# **Desenvolvimento de um Protótipo de Sistema Baseado em Blockchain para Transparência e Monitoramento de Transações Financeiras no Setor Público**

1. **Introdução**
   1. **Tema**

Implementar um sistema baseado em blockchain para registrar e tornar acessíveis, de forma transparente e imutável, todas as transações financeiras do setor público.

* 1. **Problema de pesquisa**

#### Blockchain

Blockchain é um tipo de banco de dados descentralizado e distribuído que registra transações em blocos encadeados de forma imutável. Cada bloco contém um conjunto de transações verificadas e é ligado ao bloco anterior através de um hash criptográfico, formando uma cadeia (daí o nome "blockchain"). Esse sistema garante segurança, transparência e resistência a fraudes, pois a informação registrada não pode ser alterada sem a concordância da rede. Blockchains podem ser públicas (como Bitcoin e Ethereum) ou privadas (usadas por empresas para aplicações internas).

#### Contratos Inteligentes (Smart Contracts)

Contratos inteligentes são programas auto executáveis armazenados em uma blockchain que operam de acordo com regras predefinidas. Eles eliminam a necessidade de intermediários ao automatizar processos, garantindo que ações sejam realizadas apenas quando determinadas condições são atendidas. Por exemplo, em uma transação de compra e venda, um contrato inteligente pode garantir que o pagamento só seja liberado quando o comprador receber o produto. Ethereum é uma das principais plataformas que suportam contratos inteligentes, utilizando a linguagem Solidity.

#### 1. Papel da Carteira Digital na Blockchain

A carteira digital é usada para:

* Armazenar chaves criptográficas: Cada carteira possui uma chave privada (usada para assinar transações) e uma chave pública (endereço usado para receber ativos).
* Enviar e receber criptomoedas ou tokens: As carteiras permitem a movimentação de ativos na blockchain.
* Assinar transações: Para qualquer ação ser validada na blockchain (como transferências ou execução de contratos inteligentes), a transação precisa ser assinada digitalmente com a chave privada.

#### 2. Carteira Digital e Contratos Inteligentes

As carteiras digitais também permitem que os usuários interajam com contratos inteligentes. Isso inclui:

1. Implantar um contrato inteligente: Um usuário pode enviar uma transação para a blockchain criando um novo contrato inteligente.
2. Executar funções de contratos: Se um contrato possui funções, como comprar um NFT, trocar tokens ou participar de uma DAO, a carteira assina e envia a transação para a blockchain.
3. Assinar mensagens: Algumas interações exigem que o usuário assine uma mensagem com a chave privada sem necessariamente fazer uma transação (por exemplo, login em aplicativos Web3).
   1. **Objetivos**
      1. **Objetivo Geral**

Permitir que qualquer cidadão ou órgão de controle acompanhe o caminho dos recursos públicos, desde a arrecadação até a aplicação final.

* + 1. **Objetivo especifico**
* Disponibilizar o monitoramento completo dos recursos.
* Possibilitar o acompanhamento em tempo real dos gastos governamentais.
* Identificar como e onde foram aplicados.
* Reduzindo práticas ilícitas devido à maior visibilidade e controle social.
* Mostrar o montante final do dinheiro público arrecadado.
* Rastrear dinheiro público.
* Gerenciar o dinheiro público.
* Disponibilizar uma interface na web para mostrar os dados.
  1. **Justificativa**

Desvio de verba para a Covid-19 pode chegar a R$ 300 milhões, diz CGU

<https://www.cnnbrasil.com.br/nacional/desvio-de-verba-para-a-covid-19-pode-chegar-a-r-300-milhoes-diz-cgu/?utm_source=chatgpt.com>

PF faz operação contra desvio de dinheiro público a partir de emendas parlamentares

<https://cbn.globo.com/brasil/noticia/2025/02/13/pf-faz-operacao-contra-desvio-de-dinheiro-publico-a-partir-de-emendas-parlamentares.ghtml?utm_source=chatgpt.com>

PF e CGU investigam desvio de dinheiro da saúde pública em Goiás

<https://agenciabrasil.ebc.com.br/justica/noticia/2025-02/pf-e-cgu-investigam-desvio-de-dinheiro-da-saude-publica-em-goias?utm_source=chatgpt.com>

R$ 3,3 bilhões: governo Lula tem maior gasto com diárias e passagens desde 2014

<https://www.gazetadopovo.com.br/republica/r-33-bilhoes-governo-lula-tem-maior-gasto-com-diarias-e-passagens-desde-2014/>

Elon Musk planeja usar blockchain para melhorar eficiência de governo dos EUA

<https://www.infomoney.com.br/mundo/elon-musk-planeja-usar-blockchain-para-melhorar-eficiencia-de-governo-dos-eua/>

Blockchain e tokenização: como o agro pode se beneficiar das commodities digitais

<https://dinheirorural.com.br/blockchain-e-tokenizacao-como-o-agro-pode-se-beneficiar-das-commodities-digitais/?utm_source=chatgpt.com>

* 1. **Delimitação do Escopo**

Irei criar a aplicação do momento em que o dinheiro entra no contrato/blockchain através de uma carteira digital até o momento que sai do contrato/blockchain para outra carteira digital.

Possível implementação seria utilizar o gateway de pagamento como sandbox, assim adicionando a transferência/conversão direta dos fundos/tokens para moeda fiduciária.

1. **Primeiro Capítulo da Fundamentação Teórica**

A arrecadação de impostos poderia ocorrer de duas formas:

Empresas e cidadãos realizam o pagamento dos impostos por meio de um gateway de pagamentos, convertendo dinheiro fiduciário em tokens BRZ, lastreados na proporção de 1:1 com o real brasileiro e registrados na blockchain por um contrato inteligente.

Alternativamente, o valor pode ser transferido para uma carteira digital, sendo convertido em tokens BRZ antes do pagamento e registro na blockchain por um contrato inteligente.

Os dados são armazenados na blockchain, mas gerenciados pelo contrato inteligente. Cada empresa ou cidadão deve registrar sua carteira digital (Metamask, Trust Wallet, Phantom, etc.), essencial para identificação equivalente ao CPF.

Os fundos dos pagamentos são armazenados em um contrato inteligente, funcionando como um banco centralizado para impostos. Cada pagamento gera um evento que pode ser monitorado em tempo real, semelhante ao funcionamento de WebSockets na Web 2.0. Os fundos permanecem no contrato, e apenas um endereço autorizado pode transferi-los para outros destinos, como setores públicos específicos (político A, político B, saúde, educação e etc), previamente registrados no contrato.

Cada função no contrato pode emitir eventos para permitir monitoramento. Servidores públicos e entidades governamentais possuem carteiras digitais/endereço, e, ao receberem fundos, podem transferi-los para uma corretora e convertê-los em dinheiro fiduciário ou utilizar um gateway para transferir diretamente para suas contas bancárias. No caso de recursos destinados à saúde, educação e outros setores, deve-se registrar como os fundos foram gastos. (Não tenho certeza desse fluxo)

Para maior controle, pode-se exigir o registro de comprovantes de gastos na blockchain no formato PNG, utilizando um contrato inteligente específico para isso, com padrões ERC-721 ou ERC-1155 para NFTs. Isso garantiria rastreabilidade dos gastos públicos, permitindo que qualquer órgão ou cidadão monitore o uso do dinheiro público por meio dos eventos emitidos pelo contrato inteligente.

Além disso, o sistema pode exibir os dados em tempo real por meio de uma interface e permitir consultas específicas por carteira/endereço. Como a blockchain é pública, qualquer pessoa pode consultar o contrato, mas sem expor dados pessoais (CPF, endereço, etc.).

Melhorias podem ser implementadas, como o uso de contratos inteligentes intermediários para fornecedores na área da saúde. Por exemplo, ao comprar medicamentos, os fundos podem ser depositados em um contrato que libera o pagamento apenas após a confirmação da entrega. Caso seja necessário lidar com dados mais sensíveis, um banco de dados pode ser utilizado junto ao contrato inteligente

1. **Segundo Capítulo da Fundamentação Teórica**
2. **Modelagem do Protótipo**
3. **Metodologia**
4. **Cronograma**
5. **Orçamento**

Como cada operação/função no contrato no qual grava os dados na blockchain são cobradas taxas de operação ou comumente chamadas de (gas fee) taxa de gás. Essas taxas são para os mineradores e validadores da rede/blockchain (Explicar corretamente os conceitos entre: rede, blockchain, smart contract, carteira digital, gas fee). Funções de leitura de dados não são cobradas taxas de gás. Dependendo da rede de utilização do contrato as taxas podem ser mais custosas ou menos custosas.

1. **Referencias Bibliográficas**