UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

CURSO DE GRADUAÇÃO EM ENGENHARIA ELÉTRICA

JULIO CESAR FERREIRA LIMA

PROPOSTA DE REFORMA PREVIDENCIÁRIA: UM MERCADO FINANCEIRO POUPADOR VIA BLOCKCHAIN COMO ALTERNATIVA AO INSS E FGTS

SOBRAL

2026

JULIO CESAR FERREIRA LIMA

PROPOSTA DE REFORMA PREVIDENCIÁRIA: UM MERCADO FINANCEIRO POUPADOR VIA BLOCKCHAIN COMO ALTERNATIVA AO INSS E FGTS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia Elétrica do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia Elétrica.

Orientador: Prof. Dr. José Cláudio do Nascimento

SOBRAL

2026

JULIO CESAR FERREIRA LIMA

PROPOSTA DE REFORMA PREVIDENCIÁRIA: UM MERCADO FINANCEIRO POUPADOR VIA BLOCKCHAIN COMO ALTERNATIVA AO INSS E FGTS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia Elétrica do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia Elétrica.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. José Cláudio do Nascimento (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Xxxxxxx Xxxxxx Xxxxxxx
Universidade do Membro da Banca Dois (SIGLA)

Prof. Dr. Xxxxxxx Xxxxxx Xxxxxxx
Universidade do Membro da Banca Três (SIGLA)

Prof. Dr. Xxxxxxx Xxxxxx Xxxxxxx
Universidade do Membro da Banca Quatro (SIGLA)

À minha mãe e ao meu pai e família, por todo o apoio incondicional durante essa jornada. A minha esposa, por finalmente decidir o assunto final ao qual deveria ser esse trabalho.

AGRADECIMENTOS

Em primeiro lugar, a Deus, o qual permitiu que meus objetivos fossem alcançados, durante todos os meus anos de estudos, dando-me saúde e resiliência.

A todos os colegas e amigos que me apoiaram, direta ou indiretamente, durante a realização desses árduos anos de graduação. Em especial a Mikhail Antonovich A. Barros, que me explicou que para vencer a graduação, eu só precisaria encontrar meu jeito, o que fora o começo do ponto de virada.

Ao Prof. Dr. David Nascimento Coelho, por me incentivar a terminar algo.

E principalmente ao Prof. Dr. José Cláudio do Nascimento, por ser inicialmente um ouvinte dos meus interesses, por me explicar temas tão complexos, mesmo que eu não os conseguisse entender, e principalmente por nunca ter desistido de mim.

“Qualquer um pode chegar onde cheguei, talvez até ultrapassar os limites que cheguei. Tenho certeza de que as ações proporcionam isso.”

(Luiz Barsi Filho)

RESUMO

O sistema previdenciário brasileiro, composto pelo Instituto Nacional do Seguro Social (INSS) e pelo Fundo de Garantia do Tempo de Serviço (FGTS), enfrenta desafios estruturais que comprometem sua sustentabilidade fiscal e a proteção efetiva dos trabalhadores. O déficit previdenciário consome parcela significativa do orçamento federal, enquanto o FGTS oferece rentabilidade historicamente inferior à inflação. Este trabalho propõe um modelo alternativo de mercado financeiro poupador baseado em tecnologia blockchain, inspirado no sistema australiano de *Superannuation*. A proposta consiste em um sistema onde os trabalhadores investem suas contribuições diretamente em empresas brasileiras, com governança compartilhada através de carteiras multi-assinatura (multi-sig) que requerem autorização conjunta do trabalhador e do governo para movimentações. O modelo preserva a propriedade individual dos recursos, garante a herança integral do patrimônio, promove transparência nas regras através de código auditável em blockchain – preservando a privacidade individual das transações – e restringe operações especulativas ao permitir apenas uma transação mensal. A fundamentação teórica aborda as escolas econômicas Austríaca e Desenvolvimentista, analisa o sistema previdenciário brasileiro, estuda o modelo australiano e introduz conceitos de blockchain. A metodologia adotada é de pesquisa exploratória e qualitativa, baseada em revisão bibliográfica e análise documental. Os resultados apresentam a arquitetura detalhada do sistema, incluindo camadas de blockchain, smart contracts e interface de usuário, além de regras operacionais e mecanismos de herança. Conclui-se que a proposta oferece uma alternativa viável aos problemas identificados, embora sua implementação enfrente desafios técnicos, políticos e sociais que demandam estudos futuros.

Palavras-chave: Previdência Social. Blockchain. Multi-assinatura. INSS. FGTS. Superannuation. Mercado de Capitais.

ABSTRACT

The Brazilian social security system, comprising the National Social Security Institute (INSS) and the Severance Indemnity Fund (FGTS), faces structural challenges that compromise its fiscal sustainability and effective worker protection. The pension deficit consumes a significant portion of the federal budget, while FGTS has historically offered returns below inflation. This work proposes an alternative savings-based financial market model built on blockchain technology, inspired by the Australian Superannuation system. The proposal consists of a system where workers invest their contributions directly in Brazilian companies, with shared governance through multi-signature (multi-sig) wallets that require joint authorization from both worker and government for any transactions. The model preserves individual ownership of resources, guarantees full inheritance of assets, promotes transparency in rules through auditable code on blockchain – while preserving individual transaction privacy – and restricts speculative operations by allowing only one transaction per month. The theoretical foundation addresses the Austrian and Developmentalist economic schools, analyzes the Brazilian pension system, studies the Australian model, and introduces blockchain concepts. The methodology adopted is exploratory and qualitative research, based on literature review and document analysis. The results present the detailed system architecture, including blockchain layers, smart contracts, and user interface, as well as operational rules and inheritance mechanisms. It is concluded that the proposal offers a viable alternative to the identified problems, although its implementation faces technical, political, and social challenges that require further studies.

Keywords: Social Security. Blockchain. Multi-signature. INSS. FGTS. Superannuation. Capital Markets.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O Brasil enfrenta desafios econômicos estruturais que limitam seu desenvolvimento há décadas. Embora temas como corrupção, disputas políticas e polarização ideológica dominem o debate público e engajem intensamente a opinião popular, esses fenômenos são inerentes à natureza humana e ao processo político em si — a corrupção nasce da autopreservação e de interesses pessoais, características intrínsecas à ação humana em sociedade. Paradoxalmente, o foco excessivo nesses temas desvia a atenção dos problemas verdadeiramente estruturantes: a infraestrutura deficiente, a baixa taxa de poupança nacional, o crédito historicamente caro e a falta de oportunidades que elevem o nível de qualidade de vida da população (GIAMBIAGI; ALéM, 2011). Afinal, todo povo aspira à prosperidade, independentemente de sua posição no espectro político.

O sistema previdenciário brasileiro, composto principalmente pelo Instituto Nacional do Seguro Social (INSS) e pelo Fundo de Garantia do Tempo de Serviço (FGTS), foi concebido com o objetivo de garantir proteção social aos trabalhadores. Contudo, ao longo das décadas, esses mecanismos tornaram-se um peso fiscal significativo — os gastos com previdência e assistência social representam aproximadamente 54% das despesas primárias do governo federal — limitando severamente a capacidade de investimento do Estado em áreas essenciais como educação, saúde e infraestrutura (Instituição Fiscal Independente, 2023).

O modelo atual opera sob o regime de repartição simples, onde as contribuições dos trabalhadores ativos financiam os benefícios dos aposentados. Este sistema, embora solidário em sua concepção, apresenta vulnerabilidades frente ao envelhecimento populacional e às mudanças no mercado de trabalho. Além disso, os recursos do FGTS são direcionados ao governo, que os utiliza para financiamento habitacional e infraestrutura, oferecendo ao trabalhador rentabilidade inferior à inflação (AFONSO *et al.*, 2016).

Diante desse cenário, este trabalho propõe uma alternativa inspirada no modelo australiano de aposentadoria (*Superannuation*), adaptada à realidade brasileira e potencializada pela tecnologia blockchain. A proposta consiste em criar um mercado financeiro poupador que substitua gradualmente o INSS e FGTS, permitindo que os trabalhadores invistam diretamente em empresas nacionais, com controle compartilhado entre governo e cidadão, garantindo segurança jurídica e transparência.

Justificativa

A relevância deste estudo reside na necessidade urgente de reformar o sistema previdenciário brasileiro, que se encontra em situação de insustentabilidade fiscal. As reformas implementadas até o momento têm sido paliativas, ajustando parâmetros como idade mínima e tempo de contribuição, sem alterar a estrutura fundamental do sistema.

A tecnologia blockchain oferece uma oportunidade única de implementar um sistema transparente, imutável e descentralizado, capaz de garantir a propriedade individual dos recursos previdenciários enquanto mantém mecanismos de controle que evitem a liquidação prematura ou uso inadequado dos fundos.

Objetivos

O objetivo geral deste trabalho é propor um modelo de mercado financeiro poupador baseado em blockchain como alternativa ao sistema previdenciário atual (INSS e FGTS).

Os objetivos específicos são:

a) Analisar os problemas estruturais do sistema previdenciário brasileiro atual;
b) Estudar o modelo australiano de *Superannuation* como referência internacional;
c) Propor uma arquitetura de sistema blockchain para gestão previdenciária;
d) Identificar os benefícios e desafios da implementação do modelo proposto.

Estrutura do Trabalho

Este trabalho está organizado da seguinte forma: o Capítulo 2 apresenta a fundamentação teórica, abordando as escolas econômicas, o sistema previdenciário brasileiro, o modelo australiano e a tecnologia blockchain. O Capítulo 3 descreve a metodologia utilizada. O Capítulo 4 apresenta a proposta detalhada do sistema. Por fim, o Capítulo 5 traz as conclusões e sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta os fundamentos teóricos necessários para a compreensão da proposta deste trabalho. Inicialmente, são discutidas as duas principais correntes econômicas que influenciam o debate sobre política econômica brasileira. Em seguida, analisa-se o sistema previdenciário brasileiro atual. Posteriormente, apresenta-se o modelo australiano de aposentadoria como referência internacional. Por fim, introduz-se a tecnologia blockchain e suas aplicações potenciais.

2.1 Escolas Econômicas e o Debate Brasileiro

O debate econômico brasileiro é historicamente marcado pela contraposição entre duas visões distintas sobre o papel do Estado e os mecanismos de desenvolvimento econômico.

2.1.1 Escola Austríaca de Economia

A Escola Austríaca de Economia, cujos principais expoentes incluem Ludwig von Mises, Friedrich Hayek e Carl Menger, fundamenta-se em princípios que enfatizam o papel da poupança e do livre mercado no desenvolvimento econômico (MISES, 1949).

Segundo esta corrente, a poupança é a base fundamental para o investimento produtivo. A acumulação de capital através da poupança voluntária permite o financiamento de projetos de longo prazo, aumentando a produtividade e, consequentemente, o padrão de vida da população. Para os austríacos, a interferência governamental no sistema de preços e na alocação de recursos gera distorções que resultam em má alocação de capital e ciclos econômicos (HAYEK, 1944).

A teoria austríaca defende que o livre mercado, através do sistema de preços, é o mecanismo mais eficiente para coordenar as decisões econômicas de milhões de indivíduos. A intervenção estatal, mesmo bem-intencionada, tende a gerar consequências não previstas que frequentemente agravam os problemas que pretendia resolver.

2.1.2 Escola Desenvolvimentista

Em contraposição, a escola desenvolvimentista, influenciada pelo pensamento keynesiano, argumenta que economias em crise ou subdesenvolvimento necessitam de intervenção

estatal ativa para estimular a demanda agregada e superar armadilhas de baixo crescimento (KEYNES, 1936).

Esta corrente defende que o Estado deve atuar como indutor do desenvolvimento, coordenando investimentos estratégicos, protegendo a indústria nascente e redistribuindo renda para estimular o mercado interno. O desenvolvimentismo brasileiro influenciou fortemente as políticas econômicas desde a Era Vargas, com a criação de empresas estatais e mecanismos de fomento.

Os desenvolvimentistas argumentam que o livre mercado, em países periféricos, tende a perpetuar a condição de exportador de commodities e importador de manufaturados, impedindo o desenvolvimento industrial autônomo.

2.1.3 Implicações para a Política Previdenciária

A tensão entre estas duas visões manifesta-se claramente no debate previdenciário. A perspectiva austríaca tenderia a favorecer sistemas de capitalização individual, onde cada trabalhador acumula sua própria poupança para aposentadoria. Já a visão desenvolvimentista justifica sistemas de repartição solidária, onde o Estado coordena a redistribuição intergeracional.

O sistema brasileiro atual, baseado na repartição, reflete historicamente a influência desenvolvimentista. Contudo, as dificuldades fiscais crescentes têm levado a questionamentos sobre sua sustentabilidade de longo prazo.

2.2 O Sistema Previdenciário Brasileiro

O sistema previdenciário brasileiro é composto por três pilares principais: o Regime Geral de Previdência Social (RGPS), administrado pelo INSS; os Regimes Próprios de Previdência Social (RPPS), para servidores públicos; e a Previdência Complementar, de caráter facultativo.

2.2.1 INSS: Estrutura e Funcionamento

O Instituto Nacional do Seguro Social (INSS) é responsável pela administração do RGPS, que cobre a maioria dos trabalhadores brasileiros do setor privado. O sistema opera sob o regime de repartição simples, onde as contribuições correntes dos trabalhadores ativos financiam os benefícios dos aposentados e pensionistas (GENTIL, 2006).

As alíquotas de contribuição variam de 7,5% a 14% sobre o salário de contribuição, dependendo da faixa salarial. Já os empregadores enquadrados no Lucro Real ou Lucro Presumido contribuem com 20% sobre a folha de pagamento, enquanto empresas optantes pelo Simples Nacional têm alíquotas reduzidas ou isentas conforme o anexo em que se enquadram. Estes recursos são destinados ao pagamento de aposentadorias por idade, por tempo de contribuição, aposentadorias especiais, pensões por morte e auxílios diversos.

O déficit do RGPS tem crescido consistentemente, atingindo R$ 318,4 bilhões em 2023, conforme dados do Tesouro Nacional (Tesouro Nacional, 2024). Este desequilíbrio decorre de fatores demográficos (envelhecimento populacional), estruturais (informalidade do mercado de trabalho) e políticos (regras de benefícios desconectadas da capacidade contributiva).

2.2.2 FGTS: Histórico e Problemas

O Fundo de Garantia do Tempo de Serviço (FGTS) foi criado em 1966 como alternativa à estabilidade decenal no emprego. Mensalmente, os empregadores depositam 8% do salário do trabalhador em conta vinculada, que pode ser sacada em situações específicas como demissão sem justa causa, aposentadoria, compra de imóvel ou doenças graves.

Contudo, o FGTS apresenta problemas estruturais significativos. A rentabilidade do fundo, limitada à Taxa Referencial (TR) mais 3% ao ano, historicamente ficou abaixo da inflação, resultando em perda real do poder de compra do trabalhador (AFONSO *et al.*, 2016). Estudo do Centro de Políticas Públicas do Insper indica que, ao longo de 30 anos de trabalho, o trabalhador pode perder até 40% do valor real de suas contribuições quando comparado a aplicações em índices de inflação (CARVALHO *et al.*, 2019).

Os recursos do FGTS são utilizados pelo governo para financiar programas habitacionais (Minha Casa Minha Vida) e obras de infraestrutura e saneamento, conforme estabelecido na Lei nº 8.036/1990 (Brasil, 1990). Embora estes investimentos possam gerar benefícios sociais, representam uma transferência de riqueza dos trabalhadores para políticas públicas, sem a devida remuneração pelo custo de oportunidade.

2.2.3 Impacto Fiscal e Sustentabilidade

O sistema previdenciário brasileiro consome aproximadamente 13% do PIB, percentual elevado para um país com estrutura demográfica ainda relativamente jovem. Projeções atuariais indicam que, sem reformas estruturais, este percentual pode ultrapassar 20% nas

próximas décadas (TAFNER *et al.*, 2019).

Os gastos com previdência social (RGPS e RPPS) e assistência social (BPC/LOAS e Bolsa Família) representam aproximadamente 54% das despesas primárias do governo federal, limitando severamente a capacidade de investimento público em áreas essenciais (Instituição Fiscal Independente, 2023). Esta rigidez orçamentária cria um círculo vicioso: a falta de investimento em infraestrutura e educação reduz a produtividade, que por sua vez diminui a arrecadação e agrava o déficit previdenciário.

2.3 O Modelo Australiano de Superannuation

A Austrália implementou, a partir de 1992, um sistema de aposentadoria baseado em capitalização individual obrigatória, conhecido como *Superannuation*. Este modelo é frequentemente citado como referência internacional de sucesso (BATEMAN *et al.*, 2001).

2.3.1 Estrutura do Sistema

O *Superannuation* obriga empregadores a contribuir com um percentual do salário do empregado (atualmente 11%, com previsão de aumento para 12%) para um fundo de aposentadoria em nome do trabalhador. Os recursos são geridos por fundos de pensão privados, sujeitos a regulamentação governamental.

Os trabalhadores podem escolher entre diferentes fundos e estratégias de investimento, desde opções conservadoras até mais agressivas, de acordo com seu perfil de risco e horizonte temporal. Os recursos só podem ser acessados ao atingir a idade de preservação (atualmente entre 55 e 60 anos, dependendo da data de nascimento) ou em circunstâncias específicas como invalidez permanente.

2.3.2 Resultados e Lições

Após três décadas de operação, o sistema australiano acumulou mais de 3,5 trilhões de dólares australianos em ativos, equivalente a aproximadamente 170% do PIB do país. Este volume de poupança de longo prazo contribuiu significativamente para o desenvolvimento do mercado de capitais australiano e para o financiamento de investimentos produtivos.

O modelo demonstra que sistemas de capitalização individual podem ser implementados com sucesso, desde que acompanhados de regulamentação adequada, transparência e

mecanismos de proteção ao investidor. A diversificação de investimentos e a gestão profissional resultaram em rentabilidade média superior à inflação ao longo do tempo.

Contudo, o modelo também apresenta desafios, como a cobertura inadequada de trabalhadores informais, a complexidade do sistema para trabalhadores com baixa educação financeira e a exposição a riscos de mercado.

2.4 Tecnologia Blockchain

A tecnologia blockchain, popularizada inicialmente pelo Bitcoin em 2008, apresenta características que a tornam potencialmente aplicável a sistemas de registro e gestão de ativos previdenciários (NAKAMOTO, 2008).

2.4.1 Fundamentos Criptográficos e Históricos

2.4.1.1 O Problema dos Generais Bizantinos

O **Problema dos Generais Bizantinos**, formalizado por Lamport *et al.* (1982), descreve um cenário em que múltiplos generais de um exército cercando uma cidade precisam coordenar um ataque simultâneo. Alguns generais podem ser traidores, enviando mensagens contraditórias para sabotar o plano. A questão central é: como os generais leais podem alcançar consenso sobre uma estratégia comum, mesmo na presença de traidores?

Este problema abstrato representa o desafio fundamental de sistemas distribuídos: como múltiplos nós de uma rede podem concordar sobre o estado verdadeiro de um sistema quando alguns nós podem estar comprometidos ou agindo maliciosamente. Durante décadas, cientistas da computação consideraram impossível resolver este problema em redes abertas e sem autoridade central — até o surgimento do Bitcoin.

2.4.1.2 Hashcash e Prova de Trabalho

Em 1997, Adam Back propôs o **Hashcash**, um sistema anti-spam que exigia dos remetentes de e-mail a realização de um trabalho computacional antes do envio (BACK, 2002). A ideia central é simples: encontrar um valor que, quando combinado com os dados da mensagem e processado por uma função *hash* criptográfica, produza um resultado com determinado número de zeros iniciais.

Este conceito — exigir "prova de trabalho" (*Proof of Work*) — tornou-se o mecanismo central pelo qual o Bitcoin resolve o Problema dos Generais Bizantinos. Para adicionar um bloco à cadeia, mineradores competem para encontrar um *hash* válido, gastando recursos computacionais reais. Um atacante que desejasse fraudar o sistema precisaria refazer todo esse trabalho, tornando ataques economicamente inviáveis.

A função *hash* criptográfica possui propriedades essenciais:

a) **Determinística**: A mesma entrada sempre produz a mesma saída;
b) **Unidirecional**: É computacionalmente inviável obter a entrada a partir da saída;
c) **Sensível**: Qualquer alteração mínima na entrada produz saída completamente diferente;
d) **Resistente a colisões**: É extremamente improvável encontrar duas entradas que produzam a mesma saída.

2.4.1.3 O Problema do Gasto Duplo

Em sistemas monetários digitais anteriores ao Bitcoin, o **problema do gasto duplo** (*double spending*) representava o obstáculo fundamental. Diferentemente de moedas físicas, dados digitais podem ser copiados infinitamente. O que impede alguém de gastar a mesma "moeda digital" múltiplas vezes?

Soluções centralizadas, como bancos, resolvem isso mantendo um livro-razão único e autoritativo. Porém, isso reintroduz a necessidade de confiar em terceiros e cria pontos únicos de falha.

A inovação do Bitcoin foi combinar a prova de trabalho com uma cadeia de blocos (*blockchain*) onde cada bloco referencia o *hash* do bloco anterior, criando uma sequência cronológica imutável. Quando dois nós tentam gastar a mesma moeda simultaneamente, a rede aceita apenas a transação incluída no bloco que eventualmente se torna parte da cadeia mais longa. A regra do "maior trabalho acumulado" resolve conflitos de forma determinística, sem necessidade de autoridade central.

2.4.2 Criptografia de Chaves Assimétricas

2.4.2.1 Chaves Privadas e Públicas

A blockchain utiliza criptografia de chaves assimétricas, onde cada participante possui um par de chaves matematicamente relacionadas:

a) **Chave Privada**: Número secreto de 256 bits, gerado aleatoriamente. Quem possui a chave privada tem controle absoluto sobre os fundos associados. Deve ser mantida em segredo absoluto — se perdida, os fundos tornam-se permanentemente inacessíveis; se roubada, podem ser transferidos pelo ladrão;

b) **Chave Pública**: Derivada matematicamente da chave privada através de multiplicação por curva elíptica. Pode ser compartilhada livremente e é usada para gerar endereços de recebimento. É computacionalmente inviável calcular a chave privada a partir da pública.

A relação entre as chaves segue o princípio da "função de mão única com alçapão" (*trapdoor function*): é trivial calcular a chave pública a partir da privada, mas virtualmente impossível fazer o inverso, a menos que se possua a chave privada original.

Para autorizar uma transação, o proprietário utiliza sua chave privada para gerar uma **assinatura digital**. Qualquer pessoa pode verificar a validade desta assinatura usando a chave pública correspondente, confirmando que apenas o legítimo proprietário poderia ter autorizado a operação — sem que a chave privada seja revelada.

2.4.2.2 Carteiras Hierárquicas Determinísticas (HD Wallets)

Uma limitação da abordagem original era a necessidade de gerar e armazenar separadamente cada par de chaves. Os padrões **BIP-32** (WUILLE, 2012), **BIP-39** (PALATINUS *et al.*, 2013) e **BIP-44** introduziram o conceito de **Carteiras Hierárquicas Determinísticas** (*HD Wallets*).

A partir de uma única **semente mnemônica** — tipicamente 12 ou 24 palavras em linguagem natural — é possível derivar deterministicamente uma árvore virtualmente infinita de chaves privadas e públicas. Esta abordagem oferece vantagens significativas:

a) **Backup simplificado**: Anotar 24 palavras em papel é suficiente para recuperar todas as carteiras;

b) **Derivação hierárquica**: É possível criar sub-carteiras para diferentes propósitos

(conta corrente, poupança, investimentos) a partir da mesma semente;

c) **Privacidade aumentada**: Gerar novo endereço para cada transação dificulta rastreamento;

d) **Carteiras frias**: A semente pode ser gerada e armazenada *offline*, em dispositivos jamais conectados à internet.

Ferramentas como o **BIP39 Mnemonic Code Converter** de Ian Coleman (COLEMAN, 2015) permitem gerar e verificar sementes mnemônicas de forma transparente, sendo amplamente utilizadas para criação de carteiras frias. A geração deve ocorrer em ambiente *offline* e seguro, preferencialmente em sistema operacional efêmero (como Tails OS) executado a partir de mídia somente-leitura.

2.4.3 Características Arquiteturais

Blockchain é uma estrutura de dados distribuída que mantém um registro imutável e transparente de transações. As principais características incluem:

a) **Descentralização**: Os dados são replicados em múltiplos nós da rede, eliminando pontos únicos de falha;

b) **Imutabilidade**: Uma vez registradas, as transações não podem ser alteradas ou excluídas;

c) **Transparência ou privacidade**: Dependendo da implementação, as transações podem ser públicas e verificáveis, ou privadas com valores e destinatários ocultos;

d) **Segurança criptográfica**: As transações são protegidas por algoritmos criptográficos robustos.

2.4.4 Smart Contracts e Multi-sig

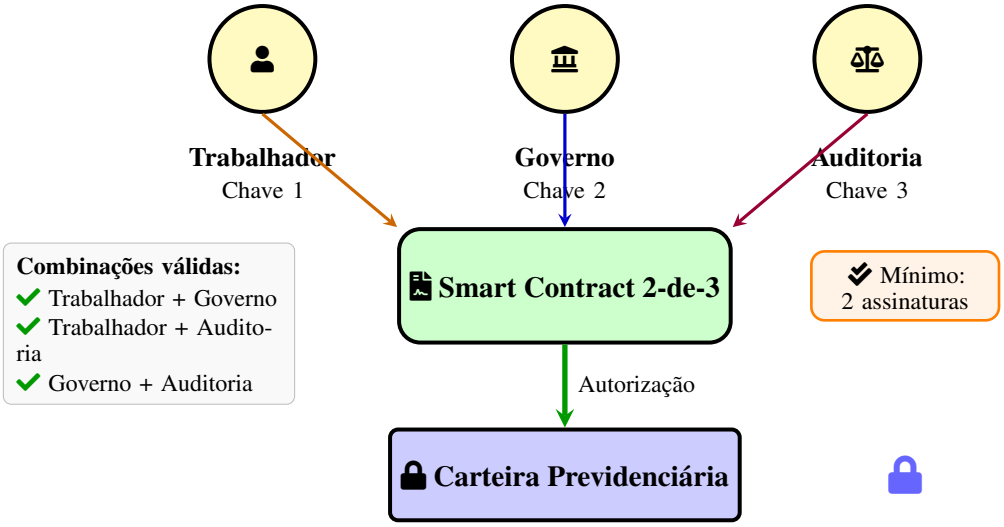
Smart contracts são programas autoexecutáveis armazenados na blockchain que executam automaticamente quando condições predefinidas são satisfeitas. Esta funcionalidade permite a automação de regras complexas de governança (BUTERIN, 2014).

Carteiras multi-assinatura (multi-sig) requerem múltiplas chaves privadas para autorizar uma transação. Por exemplo, uma carteira 2-de-3 requer que pelo menos duas de três chaves autorizem qualquer movimentação. Este mecanismo permite implementar sistemas de controle compartilhado, onde nenhuma parte individual possui controle total sobre os recursos.

A Figura 1 ilustra o funcionamento de uma carteira multi-assinatura 2-de-3 no

contexto do sistema proposto.

Figura 1 – Arquitetura de Carteira Multi-assinatura 2-de-3



Fonte: Elaborada pelo autor (2026).

Neste modelo, o trabalhador mantém uma das chaves, o governo (ou órgão regulador) mantém outra, e uma entidade de auditoria independente possui a terceira. Operações rotineiras, como contribuições mensais e investimentos dentro de parâmetros pré-aprovados, podem ser executadas com a assinatura do trabalhador e do sistema automatizado do governo. Operações excepcionais — como saques antecipados ou transferências para herdeiros — requerem verificação adicional pela auditoria.

Este arranjo garante que: (1) o trabalhador não pode ser impedido de acessar seus recursos sem justa causa; (2) o governo não pode confiscar unilateralmente os fundos; (3) fraudes requerem conluio entre pelo menos duas das três partes.

2.4.5 Aplicações em Sistemas Financeiros

Diversas aplicações de blockchain em sistemas financeiros têm sido desenvolvidas, incluindo moedas digitais de bancos centrais (CBDCs), sistemas de liquidação de ativos, registro de propriedade e identidade digital. Estas aplicações demonstram a viabilidade técnica de utilizar blockchain para gerenciar ativos de valor significativo com segurança e transparência.

A tokenização de ativos, processo de representar direitos de propriedade sobre ativos reais em tokens na blockchain, abre possibilidades para fracionamento de investimentos e aumento da liquidez de ativos tradicionalmente ilíquidos.

2.5 Síntese

A fundamentação teórica apresentada estabelece as bases para a proposta deste trabalho. O sistema previdenciário brasileiro enfrenta desafios fiscais estruturais que demandam soluções inovadoras. O modelo australiano demonstra a viabilidade de sistemas de capitalização individual. A tecnologia blockchain oferece mecanismos técnicos para implementar sistemas transparentes, seguros e com governança compartilhada. A convergência destes elementos fundamenta a proposta de um mercado financeiro poupador baseado em blockchain, a ser detalhada nos capítulos seguintes.

2.6 Soluções para Pagamento da Dívida Previdenciária

Qualquer reforma em larga escala deve evitar gerar desânimo social, especialmente quando decisões burocráticas podem ser vistas como expropriação ou calote das contribuições feitas com o esforço de uma vida inteira. Além disso, medidas que desconsiderem os direitos dos trabalhadores podem prejudicar o *rating* econômico do país e minar a confiança na previdência.

É essencial preservar a dignidade daqueles que trabalharam durante toda a vida, garantindo que suas contribuições sejam corrigidas pela inflação, mesmo que ajustes sejam necessários, como descontos por benefícios já usufruídos (auxílio-maternidade, auxílio-doença, entre outros). Sem essa consideração, o trabalhador pode perder a motivação para investir em trabalho e educação, comprometendo o desenvolvimento de futuras gerações. Assim como a **Curva de Laffer** demonstra que existe um ponto ótimo de tributação — onde aumentar impostos além de certo limite reduz a arrecadação total — é possível traçar uma analogia com o empenho do trabalhador em relação aos seus direitos previdenciários (LAFFER, 2004).

Se o trabalhador percebe que suas contribuições ao longo de décadas serão confiscadas, diluídas pela inflação ou simplesmente não retornarão com juros reais, o incentivo para trabalhar formalmente, estudar e contribuir para o sistema diminui drasticamente. Portanto, o primeiro passo para implementação de uma reforma deve ser pagar, com juros e correção, os depósitos feitos ao longo da vida de todos os brasileiros vivos, convertidos na forma de ativos no novo sistema.

Custe o que custar, o país deve estar à venda.

2.6.1 Aluguel do Patrimônio Nacional

A alienação permanente do patrimônio natural de um país para equilibrar as contas de um governo específico suscita questionamentos legítimos sobre a relação custo-benefício intergeracional. O caso da Companhia Vale do Rio Doce ilustra essa controvérsia: conforme documentado por Pinheiro (2000), críticos apontam que o valor arrecadado na privatização de 1997 foi recuperado pelos novos controladores em poucos anos de operação, levantando dúvidas sobre a adequação do preço de venda. Em contrapartida, a privatização da Telebrás representa um caso de menor contestação, tendo sido responsável pela universalização do acesso à telefonia e pela criação da infraestrutura que posteriormente viabilizou a expansão da internet no país (PIRES, 1999).

A análise desses dois casos revela um padrão: a crítica concentra-se menos na transferência de gestão ao setor privado e mais na **perda definitiva** de ativos estratégicos. Essa observação conduz a uma alternativa intermediária: o **arrendamento** de longo prazo. Diferentemente da venda, o aluguel preserva a titularidade do patrimônio nacional enquanto gera fluxo de receita — não há alienação permanente, apenas concessão temporária de uso.

Nesse modelo, praias, parques, patrimônios tombados e edifícios públicos poderiam ser arrendados por períodos de 5, 10, 20 ou 30 anos, conforme a natureza do ativo. Os recursos captados seriam direcionados ao equacionamento das dívidas atuariais do FGTS e do INSS, atacando diretamente o problema central desta proposta. Ao término do contrato, o patrimônio retornaria integralmente ao Estado, possivelmente valorizado pelos investimentos realizados durante a concessão.

Um aspecto crucial dessa estratégia é a preferência pelo mercado externo como contraparte. A captação de recursos estrangeiros evita o risco de bancos nacionais financiarem o arrendamento com recursos domésticos, o que configuraria uma mera transferência contábil sem entrada efetiva de capital novo na economia.

2.6.2 Arrendamento de Tributação de Cidades Turísticas

Uma verdade difícil de aceitar é que o Brasil não sabe gerir sua infraestrutura de turismo. Para ilustrar: apenas a ilha de Mallorca, na Espanha, gerou receita turística de aproximadamente 16 bilhões de euros em 2023, enquanto todo o Brasil arrecadou cerca de 6 bilhões de dólares no mesmo período (Instituto Nacional de Estadística, 2023; Embratur, 2023;

UNWTO, 2023).

Essa ineficiência brasileira no setor turístico pode, paradoxalmente, ser transformada em um ativo valioso. Cada cidade minimamente popular no Nordeste brasileiro representa um potencial de bilhões de dólares caso sua tributação seja arrendada para gestão estrangeira. Após 30 anos de contrato, o Brasil retomaria o controle com um bônus significativo: o aprendizado sobre como desenvolver seu próprio turismo de forma eficiente.

2.6.3 Arrendamento para Lançamento de Foguetes

A eficiência dos lançamentos espaciais aumenta significativamente quanto mais próximo da linha do Equador, devido à maior velocidade tangencial da rotação terrestre nessa região, o que reduz o consumo de combustível necessário para atingir a órbita (WERTZ; LARSON, 2011).

A Tabela 1 demonstra a vantagem geográfica do Brasil em relação aos principais centros de lançamento do mundo.

Tabela 1 – Comparativo de Localização de Bases de Lançamento

Local	**Latitude**	**Distância ao Equador**
Cabo Canaveral (Flórida – EUA)	$\sim$28,5° Norte	$\approx$ 3.160 km
Alcântara (Maranhão – Brasil)	$\sim$2,3° Sul	$\approx$ 255 km
Sobral (Ceará – Brasil)	$\sim$3,7° Sul	$\approx$ 410 km

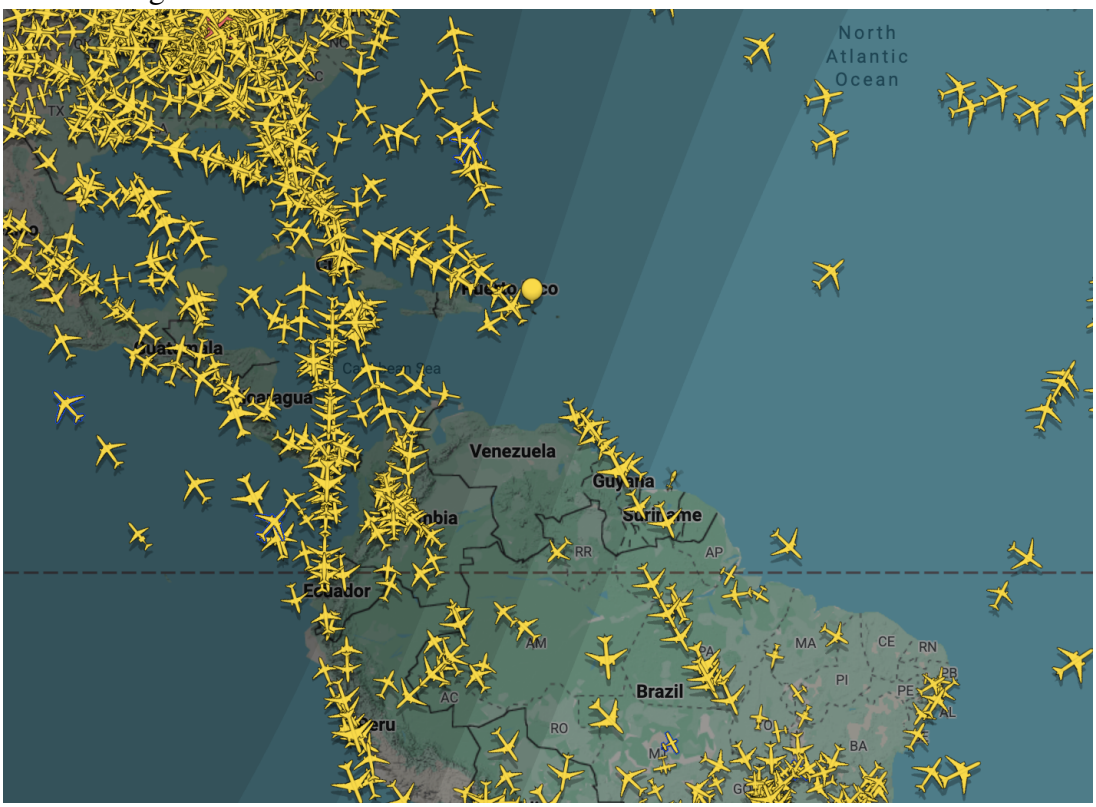
Fonte: Elaborado pelo autor (2026).

Fatores adicionais favorecem a região Norte e Nordeste do Brasil:

a) **Ausência de furacões**: diferentemente de Cabo Canaveral, a região não sofre com fenômenos climáticos extremos que causam cancelamentos frequentes;
b) **Baixo tráfego aéreo**: menor interferência no espaço aéreo reduz atrasos operacionais, conforme demonstrado na Figura 2;
c) **Condições meteorológicas estáveis**: clima predominantemente ensolarado durante todo o ano, com alta previsibilidade (INMET, 2023; FUNCEME, 2022).

Cidades como **Sobral (CE)**, situada a apenas 155 km adicionais do Equador em relação a Alcântara, apresentam vantagens competitivas relevantes: proximidade do Porto do Pecém — um dos mais modernos do país, com capacidade para receber cargas de grande porte —, e localização estratégica a 230 km de Fortaleza, capital com aeroporto internacional e infraestrutura logística consolidada.

Figura 2 – Tráfego Aéreo sobre a América Latina



Fonte: Flightradar24 (Flightradar24, 2024).

Do ponto de vista de capital humano, a região concentra diversas instituições de ensino superior e técnico, com cursos de engenharia, física e automação industrial que formam profissionais com perfil adequado às demandas do setor aeroespacial. O Ceará destaca-se historicamente pelo alto índice de aprovação no Instituto Tecnológico de Aeronáutica (ITA), evidenciando uma cultura educacional voltada para áreas de alta complexidade tecnológica. Isso indica que a mão de obra qualificada necessária para operações espaciais poderia ser recrutada e capacitada localmente, reduzindo custos operacionais e gerando desenvolvimento regional.

Com base em dados públicos da SpaceX, o custo médio de um lançamento do Falcon 9 é de aproximadamente US$ 67 milhões (SpaceX, 2023). A economia de 30% em combustível proporcionada pela proximidade ao Equador pode representar uma redução de US$ 15 a 20 milhões por lançamento, considerando que o propelente representa cerca de 50-70% dos custos operacionais de uma missão (WERTZ; LARSON, 2011).

3 METODOLOGIA

Este capítulo apresenta os procedimentos metodológicos adotados para o desenvolvimento deste trabalho, incluindo a classificação da pesquisa, os métodos utilizados e as etapas de desenvolvimento da proposta.

3.1 Classificação da Pesquisa

Quanto à natureza, esta pesquisa classifica-se como aplicada, pois visa gerar conhecimentos para aplicação prática, direcionados à solução de um problema específico: a insustentabilidade do sistema previdenciário brasileiro (GIL, 2008).

Quanto aos objetivos, a pesquisa é exploratória e propositiva. É exploratória porque busca proporcionar maior familiaridade com o problema, tornando-o mais explícito através da análise de diferentes modelos previdenciários e tecnologias disponíveis. É propositiva porque culmina na apresentação de uma proposta de solução estruturada.

Quanto à abordagem, adota-se a perspectiva qualitativa, caracterizada pela análise interpretativa e contextualizada de fontes primárias e secundárias — incluindo legislação vigente, relatórios de organismos internacionais, dados econômicos públicos e estudos comparados de modelos previdenciários estrangeiros. Diferentemente de abordagens quantitativas, que privilegiam a mensuração estatística de variáveis, a pesquisa qualitativa permite explorar as relações conceituais entre sistemas complexos e propor soluções fundamentadas em princípios teóricos, ainda que não empiricamente testadas em larga escala (CRESWELL, 2014).

3.2 Procedimentos Técnicos

Os procedimentos técnicos utilizados incluem:

3.2.1 Pesquisa Bibliográfica

A pesquisa bibliográfica foi conduzida em bases de dados acadêmicas, incluindo Google Scholar, Scielo, Web of Science e repositórios institucionais. Foram consultadas obras clássicas de economia (Escola Austríaca e Desenvolvimentista), estudos sobre previdência social, documentação técnica sobre blockchain e relatórios de organismos internacionais.

Os termos de busca incluíram: “reforma previdenciária”, “sistema de capitalização”,

"superannuation", "blockchain financial applications", "multi-signature wallets", "INSS déficit", "FGTS rentabilidade", entre outros.

3.2.2 Pesquisa Documental

Foram analisados documentos oficiais, incluindo:

a) Legislação previdenciária brasileira (Lei 8.213/91, Emendas Constitucionais 20/98, 41/03 e 103/19);
b) Relatórios do Tesouro Nacional sobre resultado previdenciário;
c) Documentação do sistema australiano de Superannuation;
d) Whitepapers e documentação técnica de protocolos blockchain.

3.2.3 Análise Comparativa

Foi realizada análise comparativa entre o modelo brasileiro atual e o modelo australiano de Superannuation, identificando semelhanças, diferenças, pontos fortes e fragilidades de cada sistema. Esta análise fundamentou a identificação de elementos adaptáveis à realidade brasileira.

3.3 Etapas de Desenvolvimento

O desenvolvimento deste trabalho seguiu as seguintes etapas:

3.3.1 Etapa 1: Diagnóstico do Sistema Atual

Nesta etapa, foi realizado um levantamento detalhado do funcionamento do INSS e FGTS, incluindo:

a) Estrutura de contribuições e benefícios;
b) Evolução histórica do déficit;
c) Projeções atuariais;
d) Identificação dos principais problemas estruturais.

3.3.2 Etapa 2: Estudo de Modelos Internacionais

Foi estudado o modelo australiano de Superannuation como principal referência, analisando:

a) Estrutura de funcionamento;
b) Resultados após três décadas de operação;
c) Lições aprendidas e desafios;
d) Elementos adaptáveis ao contexto brasileiro.

3.3.3 Etapa 3: Estudo da Tecnologia Blockchain

Foram estudados os fundamentos técnicos de blockchain relevantes para a proposta:

a) Arquitetura de redes distribuídas;
b) Mecanismos de consenso;
c) Smart contracts e sua programabilidade;
d) Carteiras multi-assinatura e governança;
e) Casos de uso em sistemas financeiros.

3.3.4 Etapa 4: Elaboração da Proposta

Com base nas etapas anteriores, foi elaborada a proposta de sistema, contemplando:

a) Arquitetura geral do sistema;
b) Mecanismos de contribuição e investimento;
c) Sistema de governança com chaves multi-sig;
d) Regras de operação e restrições;
e) Mecanismos de herança e sucessão;
f) Análise de viabilidade e desafios.

3.3.5 Etapa 5: Validação Conceitual

A proposta foi validada conceitualmente através de:

a) Verificação de consistência interna;
b) Análise de aderência aos objetivos propostos;
c) Identificação de limitações e trabalhos futuros.

3.4 Limitações Metodológicas

Este trabalho apresenta limitações inerentes à sua natureza propositiva:

a) Não foi implementado um protótipo funcional do sistema proposto;

b) Não foram realizadas simulações quantitativas de impacto fiscal;

c) A proposta não aborda aspectos jurídicos detalhados de implementação;

d) Não foram conduzidas pesquisas de campo sobre aceitação social da proposta.

Estas limitações apontam direções para trabalhos futuros que possam aprofundar e validar empiricamente a proposta apresentada.

4 PROPOSTA DO SISTEMA

Este capítulo apresenta a proposta detalhada de um mercado financeiro poupador baseado em blockchain como alternativa ao sistema previdenciário atual. A proposta é estruturada em cinco componentes principais: arquitetura geral, mecanismo de contribuição e investimento, sistema de governança, regras operacionais e mecanismos de herança.

4.1 Visão Geral da Proposta

O sistema proposto visa criar um mercado financeiro poupador que substitua gradualmente o INSS e o FGTS, permitindo que os trabalhadores brasileiros acumulem patrimônio próprio através de investimentos em empresas nacionais. A proposta combina elementos do modelo australiano de Superannuation com as capacidades da tecnologia blockchain para criar um sistema transparente, seguro e com governança compartilhada.

Os princípios fundamentais do sistema são:

a) **Propriedade individual**: Os recursos pertencem ao trabalhador, não ao Estado;
b) **Investimento produtivo**: Os recursos são direcionados a empresas reais, gerando retorno econômico;
c) **Governança compartilhada**: Controle dividido entre trabalhador e governo, evitando uso indevido;
d) **Transparência nas regras**: Código auditável, com privacidade nas transações individuais;
e) **Automatização**: Regras executadas por smart contracts, reduzindo burocracia.

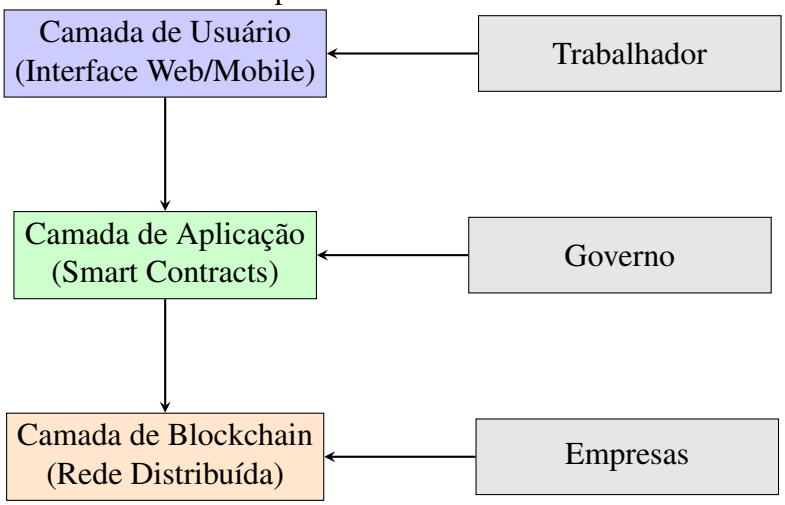
4.2 Arquitetura do Sistema

A arquitetura proposta é composta por três camadas principais, conforme ilustrado na Figura 3.

4.2.1 Camada de Blockchain

A camada base utiliza uma blockchain permissionada, operada por nós validadores distribuídos entre diferentes instituições (Banco Central, órgãos reguladores, grandes instituições financeiras). A escolha por blockchain permissionada, em vez de pública, justifica-se por:

Figura 3 – Arquitetura do Sistema Proposto



Fonte: Elaborado pelo autor (2026).

a) Maior controle sobre quem pode validar transações;
b) Melhor desempenho em termos de transações por segundo;
c) Conformidade regulatória mais facilitada;
d) Menor consumo energético comparado a redes de prova de trabalho.

4.2.2 Camada de Smart Contracts

Esta camada implementa toda a lógica de negócio do sistema através de smart contracts, incluindo:

a) **Contrato de Contribuição**: Recebe os depósitos mensais e registra na conta do trabalhador;
b) **Contrato de Investimento**: Gerencia as ordens de compra e venda de ativos;
c) **Contrato Multi-sig**: Implementa a governança compartilhada;
d) **Contrato de Herança**: Gerencia a transferência de ativos em caso de falecimento;
e) **Contrato de Compliance**: Verifica o cumprimento das regras operacionais.

4.2.3 Camada de Usuário

A interface de usuário consiste em aplicativo móvel e plataforma web que permitem ao trabalhador:

a) Visualizar seu saldo e histórico de contribuições;
b) Consultar sua carteira de investimentos;

c) Solicitar a operação mensal permitida;

d) Acompanhar a rentabilidade de seus investimentos;

e) Gerenciar beneficiários para herança.

4.3 Mecanismo de Contribuição e Investimento

4.3.1 Fluxo de Contribuição

O fluxo de contribuição proposto mantém a estrutura atual de desconto em folha, porém com destino diferente:

1. O empregador desconta o percentual do salário do trabalhador (similar ao atual);
2. O valor é convertido em tokens estáveis (stablecoins pareadas ao Real);
3. Os tokens são depositados automaticamente na carteira multi-sig do trabalhador;
4. O smart contract registra a transação e atualiza o saldo disponível para investimento.

4.3.2 Universo de Investimentos

O sistema propõe a criação de uma **bolsa tokenizada pareada em 1:1 com a B3**, onde cada ativo negociado na bolsa tradicional possui um token correspondente na blockchain previdenciária. Essa estrutura permite que os trabalhadores invistam nos mesmos ativos disponíveis no mercado convencional, porém com uma diferença fundamental: **privacidade de propriedade**.

Diferentemente do sistema tradicional, onde a CVM, corretoras e diversos intermediários têm acesso à identidade dos acionistas, os tokens previdenciários são projetados para que **apenas o próprio titular conheça sua carteira de investimentos**. A blockchain registra a existência e validade dos tokens, mas a vinculação entre endereço da carteira e identidade do trabalhador permanece criptograficamente protegida. Essa arquitetura:

a) Impede que governos futuros identifiquem e tributem seletivamente determinados perfis de investidores;

b) Protege o trabalhador contra perseguições políticas baseadas em suas escolhas de investimento;

c) Elimina o risco de "caça às bruxas" contra quem investiu em setores posteriormente considerados controversos;

d) Preserva a fungibilidade dos tokens, já que não carregam histórico de propriedade

rastreável.

Os recursos podem ser investidos exclusivamente em ativos de empresas brasileiras, incluindo:

a) Ações de empresas listadas na B3;
b) Debêntures de empresas brasileiras;
c) Fundos de investimento em infraestrutura (FI-Infra);
d) Fundos imobiliários (FIIs);
e) Títulos públicos federais (como opção conservadora).

A restrição a ativos nacionais tem como objetivo:

a) Fomentar o mercado de capitais brasileiro;
b) Financiar o crescimento de empresas nacionais;
c) Evitar a evasão de divisas;
d) Criar um ciclo virtuoso de poupança e investimento interno.

4.3.3 Tokenização de Ativos

Os ativos elegíveis seriam tokenizados, ou seja, representados por tokens na blockchain. Cada token representa uma fração do ativo subjacente, permitindo:

a) Investimentos fracionados, acessíveis a pequenos poupadores;
b) Liquidação instantânea de operações;
c) Registro imutável de propriedade;
d) Auditabilidade completa das transações.

4.4 Sistema de Governança Multi-sig

O elemento central da proposta é o sistema de governança baseado em carteiras multi-assinatura, que implementa o controle compartilhado entre trabalhador e governo.

4.4.1 Estrutura das Chaves

Cada carteira previdenciária opera com um esquema 2-de-2, onde ambas as chaves são necessárias para autorizar transações:

a) **Chave do Trabalhador**: Controlada exclusivamente pelo titular da conta, armazenada em dispositivo pessoal seguro;

b) **Chave do Governo**: Controlada por órgão regulador (ex: Banco Central ou nova autarquia), utilizada para co-assinar transações válidas.

4.4.2 Fluxo de Autorização

Para realizar qualquer movimentação, o seguinte fluxo é executado:

1. O trabalhador inicia a solicitação através do aplicativo, assinando com sua chave;
2. O smart contract verifica se a operação está dentro das regras permitidas;
3. Se válida, a solicitação é encaminhada ao sistema governamental;
4. O sistema governamental co-assina automaticamente se todas as regras forem cumpridas;
5. A transação é executada e registrada na blockchain.

Este modelo garante que:

a) O governo sozinho não pode mover os recursos do trabalhador;

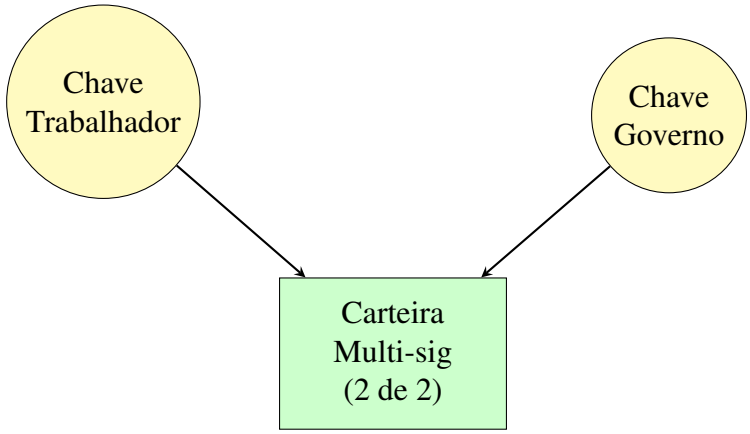
b) O trabalhador sozinho não pode violar as regras do sistema;

c) Há transparência nas regras, preservando a privacidade individual das transações.

4.4.3 Diagrama do Sistema Multi-sig

A Figura 4 ilustra o funcionamento do sistema de governança multi-sig.

Figura 4 – Sistema de Governança Multi-sig



Fonte: Elaborado pelo autor (2026).

4.5 Regras Operacionais

Para garantir que o sistema cumpra seu objetivo previdenciário, são impostas regras operacionais rígidas, implementadas diretamente nos smart contracts.

4.5.1 Restrição de Operações

Cada trabalhador pode realizar no máximo um lote de operações de compra e venda por mês. Esta restrição visa:

a) Evitar comportamento especulativo de curto prazo;

b) Incentivar visão de longo prazo nos investimentos;

c) Reduzir custos operacionais e de processamento;

d) Simplificar a gestão da carteira pelo trabalhador médio.

4.5.2 Bloqueio de Liquidação

Os recursos são bloqueados até a aposentadoria, com exceções limitadas:

a) Aposentadoria por idade ou tempo de contribuição;

b) Invalidez permanente comprovada;

c) Doenças graves especificadas em lei;

d) Falecimento (transferência para herdeiros).

Diferentemente do FGTS atual, não há saque para compra de imóvel ou demissão, reforçando o caráter estritamente previdenciário dos recursos.

4.5.3 Limites de Concentração

Para proteção do trabalhador, o sistema oferece limites de diversificação configuráveis. Os valores específicos — como percentual máximo por empresa ou por setor — podem ser definidos de forma flexível no momento da adesão. Contudo, uma vez escolhidos e aceitos pelo trabalhador, esses limites tornam-se **imutáveis** para aquela carteira, garantindo que regras não sejam alteradas retroativamente em prejuízo do titular.

Alternativamente, o sistema pode oferecer **atualizações opcionais** de regras: quando novos limites forem propostos pelo órgão regulador, o trabalhador recebe notificação e decide se aceita ou não a mudança. Caso recuse, sua carteira continua operando sob as regras originalmente contratadas. Exemplos de limites configuráveis:

a) Percentual máximo do patrimônio em uma única empresa;

b) Percentual máximo em um único setor da economia;

c) Percentual mínimo em ativos de baixo risco (títulos públicos ou equivalentes).

Essa arquitetura preserva a autonomia do trabalhador enquanto impede que governos

futuros imponham unilateralmente restrições prejudiciais aos investimentos já realizados.

4.5.4 Tabela de Regras Operacionais

A Tabela 2 resume as principais regras operacionais do sistema.

Tabela 2 – Resumo das Regras Operacionais

Regra	**Descrição**
Operações mensais	Máximo 1 lote de compra/venda por mês
Ativos elegíveis	Apenas empresas/ativos brasileiros
Limites de concentração	Configuráveis na adesão, imutáveis após aceite
Saque	Apenas na aposentadoria ou exceções legais
Governança	Multi-sig 2-de-2 (trabalhador + governo)

Fonte: Elaborado pelo autor (2026).

4.6 Mecanismo de Herança

Um diferencial importante do sistema proposto é o tratamento da herança, que difere fundamentalmente do INSS atual.

4.6.1 Herança Total do Patrimônio

No sistema proposto, em caso de falecimento do titular, 100% do patrimônio acumulado é transferido para os herdeiros designados. Isso contrasta com o sistema atual, onde o trabalhador que falece antes de se aposentar perde grande parte de suas contribuições.

Um princípio fundamental desta proposta é que **o governo não deve ter gerência sobre como os ganhos do trabalhador serão usufruídos após sua morte**. Diferentemente do direito sucessório tradicional, que impõe regras de parentesco e quotas obrigatórias, o sistema previdenciário proposto confere ao titular **autonomia absoluta** na designação de seus beneficiários. O trabalhador pode escolher livremente quem receberá seu patrimônio — sejam familiares, amigos, instituições ou qualquer pessoa de sua confiança — assumindo integralmente o risco de suas escolhas.

É importante ressaltar que esse nível de autonomia patrimonial **já existe para os mais ricos**, através de estruturas jurídicas sofisticadas como *holdings* familiares, *trusts* internacionais e fundações privadas. Esses instrumentos permitem às elites econômicas contornar as regras de sucessão obrigatória, proteger patrimônio de credores e designar livremente seus beneficiários.

Contudo, os custos de implementação e manutenção dessas estruturas — honorários advocatícios, taxas de constituição, contabilidade especializada e consultoria tributária — frequentemente superam o patrimônio total acumulado por um trabalhador médio ao longo de toda sua vida. O sistema proposto **democratiza esse direito**, conferindo ao trabalhador comum as mesmas garantias patrimoniais hoje restritas às elites, sem custos adicionais além da própria contribuição previdenciária.

Esta abordagem evita distorções do sistema jurídico atual. O caso de Elize Matsunaga ilustra a falha do modelo vigente: condenada pelo homicídio do marido Marcos Matsunaga em 2012, ela ainda assim herdou parte do patrimônio da vítima, conforme as regras de sucessão brasileiras que priorizam vínculos formais sobre a vontade presumida do falecido (Tribunal de Justiça de São Paulo, 2012). No sistema proposto, apenas os beneficiários *expressamente designados* pelo titular — e que possuam a chave privada compartilhada em vida — teriam acesso ao patrimônio, eliminando heranças indesejadas decorrentes de vínculos legais que não refletem a real vontade do trabalhador.

O trabalhador pode, a qualquer momento, cadastrar seus beneficiários no sistema, especificando:

a) Endereço da carteira do sucessor;
b) Percentual destinado a cada beneficiário.

4.6.2 Processo de Transferência

Em caso de falecimento:

1. A família apresenta certidão de óbito e a chave privada do titular falecido;
2. O patrimônio é transferido para novas carteiras multi-sig dos herdeiros;
3. Os herdeiros assumem o controle, mantendo as mesmas regras operacionais;
4. Os recursos permanecem bloqueados até que cada herdeiro atinja sua própria idade de aposentadoria.

Esta regra de bloqueio até a aposentadoria do herdeiro garante o incentivo à produção e à necessidade do trabalho ao longo de toda a vida, evitando que heranças previdenciárias se tornem mecanismo de ociosidade.

4.7 Transição do Sistema Atual

A implementação do sistema proposto requer o pagamento integral da dívida previdenciária acumulada antes da migração completa. Esta premissa é inegociável: nenhum trabalhador deve ser prejudicado pela transição.

4.7.1 Estratégia de Transição Gradual

A migração inicia obrigatoriamente pelos **trabalhadores mais jovens**, ordenados por ano de nascimento. Esta escolha é estratégica: os cidadãos mais novos acumularam relativamente poucas contribuições ao sistema atual, resultando em valores de quitação significativamente menores. Um trabalhador de 20 anos pode ter contribuído por apenas 2-3 anos, enquanto um de 55 anos acumula décadas de contribuições que precisam ser reconhecidas e pagas.

Simultaneamente, o governo deve iniciar o pagamento aos **trabalhadores mais velhos**, demonstrando seu comprometimento genuíno com a transição. Contudo, há uma diferença fundamental no cálculo da dívida para esta faixa etária: **os idosos já receberam boa parte do que aportaram em vida**. Um aposentado de 80 anos que contribuiu por 35 anos e já recebe benefícios há 15 anos teve grande parte de suas contribuições retornadas na forma de aposentadoria mensal. O saldo devedor, portanto, é substancialmente menor do que o valor bruto contribuído — podendo inclusive ser negativo para aqueles que já receberam mais do que aportaram.

Esta realidade altera significativamente a dinâmica de custos da transição. Enquanto os jovens possuem valores individuais baixos mas são numerosos, os idosos possuem valores individuais potencialmente baixos (ou nulos) e são menos numerosos. O resultado é que, com a mesma dotação orçamentária, a frente jovem avança mais lentamente em termos de faixas etárias cobertas, enquanto a frente sênior pode cobrir rapidamente as idades mais avançadas.

Esta abordagem bidirecional — jovens e idosos sendo atendidos em paralelo — cria um efeito pedagógico importante: assim como na transição tecnológica digital, onde os jovens frequentemente ensinam os mais velhos a utilizar novas ferramentas, espera-se que a familiaridade dos jovens com o novo sistema facilite a adoção pelos mais experientes.

As **velocidades de migração** devem ser proporcionais à capacidade de pagamento. Propõe-se alocar metade do valor disponível em caixa para cada frente:

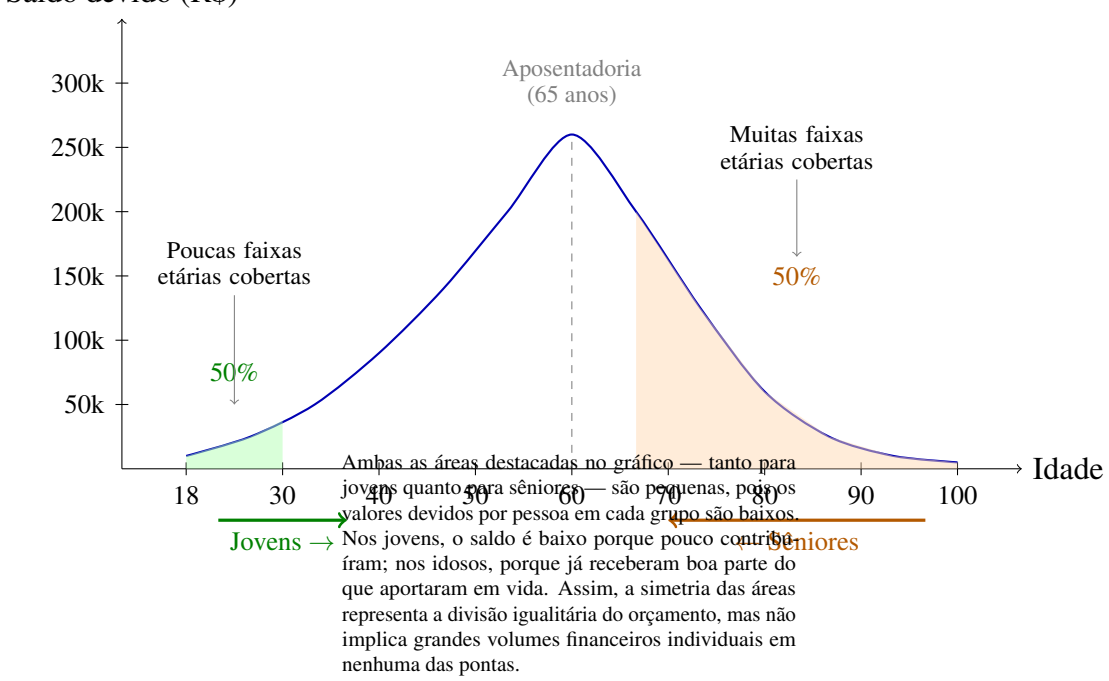
a) **50% para a frente jovem**: Cobre poucas faixas etárias por período, pois há

muitas pessoas com valores baixos cada;

b) **50% para a frente sênior**: Cobre muitas faixas etárias rapidamente, pois há poucas pessoas com saldo devedor reduzido.

A Figura 5 ilustra esta dinâmica, mostrando a relação entre idade e valor *líquido* devido — ou seja, contribuições menos benefícios já recebidos.

Figura 5 – Estratégia de Transição Bidirecional por Faixa Etária



Fonte: Elaborado pelo autor com base em dados do Anuário Estatístico da Previdência Social (Ministério da Previdência Social, 2023).

Esta estratégia bidirecional apresenta vantagens significativas:

a) **Viabilidade financeira**: Com o mesmo orçamento, a frente sênior avança mais rápido em número de faixas etárias;

b) **Sinalização política**: O pagamento aos sêniores demonstra que não se trata de calote geracional;

c) **Transferência de conhecimento**: Os jovens, nativos digitais, auxiliam os mais velhos na adaptação ao novo sistema;

d) **Convergência gradual**: As duas frentes eventualmente se encontram na faixa etária intermediária (40-50 anos), onde estão os maiores saldos devedores.

4.7.2 Financiamento da Transição

O principal desafio da transição é o financiamento dos benefícios atuais enquanto as contribuições são direcionadas ao novo sistema. Propõe-se:

a) Utilização de receitas do patrimônio público (royalties, dividendos de estatais);
b) Recursos provenientes do arrendamento do patrimônio nacional conforme proposto na Seção 2;
c) Redução gradual do déficit primário através de reformas administrativas;
d) Emissão de títulos de longo prazo específicos para a transição previdenciária.

4.8 Benefícios Esperados

A implementação do sistema proposto traria benefícios em múltiplas dimensões:

4.8.1 Para o Trabalhador

a) Propriedade real sobre os recursos poupados;
b) Rentabilidade potencialmente superior à inflação;
c) Herança garantida para a família;
d) Transparência nas regras, com privacidade sobre saldos individuais.

4.8.2 Para a Economia

a) Aumento da taxa de poupança nacional;
b) Desenvolvimento do mercado de capitais;
c) Redução do custo de capital para empresas;
d) Financiamento de investimentos produtivos.

4.8.3 Para o Estado

a) Eliminação gradual do déficit previdenciário;
b) Liberação de recursos para investimentos públicos;
c) Redução da carga tributária potencial no longo prazo;
d) Modernização da infraestrutura financeira.

4.9 Desafios e Riscos

A proposta também apresenta desafios significativos:

4.9.1 Desafios Técnicos

a) Escalabilidade da blockchain para milhões de usuários;
b) Segurança cibernética e proteção das chaves privadas;
c) Integração com sistemas legados e bases governamentais;
d) Educação financeira da população.

4.9.2 Desafios Políticos

a) Resistência de grupos beneficiados pelo sistema atual;
b) Necessidade de reforma constitucional;
c) Coordenação entre múltiplos órgãos governamentais;
d) Comunicação efetiva com a população.

4.9.3 Riscos de Mercado

a) Exposição dos trabalhadores a volatilidade do mercado;
b) Possibilidade de perdas em períodos de crise;
c) Necessidade de mecanismos de proteção para trabalhadores próximos à aposentadoria.

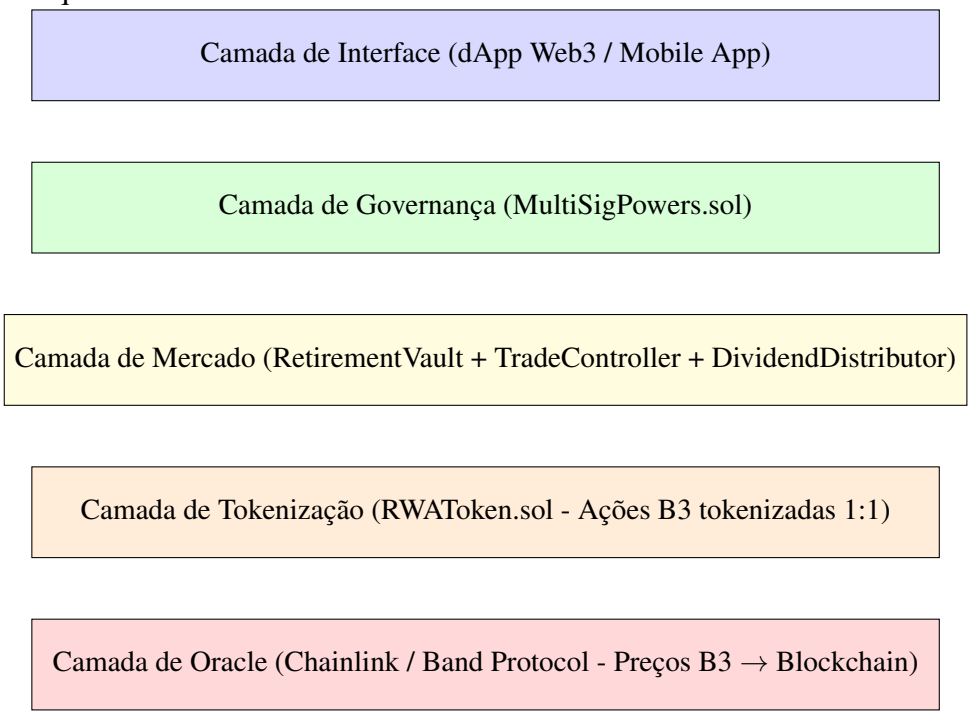
4.10 Arquitetura Descentralizada do Mercado

Esta seção detalha como o mercado financeiro poupador pode ser concebido de maneira descentralizada, utilizando tecnologia blockchain para garantir transparência, segurança e governança distribuída.

4.10.1 Camadas da Arquitetura Descentralizada

O sistema é organizado em cinco camadas interdependentes, conforme ilustrado na Figura 6.

Figura 6 – Arquitetura em Camadas do Mercado Descentralizado



Fonte: Elaborado pelo autor (2026).

4.10.1.1 Camada de Tokenização (RWA - Real World Assets)

A tokenização de ativos reais é o fundamento do mercado descentralizado. Cada ação negociada na B3 é representada por um token ERC-20 na blockchain, mantendo paridade 1:1 com o ativo custodiado:

a) **Custódia Regulada**: Instituição custodiante autorizada pela CVM mantém as ações reais na CBLC (Central de Custódia e Liquidação);
b) **Mint/Burn Controlado**: Tokens só podem ser criados (mint) quando ações são depositadas, e destruídos (burn) quando ações são resgatadas;
c) **Auditoria Trimestral**: Verificação independente de que totalSupply() = ações custodiadas;
d) **Pausabilidade**: Mecanismo de emergência para pausar operações em caso de inconsistências.

4.10.1.2 Camada de Oracle

Os oracles são responsáveis por sincronizar informações do mundo real (preços da B3) com a blockchain:

a) **Múltiplas Fontes**: Agregação de dados de B3, Bloomberg, Reuters e Yahoo Finance;

b) **Mediana de Preços**: Utilização da mediana para resistir a manipulação de uma única fonte;

c) **Heartbeat Check**: Atualização obrigatória a cada 15 minutos durante pregão;

d) **Circuit Breaker**: Pausa automática se o desvio entre fontes exceder 10%.

4.10.1.3 Camada de Mercado

O mercado pode ser implementado através de duas abordagens:

Opção A - Automated Market Maker (AMM): Pools de liquidez para cada par de ativos (ex: PETR4/BRL), onde o preço é determinado algoritmicamente pela proporção de ativos no pool. Vantagens: liquidez constante, operação 24/7.

Opção B - Order Book On-Chain: Livro de ordens descentralizado onde compradores e vendedores postam ordens limite. Vantagens: menor slippage para grandes volumes, descoberta de preço mais eficiente.

4.10.2 Poderes do Smart Contract Multi-Sig

O elemento central da governança é a definição precisa dos poderes de cada parte. A Tabela 3 apresenta a matriz de poderes implementada no smart contract.

Tabela 3 – Matriz de Poderes do Smart Contract Multi-Sig

Operação	**Indivíduo**	**Governo**	**Condição**
Trade mensal	✓Exclusivo	× Bloqueado	Cooldown 30 dias
Liquidação total	× Bloqueado	× Bloqueado	Idade $<$ 65 anos
Liquidação total	✓Livre	– N/A	Idade $\geq$ 65 anos
Adicionar herdeiro	✓Exclusivo	× Bloqueado	Sempre
Confisco judicial	– N/A	✓Exclusivo	Com ordem judicial
Registrar óbito	– N/A	✓Exclusivo	Com certidão
Distribuir herança	– N/A	✓Autoriza	Após óbito
Liquidar estate	– N/A	✓Pleno	Após 100 anos
Whitelist de ativos	× Bloqueado	✓Exclusivo	Sempre

Fonte: Elaborado pelo autor (2026).

4.10.2.1 Poderes do Indivíduo

O indivíduo (trabalhador) possui os seguintes poderes exclusivos:

a) **Executar Trades**: Pode comprar e vender ativos livremente dentro do universo

de investimentos permitido, respeitando o limite de 1 operação por mês;

b) **Gerenciar Beneficiários**: Tem controle exclusivo sobre quem são seus herdeiros e qual percentual cada um receberá;

c) **Prova de Vida**: Deve submeter prova de vida anual para manter sua carteira ativa;

d) **Plenos Poderes após 65 anos**: Ao atingir a idade de aposentadoria, pode liquidar qualquer posição sem necessidade de aprovação governamental.

É fundamental notar que o governo **não pode** fazer trades em nome do indivíduo. Esta restrição garante que a alocação de capital seja feita pela "mão invisível" das decisões individuais agregadas, não por uma autoridade central.

4.10.2.2 Poderes do Governo

O governo possui poderes específicos e limitados:

a) **Whitelist de Ativos**: Controla quais ativos podem ser negociados no sistema, garantindo que apenas empresas brasileiras reguladas participem;

b) **Registro de Óbito**: Único autorizado a registrar falecimento no sistema, mediante apresentação de certidão;

c) **Distribuição de Herança**: Autoriza a transferência de ativos para os beneficiários cadastrados;

d) **Confisco Judicial**: Pode executar ordens judiciais de confisco, mas apenas com autorização do Poder Judiciário;

e) **Plenos Poderes após 100 anos**: Em caso de ausência de prova de vida por 100 anos, assume controle total para liquidação do estate.

É crucial observar que o governo **não pode** confiscar ativos sem ordem judicial. O smart contract exige a role `JUDICIAL_ROLE` além de `GOVERNMENT_ROLE` para executar qualquer confisco.

4.10.2.3 Checks and Balances

O sistema implementa um mecanismo de freios e contrapesos onde:

a) O indivíduo sozinho não pode liquidar antes dos 65 anos (protege contra gastos impulsivos);

b) O governo sozinho não pode mover os ativos (protege contra confisco arbitrário);

c) O código é imutável após deploy (protege contra mudanças políticas);
d) O código é público e auditável (garante transparência das regras, não dos saldos individuais).

4.10.3 Descentralização Progressiva

A implementação do sistema pode seguir um caminho de descentralização progressiva:

Fase 1 - Federada (Anos 1-5): Governo opera os nós validadores, custodiantes regulados pela CVM, contratos auditados mas upgradáveis via timelock.

Fase 2 - Híbrida (Anos 6-15): Validadores distribuídos (40% governo, 60% entidades privadas), DAO para propostas de mudança, contratos com timelock de 30 dias para upgrades.

Fase 3 - Descentralizada (Anos 16+): Validadores eleitos por stake, governança 100% on-chain, contratos imutáveis.

4.11 O Problema do Bloqueio

Historicamente, governos exercem pressão sobre a segurança jurídica dos indivíduos e buscam controlar o valor de seus bens. Na criação do Bitcoin, Satoshi Nakamoto incluiu a seguinte mensagem no bloco gênesis (NAKAMOTO, 2009):

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Essa referência à manchete do jornal *The Times* sobre o segundo resgate governamental aos bancos britânicos evidencia a predileção estatal pelas grandes elites financeiras, fenômeno amplamente documentado por Frédéric Bastiat em sua obra *A Lei* (1850) (BASTIAT, 1850), onde o autor francês argumenta:

> *"A lei pervertida! E os poderes de polícia do Estado pervertidos junto com ela! A lei, digo eu, não apenas desviada de seu propósito adequado, mas transformada para seguir um propósito inteiramente contrário! [...] A lei convertida em instrumento de espoliação!"*

Portanto, deve haver uma maneira de o cidadão comum — que não usufrui da mesma proteção jurídica aplicada a poucos — obter algum benefício ao aportar em sua previdência sem correr risco de confisco.

4.11.1 O Risco do Bloqueio de Ativos

Para que o sistema funcione, os ativos de um indivíduo devem ser auditáveis: ele precisa ter acesso real aos tokens e o direito de trocá-los. Contudo, surge um problema crítico: se o governo conseguir vincular determinado token a determinado indivíduo, basta ordenar que todas as entidades financeiras sob sua jurisdição bloqueiem aquele token específico. Isso invalidaria completamente a proposta de segurança via blockchain.

O caso da China com o Bitcoin ilustra essa vulnerabilidade (HUANG *et al.*, 2021). O governo chinês não perseguiu diretamente os detentores de criptomoedas — foi atrás das *exchanges* centralizadas, que serviam como pontos de entrada e saída do ecossistema. Ao pressionar esses intermediários, conseguiu restringir significativamente o uso de Bitcoin no país sem precisar identificar cada usuário individualmente.

4.11.2 Inviabilidade Prática do Bloqueio Massivo

Para identificar e bloquear os ativos de um único indivíduo em um sistema com privacidade robusta, o governo precisaria dissolver todo o mecanismo de anonimização — forçando **todos** os participantes a revelarem suas identidades e converterem seus tokens para ativos rastreáveis.

Para ilustrar a inviabilidade dessa abordagem, considere o seguinte cenário hipotético:

A **Klabin S.A.** (KLBN11), maior produtora e exportadora de papéis do Brasil, possui aproximadamente **1,1 milhão de acionistas pessoas físicas** registrados na B3 (dados de 2023). Se apenas **30% desses acionistas** participassem do sistema previdenciário proposto, teríamos cerca de **330 mil indivíduos** cujos ativos estariam protegidos por anonimização.

Para bloquear os tokens de **um único suspeito**, o governo precisaria:

1. Ordenar que todos os 330 mil participantes revelem suas identidades;
2. Suspender temporariamente a negociação de todos os tokens vinculados à Klabin;
3. Reemitir tokens rastreáveis após identificação completa;
4. Reintegrar os participantes legítimos ao sistema.

O custo operacional, jurídico e político de tal operação seria astronomicamente superior ao benefício de identificar um indivíduo. Multiplique esse cenário pelas **400+ empresas listadas na B3** e a impossibilidade prática torna-se evidente: o sistema seria autoimune a bloqueios cirúrgicos, protegendo o trabalhador comum sem impedir investigações legítimas em larga escala.

4.11.2.1 Custo Financeiro de Bloqueio em Escala Nacional

Para dimensionar a inviabilidade econômica de bloqueios massivos, considere os custos operacionais envolvidos. O Brasil possui aproximadamente **110 milhões de pessoas economicamente ativas** (PNAD 2023). Se todas participassem do sistema proposto:

Tabela 4 – Custo Estimado de Bloqueio em Escala Nacional

Métrica	**Valor**
População economicamente ativa	110 milhões
Custo de bloqueio por pessoa	R$ 250-400
Custo total para dissolução do sistema	**R$ 27,5 - 44 bilhões**
Tempo estimado de processamento	5-10 anos
Processos judiciais gerados	$\sim$30-50 milhões

Fonte: Elaborado pelo autor (2026).

Essa assimetria de custos cria uma **barreira econômica natural** contra abusos estatais: perseguir um indivíduo exigiria atacar milhões.

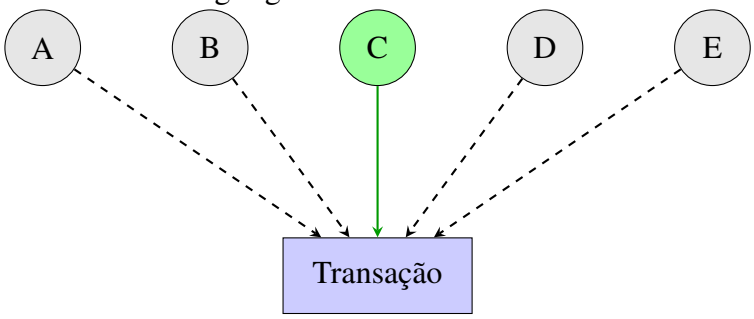
4.11.3 A Solução da Monero: Privacidade por Design

Criptomoedas como **Monero (XMR)** demonstram que a anonimização é tecnicamente viável (The Monero Project, 2023). A Monero utiliza três mecanismos principais para desvincular tokens de indivíduos:

4.11.3.1 Ring Signatures (Assinaturas em Anel)

Cada transação mistura a assinatura do remetente com outras assinaturas aleatórias, tornando impossível identificar quem realmente enviou os fundos. O remetente real é “escondido” entre múltiplos participantes fictícios, conforme ilustrado na Figura 7.

Figura 7 – Funcionamento das Ring Signatures



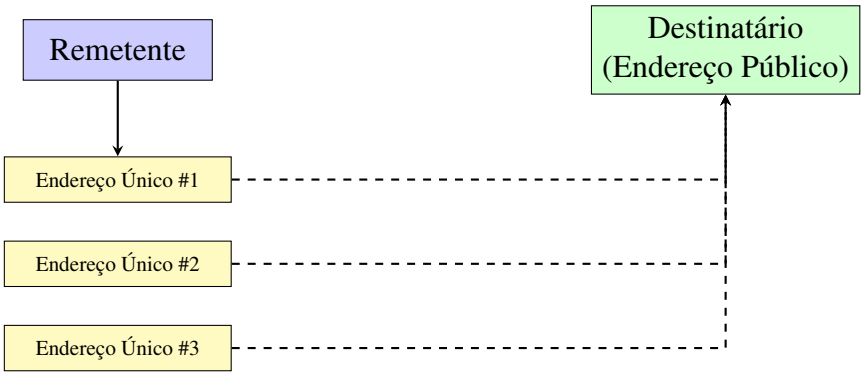
Observador não consegue distinguir
qual usuário é o remetente real

Fonte: Elaborado pelo autor (2026).

4.11.3.2 Stealth Addresses (Endereços Furtivos)

Para cada transação, um endereço único e descartável é gerado automaticamente. Mesmo que alguém conheça o endereço público de um usuário, não consegue rastrear os recebimentos na blockchain. A Figura 8 ilustra este mecanismo.

Figura 8 – Funcionamento dos Stealth Addresses



Na blockchain, cada transação
aparece com endereço diferente

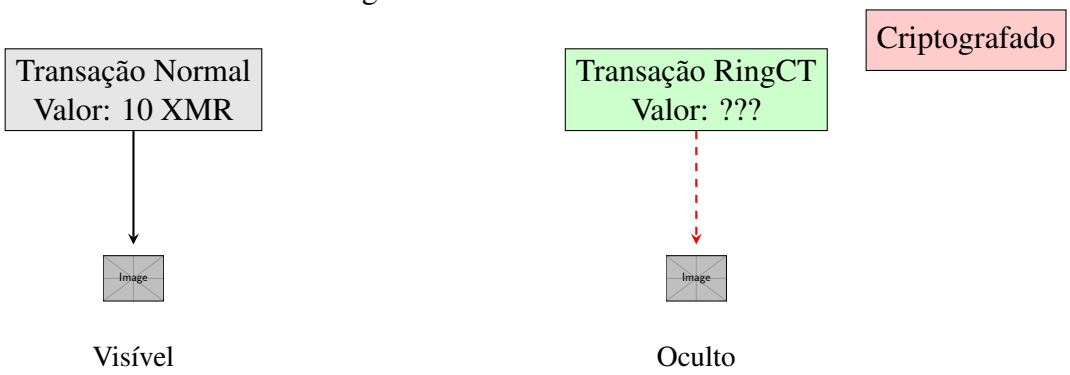
Fonte: Elaborado pelo autor (2026).

4.11.3.3 RingCT (Ring Confidential Transactions)

Os valores transacionados são criptografados, impedindo que observadores externos saibam quanto foi transferido. A Figura 9 demonstra como os valores são ocultados.

Essas técnicas garantem que, mesmo com a blockchain sendo pública, não seja possível vincular transações a indivíduos específicos — validando a possibilidade de um sistema

Figura 9 – Funcionamento do RingCT



Fonte: Elaborado pelo autor (2026).

previdenciário resistente a bloqueios arbitrários.

4.11.4 Comparativo: Sistema Atual vs Sistema Proposto

A Tabela 5 apresenta um comparativo entre as características do sistema atual (INSS/FGTS) e o sistema proposto baseado em blockchain.

Tabela 5 – Comparativo entre Sistema Atual e Sistema Proposto

Aspecto	**Sistema Atual**	**Sistema Proposto**
Transparência	Opaca, difícil auditoria	100% transparente, auditável
Propriedade	Governo é dono dos recursos	Indivíduo é dono (com regras)
Herança	Limitada por lei	Configurável pelo titular
Rendimento	Abaixo da inflação (FGTS)	Mercado de ações brasileiro
Portabilidade	Nenhuma	Global (chave privada)
Resistência a mudanças	Sujeito a políticas	Código imutável é lei
Custo operacional	Alto (burocracia estatal)	Baixo (automação)

Fonte: Elaborado pelo autor (2026).

4.11.5 Mitigação de Riscos da Descentralização

A Tabela 6 apresenta os principais riscos do sistema descentralizado e suas respectivas mitigações.

Tabela 6 – Riscos e Mitigações do Sistema Descentralizado

Risco	**Mitigação**
Perda de chave privada	Social recovery wallets, custódia colaborativa, federações de custódia (Fedimint)
Bug em smart contract	Múltiplas auditorias independentes, programa de bug bounty, deploy gradual
Manipulação de oracle	Múltiplas fontes de dados, mediana, circuit breakers
Colapso do mercado	Diversificação obrigatória, circuit breakers, reserva em ativos de baixo risco
Ataque 51%	Utilização de redes estabelecidas (Ethereum, Polygon) com alta segurança

Fonte: Elaborado pelo autor (2026).

5 CONCLUSÕES E TRABALHOS FUTUROS

Este capítulo apresenta as conclusões do trabalho, sintetizando os principais resultados obtidos e indicando direções para trabalhos futuros.

5.1 Conclusões

Este trabalho propôs um modelo de mercado financeiro poupador baseado em blockchain como alternativa ao sistema previdenciário brasileiro atual, composto pelo INSS e FGTS. A proposta foi desenvolvida a partir da análise crítica do sistema vigente, do estudo do modelo australiano de Superannuation e das possibilidades oferecidas pela tecnologia blockchain.

O diagnóstico do sistema previdenciário brasileiro revelou problemas estruturais significativos. O INSS opera com déficits crescentes que comprometem o orçamento federal e limitam a capacidade de investimento do Estado. O FGTS oferece rentabilidade inferior à inflação, representando uma transferência silenciosa de riqueza dos trabalhadores para o financiamento de políticas públicas. Ambos os sistemas operam sob lógica de repartição ou gestão estatal, onde o trabalhador não possui propriedade real sobre suas contribuições.

O modelo australiano de Superannuation demonstrou que sistemas de capitalização individual podem ser implementados com sucesso, gerando acumulação significativa de poupança de longo prazo e contribuindo para o desenvolvimento do mercado de capitais. Após três décadas de operação, o sistema acumulou volume de recursos equivalente a 170% do PIB australiano.

A tecnologia blockchain oferece mecanismos técnicos para implementar um sistema com características desejáveis: transparência através de registros públicos e auditáveis, segurança através de criptografia e descentralização, e governança compartilhada através de carteiras multi-assinatura.

A proposta desenvolvida combina estes elementos em um sistema onde:

a) Os trabalhadores são proprietários reais de seus recursos previdenciários;
b) Os recursos são investidos em empresas brasileiras, fomentando o desenvolvimento nacional;
c) A governança é compartilhada entre trabalhador e governo através de carteiras multi-sig 2-de-3;
d) Regras operacionais restritivas garantem o uso previdenciário dos recursos;
e) O patrimônio é integralmente herdável em caso de falecimento.

Os objetivos específicos propostos foram atingidos:

1. Foi realizada análise dos problemas estruturais do sistema previdenciário brasileiro, identificando déficits crescentes, rentabilidade negativa do FGTS e ausência de propriedade individual;
2. Foi estudado o modelo australiano de Superannuation, extraindo lições sobre estrutura de funcionamento, regulamentação e resultados de longo prazo;
3. Foi proposta uma arquitetura de sistema blockchain para gestão previdenciária, incluindo camadas de blockchain, smart contracts e interface de usuário, com detalhamento do sistema de governança multi-sig;
4. Foram identificados benefícios (propriedade individual, rentabilidade, herança, desenvolvimento do mercado de capitais) e desafios (escalabilidade técnica, resistência política, educação financeira) da implementação.

A proposta representa uma mudança paradigmática na concepção do sistema previdenciário, transitando de um modelo onde o Estado administra recursos coletivos para um modelo onde o indivíduo é proprietário de sua poupança, com supervisão estatal para garantir o cumprimento das regras.

Reconhece-se que a implementação de tal proposta enfrentaria desafios significativos, incluindo resistência política de grupos beneficiados pelo sistema atual, necessidade de reformas constitucionais, desafios técnicos de escalabilidade e segurança, e a necessidade de ampla educação financeira da população.

Contudo, diante da trajetória insustentável do sistema atual, a busca por alternativas inovadoras torna-se imperativa. Este trabalho contribui para esse debate ao apresentar uma proposta estruturada que aproveita tecnologias emergentes para criar um sistema mais justo, transparente e sustentável.

5.2 Trabalhos Futuros

Este trabalho abre diversas possibilidades para pesquisas futuras:

5.2.1 Desenvolvimento Técnico

a) Implementação de um protótipo funcional do sistema em ambiente de teste (testnet);

b) Análise de escalabilidade de diferentes plataformas blockchain para o volume esperado de transações;
c) Desenvolvimento de interfaces de usuário acessíveis para diferentes perfis de trabalhadores;
d) Estudo de mecanismos de segurança para proteção das chaves privadas dos usuários.

5.2.2 Análise Quantitativa

a) Simulação do impacto fiscal da transição em diferentes cenários;
b) Modelagem atuarial comparando resultados projetados do novo sistema versus manutenção do sistema atual;
c) Análise de sensibilidade a diferentes parâmetros (alíquotas, rentabilidade, tempo de transição).

5.2.3 Aspectos Jurídicos e Regulatórios

a) Análise detalhada das alterações constitucionais e legais necessárias;
b) Estudo comparativo de marcos regulatórios de outros países que implementaram reformas similares;
c) Proposta de arcabouço regulatório para custódia e negociação de ativos tokenizados.

5.2.4 Aspectos Sociais

a) Pesquisa de campo sobre percepção e aceitação da proposta pela população;
b) Desenvolvimento de programas de educação financeira adequados ao público-alvo;
c) Estudo de mecanismos de proteção para trabalhadores vulneráveis durante a transição.

5.2.5 Extensões do Modelo

a) Integração com sistema de identidade digital nacional;
b) Possibilidade de portabilidade internacional para trabalhadores migrantes;

c) Aplicação do modelo para outros tipos de poupança compulsória;

d) Estudo de mecanismos de seguro coletivo para proteção contra riscos de mercado.

A continuidade destas pesquisas poderá contribuir para amadurecer a proposta e eventualmente viabilizar sua implementação, contribuindo para a construção de um sistema previdenciário mais justo, sustentável e alinhado com as tecnologias do século XXI.

REFERÊNCIAS

AFONSO, L. E.; ZYLBERSTAJN, H.; SOUZA, A. P. Mudanças na previdência social: Uma avaliação dos efeitos de reformas paramétricas no RGPS. **Economia Aplicada**, v. 20, n. 4, p. 405–433, 2016.

BACK, A. Hashcash - a denial of service counter-measure. In: . [S.l.: s.n.], 2002. Disponível em: <http://www.hashcash.org/papers/hashcash.pdf>. Proposta original do sistema de prova de trabalho que inspirou o Bitcoin.

BASTIAT, F. **A Lei**. [S.l.]: Instituto Ludwig von Mises Brasil, 1850. Discussão sobre a perversão da lei como instrumento de espoliação.

BATEMAN, H.; KINGSTON, G.; PIGGOTT, J. **Forced Saving: Mandating Private Retirement Incomes**. Cambridge: Cambridge University Press, 2001.

Brasil. **Lei nº 8.036, de 11 de maio de 1990**. 1990. Dispõe sobre o Fundo de Garantia do Tempo de Serviço, e dá outras providências.

BUTERIN, V. A next-generation smart contract and decentralized application platform. 2014. Ethereum Whitepaper. Disponível em: <https://ethereum.org/whitepaper>.

CARVALHO, L.; SACHSIDA, A.; MENDES, M. **O FGTS e a Perda de Rendimento do Trabalhador Brasileiro**. São Paulo, 2019.

COLEMAN, I. **BIP39 Mnemonic Code Converter**. 2015. Ferramenta online. Acesso em: 16 jan. 2026. Disponível em: <https://iancoleman.io/bip39/>.

CRESWELL, J. W. **Research Design: Qualitative, Quantitative, and Mixed Methods Approaches**. 4. ed. Thousand Oaks: SAGE Publications, 2014.

Embratur. **Anuário Estatístico de Turismo 2023**. 2023. Ministério do Turismo. Estatísticas oficiais do turismo brasileiro, incluindo receita cambial. Disponível em: <https://www.gov.br/turismo/pt-br/acesso-a-informacao/acoes-e-programas/observatorio/anuario-estatistico-de-turismo>.

Flightradar24. **Live Air Traffic**. 2024. Flightradar24 AB. Dados em tempo real de tráfego aéreo global, demonstrando baixa densidade de voos sobre o Nordeste brasileiro. Disponível em: <https://www.flightradar24.com/>.

FUNCEME. Caracterização climática do estado do ceará. **Boletim Climatológico**, Fundação Cearense de Meteorologia e Recursos Hídricos, 2022. Análise do clima do Ceará, destacando a estabilidade meteorológica e ausência de fenômenos extremos. Disponível em: <http://www.funceme.br/>.

GENTIL, D. L. A política fiscal e a falsa crise da seguridade social brasileira: Análise financeira do período 1990-2005. **Texto para Discussão**, IPEA, n. 1207, 2006.

GIAMBIAGI, F.; ALéM, A. C. **Finanças Públicas: Teoria e Prática no Brasil**. 4. ed. Rio de Janeiro: Elsevier, 2011.

GIL, A. C. **Métodos e Técnicas de Pesquisa Social**. 6. ed. São Paulo: Atlas, 2008.

HAYEK, F. A. **The Road to Serfdom**. Chicago: University of Chicago Press, 1944.

HUANG, Y.; MIAO, M.; WANG, P.; XUE, L. The effects of china's cryptocurrency ban on digital asset markets. **Journal of Financial Economics**, v. 144, n. 2, p. 711–731, 2021. Análise empírica dos efeitos da proibição chinesa de criptomoedas sobre o mercado de ativos digitais, incluindo o fechamento de exchanges centralizadas.

INMET. **Normais Climatológicas do Brasil 1991-2020**. 2023. Instituto Nacional de Meteorologia. Dados climatológicos oficiais do Brasil, incluindo informações sobre o clima semiárido do Ceará. Disponível em: <https://portal.inmet.gov.br/normais>.

Instituição Fiscal Independente. **Relatório de Acompanhamento Fiscal**. [S.l.], 2023. Análise da composição das despesas primárias do governo federal.

Instituto Nacional de Estadística. **Estadística de Movimientos Turísticos en Fronteras (FRONTUR)**. 2023. Gobierno de España. Dados oficiais sobre movimento turístico nas Ilhas Baleares (Mallorca). Disponível em: <https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176996&menu=ultiDatos&idp=1254735576863>.

KEYNES, J. M. **The General Theory of Employment, Interest and Money**. London: Macmillan, 1936.

LAFFER, A. B. The laffer curve: Past, present, and future. **Backgrounder**, The Heritage Foundation, n. 1765, 2004. Análise histórica e aplicações da Curva de Laffer na política tributária. Disponível em: <https://www.heritage.org/taxes/report/the-laffer-curve-past-present-and-future>.

LAMPORT, L.; SHOSTAK, R.; PEASE, M. The byzantine generals problem. **ACM Transactions on Programming Languages and Systems**, ACM, v. 4, n. 3, p. 382–401, 1982. Formalização do problema fundamental de consenso em sistemas distribuídos.

Ministério da Previdência Social. **Anuário Estatístico da Previdência Social – AEPS 2023**. 2023. Brasília: MPS. Dados sobre contribuições, benefícios e perfil demográfico dos segurados do RGPS.

MISES, L. v. **Human Action: A Treatise on Economics**. New Haven: Yale University Press, 1949.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>.

NAKAMOTO, S. **Bitcoin Genesis Block**. 2009. Bloco #0 da blockchain do Bitcoin. Mensagem embutida no coinbase do bloco gênesis: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". Referência à manchete do jornal The Times sobre o resgate aos bancos britânicos. Disponível em: <https://blockchair.com/bitcoin/block/0>.

PALATINUS, M.; RUSNAK, P.; VOISINE, A.; BOWE, S. **BIP-39: Mnemonic code for generating deterministic keys**. 2013. Bitcoin Improvement Proposal. Padrão para geração de sementes mnemônicas de 12 ou 24 palavras.

PINHEIRO, A. C. A privatização no brasil: O caso da vale do rio doce. **Pesquisa e Planejamento Econômico**, IPEA, v. 30, n. 1, p. 1–36, 2000. Análise crítica do processo de privatização da Companhia Vale do Rio Doce.

PIRES, J. C. L. A reestruturação do setor de telecomunicações no brasil. **Revista do BNDES**, Banco Nacional de Desenvolvimento Econômico e Social, v. 6, n. 11, p. 187–214, 1999. Análise do processo de privatização do Sistema Telebrás e seus impactos na universalização dos serviços de telecomunicações no Brasil.

SpaceX. **Falcon 9: The World's First Orbital Class Reusable Rocket**. 2023. Space Exploration Technologies Corp. Especificações técnicas e custos operacionais do foguete Falcon 9. Disponível em: <https://www.spacex.com/vehicles/falcon-9/>.

TAFNER, P.; BOTELHO, C.; ERBISTI, R. **Reforma da Previdência: Por que o Brasil não pode esperar?** Rio de Janeiro: Elsevier, 2019.

Tesouro Nacional. Relatório, **Resultado do Regime Geral de Previdência Social (RGPS)**. 2024. Dados consolidados de 2023.

The Monero Project. **About Monero: Technical Information**. 2023. Documentação oficial do projeto Monero. Descrição das principais tecnologias de privacidade: Ring Signatures, Stealth Addresses e RingCT (Ring Confidential Transactions). Disponível em: <https://www.getmonero.org/resources/about/>.

Tribunal de Justiça de São Paulo. **Caso Elize Matsunaga: Processo de homicídio e questões sucessórias**. 2012. Elize Matsunaga foi condenada pelo homicídio do marido Marcos Matsunaga, mas manteve direitos sucessórios sobre parte do patrimônio conforme legislação brasileira.

UNWTO. **World Tourism Barometer**. 2023. World Tourism Organization. Estatísticas globais de turismo, incluindo receitas por país e região. Disponível em: <https://www.unwto.org/tourism-statistics/key-tourism-statistics>.

WERTZ, J. R.; LARSON, W. J. Space mission engineering: The new smad. **Space Technology Library**, Microcosm Press, 2011. Referência técnica sobre engenharia de missões espaciais, incluindo análise de custos de propelente e vantagens de lançamento equatorial.

WUILLE, P. **BIP-32: Hierarchical Deterministic Wallets**. 2012. Bitcoin Improvement Proposal. Especificação técnica para derivação hierárquica de chaves criptográficas.