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 Comunitária 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

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE SIGLAS

LAI Lei de Acesso à Informação.

LGPD Lei de Geral de Proteção de Dados.

SUMÁRIO

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 uma blockchain pública existente, voltado exclusivamente para a rastreabilidade do dinheiro público a partir do momento em que os recursos são registrados e movimentados por contratos inteligentes. O sistema permitirá acompanhar, de forma clara e acessível, como os valores são alocados entre setores como saúde, educação e infraestrutura.

O escopo limita-se ao registro, distribuição e visualização dos recursos a partir de uma etapa simulada de liberação de verbas, não abrangendo processos anteriores de arrecadação tributária nem integrações com sistemas governamentais reais. Também não serão abordadas outras aplicações da blockchain no setor público, como autenticação de identidade digital ou registro de documentos.

O foco central é fornecer uma ferramenta demonstrativa que evidencie como a tecnologia blockchain, aliada a contratos inteligentes, pode reforçar a transparência e o controle social sobre a alocação de recursos públicos.

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

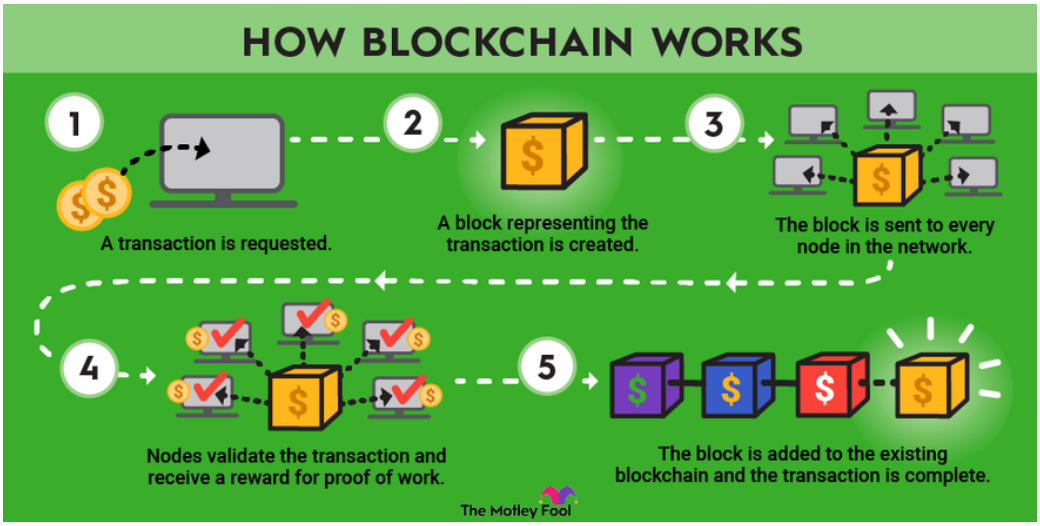
A ideia de blockchain começou a ser desenvolvida entre as décadas de 1980 e 1990, sendo oficialmente apresentada em 1991 por Stuart Haber e W. Scott Stornetta no artigo "How to Time-Stamp a Digital Document"("Como marcar a data e hora em um documento digital"). O objetivo inicial era criar um método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

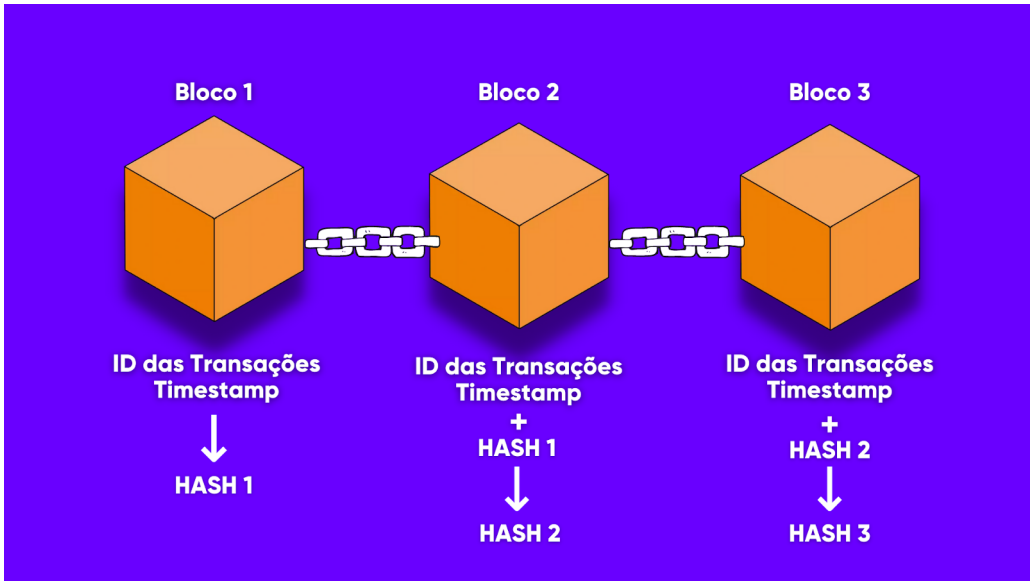
A segurança da blockchain aumenta à medida que mais nós (computadores) ingressam na rede, pois os dados ficam distribuídos de forma descentralizada, eliminando a existência de um ponto único de falha. Alterar qualquer informação em um bloco exigiria alterar todos os blocos subsequentes em todos os nós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

2.4 Comparativo entre Ethereum e Subcamadas (Layer 2)

Embora a rede Ethereum tenha revolucionado o desenvolvimento de aplicações descentralizadas, ela enfrenta desafios significativos relacionados à escalabilidade e ao custo das transações. Com o crescimento da demanda, a rede principal (Layer 1) frequentemente atinge sua capacidade máxima, resultando em altas taxas de transação (gas) e lentidão no processamento.

Para mitigar esses problemas, surgiram as chamadas soluções de segunda camada, ou Layer 2 (L2). Essas subcamadas são construídas sobre a Ethereum e têm como objetivo principal aumentar a capacidade de processamento de transações, reduzir custos e melhorar a experiência do usuário, sem comprometer a segurança e a descentralização oferecidas pela camada principal.

As soluções Layer 2 operam de formas distintas, mas geralmente executam transações fora da Ethereum principal (off-chain) e registram apenas dados resumidos na L1. Isso permite que milhares de transações sejam processadas por segundo com custos extremamente baixos(KUNTZ, 2022). As principais abordagens incluem:

- Rollups: Agrupam várias transações e as registram em lote na Ethereum (ex: Arbitrum, Optimism).
- Sidechains: São blockchains paralelas que interagem com a Ethereum, mas operam de forma mais independente (ex: Polygon PoS).
- Validium/ZK-Rollups: Usam provas criptográficas para garantir a validade das transações fora da cadeia.

A seguir, 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

* A segurança da Polygon depende de seus próprios validadores e checkpoints na Ethereum.
Fonte: Elaborado pelo autor com base em Ethereum.org (2024), Polygon Docs (2024), Arbitrum Docs (2024) e Optimism Docs (2024).

2.5 Considerações Finais

Neste capítulo, foi possível compreender de forma aprofundada os fundamentos da tecnologia blockchain e dos contratos inteligentes, destacando sua evolução, funcionamento técnico e relevância no contexto atual da transformação digital. A blockchain mostrou-se uma solução inovadora para o armazenamento seguro e descentralizado de informações, com forte resistência a fraudes e ataques cibernéticos, graças à sua estrutura de dados imutável e distribuída.

Além disso, a introdução dos contratos inteligentes pela plataforma Ethereum representou um marco importante, permitindo a execução automatizada e confiável de regras de negócio sem a necessidade de intermediários. Essa inovação impulsionou a chamada Web 3.0, abrindo caminhos para aplicações mais transparentes, auditáveis e seguras em diferentes setores, como saúde, finanças e administração pública.

Por fim, foram abordadas não apenas as potencialidades dessa tecnologia, mas também suas limitações e desafios, como a escalabilidade e o custo computacional das operações. Ainda assim, a blockchain e os contratos inteligentes consolidam-se como elementos centrais no desenvolvimento de sistemas mais confiáveis e descentralizados, contribuindo para a construção de um novo paradigma digital baseado em confiança algorítmica e autonomia dos usuários.

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 Áreas de Aplicação

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.

3.1.1 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.

falar sobre o INSS mais recente

3.2 Problemas na Distribuição de Dinheiro 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.

3.3 Blockchain como Alternativa Tecnológica

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.

3.4 Blockchain no Rastreamento de Vacinas e na Saúde Pública

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;

3.5 Impacto Social e Econômico da Blockchain na Gestão Pública

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

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

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

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

3.6 Considerações Finais

A aplicação da tecnologia blockchain no setor público representa um avanço significativo na busca por maior transparência, eficiência e justiça na administração dos recursos públicos. Ao longo deste capítulo, foram explorados diversos contextos em que essa tecnologia já vem sendo utilizada, tanto no Brasil quanto internacionalmente — desde o registro de propriedades e a distribuição de benefícios sociais até o rastreamento de vacinas em sistemas de saúde.

Esses exemplos demonstram que a blockchain tem o potencial de corrigir falhas estruturais históricas, oferecendo registros imutáveis, auditáveis e acessíveis que fortalecem a confiança entre governo e sociedade. Em cenários de crise, como a pandemia da COVID-19, fica evidente a urgência de ferramentas capazes de garantir rastreabilidade, segurança e agilidade na execução de políticas públicas.

Apesar dos desafios — como a resistência institucional, a qualidade dos dados e a necessidade de infraestrutura tecnológica adequada — a adoção da blockchain como ferramenta de governança já deixou de ser uma promessa distante. Combinada a instrumentos como contratos

inteligentes e moedas digitais locais, ela permite não apenas monitorar o uso do dinheiro público, mas também orientar seu impacto de forma mais eficaz e inclusiva.

Assim, ao se considerar o futuro da gestão pública, torna-se imprescindível explorar soluções que conciliem inovação tecnológica com participação social. A blockchain, quando bem implementada, pode ser a base de uma nova arquitetura institucional mais aberta, confiável e orientada ao bem comum.

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 sistema baseado em blockchain que possibilite a rastreabilidade do dinheiro público. A pesquisa também pode ser classificada como descritiva, uma vez que busca detalhar as funcionalidades, os componentes tecnológicos e os processos envolvidos na construção da solução.

4.2 Técnicas e Ferramentas Utilizadas

O desenvolvimento do protótipo foi conduzido com base em ferramentas amplamente utilizadas no ecossistema de desenvolvimento blockchain, escolhidas por sua acessibilidade, suporte à prototipagem e integração com tecnologias web modernas.

- Remix IDE: Plataforma online utilizada para a escrita, compilação e teste inicial de contratos inteligentes em Solidity. Permite simulação de transações e interações com a blockchain sem a necessidade de ambiente externo.
- Ganache: Ferramenta que simula uma blockchain local compatível com Ethereum. Foi empregada para testes integrados com a aplicação web, proporcionando controle total sobre as transações e a visualização de blocos.
- Solidity: Linguagem de programação específica para contratos inteligentes na plataforma Ethereum. Utilizada para implementar as regras de negócio relacionadas à gestão e distribuição dos fundos públicos simulados.
- OpenZeppelin: Conjunto de bibliotecas com padrões de segurança amplamente utilizados no desenvolvimento de contratos inteligentes. Auxilia na criação de contratos seguros e modulares.
- React: Framework JavaScript utilizado no desenvolvimento da interface web do protótipo. Permite a criação de componentes dinâmicos e responsivos para exibir os dados da blockchain em tempo real.
- ECharts: Biblioteca gráfica utilizada para exibir visualmente os dados de alocação de recursos, histórico de transações e estatísticas relevantes.
- GitHub: Utilizado para controle de versão, rastreamento de mudanças e documentação colaborativa do projeto.

4.3 Arquitetura do Protótipo

O sistema desenvolvido é composto por três camadas principais:

- Camada de apresentação (front-end): Responsável pela visualização das informações. Desenvolvida com React, permite que o usuário interaja com os dados da blockchain e visualize gráficos e históricos de transações em tempo real.
- Camada de aplicação (lógica de integração): Realiza a mediação entre a interface web e os contratos inteligentes implantados na blockchain local, utilizando bibliotecas como Ethers.js.
- Camada de dados (blockchain): Composta pelos contratos inteligentes implantados na rede simulada via Ganache. Todas as transações são armazenadas de forma imutável, permitindo rastreamento e auditoria pública.

4.4 Etapas de Desenvolvimento

O desenvolvimento do protótipo seguiu as seguintes etapas:

1. Levantamento de requisitos funcionais e não funcionais.
2. Definição da arquitetura do sistema e escolha das ferramentas.
3. Implementação dos contratos inteligentes com regras de alocação de recursos.
4. Desenvolvimento da interface web para exibição e interação com os dados.
5. Integração entre a aplicação web e a blockchain simulada.
6. Testes de funcionalidades e validação da rastreabilidade das transações.

4.5 Regras de Funcionamento do Contrato Inteligente

O contrato inteligente centraliza a lógica de gestão dos recursos e define as seguintes regras:

- Gestão de fundos: Permite depósitos e movimentações de valores de forma segura.
- Distribuição automática: O contrato distribui automaticamente os valores recebidos com base em percentuais pré-definidos para setores como saúde, educação e infraestrutura.
- Configuração de alocação: Percentuais de distribuição podem ser definidos e ajustados pelo administrador, sendo essas alterações registradas on-chain.
- Controle de permissões: Apenas endereços autorizados (gestores) podem executar ações específicas, como movimentações e atualizações.

– Rastreamento transparente: Todas as transações, alterações de configuração e permissões ficam registradas na blockchain, permitindo auditoria completa.

4.6 Funcionalidades da Interface Web

A interface do sistema foi projetada para tornar o acesso à informação transparente e acessível:

– Visualização de arrecadação: Mostra o saldo total armazenado no contrato inteligente, com filtros por período.

– Histórico de transações: Lista todas as movimentações de valores, com data, valor, origem e destino.

– Consulta por endereço: Permite buscar transações associadas a um endereço específico.

– Gráficos interativos: Apresenta dados sobre a distribuição dos recursos por setor e ao longo do tempo.

– Gerenciamento de permissões: Página administrativa onde é possível consultar e modificar endereços autorizados.

– Configuração de distribuição: Interface restrita a gestores para alterar os percentuais de alocação de forma segura.

4.7 Limitações e Trabalhos Futuros

Embora o protótipo demonstre o potencial da blockchain para promover transparência no uso de dinheiro público, algumas limitações devem ser consideradas:

– O sistema opera em ambiente de simulação e não está integrado a bases de dados governamentais reais.

– A entrada de valores no contrato é manual, simulando a liberação de recursos públicos.

– Não há validação automática de veracidade dos dados inseridos.

– O uso de redes públicas reais pode implicar em custos de transação que não estão presentes na simulação local.

Como trabalhos futuros, propõe-se:

– A integração com APIs públicas, como o Portal da Transparência.

– O uso de oráculos para inserção de dados externos confiáveis.

- A implementação em redes de teste públicas (como Goerli ou Sepolia).
- A ampliação da solução para contemplar outros tipos de rastreabilidade no setor público.

4.8 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>.