



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

**PROTÓTIPO DE SISTEMA DE RASTREABILIDADE DE DINHEIRO PÚBLICO
BASEADO EM BLOCKCHAIN**

WILLIAN BINDA

CHAPECÓ, JULHO DE 2025

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

PROTÓTIPO DE SISTEMA DE RASTREABILIDADE DE DINHEIRO PÚBLICO
BASEADO EM BLOCKCHAIN

**Relatório Parcial do Trabalho de Conclusão
de Curso submetido à Universidade Comuni-
tária da Região de Chapecó para a disciplina
de Ciência da Computação.**

WILLIAN BINDA

Orientador: Prof. Radamés Pereira, M.Sc.

CHAPECÓ, JULHO DE 2025

LISTA DE ILUSTRAÇÕES

Figura 1 – Funcionamento da Blockchain	5
Figura 2 – Funcionamento inicial da Blockchain	6

LISTA DE QUADROS

QUADRO 1 – Cronograma de 02/2025 a 07/2025	14
---	-----------

LISTA DE SIGLAS

LAI Lei de Acesso à Informação.

LGPD Lei de Geral de Proteção de Dados.

SUMÁRIO

LISTA DE ILUSTRAÇÕES	iii
LISTA DE QUADROS	iv
LISTA DE SIGLAS	v
1 INTRODUÇÃO	1
1.1 Delimitação do problema	1
1.2 Objetivos	2
1.2.1 Objetivo geral	2
1.2.2 Objetivos específicos	2
1.3 Justificativa	2
1.4 Delimitação do Escopo	3
2 BLOCKCHAIN E CONTRATOS INTELIGENTES: CONCEITOS, FUN- CIONAMENTO E SEGURANÇA DOS DADOS	4
2.1 Histórico do Blockchain	4
2.2 Carteiras Digitais	6
2.3 Ethereum e Contratos Inteligentes: A Revolução da Web 3.0	7
3 UTILIZAÇÃO DA BLOCKCHAIN PARA GOVERNOS	8
3.1 Areas de aplicação	8
3.2 Problemas na Distribuição de dinheiro covid19	10
4 PROCEDIMENTOS METODOLÓGICOS	11
4.1 Tipo de Pesquisa	11
4.2 Técnicas e Ferramentas Utilizadas	11
4.3 Etapas de Desenvolvimento do Protótipo	12
4.4 Regras do Contrato Inteligente	12
4.5 Funcionalidades da Interface	12
4.6 Considerações Éticas	13
REFERÊNCIAS	15

1 INTRODUÇÃO

A implementação de um protótipo de sistema baseado em blockchain para registrar e disponibilizar, de forma transparente e imutável, todas as transações financeiras no setor público se apresenta como uma solução inovadora e urgente diante dos recorrentes casos de corrupção e desvio de verbas no Brasil. Apesar dos elevados valores arrecadados através de impostos, a destinação desses recursos ainda é de difícil acesso para a população, dificultando o acompanhamento e a fiscalização de sua utilização. O uso da blockchain, com sua característica de transparência e imutabilidade, fortalece significativamente os mecanismos de controle, garantindo que todas as transações sejam verificáveis e acessíveis publicamente.

Além disso, para que a aplicação dessa tecnologia seja eficaz e não entre em conflito com as legislações vigentes, como a a Lei de Acesso à Informação (LAI) e a Lei de Geral de Proteção de Dados (LGPD), é essencial que o protótipo seja projetado de modo a garantir a transparência sem comprometer a privacidade e a segurança dos dados dos cidadãos. O alinhamento com essas normativas será crucial para o sucesso do projeto, garantindo que o sistema respeite os direitos dos indivíduos ao mesmo tempo em que assegura o controle social sobre a alocação dos recursos públicos.

Este trabalho propõe o desenvolvimento de um protótipo de sistema baseado em blockchain, com foco na rastreabilidade do dinheiro público, permitindo o monitoramento preciso dos fundos públicos desde sua arrecadação até a sua aplicação final. A imutabilidade e a transparência proporcionadas por essa tecnologia garantem que todas as transações sejam registradas de forma pública e verificável, reduzindo significativamente as possibilidades de ocultação de irregularidades e aumentando a confiança da população na administração dos recursos públicos.

Nos capítulos seguintes, será apresentada uma revisão bibliográfica sobre o uso da blockchain e contratos inteligentes no setor público, detalhando as soluções existentes e os desafios enfrentados por sistemas semelhantes.

1.1 Delimitação do problema

O presente trabalho desenvolverá um protótipo de sistema baseado em blockchain, com foco na rastreabilidade do dinheiro público. O sistema será limitado ao acompanhamento das transações financeiras desde o momento em que forem processadas por contratos inteligentes, registradas na blockchain e movimentadas entre carteiras digitais. Não serão abordados processos completos de arrecadação tributária nem mecanismos internos de auditoria governamental, restringindo-se à criação de um modelo de rastreio transparente e acessível à sociedade.

1.2 Objetivos

1.2.1 Objetivo geral

Desenvolver um protótipo de sistema baseado em blockchain que permita a qualquer cidadão ou órgão de controle acompanhar o fluxo do dinheiro público a partir do momento em que as transações são registradas na blockchain por meio de contratos inteligentes, garantindo maior transparência e fiscalização sobre a movimentação e a aplicação dos recursos.

1.2.2 Objetivos específicos

- Conceituar e fundamentar a tecnologia blockchain, destacando suas principais características e aplicações relacionadas à transparência de informações;
- Analisar soluções existentes que utilizam blockchain para rastreabilidade de recursos públicos, incluindo dinheiro público, documentos e registros oficiais;
- Desenvolver uma interface web intuitiva para visualização e acompanhamento das transações financeiras registradas na blockchain, visando facilitar o entendimento para cidadãos e órgãos de controle;
- Proporcionar meios para mitigar a falta de transparência no setor público, permitindo o acesso a informações detalhadas sobre a movimentação do dinheiro público;

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 tem como objetivo o desenvolvimento de um protótipo de sistema baseado em blockchain, focado na rastreabilidade do dinheiro público. O protótipo permitirá a visualização transparente da arrecadação e aplicação desses recursos nas áreas de saúde, educação e infraestrutura. A principal função do protótipo será garantir que cidadãos e órgãos de controle possam acompanhar, em tempo real, como o dinheiro público está sendo movimentado e alocado.

O protótipo será baseado em uma blockchain pública existente e não envolverá a criação de uma blockchain própria. Ele será voltado especificamente para a transparência financeira e monitoramento da alocação de recursos dentro de uma área restrita, sem incluir outras possíveis utilizações de blockchain no setor público, como a rastreabilidade de documentos ou autenticação de identidade.

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

Neste capítulo, será explorado o conceito da tecnologia blockchain, desmistificando seu funcionamento e abordando suas principais características, como a descentralização, a segurança e a transparência. Serão também analisados os contratos inteligentes (smart contracts), destacando seu papel na automatização de processos, no aumento da confiabilidade e na redução da necessidade de intermediários. Além disso, discutir-se-á por que a blockchain é menos suscetível a vazamentos de dados e ataques cibernéticos, evidenciando os mecanismos de segurança que a tornam resistente a fraudes. Por fim, serão apresentadas as principais aplicações e limitações dessa tecnologia, bem como sua relação com a Web 3.0, apontando o potencial impacto de sua adoção em diferentes setores, incluindo o governo e a administração pública.

2.1 Histórico do Blockchain

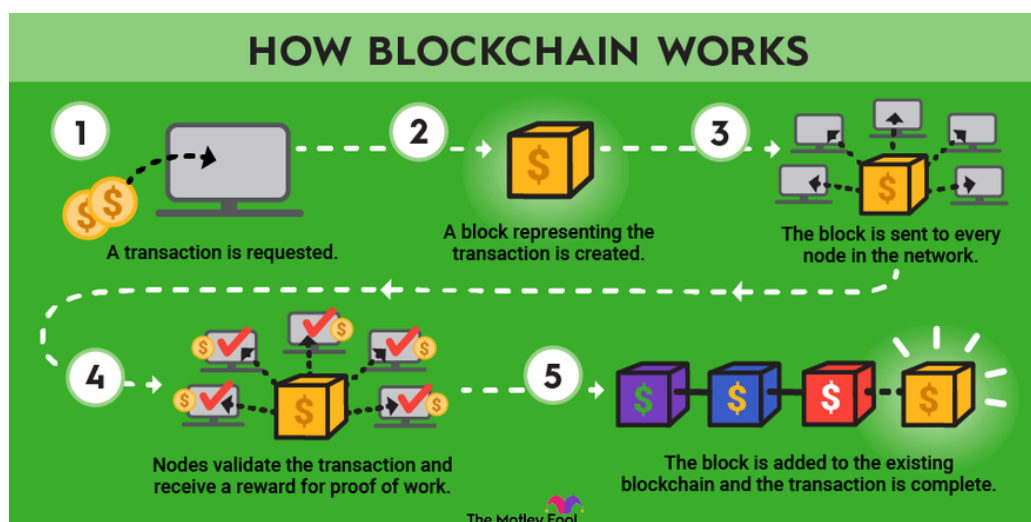
A ideia de blockchain começou a ser desenvolvida entre as décadas de 1980 e 1990, sendo oficialmente apresentada em 1991 por Stuart Haber e W. Scott Stornetta no artigo "How to Time-Stamp a Digital Document" ("Como marcar a data e hora em um documento digital"). O objetivo inicial era criar um método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

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

Figura 1 – Funcionamento da Blockchain



Fonte: (Fool, 2025).

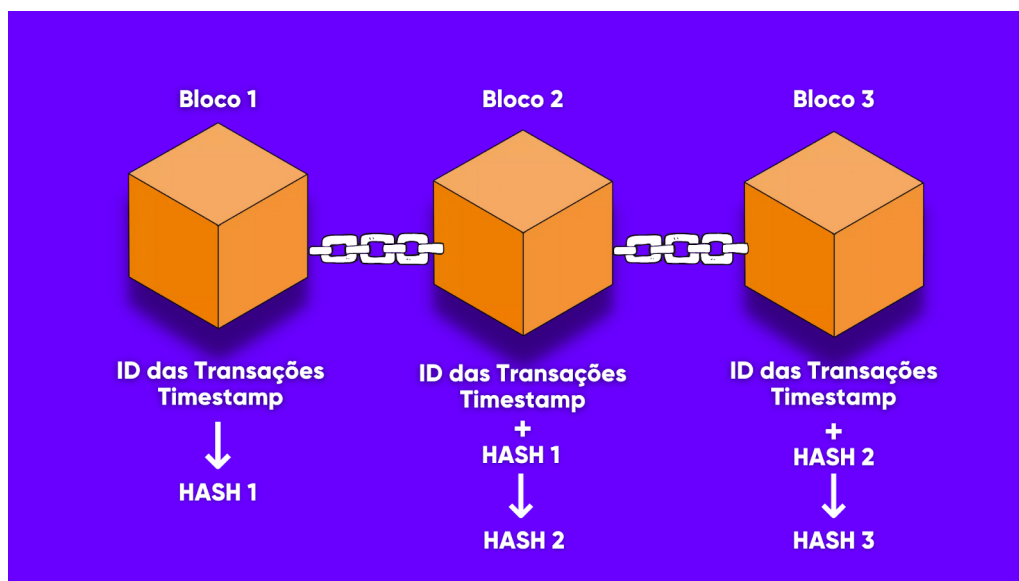
matemático complexo, conhecido como prova de trabalho (proof-of-work), um processo que requer grande capacidade computacional, chamado de mineração.

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 1.1. 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).

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

Figura 2 – Funcionamento inicial da Blockchain

Fonte: (AreaBitcoin, 2025).

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, um protocolo amplamente utilizado para compartilhamento de arquivos. 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 "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).

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.

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 para medir o esforço computacional necessário para realizar operações na rede. Cada transação ou execução de contrato inteligente exige uma quantidade específica de Gas, 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 Ethereum Virtual Machine (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.

3 UTILIZAÇÃO DA BLOCKCHAIN PARA GOVERNOS

A aplicação da tecnologia blockchain vai muito além das criptomoedas, estendendo-se a setores como saúde, logística, meio ambiente e, especialmente, à administração pública. Sua estrutura descentralizada e imutável oferece uma base sólida para aprimorar a transparência, a rastreabilidade e a segurança dos dados governamentais. Com isso, torna-se possível implementar sistemas que acompanhem, em tempo real, o fluxo de recursos públicos — desde a arrecadação até a aplicação final — reduzindo significativamente os riscos de corrupção, desvios e má gestão.

A tecnologia blockchain ainda é desconhecida para grande parte da população brasileira e de outros países, mas já possui aplicações em uso no Brasil, embora pouco divulgadas. Um exemplo é a nova Carteira de Identidade Nacional (CIN), cuja emissão utiliza blockchain para garantir maior rastreabilidade, segurança e consistência no serviço prestado. Segundo o secretário de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), Rogério Mascarenhas, essa tecnologia também permite a inscrição do CPF diretamente no balcão do órgão de identificação, trazendo benefícios diretos para os cidadãos (GOVBR, 2023). No cenário internacional, a Estônia se destaca como referência na adoção de blockchain na administração pública. O país implementou o e-Residency, um sistema descentralizado que funciona como documento de identificação digital, registrando dados como número de registro, escolaridade e histórico de trabalho desde o nascimento do cidadão (SAVIO, 2020). Além disso, o DREX, a moeda digital do Banco Central do Brasil, foi desenvolvido utilizando tecnologia blockchain para oferecer mais segurança e transparência nas transações. Grandes bancos brasileiros, como Itaú e Banco do Brasil, também exploram essa tecnologia, ainda que de forma limitada, principalmente para reforçar a segurança e a rastreabilidade de operações financeiras.

Diante dessas possibilidades, torna-se evidente o potencial da blockchain como ferramenta para aprimorar a gestão pública. Este capítulo explora as aplicações já existentes em governos ao redor do mundo, examina os benefícios e os desafios envolvidos e, por fim, propõe uma abordagem de rastreabilidade do dinheiro público com base em contratos inteligentes e registros descentralizados — como forma de promover maior transparência, controle social e confiança nas instituições.

3.1 Áreas de aplicação

Uma das aplicações mais promissoras da tecnologia blockchain no setor público é na gestão de registros de propriedade de terras. Em muitos países em desenvolvimento, os sistemas atuais de rastreamento de direitos de propriedade são frágeis, incompletos ou até inexistentes, o que impede a comprovação da titularidade e prejudica economicamente milhões de pessoas (Kshetri; Rogers, 2018).

No caso do Haiti, por exemplo, o terremoto de 2010 destruiu todos os registros físicos municipais, deixando inúmeros agricultores sem qualquer documentação formal que comprovasse

a posse das terras que cultivavam. Esse tipo de situação se repete em várias regiões do mundo, impactando o acesso a crédito, a resolução de disputas fundiárias e a segurança patrimonial das famílias (Kshetri; Rogers, 2018).

Estima-se que as oportunidades econômicas perdidas por ativos sem documentação formal alcancem cerca de 20 trilhões de dólares globalmente. Diante disso, os sistemas baseados em blockchain emergem como uma alternativa segura e transparente para registro de propriedade, sendo já testados em países como Bermudas, Brasil, Geórgia, Gana, Honduras, Índia, Rússia e Ruanda (Kshetri; Rogers, 2018).

O uso de blockchain nesse contexto permite a criação de registros imutáveis, com histórico completo de transações, identificando quem realizou cada alteração, quando e com qual propósito. Isso reduz significativamente a possibilidade de fraudes, falsificações e disputas judiciais (Kshetri; Rogers, 2018).

No Brasil, a ausência de um sistema centralizado e a existência de milhares de cartórios autônomos tornam o processo de registro de terras confuso e vulnerável à corrupção e sobreposição de títulos. A introdução da blockchain em municípios como Pelotas e Morro Redondo tem proporcionado maior integridade aos registros, contendo dados como endereço, regras de zoneamento, identidade do proprietário e coordenadas geográficas (Kshetri; Rogers, 2018).

Além disso, a redução de custos com o uso da tecnologia também é um fator relevante. Em países como a Geórgia, a migração do processo de registro para a blockchain pode reduzir taxas que variam entre US\$ 50 e US\$ 200 para valores tão baixos quanto US\$ 0,10 (Kshetri; Rogers, 2018).

No entanto, é importante destacar que a tecnologia, por si só, não resolve todos os desafios. A qualidade dos dados inseridos, a legitimidade dos registros e a resistência de agentes públicos que podem se sentir ameaçados por sistemas mais transparentes ainda são obstáculos a serem superados (Kshetri; Rogers, 2018).

Apesar desses desafios, quando implementada com transparência, justiça e imparcialidade, a blockchain pode ser um instrumento poderoso para conceder às populações marginalizadas o seu primeiro ativo real e legalmente reconhecido, rompendo ciclos de pobreza e exclusão (Kshetri; Rogers, 2018).

Os registros públicos baseados em blockchain também permitem alto grau de confiança e responsabilidade, pois quaisquer alterações nos registros de propriedade da terra criam um log de auditoria imutável, com assinaturas criptográficas que atestam a aprovação daquela alteração por um funcionário individual. Uma vez que se descobre que uma determinada entrada em um registro baseado em blockchain é fraudulenta, o funcionário em questão pode ser identificado e investigado (Zia et al., 2022, p. 7).

3.2 Problemas na Distribuição de dinheiro covid19

. Durante a pandemia de COVID-19, os governos enfrentaram um desafio sem precedentes na distribuição emergencial de recursos públicos. A necessidade de oferecer auxílio financeiro a milhões de pessoas rapidamente sobrecarregou a infraestrutura existente, que foi desenhada para atender principalmente indivíduos formalmente registrados no sistema (Zia et al., 2022).

No Brasil, por exemplo, o auxílio emergencial chegou a beneficiar cerca de 66 milhões de pessoas, com transferências que somaram aproximadamente 280 bilhões de reais – o equivalente a quase 4% do PIB nacional. No entanto, apesar do montante significativo, houve demora na entrega do auxílio e falhas na identificação de beneficiários, deixando muitos cidadãos elegíveis sem receber os valores (Zia et al., 2022).

Além disso, as prefeituras tentaram contribuir com recursos próprios para estimular economias locais, mas esbarraram em um problema recorrente: a falta de controle e rastreabilidade do destino do dinheiro. Os beneficiários, por não estarem limitados a utilizar os recursos em suas comunidades, acabavam consumindo em outras regiões ou em grandes redes comerciais, fugindo da proposta de fortalecimento da economia local (Zia et al., 2022).

Diante desse cenário, surgiram alternativas para garantir maior controle e transparência na utilização dos recursos públicos. Um exemplo notável é o do município de Maricá (RJ), que implementou um sistema de benefícios sociais por meio de uma moeda digital local, a Moeda Mumbuca. O modelo permitiu ao município distribuir o auxílio de forma mais direcionada, priorizando a circulação do dinheiro dentro da própria comunidade (Zia et al., 2022).

Ainda que a Moeda Mumbuca inicialmente não estivesse baseada em blockchain, pesquisadores estudam como a tecnologia pode ser incorporada para ampliar a transparência, a confiança pública e a prestação de contas. Por meio do registro imutável e verificável da blockchain, seria possível rastrear todas as transações realizadas com os recursos públicos, permitindo auditorias em tempo real e a geração de dados para políticas públicas mais eficazes (Zia et al., 2022).

4 PROCEDIMENTOS METODOLÓGICOS

4.1 Tipo de Pesquisa

Este trabalho caracteriza-se como uma pesquisa aplicada, com abordagem qualitativa e natureza tecnológica. Seu objetivo principal é desenvolver um protótipo funcional de um sistema que auxilia e permita a rastreabilidade de dinheiro público utilizando tecnologia blockchain. A pesquisa é também descritiva, pois busca detalhar as funcionalidades, as tecnologias empregadas e os processos envolvidos no desenvolvimento da solução proposta.

4.2 Técnicas e Ferramentas Utilizadas

- Interface de programação: Será utilizada a IDE online Remix, que oferece ambiente completo para desenvolvimento, teste e implantação inicial de contratos inteligentes. A plataforma fornece recursos para simulação de blockchain, testes de transações e acesso facilitado a bibliotecas.
- Versionamento de código: O controle de versão do código-fonte será feito por meio da plataforma GitHub, possibilitando rastreamento de alterações e colaboração no desenvolvimento.
- Linguagem de programação para contratos inteligentes: Os contratos inteligentes serão desenvolvidos em linguagem Solidity, com apoio das bibliotecas da OpenZeppelin, que oferecem padrões de segurança e funcionalidades reutilizáveis.
- Blockchain local: Durante a fase inicial de desenvolvimento, será utilizada a blockchain simulada no Remix IDE. Para fins de integração com a interface web e testes de interação com o front-end, será empregada uma blockchain local executada na máquina do desenvolvedor, utilizando a ferramenta Ganache, que simula uma rede Ethereum completa para desenvolvimento e testes.
- Contratos inteligentes: Os contratos serão responsáveis por definir a lógica de negócio e as regras de movimentação dos recursos públicos, garantindo integridade, transparência e rastreabilidade das ações.
- Interface web: Será desenvolvida uma aplicação web com foco em acessibilidade e visualização intuitiva dos dados. Serão utilizadas as tecnologias HTML, CSS e JavaScript, com o framework React.
- Visualização de dados: Para a exibição gráfica das informações, serão empregadas bibliotecas como o ECharts, permitindo gerar gráficos em tempo real sobre o fluxo de recursos, distribuição setorial e comparações.

- Ambiente de testes: Os testes e validações dos contratos inteligentes serão realizados por meio do próprio Remix IDE, que fornece ferramentas nativas para simulação de transações.

4.3 Etapas de Desenvolvimento do Protótipo

1. Levantamento de requisitos funcionais e não funcionais;
2. Definição da arquitetura do protótipo;
3. Modelagem e implementação do contrato inteligente;
4. Desenvolvimento da interface web para visualização das informações;
5. Integração entre front-end e blockchain;

4.4 Regras do Contrato Inteligente

- Gestão de fundos: Funções para depósito e retirada de valores do contrato, controlando o armazenamento e a movimentação dos fundos.
- Distribuição de recursos: Implementação de uma função que permite distribuir os fundos automaticamente entre os setores definidos (educação, saúde, infraestrutura), com base nas porcentagens previamente configuradas.
- Configuração de percentuais: Possibilidade de definir as porcentagens de alocação dos recursos públicos para cada setor, com alterações registradas on-chain.
- Administrador: Responsável por configurar os parâmetros do contrato, ajustar as porcentagens de distribuição e cadastrar os endereços autorizados a movimentar os fundos.
- Gestores de fundos: Usuários com permissão para executar a função de distribuição dos recursos e realizar transações, respeitando os limites definidos para cada setor.
- Cadastro de permissões: Apenas o administrador poderá autorizar ou revogar permissões de endereços para atuarem como gestores.
- Execução da distribuição: A distribuição dos fundos é feita de forma automática no momento do recebimento dos valores, com base nos percentuais definidos.

4.5 Funcionalidades da Interface

- Visualização de arrecadação: Exibição do total de recursos arrecadados no contrato inteligente, em tempo real ou com filtros por data (dia, mês e ano).
- Histórico de transações: Consulta detalhada de todas as transações realizadas no contrato, incluindo data, valor, endereço de origem e destino.

- Consulta por endereço: Visualização do histórico de transações associadas a um endereço específico, permitindo o rastreamento individualizado.
- Gráficos dinâmicos: Utilização de gráficos do tipo pizza, barras e linha para representar a distribuição dos recursos entre setores, comparativos entre órgãos e evolução dos valores ao longo do tempo.
- Gerenciamento de permissões: Página dedicada para listar os endereços autorizados e os setores que cada um pode acessar ou movimentar, conforme definido no contrato inteligente.
- Configuração de distribuição: Interface restrita a gestores para definir e atualizar as porcentagens de distribuição dos fundos entre os setores.

4.6 Considerações Éticas

O desenvolvimento do protótipo considera os princípios da ética em pesquisa tecnológica. Não serão utilizados dados reais, e todas as informações geradas são simuladas com o propósito de teste e validação do protótipo. O projeto visa promover a transparência e o acesso público à informação, contribuindo com iniciativas de controle social e participação cidadã.

CRONOGRAMA

QUADRO 1 – Cronograma de 02/2025 a 07/2025

Atividades	Fev/2025	Mar/2025	Abr/2025	Mai/2025	Jun/2025	Jul/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).

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/>>.

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/>>.

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>>.

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>>.

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>>.