreabilidade das alterações e facilitando a organização do projeto durante todas as etapas do desenvolvimento. Essa combinação de ferramentas visa garantir um ambiente de desenvolvimento eficiente, seguro e alinhado às boas práticas da engenharia de software para aplicações descentralizadas.

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

AREABITCOIN. **Blockchain: entenda de forma fácil o que é e como funciona**. 2025. Acesso em: 30 mar. 2025. Disponível em: <https://blog.areabitcoin.com.br/o-que-e-blockchain-e-como-funciona/>.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. 1988. <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. <https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc29.htm>. Acesso em: 24 maio 2025.

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

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

ETHEREUM; POLYGON; ARBITRUM; OPTIMISM; BUTERIN, V. **Layer 2 scaling**. 2024. Acesso em: 17 maio 2025. Disponível em: <https://ethereum.org/en/layer-2/>.

FOOL, T. M. **What Is Blockchain?** 2025. Acesso em: 30 mar. 2025. Disponível em: <https://www.fool.com/terms/b/blockchain/>.

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

KSHETRI, N.; ROGERS, R. **Registros de propriedade baseados em blockchain podem ajudar a tirar pessoas pobres da pobreza**. 2018. Disponível em: <https://theconversation.com/blockchain-based-property-registries-may-help-lift-poor-people-out-of-poverty-98796>.

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>.

PINTU. **Understanding Ethereum Virtual Machine**. 2023. Acesso em: 24 mai. 2025. Disponível em: <https://pintu.co.id/en/academy/post/what-is-ethereum-virtual-machine#what-is-ethereum-virtual-machine>.

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>.

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

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

ZIA, M.; WINTHER-TAMAKI, M.; KOVACS-GOODMAN, J.; SANCHES, B. H.; HARMALKAR, K. **Introdução à Blockchain para Governos Municipais**. itsrio, 2022. Disponível em: <https://itsrio.org/wp-content/uploads/2022/08/Introdu%C3%A7%C3%A3o-%C3%A0-Blockchain-para-Governos-Municipais.pdf>.