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 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 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

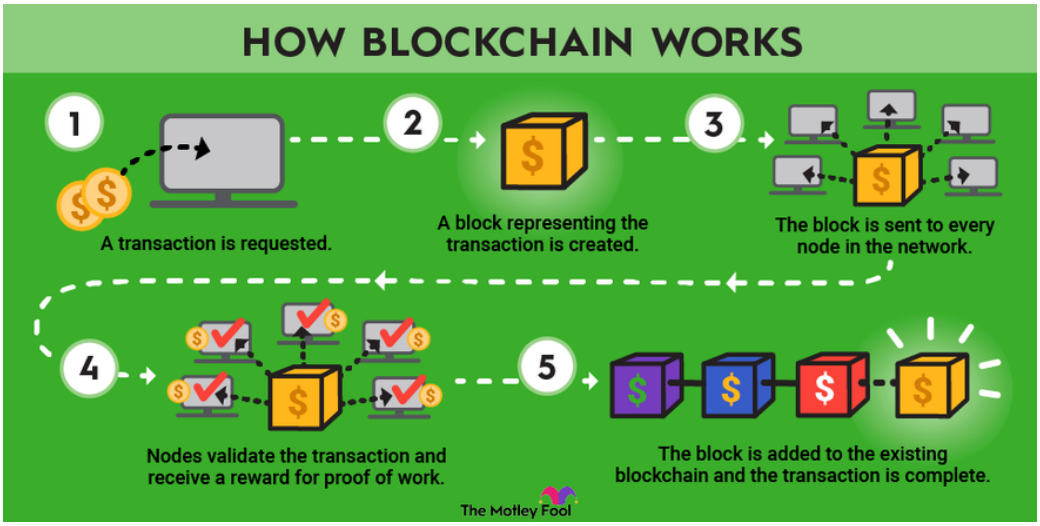
A ideia de blockchain começou a ser desenvolvida entre as décadas de 1980 e 1990, sendo oficialmente apresentada em 1991 por Stuart Haber e W. Scott Stornetta no artigo "How to Time-Stamp a Digital Document"("Como marcar a data e hora em um documento digital"). O objetivo inicial era criar um método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

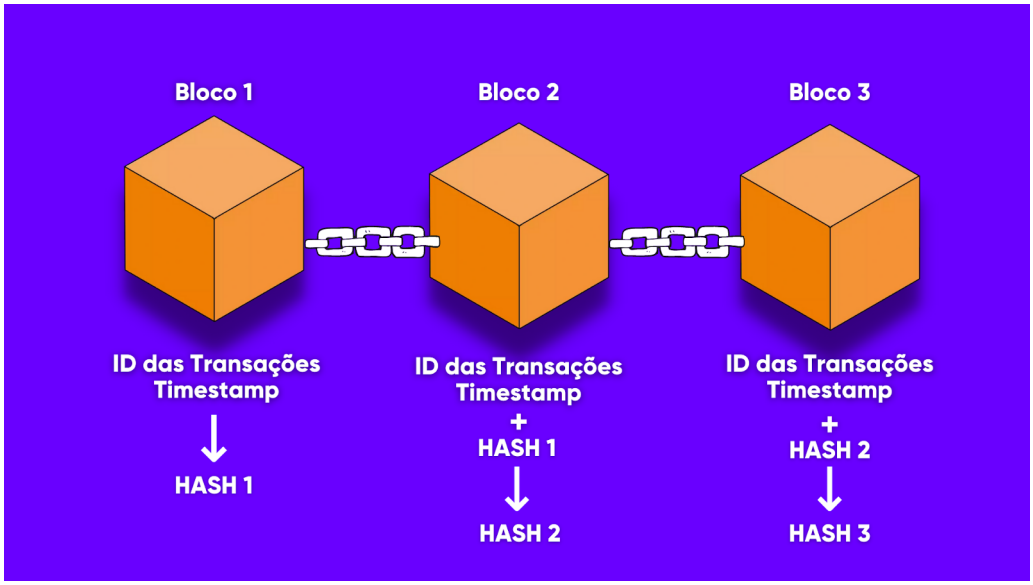
A segurança da blockchain aumenta à medida que mais nós (computadores) ingressam na rede, pois os dados ficam distribuídos de forma descentralizada, eliminando a existência de um ponto único de falha. Alterar qualquer informação em um bloco exigiria alterar todos os blocos subsequentes em todos os nós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

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

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/>.

KUNTZ, J. **Blockchain Ethereum Fundamentos de arquitetura, desenvolvimento de contratos e aplicações**. [S.l.]: Casa do Código, 2022.