



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.

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

E principalmente ao Prof. Dr. José Cláudio, 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 total através de registros em blockchain 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 total transparency through blockchain records, 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

Figura 1 – Arquitetura do Sistema Proposto	26
Figura 2 – Sistema de Governança Multi-sig	29
Figura 3 – Arquitetura em Camadas do Mercado Descentralizado	34

LISTA DE TABELAS

Tabela 1 – Resumo das Regras Operacionais	30
Tabela 2 – Matriz de Poderes do Smart Contract Multi-Sig	36
Tabela 3 – Comparativo entre Sistema Atual e Sistema Proposto	38
Tabela 4 – Riscos e Mitigações do Sistema Descentralizado	38

SUMÁRIO

1	INTRODUÇÃO	13
2	FUNDAMENTAÇÃO TEÓRICA	15
2.1	Escolas Econômicas e o Debate Brasileiro	15
2.1.1	<i>Escola Austríaca de Economia</i>	<i>15</i>
2.1.2	<i>Escola Desenvolvimentista</i>	<i>15</i>
2.1.3	<i>Implicações para a Política Previdenciária</i>	<i>16</i>
2.2	O Sistema Previdenciário Brasileiro	16
2.2.1	<i>INSS: Estrutura e Funcionamento</i>	<i>16</i>
2.2.2	<i>FGTS: Histórico e Problemas</i>	<i>17</i>
2.2.3	<i>Impacto Fiscal e Sustentabilidade</i>	<i>17</i>
2.3	O Modelo Australiano de Superannuation	18
2.3.1	<i>Estrutura do Sistema</i>	<i>18</i>
2.3.2	<i>Resultados e Lições</i>	<i>18</i>
2.4	Tecnologia Blockchain	19
2.4.1	<i>Conceitos Fundamentais</i>	<i>19</i>
2.4.2	<i>Smart Contracts e Multi-sig</i>	<i>19</i>
2.4.3	<i>Aplicações em Sistemas Financeiros</i>	<i>19</i>
2.5	Síntese	20
3	METODOLOGIA	21
3.1	Classificação da Pesquisa	21
3.2	Procedimentos Técnicos	21
3.2.1	<i>Pesquisa Bibliográfica</i>	<i>21</i>
3.2.2	<i>Pesquisa Documental</i>	<i>22</i>
3.2.3	<i>Análise Comparativa</i>	<i>22</i>
3.3	Etapas de Desenvolvimento	22
3.3.1	<i>Etapa 1: Diagnóstico do Sistema Atual</i>	<i>22</i>
3.3.2	<i>Etapa 2: Estudo de Modelos Internacionais</i>	<i>22</i>
3.3.3	<i>Etapa 3: Estudo da Tecnologia Blockchain</i>	<i>23</i>
3.3.4	<i>Etapa 4: Elaboração da Proposta</i>	<i>23</i>
3.3.5	<i>Etapa 5: Validação Conceitual</i>	<i>23</i>

3.4	Limitações Metodológicas	23
3.5	Ferramentas Utilizadas	24
4	PROPOSTA DO SISTEMA	25
4.1	Visão Geral da Proposta	25
4.2	Arquitetura do Sistema	25
4.2.1	<i>Camada de Blockchain</i>	25
4.2.2	<i>Camada de Smart Contracts</i>	26
4.2.3	<i>Camada de Usuário</i>	26
4.3	Mecanismo de Contribuição e Investimento	27
4.3.1	<i>Fluxo de Contribuição</i>	27
4.3.2	<i>Universo de Investimentos</i>	27
4.3.3	<i>Tokenização de Ativos</i>	27
4.4	Sistema de Governança Multi-sig	28
4.4.1	<i>Estrutura das Chaves</i>	28
4.4.2	<i>Fluxo de Autorização</i>	28
4.4.3	<i>Diagrama do Sistema Multi-sig</i>	29
4.5	Regras Operacionais	29
4.5.1	<i>Restrição de Operações</i>	29
4.5.2	<i>Bloqueio de Liquidação</i>	30
4.5.3	<i>Limites de Concentração</i>	30
4.5.4	<i>Tabela de Regras Operacionais</i>	30
4.6	Mecanismo de Herança	30
4.6.1	<i>Herança Total do Patrimônio</i>	31
4.6.2	<i>Processo de Transferência</i>	31
4.6.3	<i>Proteção contra Fraudes</i>	31
4.7	Transição do Sistema Atual	31
4.7.1	<i>Estratégia de Transição Gradual</i>	32
4.7.2	<i>Financiamento da Transição</i>	32
4.8	Benefícios Esperados	32
4.8.1	<i>Para o Trabalhador</i>	32
4.8.2	<i>Para a Economia</i>	32
4.8.3	<i>Para o Estado</i>	33

4.9	Desafios e Riscos	33
4.9.1	<i>Desafios Técnicos</i>	33
4.9.2	<i>Desafios Políticos</i>	33
4.9.3	<i>Riscos de Mercado</i>	33
4.10	Arquitetura Descentralizada do Mercado	33
4.10.1	<i>Camadas da Arquitetura Descentralizada</i>	34
4.10.1.1	<i>Camada de Tokenização (RWA - Real World Assets)</i>	34
4.10.1.2	<i>Camada de Oracle</i>	35
4.10.1.3	<i>Camada de Mercado</i>	35
4.10.2	<i>Poderes do Smart Contract Multi-Sig</i>	35
4.10.2.1	<i>Poderes do Indivíduo</i>	35
4.10.2.2	<i>Poderes do Governo</i>	36
4.10.2.3	<i>Checks and Balances</i>	37
4.10.3	<i>Descentralização Progressiva</i>	37
4.10.4	<i>Comparativo: Sistema Atual vs Sistema Proposto</i>	37
4.10.5	<i>Mitigação de Riscos da Descentralização</i>	37
5	CONCLUSÕES E TRABALHOS FUTUROS	39
5.1	Conclusões	39
5.2	Trabalhos Futuros	40
5.2.1	<i>Desenvolvimento Técnico</i>	40
5.2.2	<i>Análise Quantitativa</i>	41
5.2.3	<i>Aspectos Jurídicos e Regulatórios</i>	41
5.2.4	<i>Aspectos Sociais</i>	41
5.2.5	<i>Extensões do Modelo</i>	41
	REFERÊNCIAS	43

1 INTRODUÇÃO

O Brasil enfrenta desafios econômicos estruturais que limitam seu desenvolvimento há décadas. Entre os principais problemas, destacam-se 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).

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, comprometendo aproximadamente 70% do orçamento federal e limitando a capacidade de investimento do Estado em áreas essenciais como educação, saúde e infraestrutura (TAFNER *et al.*, 2019).

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, conseqüentemente, 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 conseqüências não previstas que frequentemente agravam os problemas que pretendia resolver.

2.1.2 *Escola Desenvolvimentista*

Em contraposição, a escola desenvolvimentista, influenciada pelo pensamento keynesiano e cepalino, argumenta que países em desenvolvimento necessitam de intervenção estatal

ativa para superar o subdesenvolvimento (FURTADO, 1961).

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, enquanto os empregadores contribuem com 20% sobre a folha de pagamento. 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 valores superiores a R\$ 300 bilhões anuais. 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). Estudos indicam que, ao longo de décadas de trabalho, o trabalhador pode perder até 40% do valor real de suas contribuições.

Os recursos do FGTS são utilizados pelo governo para financiar programas habitacionais (Minha Casa Minha Vida) e obras de infraestrutura e saneamento. 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).

O comprometimento de cerca de 70% do orçamento federal com benefícios previdenciários e assistenciais limita severamente a capacidade de investimento público em áreas essenciais. 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 *Conceitos Fundamentais*

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:** Todas as transações são públicas e verificáveis por qualquer participante;
- d) **Segurança criptográfica:** As transações são protegidas por algoritmos criptográficos robustos.

2.4.2 *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.

2.4.3 *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.

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, trata-se de pesquisa qualitativa, fundamentada na análise interpretativa de documentos, legislação, dados econômicos e modelos internacionais, sem utilização de métodos estatísticos como principal meio de análise (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.

3.5 Ferramentas Utilizadas

Para o desenvolvimento deste trabalho, foram utilizadas as seguintes ferramentas:

- a) \LaTeX para elaboração do documento, utilizando a classe abnTeX2;
- b) Mendeley e Zotero para gerenciamento de referências bibliográficas;
- c) Draw.io para elaboração de diagramas e figuras;
- d) Git para controle de versão do documento.

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 total:** Todas as transações são públicas e auditáveis;
- e) **Automatização:** Regras executadas por smart contracts, reduzindo burocracia.

4.2 Arquitetura do Sistema

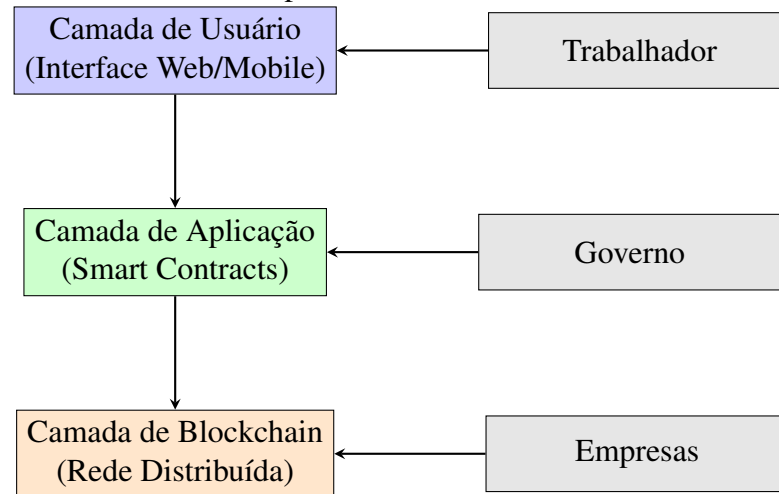
A arquitetura proposta é composta por três camadas principais, conforme ilustrado na Figura 1.

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:

- a) Maior controle sobre quem pode validar transações;

Figura 1 – Arquitetura do Sistema Proposto



Fonte: Elaborado pelo autor (2026).

- 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

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 block-chain. 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-3, onde três chaves são necessárias, mas apenas duas são suficientes 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;
- c) **Chave de Recuperação:** Armazenada em cofre seguro, para uso apenas em casos de perda de uma das outras chaves.

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.

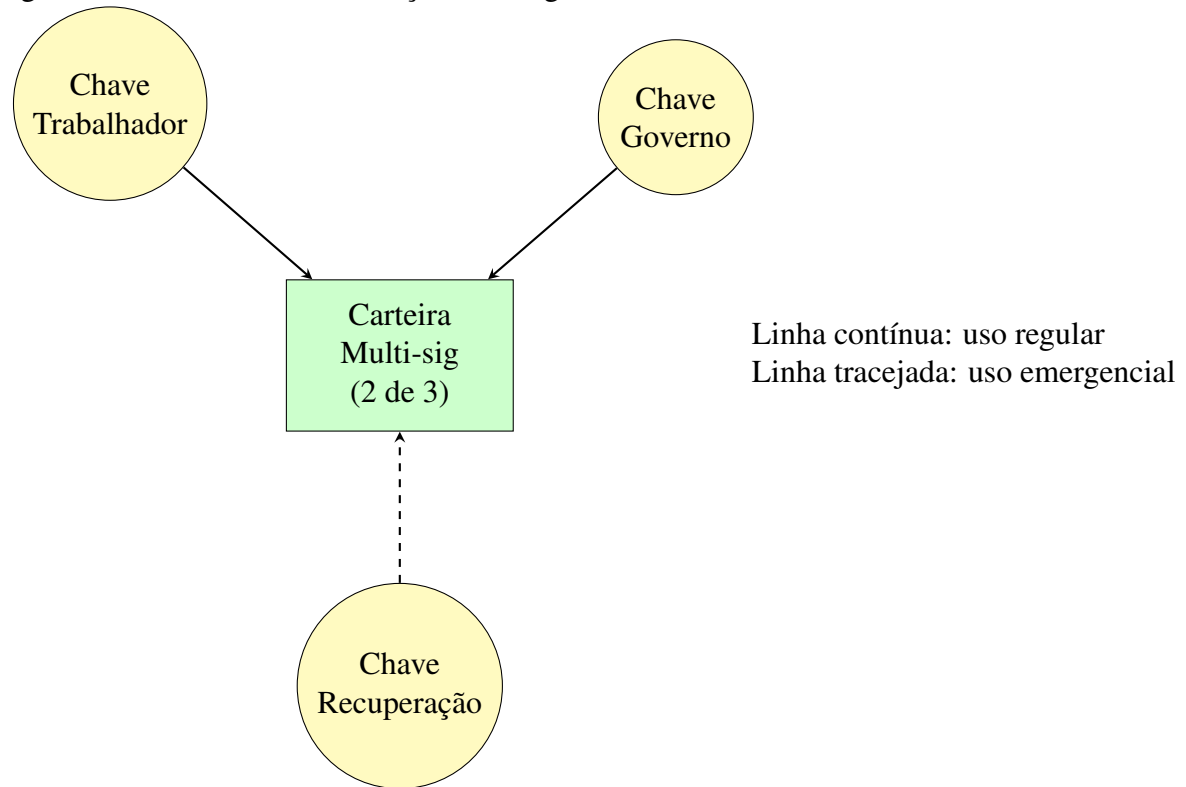
Este modelo garante que:

- 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 total sobre todas as operações realizadas.

4.4.3 Diagrama do Sistema Multi-sig

A Figura 2 ilustra o funcionamento do sistema de governança multi-sig.

Figura 2 – 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 uma operação de compra ou 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, são impostos limites de diversificação:

- a) Máximo de 10% do patrimônio em uma única empresa;
- b) Máximo de 30% em um único setor da economia;
- c) Mínimo de 20% em ativos de baixo risco (títulos públicos ou equivalentes).

4.5.4 *Tabela de Regras Operacionais*

A Tabela 1 resume as principais regras operacionais do sistema.

Tabela 1 – Resumo das Regras Operacionais

Regra	Descrição
Operações mensais	Máximo 1 operação de compra/venda por mês
Ativos elegíveis	Apenas empresas/ativos brasileiros
Concentração máxima	10% por empresa, 30% por setor
Reserva obrigatória	Mínimo 20% em baixo risco
Saque	Apenas na aposentadoria ou exceções legais
Governança	Multi-sig 2-de-3 (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.

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

- a) Nome e identificação dos beneficiários;
- b) Percentual destinado a cada beneficiário;
- c) Condições especiais (ex: liberação gradual para filhos menores).

4.6.2 Processo de Transferência

Em caso de falecimento:

1. A família apresenta certidão de óbito ao sistema;
2. O smart contract verifica a autenticidade do documento (integração com cartórios digitais);
3. O patrimônio é transferido para novas carteiras multi-sig dos herdeiros;
4. Os herdeiros assumem o controle, mantendo as mesmas regras operacionais;
5. Herdeiros podem optar por liquidar gradualmente ou manter os investimentos.

4.6.3 Proteção contra Fraudes

Para evitar fraudes, o sistema implementa:

- a) Período de carência de 30 dias antes da transferência;
- b) Verificação cruzada com bases de óbito oficiais;
- c) Notificação a todos os beneficiários cadastrados;
- d) Possibilidade de contestação durante o período de carência.

4.7 Transição do Sistema Atual

A implementação do sistema proposto requer um período de transição cuidadosamente planejado.

4.7.1 *Estratégia de Transição Gradual*

Propõe-se uma transição de 30 anos:

- a) **Anos 1-5:** Sistema piloto voluntário para novos entrantes no mercado de trabalho;
- b) **Anos 6-15:** Obrigatoriedade para novos trabalhadores, opcional para demais;
- c) **Anos 16-30:** Migração gradual dos trabalhadores em atividade que optarem pelo novo sistema;
- d) **Após ano 30:** INSS mantido apenas para aposentados atuais e trabalhadores que não migraram.

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) Redução gradual do déficit primário através de reformas administrativas;
- c) 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 total sobre aplicações e rendimentos.

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

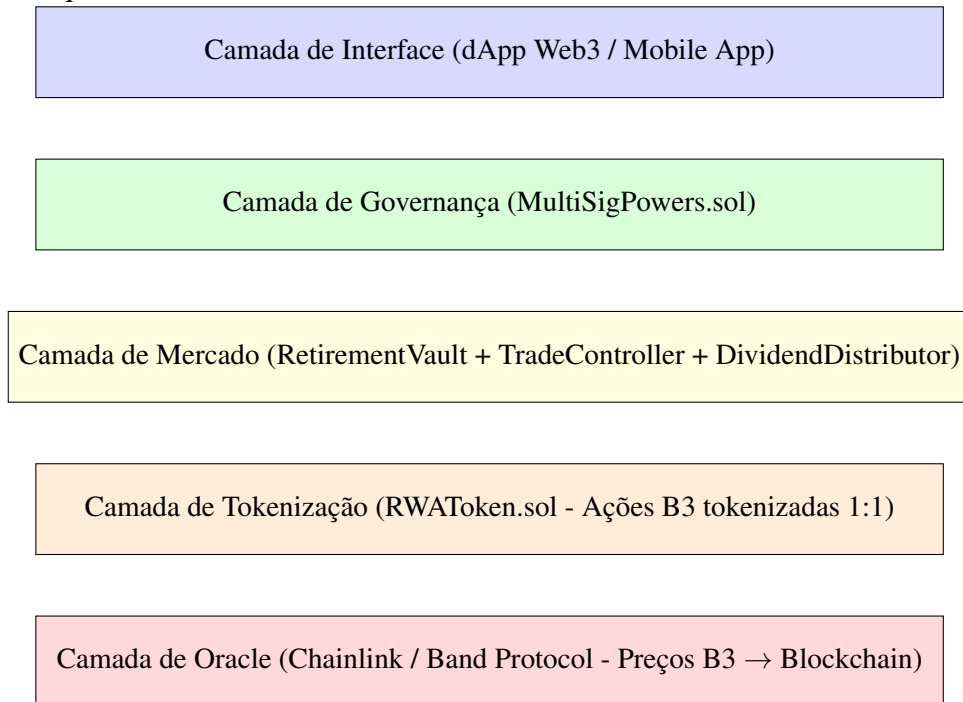
Esta seção detalha como o mercado financeiro poupador pode ser concebido de maneira descentralizada, utilizando tecnologia blockchain para garantir transparência, segurança

e governança distribuída.

4.10.1 Camadas da Arquitetura Descentralizada

O sistema é organizado em cinco camadas interdependentes, conforme ilustrado na Figura 3.

Figura 3 – 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 $\text{totalSupply}() = \text{ações custodiadas}$;
- 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 2 apresenta a matriz de poderes implementada no smart contract.

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;

Tabela 2 – 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 ≥ 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).

- 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) Todas as transações são públicas e auditáveis (garante transparência).

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.

4.10.4 *Comparativo: Sistema Atual vs Sistema Proposto*

A Tabela 3 apresenta um comparativo entre as características do sistema atual (INSS/FGTS) e o sistema proposto baseado em blockchain.

4.10.5 *Mitigação de Riscos da Descentralização*

A Tabela 4 apresenta os principais riscos do sistema descentralizado e suas respectivas mitigações.

Tabela 3 – 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).

Tabela 4 – 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.
- BATEMAN, H.; KINGSTON, G.; PIGGOTT, J. **Forced Saving: Mandating Private Retirement Incomes**. Cambridge: Cambridge University Press, 2001.
- BUTERIN, V. A next-generation smart contract and decentralized application platform. 2014. Ethereum Whitepaper. Disponível em: <<https://ethereum.org/whitepaper>>.
- CRESWELL, J. W. **Research Design: Qualitative, Quantitative, and Mixed Methods Approaches**. 4. ed. Thousand Oaks: SAGE Publications, 2014.
- FURTADO, C. **Desenvolvimento e Subdesenvolvimento**. Rio de Janeiro: Fundo de Cultura, 1961.
- 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.
- 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>>.
- TAFNER, P.; BOTELHO, C.; ERBISTI, R. **Reforma da Previdência: Por que o Brasil não pode esperar?** Rio de Janeiro: Elsevier, 2019.