

UNIVERSIDADE PAULISTA
VICE-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
INICIAÇÃO CIENTÍFICA E INICIAÇÃO EM DESENVOLVIMENTO
TECNOLÓGICO E INOVAÇÃO

RELATÓRIO SEMESTRAL DE PESQUISA

**ASPECTOS TÉCNICO-OPERACIONAIS E REGULATÓRIOS
DA EMISSÃO DE UM CRIPTOATIVO PARA REPRESENTAR
DIREITOS SOBRE LUCRO EM STARTUPS EM ESTÁGIO
INICIAL NO BRASIL**

Autor: Leonardo de Souza Borges

Curso: Ciência da Computação

Campus: Campinas (Swift)

Orientadora: Prof^a. Dr^a. Karem Daiane Marcomini

Pesquisa Apoiada pela Vice-Reitoria de Pós-Graduação e Pesquisa da
Universidade Paulista – UNIP, no Programa “Iniciação Científica e
Desenvolvimento Tecnológico e Inovação”.

Campinas
2026

RESUMO

ASPECTOS TÉCNICO-OPERACIONAIS E REGULATÓRIOS DA EMISSÃO DE UM CRIPTOATIVO PARA REPRESENTAR DIREITOS SOBRE LUCRO EM STARTUPS EM ESTÁGIO INICIAL NO BRASIL

Autor: Leonardo de Souza Borges

Esta pesquisa de iniciação científica investiga o uso de criptoativos para representar direitos econômicos em startups brasileiras em estágio inicial. O ponto de partida é um desafio estrutural do ecossistema nacional: a escassez de mecanismos acessíveis para financiamento e estruturação. A hipótese é que a tecnologia *blockchain* pode oferecer caminhos alternativos para novas dinâmicas de governança e mobilização de recursos. A investigação parte da premissa de que *tokens* podem transcender a função de ativos financeiros, atuando como instrumentos para quantificar e registrar a contribuição *de facto* de cada *stakeholder* – fundadores, colaboradores e investidores. *Smart contracts* possibilitam não apenas a emissão de tokens, mas também a automação e execução computacional da distribuição de lucros aos seus detentores. Assim a tecnologia permite estruturar uma empresa com base no valor efetivamente agregado por cada parte, fomentando uma cultura de meritocracia e participação desde a gênese do negócio. O percurso atravessa a fundamentação teórica, dos fundamentos da *blockchain* à flexibilidade dos contratos inteligentes do *Ethereum*, e o panorama regulatório nacional. No plano técnico, foi desenvolvido o contrato *ProfitToken* em *Solidity*, com padrão ERC-20 e mecanismos de *whitelist*, implantado e validado na *testnet Polygon Amoy*. Paralelamente, iniciou-se o sistema *Argos*, protótipo de código aberto GPL v3 que adiciona uma camada de valor com usabilidade, *compliance* e gestão dos *tokens*. O principal resultado deste semestre é a demonstração da viabilidade técnica da proposta, acompanhada da discussão dos desafios operacionais e regulatórios identificados. A pesquisa prossegue com o objetivo de implementar a distribuição automatizada de lucros e aprofundar a análise de segurança jurídica a fim de investigar a viabilidade da aplicação da tecnologia por startups brasileiras em estágio inicial.

Palavras-chave: *Blockchain*, *Security Tokens*, Startups em Estágio Inicial, Tokenização de Ativos, Contratos Inteligentes, Regulação de Criptoativos, Distribuição de Lucros, Financiamento Descentralizado, *Ethereum*, *Polygon*, Segurança Jurídica, ERC-20.

SUMÁRIO

1	INTRODUÇÃO	4
1.1	Contextualização e Relevância	4
1.2	Objetivos	7
2	FUNDAMENTAÇÃO TEÓRICA	8
2.1	Fundamentos tecnológicos e evolução histórica	8
2.2	Tokenização e aplicações da tecnologia	10
2.3	Segurança jurídica e panorama regulatório	12
3	MATERIAIS E MÉTODOS	16
3.1	Etapas Realizadas	16
3.2	Etapas Futuras	18
3.3	Uso de Ferramentas de Inteligência Artificial	19
4	RESULTADOS	20
4.1	Seleção de plataforma: Polygon	20
4.2	Desenvolvimento do contrato inteligente <i>ProfitToken</i>	21
4.3	Desenvolvimento do sistema <i>Argos</i>	22
4.4	Estratégias de <i>compliance</i> adotadas no protótipo	23
5	DISCUSSÃO	25
5.1	O que foi e o que não foi demonstrado	25
5.2	Sobre a escolha técnica: Polygon e ERC-20	25
5.3	O achado central: o token precisa estar inserido em um contexto no qual ele possua valor	26
5.4	Sobre a estratégia regulatória	26
5.5	Possíveis vantagens estratégicas da tokenização em empresas em estágio inicial	26
5.6	Limitações identificadas e próximas etapas	27
	REFERÊNCIAS	29
6	ANEXOS	32
6.1	Anexo A – Código do contrato <i>ProfitToken</i> (trechos principais)	32
6.2	Anexo B – Evidência de deploy do contrato na Polygon Amoy	34
6.3	Anexo C – Diagramação do banco de dados do protótipo <i>Argos</i>	35
6.4	Anexo D – Estrutura de diretórios do protótipo <i>Argos</i>	37

1 INTRODUÇÃO

1.1 Contextualização e Relevância

A investigação de soluções inovadoras para o financiamento de startups em estágio inicial no Brasil é particularmente relevante diante das barreiras estruturais de acesso ao capital enfrentadas por essas empresas nascentes e a relativa fragilidade do ambiente de *venture capital* nacional quando comparado a ecossistemas consolidados como Vale do Silício, Londres e Tel Aviv (Startup Genome, 2025; XP Investimentos, 2024). Em especial, startups nas fases de ideação, validação e início de operação — coletivamente denominadas *early stage* — enfrentam restrições significativas na captação de recursos, evidenciando a necessidade de mecanismos financeiros mais eficientes, acessíveis e adaptados às especificidades do contexto brasileiro.

Desde 2009, a tecnologia *blockchain* tem-se consolidado como infraestrutura emergente em constante evolução, com aplicações diversas e documentadas em múltiplos setores, incluindo finanças, saúde, Internet das Coisas (IoT), jogos e gestão de *supply chain* (MOHAMMED; DE-PABLOS-HEREDERO; BOTELLA, 2024).

Com o advento do Bitcoin e da tecnologia *blockchain* (NAKAMOTO, 2008), o setor financeiro global a experimentar transformações relevantes (KONDOVA; SIMONELLA, 2019). Entre as propriedades centrais dessa tecnologia destaca-se o fato de que, em *blockchains* públicas, os registros são armazenados de maneira descentralizada e verificável, com elevado grau de resistência à alteração, além de serem transparentes e auditáveis por qualquer participante da rede. Nesse sentido, a *blockchain* pode ser compreendida, por analogia, como um sistema de registro digital distribuído, capaz de assegurar integridade e rastreabilidade das informações sem depender de uma autoridade central.

Anos após o Bitcoin, emergiu o conceito de contratos inteligentes descentralizados (*smart contracts*) (BUTERIN, 2013), que consiste em programas armazenados em uma *blockchain* e executados por meio de sua infraestrutura descentralizada, capazes de automatizar a execução de condições previamente definidas sem a necessidade de intermediários. Essa capacidade programável viabilizou a criação de *tokens*, entendidos como representações digitais registradas em *blockchain*, cujo ciclo de vida — emissão, transferência e eventual resgate — é integralmente regido pelas regras codificadas em um contrato inteligente. Dentre esses ativos, destacam-se os *security tokens*, que representam direitos econômicos ou societários sobre ativos reais, como ações, participações societárias ou recebíveis.

Se for plausível considerar que, em última instância, o dinheiro seja um meio pelo qual as pessoas trabalham umas pelas outras, um instrumento de intermediação de trabalho e valor; os *tokens*, de forma análoga, podem ser considerados da mesma

forma e despontar como alternativa para que startups mobilizem e organizem recursos em sua fase inicial. Esses ativos digitais podem representar frações de direitos econômicos futuros e serem distribuídos de maneira proporcional e automática entre os detentores do *token* (*stakeholders*) — fundadores, colaboradores-chave e investidores —, com base na contribuição de fato de cada um ao negócio. Com isso, mesmo sem capital expressivo no início, uma *startup* pode estruturar um modelo de governança mais eficiente.

Por exemplo, suponha que três engenheiros, com capital inicial limitado, decidam criar uma *startup*. Eles estipulam que o valor do negócio deve ser, no mínimo, um milhão de reais, e para se organizarem decidem realizar a emissão de um milhão de unidades de criptoativo, com cada *token* representando o valor nominal de um real, totalizando um milhão de reais no total. Inicialmente, todos os *tokens* ficam em posse da empresa, mas conforme os fundadores trabalham ou aportam capital, eles recebem uma quantidade de *tokens* proporcional ao valor que cada um agregou ao negócio. Essa abordagem permite não somente uma alternativa para atrair financiamento descentralizado, mas também uma forma de organização centrada no valor efetivamente depositado no negócio.

Uma vantagem adicional para empresas em estágio inicial na adoção de práticas de tokenização reside na possibilidade de estruturar, desde cedo, mecanismos formais de governança. Tal arranjo pode servir como facilitador para uma eventual transição ao mercado regulado de *security tokens* através de plataformas credenciadas pela Comissão de Valores Mobiliários (CVM) quando a empresa alcançar maior maturidade operacional e financeira, permitindo inclusive a negociação desses ativos em mercados secundários.

Estudos prospectivos apontam que o mercado de ativos tokenizados pode atingir entre US\$ 2 trilhões (MCKINSEY, 2024) e US\$ 16 trilhões (BCG, 2024) até 2030, evidenciando uma tendência de expansão substancial e a crescente relevância dessa tecnologia no cenário econômico global.

No Brasil, o Banco Central (BCB) tem demonstrado interesse na exploração de soluções baseadas em tokenização e *blockchain*, como exemplificado pelo desenvolvimento do DREX, projeto de moeda digital do BCB. Embora a iniciativa tenha enfrentado desafios em sua fase de pesquisa e desenvolvimento, **persiste o interesse nacional** na adoção da tecnologia e no aprofundamento do conhecimento científico sobre o tema (NETO, 2025; INFOMONEY, 2025; Banco Central do Brasil, 2023).

Em paralelo, nos últimos anos, a CVM e o Congresso Nacional têm avançado na regulamentação de criptoativos. O Parecer de Orientação CVM nº 40/2022 e a Lei nº 14.478/2022 (Marco Legal das Criptomoedas) constituem exemplos relevantes desse movimento normativo.

A adoção antecipada de mecanismos de tokenização também envolve impor-

tantes *trade-offs*. Para uma *startup* ainda em fase de validação de seu modelo de negócio, a tokenização pode representar um acréscimo de complexidade operacional e regulatória, desviando o foco dos fundadores e gerando custos adicionais. Além disso, persistem fatores relevantes de incerteza jurídica, dentre os quais se destacam: (i) a ausência de jurisprudência consolidada; (ii) o risco de litígios trabalhistas ou comerciais por falta de compreensão sobre a tecnologia; (iii) a inexistência de procedimentos claramente definidos para situações de incidentes; e (iv) o risco de autuação ou instauração de processo administrativo por órgãos reguladores.

Sobre esse último ponto, pode-se afirmar que, como regra geral, *tokens* que conferem direitos econômicos como lucros ou participação societária tendem a ser classificados como valores mobiliários pela CVM e, como tais, estão sujeitos às normas aplicáveis ao mercado de capitais brasileiro, inclusive registro de emissores e de ofertas públicas, divulgação de informações e demais obrigações previstas na legislação pertinente (BARRETO, 2022). Essa tributação regulatória pode, a depender do caso, impor uma série de exigências burocráticas que se revelam paralisantes para startups em estágio inicial, dada a necessidade de conformidade com padrões que tradicionalmente se aplicam a empresas já estabelecidas. Além disso, a trilha regulatória proposta pela CVM para acesso ao mercado de capitais tende a ser direcionada a empresas com maior grau de maturidade operacional e financeira: plataformas habilitadas pela Autarquia, como a KRIA, geralmente exigem que as empresas participantes apresentem tração comprovada e tese de negócio consolidada para acessar mecanismos de oferta e negociação no ambiente regulado (Kria, 2025).

Por outro lado, também há o princípio constitucional da livre iniciativa e livre mercado (CF, art. 1º, IV), que permite às empresas se organizarem da forma que melhor se adequar às suas necessidades, inclusive na utilização de novas tecnologias, desde que não haja prejuízos para terceiros. Diante desse cenário — marcado pelo potencial transformador da tokenização e pelos desafios técnicos, operacionais e regulatórios que cercam sua adoção por startups em estágio inicial —, a presente pesquisa investiga a viabilidade técnico-operacional e regulatória da emissão de criptoativos (*security tokens*) para representar direitos econômicos sobre lucro em startups brasileiras em estágio inicial, buscando discutir possíveis implicações de ordem prática, como segurança jurídica, viabilidade técnica e estruturação de governança.

Este relatório semestral apresenta o andamento da pesquisa iniciada em agosto de 2025.

1.2 Objetivos

Objetivo geral

Analisar a viabilidade técnico-operacional e regulatória da utilização de *tokens* como instrumentos de representação de direitos sobre lucro em startups brasileiras em estágio inicial (*early stage*).

Objetivos específicos

- Identificar oportunidades e potenciais benefícios que as tecnologias *blockchain*, *smart contracts* e *tokens* podem oferecer a startups brasileiras em estágio inicial;
- Analisar a segurança jurídica e o panorama regulatório aplicável à emissão de um criptoativo (*token*) destinado a representar direitos econômicos sobre lucro;
- Implementar um *token* experimental para representar direitos sobre lucro, utilizando tecnologias *blockchain* e contratos inteligentes;
- Desenvolver um protótipo de *software* que possibilite a distribuição automatizada de lucros;
- Avaliar a reprodutibilidade e adaptabilidade da solução desenvolvida, disponibilizando os artefatos no GitHub sob licenças abertas (GPL v3 e Creative Commons) de modo a permitir sua validação, crítica e eventual adoção por outras startups ou pesquisadores.

2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica desta pesquisa organiza-se em três eixos principais: (i) a evolução histórica e os fundamentos conceituais da tecnologia *blockchain*; (ii) suas aplicações potenciais no contexto de startups em estágio inicial; e (iii) o arcabouço regulatório brasileiro aplicável, com ênfase na segurança jurídica. Essa organização fornece o referencial analítico necessário para examinar os desafios e as oportunidades associados à implementação do modelo proposto.

2.1 Fundamentos tecnológicos e evolução histórica

A tecnologia *blockchain* emerge como uma infraestrutura descentralizada para registro e transferência de valor e informações, cujo marco inicial é o *white paper* do Bitcoin, publicado por Nakamoto (2008).

É fundamental distinguir *Bitcoin* de *blockchain*: enquanto o primeiro consiste em um sistema de moeda digital *peer-to-peer*, a segunda corresponde à arquitetura de registro distribuído que viabiliza essa e diversas outras aplicações descentralizadas (LI *et al.*, 2024).

Nakamoto (2008) combinou elementos tecnológicos já existentes, como criptografia assimétrica (DIFFIE; HELLMAN, 1976), funções de *hash* (MERKLE, 1989), redes *peer-to-peer* (P2P) e o mecanismo de prova de trabalho (BACK, 2002), para conceber um sistema de registro distribuído, descentralizado e resistente à alteração.

O funcionamento básico da *blockchain* do Bitcoin baseia-se no agrupamento de transações em blocos encadeados por *hashes*, formando uma corrente que torna os registros praticamente imutáveis (YERMACK; NIAN; CHUEN, 2015). A validação é realizada por mineradores que competem na solução de um problema matemático (prova de trabalho), garantindo consenso sem autoridade central (GHIMIRE; SELVARAJ, 2018).

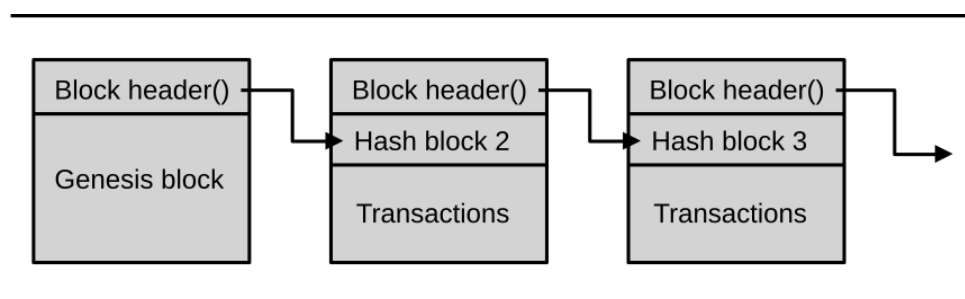


Figura 1 – Estrutura de blocos encadeados em uma *blockchain*

Fonte: Autoria própria, adaptado de Kondova e Simonella (2019).

Um significativo salto inovativo ocorreu com o Ethereum, proposto por Buterin

(2013) e lançado em 2015. O Ethereum introduziu os *smart contracts*, que são programas Turing-completos executados na Ethereum Virtual Machine (EVM) e registrados na *blockchain*, capazes de automatizar acordos e executar o cumprimento de cláusulas sem intermediários (WOOD, 2014). A EVM permitiu que indivíduos ou organizações emitissem seus próprios *tokens* e desenvolvessem aplicações descentralizadas (*dApps*) em áreas como finanças, jogos e governança, expandindo significativamente o conjunto de possibilidades da tecnologia *blockchain*.

Para viabilizar a execução descentralizada de contratos inteligentes, o Ethereum introduziu dois conceitos fundamentais e interdependentes: o *Ether* (ETH) e o *gas*. O *Ether* é a criptomoeda nativa da rede Ethereum e funciona como combustível econômico do sistema: toda operação executada na rede, seja uma simples transferência, a implantação de um contrato inteligente ou a chamada de uma de suas funções, exige o pagamento de uma taxa denominada *gas fee*, liquidada em *Ether* (Ethereum Foundation, 2026c).

O *gas*, por sua vez, é a unidade que mede o esforço computacional necessário para processar cada operação; instruções mais complexas consomem maior quantidade de *gas*. O valor final pago em ETH corresponde ao produto entre a quantidade de *gas* consumida e o preço unitário do *gas*, definido pelas condições de mercado.

Conforme Fertig e Schütz (2024), esse mecanismo cumpre duas funções essenciais: remunera os validadores da rede pelo processamento das transações e atua como mecanismo de proteção contra ataques de negação de serviço, ao impor custo econômico à execução de operações computacionais.

Com o crescimento do ecossistema, surgiram desafios relacionados à escalabilidade das redes *blockchain*. O chamado trilema da *blockchain*, que consiste na dificuldade de otimizar simultaneamente descentralização, segurança e escalabilidade, impulsionando o desenvolvimento de soluções de Camada 2 (L2) e outras abordagens arquiteturais (BUTERIN, 2017).

As soluções de Camada 2 processam transações fora da cadeia principal (*off-chain*) e periodicamente ancoram seus resultados na Camada 1, preservando o nível de segurança da rede base ao mesmo tempo em que aumentam a capacidade de processamento (*throughput*). Entre as principais implementações atuais para lidar com o trilema, destacam-se (YI, 2024):

- **State Channels:** permitem múltiplas transações entre partes sem publicar cada operação na *blockchain*, registrando apenas os estados inicial e final.
- **Sidechains:** *blockchains* independentes com mecanismos de transferência bidirecional de ativos com a cadeia principal, operando com regras de consenso próprias.

- **Rollups**: executam transações fora da cadeia mas publicam dados de transação (ou provas) na Camada 1. Subdividem-se em *Optimistic Rollups* (assumem validade, verificam sob disputa) e *Zero-Knowledge Rollups* (publicam provas criptográficas de validade).

Além das soluções de escalabilidade, observa-se o surgimento de *blockchains* especializadas, voltadas a casos de uso específicos, como cadeias de suprimentos e identidade digital, bem como de *blockchains* permissionadas, caracterizadas por restrições de acesso e maior grau de controle institucional, comumente adotadas por corporações e governos (SYED *et al.*, 2019).

Atualmente, a tecnologia *blockchain* encontra-se em estágio de amadurecimento, com desafios atuais centrados em interoperabilidade entre diferentes redes, experiência do usuário e integração com sistemas legados. Paralelamente, avanços regulatórios em diversas jurisdições, incluindo o Brasil, buscam conferir segurança jurídica ao ecossistema, especialmente no que tange à classificação de ativos digitais e à prevenção de ilícitos.

2.2 Tokenização e aplicações da tecnologia

A partir da plataforma Ethereum e da padronização de contratos inteligentes, tornou-se possível criar e gerenciar *tokens*, isto é, representações digitais de ativos ou direitos, de forma programável e descentralizada. Esses *tokens* podem ser classificados em categorias principais, que apresentam implicações jurídicas e funcionais distintas (KONDOVA; SIMONELLA, 2019):

- **Tokens de pagamento ou Criptomoedas (*payment tokens*)**: funcionam como meio de troca, unidade de conta ou reserva de valor, a exemplo do Bitcoin e do Ether (ETH). Não conferem, em geral, direitos sobre fluxos de caixa futuros ou participação em empreendimentos específicos.
- **Tokens de utilidade (*utility tokens*)**: dão acesso a produtos ou serviços oferecidos por um ecossistema digital. São comuns em plataformas de armazenamento descentralizado, redes de computação ou jogos *blockchain*. O ETH além de ser considerado um token de pagamento, também é um *token* de utilidade, pois as taxas de transação e execução de contratos inteligentes na rede Ethereum são feitas em ETH. Os tokens de utilidade não conferem direitos econômicos ou participação societária, mas sim acesso a funcionalidades específicas, o que os diferencia dos *security tokens*.
- **Tokens de valores mobiliários (*security tokens*)**: representam direitos econômicos sobre ativos subjacentes, como participação societária, dividendos, juros

ou fluxos de receita. Por envolverem expectativa de lucro oriundo de esforços de terceiros, enquadram-se na definição de valor mobiliário na maioria das jurisdições, incluindo o Brasil, sujeitando-se à regulação da CVM.

A implementação técnica desses *tokens* no ecossistema Ethereum consolidou-se por meio de padrões conhecidos como ERCs (*Ethereum Request for Comments*)

Uma ERC é um documento técnico formal utilizado para propor criação de novos recursos ou mudanças na tecnologia Ethereum (Binance Academy, 2025). Em ERCs que tratam de padrões de *tokens*, o documento especifica uma *interface* de classe (programação orientada a objetos), isto é, um conjunto mínimo obrigatório de funções e eventos que um contrato inteligente deve implementar, de modo que carteiras, *exchanges* e outros contratos possam interagir com qualquer *token* compatível sem a necessidade de conhecer os detalhes internos de sua implementação.

Entre os ERCs (Ethereum Foundation, 2026a) mais relevantes para o escopo desta pesquisa, destacam-se:

- **ERC-20**: padrão para *tokens* fungíveis, em que cada unidade é idêntica e intercambiável. É o protocolo mais utilizado para a criação de criptomoedas e *utility tokens*, definindo funções básicas como transferência, consulta de saldo e aprovação de gastos.
- **ERC-3643**: padrão voltado a *security tokens* regulados. Incorpora um registro de identidade *on-chain* (ONCHAINID), módulos de conformidade configuráveis e restrições de transferência baseadas em identidade verificada, atendendo a requisitos de KYC/AML diretamente no protocolo.

No contexto das startups, a tokenização abre novas possibilidades para mobilização de recursos financeiros, técnicos e humanos (COMITO, 2023):

- **Crowdfunding**: captação de recursos financeiros com o público em geral. No Brasil, pode ser realizado por meio de plataformas autorizadas pela CVM, em que investidores adquirem valores mobiliários (por exemplo, *tokens* de dívida ou participação). Exige registro ou dispensa regulatória e é mais adequada para startups em estágio mais maduro, com tração e modelo de negócio validado.
- **Crowdsourcing**: captação de trabalho ou conhecimento, sem implicar necessariamente aporte de capital ou relação de investimento. É a obtenção de ideias, código, design, soluções técnicas, validação de produto etc.

No campo da governança, práticas oriundas das Organizações Autônomas Descentralizadas (DAOs) podem ser adaptadas para startups tradicionais em dois ní-

veis complementares. No nível técnico, de acordo com Saesen *et al.* (2025), os *governance tokens* permitem que *stakeholders* votem em decisões estratégicas, como destinação de lucros, eleição de administradores e alterações no contrato social, com registro imutável na *blockchain*. A nível de processos, DAOs consolidaram um conjunto de práticas de governança, como propostas formalizadas, períodos de deliberação, quóruns mínimos, escolha de líderes e registros auditáveis de cada decisão, que eventualmente podem ser absorvidas por startups independentemente de tokenização.

Apesar do potencial transformador da tokenização, é preciso reconhecer suas limitações práticas. A compreensão de contratos inteligentes por *stakeholders* não técnicos pode representar um desafio significativo, uma vez que o código dos *smart contracts*, geralmente escrito em linguagens como Solidity, não é intuitivo para leigos (FERTIG; SCHÜTZ, 2024) . Adicionalmente, a implementação e gestão de sistemas baseados em *blockchain* exigem preparo e prudência de todos os *stakeholders* nas esferas tecnológica e jurídica.

2.3 Segurança jurídica e panorama regulatório

No âmbito regulatório, o Brasil conta com um arcabouço normativo em desenvolvimento, composto por múltiplos instrumentos que, em conjunto, delineiam o tratamento jurídico dos criptoativos e das ofertas de valores mobiliários digitais, sejam esses tokenizados ou não. Os principais marcos normativos são:

- **Lei nº 14.478/2022 (Marco Legal das Criptomoedas):** estabelece diretrizes gerais para o mercado de ativos virtuais no Brasil, definindo responsabilidades para prestadores de serviços de ativos virtuais e conferindo ao Banco Central a competência para regulamentar e supervisionar o setor.
- **Decreto nº 11.563/2023:** define a competência regulatória sobre criptoativos no Brasil, atribuindo ao Banco Central (BCB) a supervisão dos ativos virtuais utilizados como meio de pagamento, e à Comissão de Valores Mobiliários (CVM) a supervisão daqueles que configurem valores mobiliários.
- **Resolução CVM nº 88/2022:** regulamenta as plataformas eletrônicas de investimento coletivo (*crowdfunding*), estabelecendo regras para que sociedades empresárias de pequeno porte possam realizar ofertas públicas de valores mobiliários com dispensa de registro, desde que respeitados limites de captação e requisitos de transparência.
- **Parecer de Orientação CVM nº 40/2022:** fornece diretrizes para a classificação de criptoativos como valores mobiliários, orientando a análise caso a caso com

base em critérios que incluem a existência de investimento, expectativa de lucro e dependência de esforços de terceiros, critérios que guardam semelhança com o *Howey Test* norte-americano.

- **Resolução CVM nº 160/2022:** dispõe sobre as ofertas públicas de distribuição de valores mobiliários, estabelecendo requisitos de registro e divulgação de informações que se aplicam quando criptoativos são classificados como valores mobiliários.
- **Resoluções BCB nº 519, 520 e 521/2025:** representam um marco normativo, regulamentando a prestação de serviços com ativos virtuais no Brasil. Ela detalha os requisitos de autorização, governança, controles internos e prevenção à lavagem de dinheiro para as prestadoras de serviços de ativos virtuais, completando o arcabouço iniciado pelo Marco Legal de 2022.

Apesar da evolução regulatória, empreendedores ainda precisam enfrentar diversos fatores que geram insegurança na adoção da tecnologia.

Em primeiro lugar, há o risco de litígios entre sócios ou colaboradores caso a solução não seja bem compreendida, transparente e auditável. Em caso de divergências sobre a distribuição de *tokens* ou sobre os direitos que eles representam, a ausência de jurisprudência consolidada pode dificultar a previsão do desfecho judicial.

Em segundo lugar, conforme (BARRETO, 2022), existe o risco de autuação por parte da CVM, caso a distribuição seja interpretada como oferta irregular de valores mobiliários. Também pode haver questionamentos por parte do BCB, a depender da natureza do ativo emitido, conforme a divisão de competências estabelecida pelo Decreto nº 11.563/2023.

Por fim, surgem dúvidas técnico-operacionais igualmente relevantes. O que ocorre se um *stakeholder* for hackeado ou perder sua chave privada, tornando os *tokens* inacessíveis? Como proceder caso uma ordem judicial determine a redistribuição de ativos registrados de forma imutável em uma *blockchain* pública? Como os *tokens* devem ser registrados no contrato social da empresa?

Essas questões precisam ser enfrentadas antes de qualquer implementação prática, a fim de evitar que a adoção da tecnologia se converta em risco operacional ou jurídico para a empresa iniciante.

Outro ponto a ser considerado é que o cenário muda de acordo com o status jurídico dos *stakeholders*. É recomendável que esses estejam nomeados como tais no contrato social da empresa, embora em situações de *crowdsourcing* ou de adesão de investidores pontuais isso possa não ser possível nesses casos. Caso a startup queira seguir adiante por esse caminho, terá que buscar outras formas de resguardar seus interesses em casos de conflitos, como a formalização de termos de adesão,

acordos de confidencialidade e cláusulas de arbitragem.

Quando os *stakeholders* possuem CNPJ, isto é, são pessoas jurídicas prestando serviços à *startup*, a relação tende a ser enquadrada como contrato entre empresas. Essa configuração reduz o risco de caracterização de vínculo empregatício ou oferta pública e oferece maior flexibilidade contratual para definir os direitos representados pelos *tokens*. Já em modelos cooperativos, nos quais a *startup* se organiza sob a forma de cooperativa de trabalho ou de plataforma, os *tokens* podem representar a participação do cooperado nos resultados da cooperativa, com respaldo na legislação cooperativista (Lei nº 5.764/1971), desde que a estrutura societária seja coerente com essa forma jurídica.

Por outro lado, quando os destinatários são colaboradores convencionais com carteira assinada, a distribuição de *tokens* atrelada à remuneração pode ser interpretada como parte do salário ou como Participação nos Lucros e Resultados (PLR), o que implica incidência de encargos trabalhistas e previdenciários. Essa modalidade é, portanto, a mais delicada do ponto de vista jurídico-operacional no contexto analisado.

Atenção adicional se faz necessária em relação à terminologia utilizada para descrever os direitos representados pelos tokens, nosso ordenamento jurídico é particularmente sensível a essas nuances (TUCCI, 2021) e o ônus de eventualmente explicar a um juízo que houve equívoco pode ser particularmente custoso em termos de tempo e dinheiro. Expressões como “dividendos”, “participação nos lucros”, “divisão de lucros”, “prêmios por resultados” carregam peso jurídico específico: o primeiro costuma remeter à distribuição de resultados em sociedades anônimas; o segundo parece estar mais alinhado com o conceito de PLR e CLT, o que pode subsidiar eventual caracterização de relação de trabalho ou societária; enquanto os demais podem ser mais adequados conforme o caso.

Um referencial internacional para avaliar se determinado *token* está sujeito à regulação da CVM é o *Howey Test*, critério formulado pela Suprema Corte dos Estados Unidos em 1946 e referência para órgãos reguladores do mundo todo (BSBC Advogados, 2021). O teste define valor mobiliário como toda operação que envolva (i) um investimento em dinheiro, (ii) em um empreendimento comum, (iii) com expectativa de lucro, (iv) derivada predominantemente dos esforços de terceiros.

No Brasil, o Parecer de Orientação CVM nº 40/2022 faz menção explícita a esse teste, adotando raciocínio análogo, porém aplicado de forma autônoma e adaptada ao ordenamento nacional: a CVM analisa a substância econômica da operação, verificando se há captação de recursos do público com expectativa de ganho baseada em esforços alheios (BLASCO; BLASCO, 2022). Estruturar o *token* em circuito fechado, de modo que seus detentores sejam participantes ativos da empresa e não meros investidores passivos à espera de retorno e demonstrar que a intenção primária do token é para organizar a startup e não para prometer ganhos financeiros, é, portanto, uma

das possíveis estratégias de *compliance* para comprovar boa fé e reduzir a exposição regulatória prematura.

Para que os *tokens* não sejam futuramente enquadrados como oferta irregular de valores mobiliários, algumas precauções de *compliance* podem ser observadas em conjunto: (i) direcionar a distribuição exclusivamente a pessoas que participem diretamente no dia a dia da empresa, como sócios, colaboradores ativos, investidores conselheiros e prestadores de serviço com envolvimento operacional comprovado; (ii) formalizar e registrar a relação por meio de documentos explícitos (KYC, NDAs, termos de aceite etc.) que descrevam a natureza dos *tokens*, os direitos a eles associados, os riscos envolvidos e a ausência de promessa de retorno financeiro baseado em esforços de terceiros; (iii) abster-se de qualquer forma de publicidade ou divulgação pública dos *tokens*, seja em redes sociais, sites institucionais ou eventos; (iv) deixar explícito a substância estruturante do token, não realizando promessas de valorização, rendimento ou retorno financeiro; (v) restringir expressamente a circulação dos *tokens* a um grupo pequeno e identificável de pessoas com vínculo real e ativo com a empresa, vedando sua comercialização em mercados secundários ou plataformas de negociação; e (vi) manter registros detalhados e auditáveis de todas as transações e interações relacionadas.

Ainda assim a depender do caso pode ser necessário o registro do ativo na CVM (BARRETO, 2022; BLASCO; BLASCO, 2022). Esses procedimentos visam proteger os interesses da startup produzindo provas inequívocas de boa-fé na eventualidade de questionamentos judiciais ou administrativos por *stakeholders* ou terceiros.

A pesquisa em andamento busca integrar esses conhecimentos para propor uma solução prática, tecnicamente robusta e aderente à legislação vigente, especificamente adaptada às necessidades de startups brasileiras em estágio inicial.

3 MATERIAIS E MÉTODOS

O percurso metodológico da pesquisa foi estruturado em etapas sequenciais e complementares, algumas já iniciadas e outras previstas para o próximo semestre.

3.1 Etapas Realizadas

Revisão bibliográfica aprofundada

Cabe ressaltar que esta pesquisa possui caráter exploratório e interdisciplinar, situando-se na interseção entre tecnologia, regulação e gestão de startups no contexto brasileiro. Por se tratar de um campo emergente, o domínio técnico sobre *blockchain* foi sendo construído de forma progressiva ao longo do próprio processo de pesquisa. Nesse sentido, a leitura sistemática do livro “*Blockchain: The Comprehensive Guide to Blockchain Development, Ethereum, Solidity, and Smart Contracts*” (FERTIG; SCHÜTZ, 2024) foi fundamental para estabelecer uma base de conhecimento técnico, permitindo a compreensão dos conceitos fundamentais da tecnologia de forma estruturada, o que viabilizou as etapas subsequentes de desenvolvimento e análise.

Foram selecionados e analisados artigos científicos e/ou técnicos e documentos regulatórios sobre *blockchain*, contratos inteligentes, tokenização de ativos e legislação aplicável. As principais referências estão listadas na seção final e serviram de base para a contextualização e definição dos critérios de análise.

Análise de segurança jurídica e enquadramento regulatório

Foi realizada análise do arcabouço normativo brasileiro aplicável a criptoativos, compreendendo: a Lei nº 14.478/2022 (Marco Legal das Criptomoedas), que estabelece diretrizes gerais para o mercado de ativos virtuais; o Parecer de Orientação CVM nº 40/2022, que aplica raciocínio análogo ao *Howey Test* de forma autônoma e adaptada ao ordenamento nacional; as Resoluções CVM nº 88/2022 e nº 160/2022; e o Decreto nº 11.563/2023, que delimita as competências entre CVM e Banco Central na regulação de criptoativos.

Foram identificados alguns vetores de risco relevantes: (i) autuação pelos órgãos reguladores por oferta irregular de valores mobiliários; (ii) litígios entre partes decorrentes da ausência de jurisprudência consolidada; (iii) risco de enquadramento trabalhista quando os destinatários são colaboradores com carteira assinada; e (iv) questões técnico-operacionais como perda ou comprometimento de chaves privadas ou cumprimento de ordens judiciais sobre registros imutáveis em *blockchain*. Constatou-se ainda que a terminologia adotada — “dividendos”, “participação nos lucros” ou “divi-

são de lucros” — carrega peso jurídico específico e pode influenciar o enquadramento regulatório ao qual a empresa estaria sujeita.

Concluiu-se que uma possível estratégia para reduzir a exposição regulatória prematura consiste em estruturar a distribuição dos tokens em circuito fechado, direcionando os tokens exclusivamente a *stakeholders ativos* da empresa — sócios, colaboradores com envolvimento operacional comprovado, investidores conselheiros e prestadores de serviço com CNPJ —, e não a meros investidores passivos à espera de retorno. Essa estrutura, complementada por procedimentos de compliance como KYC, assinatura de documentos explícitos, vedação à publicidade do criptoativo e à negociação em mercados secundários, bem como a manutenção de registros auditáveis, busca **proteger os interesses da startup produzindo provas inequívocas de sua boa fé em qualquer eventual questionamento judicial ou administrativo.**

Quanto à ausência de jurisprudência consolidada, um possível caminho para mitigar riscos é prever cláusulas de arbitragem para dirimir eventuais controvérsias.

Análise comparativa entre plataformas

Após avaliação inicial de Ethereum, Binance Smart Chain e Polygon, optou-se por focar a implementação em Polygon (solução *sidechain*) porque essa solução mantém compatibilidade total com Ethereum (EVM), oferece custos significativamente mais baixos de transação e de integridade de dados através de provas de hash armazenadas na rede Ethereum principal.

Desenvolvimento do contrato inteligente e emissão do token experimental

Foi implementado o contrato *ProfitToken* em Solidity 0.8.28, adotando-se o padrão ERC-20 em razão de sua ampla adoção, simplicidade estrutural e compatibilidade com ferramentas consolidadas do ecossistema.

Embora o padrão ERC-3643 seja mais direcionado a *security tokens*, por incorporar registro de identidade *on-chain*, módulos de conformidade configuráveis e restrições de transferência baseadas em identidade verificada, optou-se por não utilizá-lo nesta etapa da pesquisa em virtude de sua substancial complexidade de implantação. Como alternativa, o contrato foi estruturado com mecanismos funcionais similares, incluindo sistema de *whitelist* e restrições de transferência, preservando a possibilidade de futura migração para o referido padrão.

A implementação baseou-se nas bibliotecas da OpenZeppelin, com o objetivo de utilizar componentes amplamente auditados e reduzir o risco de vulnerabilidades associadas ao desenvolvimento integral do código.

O contrato contempla as seguintes funcionalidades: (i) controle de transferências por meio de *whitelist*; (ii) funções de *mint* e *burn* restritas ao proprietário; (iii)

mecanismo de pausa emergencial; (iv) emissão de eventos para fins de auditoria; e (v) conjunto de testes automatizados.

Validação do contrato inteligente e do token experimental

O sistema foi testado em ambiente de desenvolvimento e posteriormente implantado na *testnet* Amoy da rede Polygon. Foram realizados testes de criação de carteiras, inclusão em *whitelist*, emissão (*mint*) e transferência de *tokens*, com verificação do correto funcionamento das restrições implementadas.

Construção do protótipo Argos

Paralelamente ao desenvolvimento do contrato inteligente, iniciou-se a construção do protótipo denominado *Argos*, destinado à gestão administrativa do *token* e ao acompanhamento de suas movimentações.

O protótipo tem natureza experimental e adota modelo de código aberto, permitindo sua utilização e adaptação para fins acadêmicos ou empresariais.

A arquitetura do sistema inclui: (i) interface administrativa baseada em AdminJS; (ii) backend REST desenvolvido em Node.js/TypeScript; (iii) banco de dados PostgreSQL com modelagem via Prisma; (iv) procedimentos de identificação de usuários (KYC); e (v) registro de logs para fins de auditoria.

3.2 Etapas Futuras

Implementação do sistema de distribuição proporcional de lucros

Desenvolver e integrar módulo responsável pela distribuição automatizada de resultados financeiros de forma proporcional aos detentores de tokens, com registro estruturado das operações em banco de dados para fins de rastreabilidade e auditoria.

Aprofundamento da análise de segurança jurídica e tecnológica

Expandir a análise de cenários de risco regulatório, societário e operacional, bem como avaliar vulnerabilidades técnicas potenciais e respectivas estratégias de mitigação.

Documentação técnica e disponibilização do código

Elaborar documentação técnica detalhada do sistema desenvolvido e disponibilizar o código-fonte em repositório público sob licença compatível com software livre, garantindo transparência e reprodutibilidade.

Análise de cenários de aplicação

Examinar possíveis contextos de utilização do sistema em startups em estágio inicial, identificando limitações, requisitos de adaptação e oportunidades de aprimoramento.

3.3 Uso de Ferramentas de Inteligência Artificial

Em conformidade com princípios de transparência científica, declara-se que ferramentas de inteligência artificial, uma realidade onipresente nos dias atuais, foram utilizadas como apoio ao longo desta pesquisa a fim de aprimorar a qualidade da produção científica. Especificamente, foram empregados:

- **Claude Sonnet 4.5 e DeepSeek V4 Lite:** para auxílio na redação de textos, revisão bibliográfica, análise de documentos regulatórios e síntese de informações complexas. Essas ferramentas contribuíram para a organização conceitual e a clareza expositiva do relatório.
- **ChatGPT 5.2 Codex:** para suporte na geração de trechos de código-fonte, desenvolvimento de contratos inteligentes em Solidity, e criação de artefatos do protótipo funcional. A ferramenta acelerou a prototipagem e permitiu testes iterativos de funcionalidades.

Todos os textos e códigos gerados por IA foram revisados, validados e adaptados pelo pesquisador, garantindo aderência aos objetivos da pesquisa, rigor metodológico e conformidade com as normas acadêmicas. O uso dessas tecnologias visa otimizar o processo de pesquisa, sem substituir o pensamento crítico e a responsabilidade autoral do pesquisador.

4 RESULTADOS

Os resultados alcançados até o momento possuem natureza predominantemente teórica e exploratória, em consonância com o estágio inicial da investigação. Ainda que um protótipo funcional tenha sido parcialmente desenvolvido, não houve validação empírica em ambiente real, de modo que suas limitações técnicas e operacionais são reconhecidas e discutidas nesta seção.

4.1 Seleção de plataforma: Polygon

Após análise comparativa entre Ethereum, Binance Smart Chain e Polygon (Tabela 1), e realização de testes exploratórios, optou-se pela Polygon como plataforma de implementação.

Tabela 1 – Comparação preliminar entre plataformas blockchain

Característica	Ethereum	Binance Smart Chain	Polygon
Custo médio por transação	Alto (variável)	Baixo	Baixo
Velocidade de bloco	15s	3s	2s
Máquina virtual	EVM	EVM	EVM
Padrões de token suportados	ERC-20, ERC-3643, etc.	BEP-20 (compatível ERC-20)	ERC-20, ERC-3643
Documentação	Muito completa	Completa	Completa
Comunidade	Grande	Grande	Grande

Fonte: Elaboração própria, com base em (Ethereum Foundation, 2026b; BNB Chain Community, 2026; Polygon Technology, 2026).

A análise considerou os seguintes aspectos de cada plataforma:

Ethereum

Ethereum é a rede de referência para contratos inteligentes e *security tokens*, dispondo da documentação mais completa, da maior comunidade de desenvolvedores e do ecossistema de ferramentas mais maduro. Seu principal obstáculo para o contexto desta pesquisa é o custo elevado de transação (*gas fees*), que pode atingir dezenas de dólares em períodos de congestionamento, tornando inviável o uso frequente por startups em estágio inicial com operações de baixo volume financeiro.

Binance Smart Chain

Binance Smart Chain (BSC) oferece custos de transação comparáveis aos da Polygon e velocidade de bloco adequada, com compatibilidade parcial com o padrão ERC-20

via BEP-20. No entanto, apresenta desvantagens relevantes: é controlada pela Binance, empresa centralizada sob escrutínio regulatório em diversas jurisdições, o que pode introduzir riscos de dependência institucional e questões de conformidade. Adicionalmente, não suporta nativamente o padrão ERC-3643 (T-REX), relevante para *security tokens* com identidade e restrições de transferência reguladas, e sua comunidade de desenvolvedores especializados em contratos inteligentes é menor do que a do Ethereum.

Polygon

Polygon é uma blockchain lateral (*sidechain*) compatível com a EVM, que opera em paralelo ao Ethereum e utiliza um conjunto próprio de validadores para atingir consenso (Polygon Technology, 2026). Embora não seja uma solução de Camada 2 no sentido técnico restrito (como os *rollups*), sua arquitetura oferece compatibilidade plena com o ecossistema Ethereum, permitindo que contratos inteligentes desenvolvidos para a EVM sejam implantados sem modificações. Essa característica, combinada com custos de transação reduzidos (frações de centavo em MATIC), velocidade de bloco superior à do Ethereum (aproximadamente 2 segundos) e suporte ao padrão ERC-3643 para *security tokens* com identidade e restrições de transferência reguladas (SCHWILBERT; DINIS; Tokeny Solutions, 2021), torna a plataforma particularmente adequada para experimentação com tokenização.

A escolha pela Polygon foi, portanto, motivada pela combinação de custo acessível, compatibilidade total com o Ethereum e suporte aos padrões técnicos necessários para *security tokens*, características que se mostraram mais adequadas ao estágio atual da pesquisa. Cabe registrar, contudo, que esta não representa uma avaliação exaustiva do ecossistema de plataformas *blockchain* disponíveis. Outras soluções, como Arbitrum, Optimism ou Base, não foram avaliadas em detalhe e podem apresentar vantagens comparativas em cenários distintos.

4.2 Desenvolvimento do contrato inteligente *ProfitToken*

Foi desenvolvido o contrato inteligente *ProfitToken* em Solidity 0.8.28, utilizando como base as implementações auditadas da biblioteca OpenZeppelin. O padrão ERC-20 foi adotado pela sua simplicidade e ampla compatibilidade com ferramentas existentes; embora o padrão ERC-3643 seja mais adequado para *security tokens* por incorporar nativamente registro de identidade *on-chain* e módulos de conformidade, sua maior complexidade foi considerada prematura para o estágio atual da pesquisa. Para compensar essa escolha, o contrato foi estruturado com mecanismos funcionalmente similares, preservando a possibilidade de migração futura.

As principais funcionalidades implementadas foram:

- **Sistema de *whitelist***: controla quais endereços podem enviar e receber tokens, restringindo a circulação ao grupo de *stakeholders* autorizados e implementando, de forma automatizada, uma das principais salvaguardas regulatórias do modelo.
- ***Mint e burn***: funções de emissão e queima de tokens, restritas ao administrador do contrato, que permitem ajustar a distribuição conforme o valor agregado por cada participante ao longo do tempo.
- **Pausa de emergência**: mecanismo que permite congelar temporariamente todas as transferências em caso de incidente de segurança ou necessidade operacional.
- **Registro de eventos**: emissão de eventos completos (*AddedToWhitelist*, *TokensMinted*, *TokensBurned* etc.) que facilitam a auditoria e a sincronização com sistemas *off-chain*.

O código-fonte completo está disponível no repositório GitHub do projeto e é apresentado parcialmente no Anexo A.

4.3 Desenvolvimento do sistema *Argos*

A construção do protótipo evidenciou um achado que, embora pareça óbvio em retrospecto, não estava explicitado na formulação inicial da pesquisa: *tokens que não podem ser comercializados em mercados secundários precisam estar inseridos em um contexto em que façam sentido e gerem valor para seus detentores*. No caso específico de tokens que representam direitos sobre lucro em startups, objeto da pesquisa, consideramos fundamental a existência de uma interface que permita a todos os stakeholders visualizar saldos, acompanhar distribuições e compreender os direitos associados, o token por si só não agrega valor perceptível aos *stakeholders* de uma startup em estágio inicial.

Essa constatação motivou o desenvolvimento do sistema *Argos*, um protótipo ou Prova de Conceito (PoC) *free software* (GNU GPL v3) de governança que encapsula o *ProfitToken* e oferece uma camada de usabilidade e *compliance* sobre o contrato inteligente. A arquitetura atual compreende:

Contratos inteligentes (Solidity + Hardhat): contrato *ProfitToken* desenvolvido em Solidity 0.8.28, compilado e testado com o framework Hardhat; scripts de *deploy* para a *testnet* Polygon Amoy e para redes de produção; suite de testes automatizados cobrindo as principais funções do contrato; e artefatos de compilação (ABI e *bytecode*) reutilizados pelo *backend* para interação com o contrato implantado.

Backend (Node.js/TypeScript): API REST para gestão de usuários, transações e interação com a *blockchain*; integração com a Polygon via biblioteca Viem;

sistema de autenticação e autorização com perfis ADMIN e STAKEHOLDER; e *listener* de eventos *blockchain* para sincronização automática com o banco de dados.

Banco de dados (PostgreSQL + Prisma ORM): modelo de dados abrangendo entidades de usuário, transação, documento e log de auditoria; sistema KYC integrado com suporte a documentos de identidade; e *checkpoint* de eventos para sincronização incremental com a *blockchain*. O PostgreSQL foi escolhido por sua robustez e por conter recursos de auditoria avançados, enquanto é Prisma foi escolhido por ser um ORM agnóstico de banco de dados, o que preserva a possibilidade de migração futura para outros sistemas relacionais ou mesmo NoSQL, caso seja necessário.

Interface administrativa (AdminJS, parcialmente desenvolvido): painel para gestão de *stakeholders*, emissão de tokens, controle de *whitelist*, visualização de histórico de transações, aprovação de KYC e upload de documentos.

Em termos funcionais, o sistema permite que uma *startup* cadastre *stakeholders* com verificação de identidade, emita tokens proporcionalmente ao valor agregado por cada membro, controle rigorosamente a circulação por meio da *whitelist* e mantenha registro completo e auditável de todas as operações — com a garantia de que os dados gravados na *blockchain* são imutáveis e verificáveis por qualquer parte interessada. O protótipo foi validado em ambiente de desenvolvimento com *deploy* real na *testnet Polygon Amoy*.

Importa ressaltar que o Argos está em estágio inicial de desenvolvimento.

4.4 Estratégias de *compliance* adotadas no protótipo

As escolhas de design do Argos foram informadas pela análise regulatória descrita anteriormente. O modelo de *compliance* adotado apoia-se nos seguintes pilares:

- **Distribuição em circuito fechado:** os tokens são emitidos exclusivamente para *stakeholders* ativos, cadastrados e verificados, sem qualquer divulgação pública ou esforço de captação junto ao público em geral.
- **Vedação à negociação em mercado secundário:** o sistema de *whitelist* no contrato inteligente impede transferências para endereços não autorizados, inviabilizando tecnicamente a comercialização em *exchanges* ou plataformas descentralizadas.
- **KYC e documentação formal:** todos os *stakeholders* passam por verificação de identidade e assinam documentos que descrevem os direitos associados aos tokens e a ausência de promessa de retorno financeiro baseado em esforços de terceiros.

- **Rastreabilidade:** o registro combinado em banco de dados relacional e na *block-chain* garante auditabilidade completa de todas as operações.

Essa estratégia busca afastar a eventual caracterização do modelo como oferta irregular de valores mobiliários, sem ignorar que a incerteza jurídica é inerente a um campo normativo ainda em construção. A análise dos quatro critérios do *Howey Test*, aplicada de forma orientativa ao modelo proposto, sugere que o quarto critério — dependência dos lucros essencialmente do esforço de terceiros — tende a ser respondido negativamente quando os detentores de tokens são participantes ativos da empresa. Contudo, essa análise não substitui a avaliação jurídica individualizada de cada caso concreto, que pode chegar a conclusões distintas dependendo das circunstâncias específicas da *startup* e da evolução do entendimento regulatório.

Os resultados apresentados nas seções anteriores descrevem o que foi construído: um contrato inteligente funcional, um protótipo em desenvolvimento e um conjunto de práticas de compliance tecnicamente sustentadas. A seção seguinte parte dessas entregas para uma análise de segunda ordem — não mais o que foi feito, mas o que isso significa, quais perguntas permanecem sem resposta e quais limitações o próprio processo de construção revelou.

5 DISCUSSÃO

Os resultados obtidos até o momento permitem esboçar algumas reflexões sobre a viabilidade da proposta, sem, contudo, antecipar conclusões que dependem de etapas ainda não realizadas. Esta discussão busca ser honesta quanto ao que foi efetivamente demonstrado e ao que permanece como hipótese de trabalho a ser verificada.

5.1 O que foi e o que não foi demonstrado

O principal resultado concreto deste semestre é a publicação e validação do contrato inteligente *ProfitToken* e parte do sistema *Argos* — que opera em ambiente de desenvolvimento e foi validado na *testnet Polygon Amoy*. Esse resultado demonstra a viabilidade técnica em condições controladas, mas não responde a perguntas mais difíceis: o sistema funcionará de forma confiável em produção? *Stakeholders* sem conhecimento técnico conseguirão utilizá-lo? Os fundadores de startups reais terão disposição para adotar uma solução baseada em *blockchain* dada a camada adicional de complexidade, o conjunto de riscos e as incertezas identificadas?

A viabilidade jurídica, por sua vez, é ainda mais difícil de afirmar. O modelo de *compliance* proposto é fundamentado, mas não foi submetido à avaliação de especialistas em direito societário ou regulatório, e não há qualquer garantia de que a CVM ou o BCB compartilhariam do mesmo entendimento diante de um caso concreto. A ausência de jurisprudência consolidada sobre o tema é, simultaneamente, uma oportunidade de originalidade para a pesquisa e um risco real para eventuais adotantes da solução.

5.2 Sobre a escolha técnica: Polygon e ERC-20

A escolha da Polygon mostrou-se adequada para os objetivos desta etapa da pesquisa. Os custos mínimos de transação viabilizaram testes iterativos sem impacto financeiro relevante, e a **compatibilidade com a EVM** garantiu que o conhecimento técnico adquirido em Solidity e nas ferramentas do ecossistema Ethereum seja aproveitável em outras plataformas caso necessário.

A adoção do padrão ERC-20, em vez do ERC-3643, foi uma escolha pragmática que merece reflexão. O ERC-3643 seria mais adequado semanticamente para o caso de uso proposto, contudo, a substancial complexidade de implementação — que exige a implantação de contratos auxiliares de identidade e *compliance* além do token em si — teria provavelmente inviabilizado a entrega de um protótipo funcional neste semestre, dadas as condições com as quais a pesquisa foi realizada e o nível de maturidade técnica inicial do pesquisador. A solução adotada — implementar um sistema de *whitelist* sobre o ERC-20 — é funcionalmente equivalente para o caso de uso

em questão, embora não ofereça a expressividade semântica e a interoperabilidade regulatória nativas do ERC-3643. Essa migração pode ser endereçada em trabalhos futuros.

5.3 O achado central: o token precisa estar inserido em um contexto no qual ele possua valor

Um dos resultados mais relevantes deste semestre não é técnico, mas conceitual: a constatação de que *tokens que não podem ser negociados em mercados secundários — condição necessária para evitar enquadramento regulatório problemático — só fazem sentido quando inseridos em um contexto que os torne valiosos para seus detentores*. No caso especificado, consideramos inserir o token no contexto de uma interface amigável e informativa, que permita a todos os *stakeholders* visualizar saldos, acompanhar distribuições e compreender os direitos associados.

5.4 Sobre a estratégia regulatória

A estratégia de *compliance* delineada — distribuição em circuito fechado, KYC, vedação a mercados secundários, ausência de publicidade e uso cuidadoso de terminologia — é plausível e fundamentada, mas deve ser lida com cautela.

Em primeiro lugar, ela se apoia em uma interpretação do *Howey Test* e do Parecer CVM nº 40/2022 que pode não ser compartilhada pelos reguladores em um caso concreto. A fronteira entre um colaborador “ativo” e um investidor “passivo” não é geometricamente nítida, e a CVM tem discricionariedade para analisar a substância econômica da operação de forma mais ampla.

Em segundo lugar, a estratégia não endereça todos os vetores de risco identificados. Questões como a perda de chave privada por um *stakeholder*, a execução de ordens judiciais sobre registros imutáveis em *blockchain* ou os impactos tributários da distribuição de resultados tokenizados permanecem em aberto e precisarão ser tratadas nas próximas etapas — idealmente com o suporte de profissionais das áreas jurídica e contábil.

5.5 Possíveis vantagens estratégicas da tokenização em empresas em estágio inicial

Não obstante os riscos e limitações mapeados ao longo desta pesquisa, a adoção antecipada da tecnologia pode trazer vantagens estratégicas, especialmente quando se considera o horizonte de desenvolvimento de uma *startup* em estágio inicial.

Organização da empresa por valor efetivamente agregado. Vantagem de natureza mais operacional, diz respeito ao potencial da tecnologia como instrumento

de organização interna equitativa. Considere o cenário de três engenheiros que decidem fundar uma *startup* sem capital expressivo. Os *tokens* podem ser distribuídos progressivamente apenas conforme cada stakeholder trabalha ou aporta capital. Assim, o grupo dispõe de um mecanismo objetivo e auditável para quantificar e registrar a contribuição individual ao longo do tempo. Esse modelo é particularmente relevante em cenários comuns em startups nascentes: um fundador que contribui predominantemente com capital intelectual, outro com dedicação de tempo integral e um terceiro que realiza aportes financeiros pontuais podem ter suas participações ajustadas de forma dinâmica, transparente e contratualmente fundamentada, sem depender de renegociações informais ou de instrumentos tradicionais de *equity* que exigem alterações societárias custosas. A tecnologia não resolve o problema humano da negociação de valor entre fundadores, mas oferece uma infraestrutura de registro que torna esse processo mais transparente e menos suscetível a disputas futuras.

Mindset tokenizado desde o início. A construção de um sistema de *tokens* em circuito fechado — ainda que em caráter experimental e juridicamente cauteloso — exige que a *startup* desenvolva, desde cedo, procedimentos eficientes de governança e *compliance*: *smart contracts* automatizados, KYC, transparência, registros auditáveis etc. Esse conjunto de rotinas não é descartável quando a empresa sobe de nível, ao contrário, pode facilitar a transição para estágios mais avançados de desenvolvimento e regulação.

Essas vantagens não invalidam os riscos identificados nem dispensam a devida análise jurídica em cada caso concreto.

5.6 Limitações identificadas e próximas etapas

As principais limitações do trabalho realizado até aqui são:

- A interface administrativa do sistema Argos ainda está em desenvolvimento
- A funcionalidade de distribuição automatizada de lucro — que é o objetivo central da pesquisa — ainda não foi implementada. O protótipo atual gerencia tokens, mas não realiza a distribuição proporcional de resultados financeiros.
- O sistema não foi testado com usuários reais, e aspectos de usabilidade, especialmente para *stakeholders* sem familiaridade com *blockchain*, não foram avaliados.
- A análise jurídica não foi validada por especialistas externos e tem caráter exploratório.
- Os aspectos tributários da tokenização de lucros não foram abordados, e podem representar uma camada adicional de complexidade.

- A documentação técnica e jurídica necessária para que a solução seja adotada por terceiros ainda precisa ser elaborada.

No próximo semestre, as prioridades serão: (i) implementar o mecanismo de distribuição automatizada de lucro, que pode envolver o uso de *stablecoins* ou integração com sistemas de transferência bancária; (ii) finalizar a implementação da interface administrativa; (iii) aprofundar a análise de segurança jurídica e tecnológica, de preferência com apoio de especialistas; (iv) realizar testes com usuários representativos do público-alvo; e (v) documentar e publicar o código sob licença GPL v3, permitindo que a solução seja avaliada, criticada e eventualmente adotada por outras startups.

A pesquisa se encontra em estágio inicial, com resultados promissores mas ainda preliminares. O protótipo demonstra que a proposta é tecnicamente realizável; o próximo desafio é demonstrar que ela é juridicamente robusta, operacionalmente usável e genuinamente útil para o ecossistema de startups brasileiras iniciantes.

REFERÊNCIAS

BACK, A. *Hashcash – A Denial of Service Counter-Measure*. [S.l.], 2002. Acesso em: 9 out. 2025. Disponível em: <<http://www.hashcash.org/papers/hashcash.pdf>>.

Banco Central do Brasil. *DREX*. 2023. Acesso em: 19 fev. 2026. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/drex>>.

BARRETO, M. M. *Oferta Pública de Tokens: Preciso Ter Autorização da CVM?* 2022. Acesso em: 15 fev. 2026. Disponível em: <<https://www.jusbrasil.com.br/artigos/oferta-publica-de-tokens-preciso-ter-autorizacao-da-cvm/1625290349>>.

BCG. *Tokenized Funds: The Third Revolution in Asset Management*. 2024. Acesso em: 15 fev. 2026. Disponível em: <<https://www.bcg.com/press/29october2024-tokenized-funds-the-third-revolution-in-asset-management-decoded>>.

Binance Academy. *What Is an Ethereum Improvement Proposal (EIP)?* 2025. Artigo explicativo sobre EIPs na plataforma Binance Academy. Disponível em: <<https://www.binance.com/en/academy/articles/what-is-an-ethereum-improvement-proposal-eip>>.

BLASCO, G. d. C.; BLASCO, F. D. C. *Regulamentação de ativos digitais pela CVM é considerada tímida por especialistas*. 2022. Artigo de opinião publicado no Consultor Jurídico (ConJur) em 26 out. 2022. Disponível em: <<https://www.conjur.com.br/2022-out-26/opinioao-regulamentacao-ativos-digitais-cvm/>>.

BNB Chain Community. *BNB Smart Chain Documentation*. 2026. BNB Chain Docs. Acesso em: 23 fev. 2026. Disponível em: <<https://docs.bnbchain.org/>>.

BSBC Advogados. Security token offerings (stos): Dlts, regulação e novas formas de financiamento. *BSBC Advogados – Publicações*, 2021. Disponível em: <<https://bsbcadvogados.com.br/publicacoes/security-token-offerings-stos-dlts-regulacao-e-novas-formas-de-financiamento/>>.

BUTERIN, V. *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. 2013. <<https://ethereum.org/en/whitepaper/>>. Acesso em: 16 fev. 2026.

BUTERIN, V. *The Meaning of Decentralization*. 2017. Medium. Acesso em: 16 fev. 2026. Disponível em: <<https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>>.

COMITO, K. Crowdfunding and crowdsourcing of aging science. *Cold Spring Harbor Perspectives in Medicine*, v. 13, n. 7, p. a041209, 2023. ISSN 2157-1422. Acesso em: 20 fev. 2026. Disponível em: <<https://perspectivesinmedicine.cshlp.org/content/13/7/a041209>>.

DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. *IEEE Transactions on Information Theory*, v. 22, n. 6, p. 644–654, 1976.

Ethereum Foundation. *ERC — Ethereum Improvement Proposals*. 2026. Lista de padrões de aplicação (ERC) na plataforma Ethereum. Disponível em: <<https://eips.ethereum.org/erc>>.

Ethereum Foundation. *Ethereum Documentation*. 2026. Ethereum.org. Acesso em: 23 fev. 2026. Disponível em: <<https://ethereum.org/en/developers/docs/>>.

Ethereum Foundation. *Technical intro to ether*. 2026. Ethereum.org. Acesso em: 23 fev. 2026. Disponível em: <<https://ethereum.org/developers/docs/intro-to-ether/>>.

FERTIG, T.; SCHÜTZ, A. *Blockchain: The Comprehensive Guide to Blockchain Development, Ethereum, Solidity, and Smart Contracts*. [S.l.]: Rheinwerk Computing, 2024.

GHIMIRE, S.; SELVARAJ, H. A survey on bitcoin cryptocurrency and its mining. In: *2018 26th International Conference on Systems Engineering (ICSEng)*. Sydney, Australia: IEEE, 2018. p. 1–6. ISBN 978-1-5386-7834-3.

INFOMONEY. *BC desliga plataforma do DREX usada até agora por problemas de privacidade*. 2025. InfoMoney. Acesso em: 16 fev. 2026. Disponível em: <<https://www.infomoney.com.br/minhas-financas/bc-suspendera-plataforma-drex-permanentemente-por-falta-de-seguranca-dizem-fontes/>>.

KONDOVA, G.; SIMONELLA, G. Blockchain in startup financing: Icos and stos in switzerland. *Journal of Strategic Innovation and Sustainability*, v. 14, n. 6, p. 43–48, 2019. Disponível em: <<https://ssrn.com/abstract=3528545>>.

Kria. *Capte investimentos com o Kria*. 2025. <<https://www.kria.vc/quero-captar>>. Acesso em: 17 fev. 2026.

LI, W.; LIU, Z.; CHEN, J.; LIU, Z.; HE, Q. Towards blockchain interoperability: A comprehensive survey on cross-chain solutions. v. 6, n. 3, p. 100286, 2024. ISSN 20967209. Disponível em: <<https://linkinghub.elsevier.com/retrieve/pii/S2096720925000132>>.

MCKINSEY. *From ripples to waves: The transformational power of tokenizing assets*. 2024. Acesso em: 16 fev. 2026. Disponível em: <<https://www.mckinsey.com/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets>>.

MERKLE, R. C. A certified digital signature. In: BRASSARD, G. (Ed.). *Advances in Cryptology – CRYPTO '89: Proceedings*. New York, NY: Springer, 1989. p. 218–238.

MOHAMMED, M. A.; DE-PABLOS-HEREDERO, C.; BOTELLA, J. L. M. A systematic literature review on the revolutionary impact of blockchain in modern business. v. 14, n. 23, p. 11077, 2024. ISSN 2076-3417. Disponível em: <<https://www.mdpi.com/2076-3417/14/23/11077>>.

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 15 fev. 2026.

NETO, R. C. O futuro da intermediação financeira. *Folha de S.Paulo*, out. 2025. Acesso em: 16 fev. 2026. Disponível em: <<https://www1.folha.uol.com.br/colunas/roberto-campos-neto/2025/10/o-futuro-da-intermediacao-financeira.shtml>>.

Polygon Technology. *Polygon Documentation*. 2026. Polygon Wiki. Acesso em: 23 fev. 2026. Disponível em: <<https://wiki.polygon.technology/>>.

SAESEN, J.; KINDERMANN, B.; ABEL, D.; STRESE, S. The power of governance: A study on the relationship between on-chain DAO governance and token performance. p. 02683962251343627, 2025. ISSN 0268-3962, 1466-4437. Disponível em: <<https://journals.sagepub.com/doi/10.1177/02683962251343627>>.

SCHWIETERT, J.; DINIS, A.; Tokeny Solutions. *ERC-3643: T-REX – Token for Regulated EXchanges*. 2021. Ethereum Improvement Proposals. Acesso em: 23 fev. 2026. Disponível em: <<https://eips.ethereum.org/EIPS/eip-3643>>.

Startup Genome. *Global Startup Ecosystem Report 2025: Global Startup Ecosystem Ranking 2025 (Top 40)*. 2025. <<https://startupgenome.com/report/gser2025/global-startup-ecosystem-ranking-2025-top-40>>. Acesso em: 15 fev. 2026.

SYED, T. A.; ALZHRANI, A.; JAN, S.; SIDDIQUI, M. S.; NADEEM, A.; ALGHAMDI, T. A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. *IEEE Access*, v. 7, p. 176838–176869, 2019. ISSN 2169-3536.

TUCCI, J. R. C. e. A linguagem jurídica exige precisão técnica: processo ou procedimento arbitral? *Consultor Jurídico*, janeiro 2021. Disponível em: <<https://www.conjur.com.br/2021-jan-05/paradoxo-corte-linguagem-juridica-exige-precisao-tecnica>>.

WOOD, G. *Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper)*. 2014. <<https://ethereum.github.io/yellowpaper/paper.pdf>>. Acesso em: 19 nov. 2025.

XP Investimentos. *Outliers 142: Venture Capital no Brasil*. 2024. Acesso em: 15 fev. 2026. Disponível em: <<https://conteudos.xpi.com.br/fundos-de-investimento/relatorios/outliers-142/>>.

YERMACK, D.; NIAN, L. P.; CHUEN, D. L. K. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Amsterdam: Elsevier, 2015.

YI, Y. The Investigation of Layer 2 Blockchain Technologies for Decentralized Applications:. In: *Proceedings of the 1st International Conference on Data Science and Engineering*. SCITEPRESS - Science and Technology Publications, 2024. p. 326–333. ISBN 978-989-758-690-3. Disponível em: <<https://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0012837400004547>>.

6 ANEXOS

6.1 Anexo A – Código do contrato ProfitToken (trechos principais)

```
// SPDX-License-Identifier: MIT
pragma solidity 0.8.28;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
import "@openzeppelin/contracts/access/Ownable.sol";
import "@openzeppelin/contracts/utils/Pausable.sol";

/**
 * @title Profit Token
 * @notice Token ERC-20 com whitelist, mint, burn e pausa
 */
contract ProfitToken is ERC20, Ownable, Pausable {

    mapping(address => bool) private _whitelist;

    event AddedToWhitelist(address indexed account);
    event RemovedFromWhitelist(address indexed account);
    event TokensMinted(address indexed to, uint256 amount);
    event TokensBurned(address indexed from, uint256 amount);

    modifier onlyWhitelisted(address account) {
        require(_whitelist[account], "Account not whitelisted");
        _;
    }

    constructor() ERC20("Profit Share Token", "DIV")
        Ownable(msg.sender) {
        _whitelist[msg.sender] = true;
        emit AddedToWhitelist(msg.sender);
    }

    function addToWhitelist(address account) external onlyOwner {
        require(account != address(0), "Cannot whitelist zero address");
        require(!_whitelist[account], "Already whitelisted");
        _whitelist[account] = true;
        emit AddedToWhitelist(account);
    }
}
```



```

    }

    function mint(address to, uint256 amount) external onlyOwner {
        require(to != address(0), "Cannot mint to zero address");
        require(amount > 0, "Amount must be greater than zero");
        _mint(to, amount);
        emit TokensMinted(to, amount);
    }

    function burn(address from, uint256 amount) external onlyOwner {
        _burn(from, amount);
        emit TokensBurned(from, amount);
    }

    function _update(address from, address to, uint256 amount)
        internal override whenNotPaused {
        if (from != address(0)) {
            require(_whitelist[from], "Sender not whitelisted");
        }
        if (to != address(0)) {
            require(_whitelist[to], "Recipient not whitelisted");
        }
        super._update(from, to, amount);
    }
}

```

6.2 Anexo B – Evidência de deploy do contrato na Polygon Amoy

Este anexo apresenta a comprovação pública do deploy do contrato *ProfitToken* na rede *Polygon Amoy* por meio do explorador PolygonScan.

Rede: Polygon Amoy (*testnet*)

Endereço do contrato: <<https://amoy.polygonscan.com/address/0x1b5048642BeDe3e361D8653F5219e9dfe8fd1A48>>

Token identificado no explorador: ERC-20: Profit Share Token (DIV)

Transação de criação (deploy): <<https://amoy.polygonscan.com/tx/0xd1399b9acfe8b53c242be926a3544c4d0dd936b976dc74a0f8c542df987f46b5>>

Amoy Testnet

Search by Address / Txn Hash / Block / Token

Contract 0x1b5048642BeDe3e361D8653F5219e9dfe8fd1A48

Overview

POL BALANCE

0 POL

More Info

CONTRACT CREATOR

0x28725C76...69538b112 | 23 days ago

TOKEN TRACKER

Profit Share Token (DIV)

Multichain Info

N/A

Transactions Token Transfers (ERC-20) Contract Events

Latest 4 from a total of 4 transactions

Download Page Data

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
0x6a26e4b52c...	Add To WhiteList	33565855	12 days ago	0x28725C76...69538b112	0x1b504864...fe8fd1A48	0 POL	0.00371147
0x24e588318b...	Mint	33564562	12 days ago	0x28725C76...69538b112	0x1b504864...fe8fd1A48	0 POL	0.00449022
0xe2c924a3a9...	Add To WhiteList	33564544	12 days ago	0x28725C76...69538b112	0x1b504864...fe8fd1A48	0 POL	0.00469886
0x3ced2784b0...	Mint	33086341	23 days ago	0x28725C76...69538b112	0x1b504864...fe8fd1A48	0 POL	0.00224001

[Download: CSV Export]

A contract address hosts a smart contract, which is a set of code stored on the blockchain that runs when predetermined conditions are met. Learn more about addresses in our Knowledge

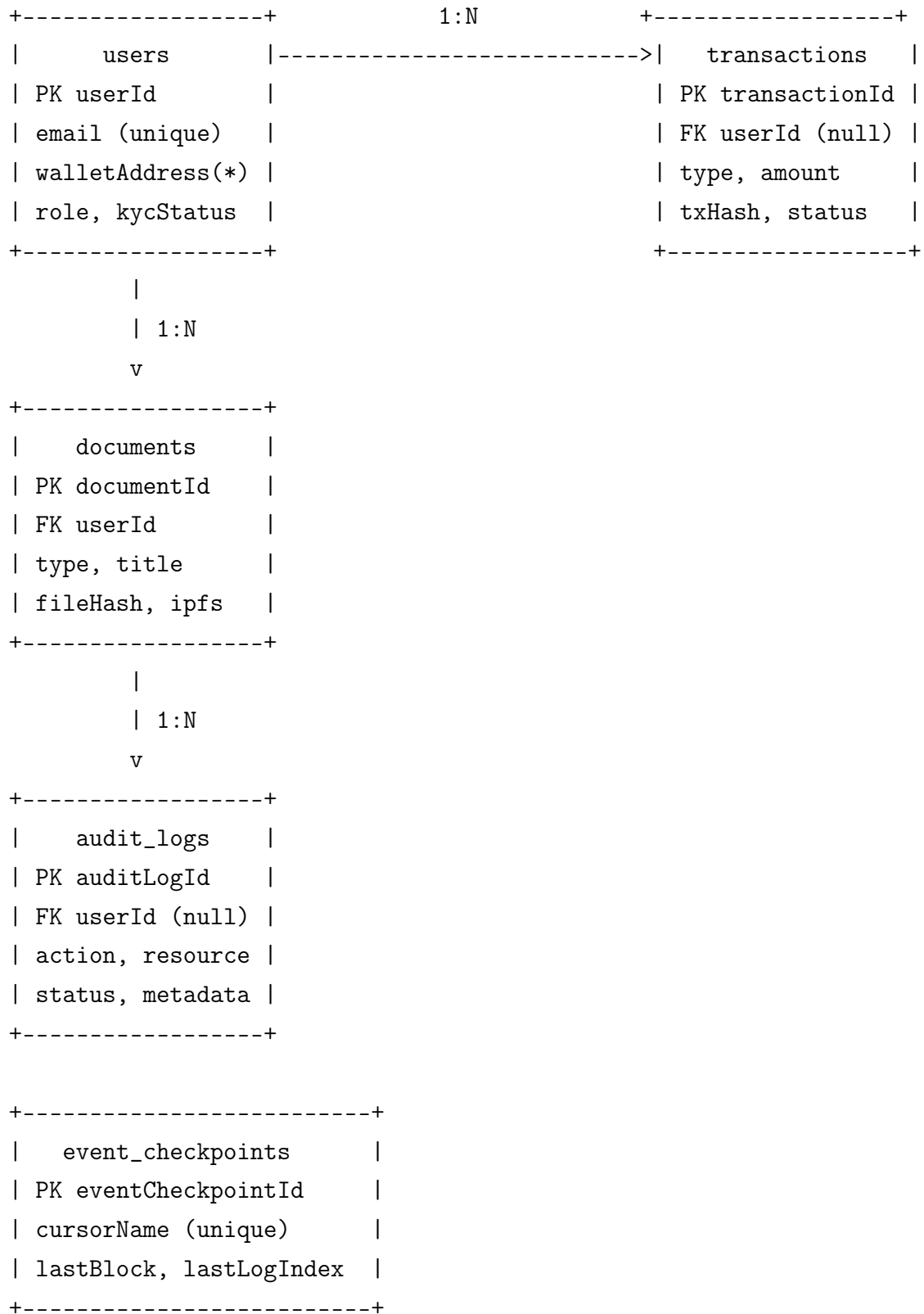
Figura 2 – Comprovação do contrato *ProfitToken* publicado na rede Polygon Amoy

Fonte: Elaboração própria, captura de tela do PolygonScan (Amoy Testnet).

Observação: Como se trata de ambiente de *testnet*, os dados apresentados servem como evidência de validação técnico-operacional da implantação e dos testes iniciais do contrato inteligente.

6.3 Anexo C – Diagramação do banco de dados do protótipo *Argos*

Diagrama lógico (entidades e relacionamentos)



(*) walletAddress é opcional, mas único quando informado.

Descrição breve das tabelas

- **users**: tabela principal de identidade e acesso. Armazena credenciais, perfil (ADMIN/STAKEHOLDER), dados de KYC e metadados de conta.
- **transactions**: registra eventos financeiros e operacionais relacionados ao token (*mint*, *transfer*, *burn*, alterações de *whitelist*), incluindo *txHash*, bloco e status de processamento.
- **documents**: armazena documentos vinculados ao usuário (ex.: KYC, contratos, termos), com hash de integridade do arquivo e suporte opcional a referência IPFS e ancoragem em *blockchain*.
- **audit_logs**: trilha de auditoria de ações do sistema (quem fez, o que fez, em qual recurso e com qual resultado), com suporte a metadados, IP e *user agent*.
- **event_checkpoints**: tabela de controle técnico para sincronização incremental de eventos da *blockchain*, guardando o último bloco processado e o índice do log.

6.4 Anexo D – Estrutura de diretórios do protótipo *Argos*

Este anexo descreve a organização de pastas do protótipo *Argos*, com base no diretório raiz `argos/`.

Visão geral da estrutura de diretórios

```
argos/  
  admin/  
    prisma/  
    src/  
  backend/  
    prisma/  
    scripts/  
    src/  
  smartcontracts/  
    contracts/  
    scripts/  
    test/  
    artifacts/  
    ignition/  
  .data/  
  docker-compose.yml  
  README.md
```

Descrição dos diretórios principais

- **admin/**: camada administrativa (painel) do sistema. Contém configuração do AdminJS, componentes de interface e integração com o banco para operações de gestão.
- **backend/**: API principal do protótipo, implementada em Node.js/TypeScript. Centraliza regras de negócio, autenticação/autorização, integração com *blockchain*, persistência de dados e rotas HTTP.
- **smartcontracts/**: projeto de contratos inteligentes (Hardhat/Solidity). Inclui o código-fonte do *ProfitToken*, scripts de *deploy*, testes automatizados e artefatos compilados.
- **.data/**: diretório de dados auxiliares de desenvolvimento e demonstração (ex.: carteiras de teste), utilizado no fluxo local do protótipo.

Observação: A estrutura foi organizada em formato modular para separar interface administrativa, lógica de aplicação e camada *on-chain*, facilitando manutenção e evolução incremental.