UNIVERSIDADE PAULISTA

VICE-RECTORY OF GRADUATE STUDIES AND RESEARCH

UNDERGRADUATE RESEARCH AND TECHNOLOGICAL DEVELOPMENT AND INNOVATION INITIATION

SEMESTER RESEARCH REPORT

TECHNICAL-OPERATIONAL AND REGULATORY ASPECTS OF ISSUING A CRYPTO-ASSET TO REPRESENT PROFIT RIGHTS IN EARLY-STAGE STARTUPS IN BRAZIL

Author: Leonardo de Souza Borges

Course: Computer Science

Campus: Campinas (Swift)

Advisor: Prof. Dr. Karem Daiane Marcomini

Research Supported by the Vice-Rectory of Graduate Studies and Research of Universidade Paulista – UNIP, under the Program “Undergraduate Research and Technological Development and Innovation”.

Campinas

2026

ABSTRACT

TECHNICAL-OPERATIONAL AND REGULATORY ASPECTS OF ISSUING A CRYPTO-ASSET TO REPRESENT PROFIT RIGHTS IN EARLY-STAGE STARTUPS IN BRAZIL

Author: Leonardo de Souza Borges

This undergraduate research project investigates the use of crypto-assets to represent economic rights in early-stage Brazilian startups. The starting point is a structural challenge in the national ecosystem: the scarcity of accessible mechanisms for financing and structuring. The hypothesis is that *blockchain* technology may offer alternative pathways for new governance dynamics and resource mobilization. The investigation is grounded in the premise that *tokens* can transcend the function of financial assets, acting as instruments to quantify and record the *de facto* contribution of each *stakeholder* – founders, collaborators, and investors. *Smart contracts* enable not only token issuance but also the automated computational execution of profit distribution to token holders. Thus, the technology allows structuring a company based on the value effectively added by each party, fostering a culture of meritocracy and participation from the very genesis of the business. The research covers the theoretical foundation, from blockchain fundamentals to the flexibility of Ethereum smart contracts, and the national regulatory landscape. On the technical side, the *ProfitToken* contract was developed in Solidity, following the ERC-20 standard with whitelist mechanisms, deployed and validated on the *Polygon Amoy testnet*. In parallel, the *Argos* system was initiated – an open-source GPL v3 prototype that adds a value layer with usability, *compliance*, and token management. The main result of this semester is the demonstration of the technical feasibility of the proposal, accompanied by a discussion of the operational and regulatory challenges identified. The research continues with the goal of implementing automated profit distribution and deepening the analysis of legal certainty in order to investigate the feasibility of applying the technology by early-stage Brazilian startups.

Keywords: *Blockchain*, *Security Tokens*, Early-Stage Startups, Asset Tokenization, Smart Contracts, Crypto-Asset Regulation, Profit Distribution, Decentralized Financing, Ethereum, Polygon, Legal Certainty, ERC-20.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background and Relevance

The investigation of innovative solutions for financing early-stage startups in Brazil is particularly relevant given the structural barriers to capital access faced by these nascent companies and the relative fragility of the national venture capital environment when compared to consolidated ecosystems such as Silicon Valley, London, and Tel Aviv (Startup Genome, 2025; XP Investimentos, 2024). In particular, startups in the ideation, validation, and early operation phases – collectively referred to as *early stage* – face significant constraints in fundraising, highlighting the need for more efficient, accessible financial mechanisms adapted to the specificities of the Brazilian context.

Since 2009, *blockchain* technology has established itself as an emerging infrastructure in constant evolution, with diverse and documented applications across multiple sectors, including finance, healthcare, the Internet of Things (IoT), gaming, and supply chain management (MOHAMMED; DE-PABLOS-HEREDERO; BOTELLA, 2024).

With the advent of Bitcoin and *blockchain* technology (NAKAMOTO, 2008), the global financial sector began to experience significant transformations (KONDOVA; SIMONELLA, 2019). Among the central properties of this technology is the fact that, in public *blockchains*, records are stored in a decentralized and verifiable manner, with a high degree of resistance to alteration, while also being transparent and auditable by any network participant. In this sense, *blockchain* can be understood, by analogy, as a distributed digital registry system capable of ensuring the integrity and traceability of information without relying on a central authority.

Years after Bitcoin, the concept of decentralized smart contracts (*smart contracts*) emerged (BUTERIN, 2013), consisting of programs stored on a *blockchain* and executed through its decentralized infrastructure, capable of automating the execution of predefined conditions without the need for intermediaries. This programmable capability enabled the creation of *tokens*, understood as digital representations recorded on a *blockchain*, whose lifecycle – issuance, transfer, and eventual redemption – is entirely governed by the rules encoded in a smart contract. Among these assets, *security tokens* stand out, as they represent economic or corporate rights over real assets, such as shares, equity stakes, or receivables.

If it is plausible to consider that money is, at its core, a medium through which people work for one another – an instrument of labor and value intermediation – then *tokens*, by analogy, can be viewed in the same light and emerge as an alternative for startups to mobilize and organize resources in their initial phase. These digital assets can represent fractions of future economic rights and be distributed automatically and proportionally among token holders (*stakeholders*) – founders, key collaborators, and investors – based on each party's actual contribution to the business. This way, even without significant capital at the outset, a *startup* can structure a more efficient governance model.

For instance, suppose three engineers, with limited initial capital, decide to create a *startup*. They stipulate that the value of the business should be at least one million Brazilian reais, and to organize themselves they decide to issue one million units of crypto-asset, with each *token* representing a nominal value of one real, totaling one million reais in all. Initially, all *tokens* remain in the company's possession, but as founders work or contribute capital, they receive a number of *tokens* proportional to the value each one has added to the business. This approach allows not only an alternative to attract decentralized financing, but also a form of organization centered on the value effectively deposited in the business.

An additional advantage for early-stage companies in adopting tokenization practices lies in the possibility of structuring, from the outset, formal governance mechanisms. Such an arrangement can serve as a facilitator for an eventual transition to the regulated *security token* market through platforms accredited by the Brazilian Securities and Exchange Commission (CVM) once the company reaches greater operational and financial maturity, including enabling the trading of these assets on secondary markets.

Prospective studies indicate that the tokenized asset market could reach between US$ 2 trillion (MCKINSEY, 2024) and US$ 16 trillion (BCG, 2024) by 2030, evidencing a trend of substantial expansion and the growing relevance of this technology in the global economic landscape.

In Brazil, the Central Bank (BCB) has demonstrated interest in exploring tokenization and *blockchain*-based solutions, as exemplified by the development of DREX, the BCB's digital currency project. Although the initiative has faced challenges in its research and development phase, **national interest persists** in adopting the technology and deepening scientific knowledge on the subject (NETO, 2025; INFOMONEY, 2025; Banco Central do Brasil, 2023).

In parallel, in recent years, the CVM and the National Congress have advanced in regulating crypto-assets. CVM Guidance Opinion No. 40/2022 and Law No. 14,478/2022 (Cryptocurrency Legal Framework) are relevant examples of this regulatory movement.

The early adoption of tokenization mechanisms also involves important *trade-offs*. For a *startup* still in the process of validating its business model, tokenization may represent an increase in operational and regulatory complexity, diverting founders' focus and generating additional costs. Furthermore, relevant factors of legal uncertainty persist, among which the following stand out: (i) the absence of consolidated jurisprudence; (ii) the risk of labor or commercial litigation due to lack of understanding of the technology; (iii) the lack of clearly defined procedures for incident situations; and (iv) the risk of administrative proceedings by regulatory bodies.

On this last point, it can be stated that, as a general rule, *tokens* that confer economic rights such as profits or equity participation tend to be classified as securities by the CVM and, as such, are subject to the rules applicable to the Brazilian capital market, including issuer and public offering registration, information disclosure, and other obligations set forth in relevant legislation (BARRETO, 2022). This regulatory burden may, depending on the case, impose a series of bureaucratic requirements that prove paralyzing for early-stage startups, given the need to comply with standards that traditionally apply to established companies. Furthermore, the regulatory pathway proposed by the CVM for access to the capital market tends to be directed at companies with a higher degree of operational and financial maturity: platforms authorized by the regulator, such as KRIA, generally require participating companies to demonstrate proven traction and a consolidated business thesis in order to access offering and trading mechanisms in the regulated environment (Kria, 2025).

On the other hand, the constitutional principle of free enterprise and free market (Brazilian Constitution, art. 1, IV) also applies, allowing companies to organize themselves in whatever way best suits their needs, including through the use of new technologies, provided no harm is caused to third parties. In light of this scenario – marked by the transformative potential of tokenization and the technical, operational, and regulatory challenges surrounding its adoption by early-stage startups – this research investigates the technical-operational and regulatory feasibility of issuing crypto-assets (*security tokens*) to represent economic rights over profits in early-stage Brazilian startups, seeking to discuss possible practical implications such as legal certainty, technical feasibility, and governance structuring.

This semester report presents the progress of the research initiated in August 2025.

1.2 Objectives

General Objective

To analyze the technical-operational and regulatory feasibility of using *tokens* as instruments to represent profit rights in early-stage Brazilian startups (*early stage*).

Specific Objectives

- Identify opportunities and potential benefits that *blockchain*, *smart contract*, and *token* technologies may offer to early-stage Brazilian startups;

– Analyze the legal certainty and regulatory landscape applicable to the issuance of a crypto-asset (*token*) intended to represent economic rights over profits;

– Implement an experimental *token* to represent profit rights, using *blockchain* technology and smart contracts;

– Develop a software prototype that enables automated profit distribution;

– Assess the reproducibility and adaptability of the developed solution, making the artifacts available on GitHub under open licenses (GPL v3 and Creative Commons) to allow their validation, critique, and eventual adoption by other startups or researchers.

2 THEORETICAL FRAMEWORK

The theoretical framework of this research is organized around three main axes: (i) the historical evolution and conceptual foundations of *blockchain* technology; (ii) its potential applications in the context of early-stage startups; and (iii) the applicable Brazilian regulatory framework, with emphasis on legal certainty. This structure provides the analytical reference needed to examine the challenges and opportunities associated with implementing the proposed model.

2.1 Technological Foundations and Historical Evolution

Blockchain technology emerges as a decentralized infrastructure for recording and transferring value and information, whose initial milestone is the Bitcoin *white paper*, published by Nakamoto (2008).

It is essential to distinguish *Bitcoin* from *blockchain*: while the former is a peer-to-peer digital currency system, the latter corresponds to the distributed ledger architecture that enables this and various other decentralized applications (LI *et al.*, 2024).

Nakamoto (2008) combined already-existing technological elements, such as asymmetric cryptography (DIFFIE; HELLMAN, 1976), hash functions (MERKLE, 1989), peer-to-peer (P2P) networks, and the proof-of-work mechanism (BACK, 2002), to conceive a distributed, decentralized, and tamper-resistant record system.

The basic operation of Bitcoin's *blockchain* is based on grouping transactions into blocks chained by *hashes*, forming a chain that makes records practically immutable (YERMACK; NIAN; CHUEN, 2015). Validation is performed by miners competing to solve a mathematical problem (proof of work), ensuring consensus without a central authority (GHIMIRE; SELVARAJ, 2018).

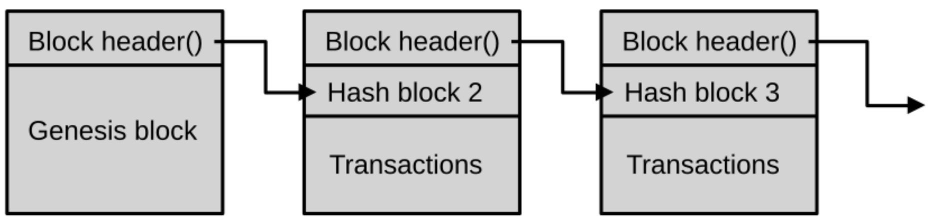

Figure 1 – Block chain structure in a *blockchain*

Fonte: Own authorship, adapted from Kondova e Simonella (2019).

A significant innovative leap occurred with Ethereum, proposed by Buterin (2013) and launched in 2015. Ethereum introduced *smart contracts* – Turing-complete programs executed in the Ethereum Virtual Machine (EVM) and recorded on the *blockchain*, capable of automating agreements and enforcing clause execution without intermediaries (WOOD, 2014). The EVM enabled individuals or organizations to issue their own *tokens* and develop decentralized applications (*dApps*) in areas such as finance, gaming, and governance, significantly expanding the set of possibilities of *blockchain* technology.

To enable the decentralized execution of smart contracts, Ethereum introduced two fundamental and interdependent concepts: *Ether* (ETH) and *gas*. *Ether* is Ethereum's native cryptocurrency and serves as the economic fuel of the system: every operation executed on the network – whether a simple transfer, the deployment of a smart contract, or the invocation of one of its functions – requires the payment of a fee called *gas fee*, settled in *Ether* (Ethereum Foundation, 2026c).

Gas, in turn, is the unit that measures the computational effort required to process each operation; more complex instructions consume greater amounts of *gas*. The final amount paid in ETH corresponds to the product of the *gas* consumed and the unit price of *gas*, defined by market conditions.

According to Fertig e Schütz (2024), this mechanism serves two essential functions: it compensates network validators for processing transactions and acts as a protection mechanism against denial-of-service attacks by imposing an economic cost on the execution of computational operations.

As the ecosystem grew, challenges related to *blockchain* scalability emerged. The so-called blockchain trilemma – the difficulty of simultaneously optimizing decentralization, security, and scalability – drove the development of Layer 2 (L2) solutions and other architectural approaches (BUTERIN, 2017).

Layer 2 solutions process transactions outside the main chain (*off-chain*) and periodically anchor their results to Layer 1, preserving the base network's security level while increasing processing throughput. Among the main current implementations for dealing with the trilemma, the following stand out (YI, 2024):

- **State Channels**: allow multiple transactions between parties without publishing each operation on the *blockchain*, recording only the initial and final states.

- **Sidechains**: independent *blockchains* with bidirectional asset transfer mechanisms with the main chain, operating with their own consensus rules.

- **Rollups**: execute transactions off-chain but publish transaction data (or proofs) on Layer 1. They are subdivided into *Optimistic Rollups* (assume validity, verify under dispute) and *Zero-Knowledge Rollups* (publish cryptographic validity proofs).

In addition to scalability solutions, the emergence of specialized *blockchains* oriented toward specific use cases – such as supply chains and digital identity – is observed, as well as permissioned *blockchains*, characterized by access restrictions and a higher degree of institutional control, commonly adopted by corporations and governments (SYED *et al.*, 2019).

Currently, *blockchain* technology is in a maturation stage, with current challenges centered on interoperability between different networks, user experience, and integration with legacy systems. In parallel, regulatory advances in various jurisdictions, including Brazil, seek to provide legal certainty to the ecosystem, especially regarding the classification of digital assets and the prevention of illicit activities.

2.2 Tokenization and Technology Applications

From the Ethereum platform and the standardization of smart contracts, it became possible to create and manage *tokens* – that is, digital representations of assets or rights – in a programmable and decentralized manner. These *tokens* can be classified into main categories that present distinct legal and functional implications (KONDOVA; SIMONELLA, 2019):

– **Payment tokens or Cryptocurrencies (*payment tokens*)**: function as a medium of exchange, unit of account, or store of value, such as Bitcoin and Ether (ETH). They generally do not confer rights over future cash flows or participation in specific ventures.

– **Utility tokens (*utility tokens*)**: provide access to products or services offered by a digital ecosystem. They are common on decentralized storage platforms, computing networks, or *blockchain* games. ETH, in addition to being considered a payment token, is also a utility token, since transaction and smart contract execution fees on the Ethereum network are paid in ETH. Utility tokens do not confer economic rights or equity participation, but rather access to specific functionalities, which distinguishes them from *security tokens*.

– **Security tokens (*security tokens*)**: represent economic rights over underlying assets, such as equity, dividends, interest, or revenue flows. Because they involve an expectation of profit derived from the efforts of third parties, they fall within the definition of a security in most jurisdictions, including Brazil, making them subject to CVM regulation.

The technical implementation of these *tokens* in the Ethereum ecosystem was consolidated through standards known as ERCs (*Ethereum Request for Comments*).

An ERC is a formal technical document used to propose the creation of new features or changes to Ethereum technology (Binance Academy, 2025). In ERCs dealing with token standards, the document specifies a class interface (object-oriented programming) – that is, a mandatory minimum set of functions and events that a smart contract must implement – so that wallets, *exchanges*, and other contracts can interact with any compatible *token* without needing to know the internal details of its implementation.

Among the most relevant ERCs (Ethereum Foundation, 2026a) for the scope of this research, the following stand out:

– **ERC-20**: standard for fungible *tokens*, where each unit is identical and interchangeable. It is the most widely used protocol for creating cryptocurrencies and *utility tokens*, defining basic functions such as transfer, balance query, and spending approval.

– **ERC-3643**: standard aimed at regulated *security tokens*. It incorporates an *on-chain* identity registry (ONCHAINID), configurable compliance modules, and transfer restrictions based on verified identity, meeting KYC/AML requirements directly at the protocol level.

In the context of startups, tokenization opens new possibilities for mobilizing financial, technical, and human resources (COMITO, 2023):

– ***Crowdfunding***: raising financial resources from the general public. In Brazil, this can be done through CVM-authorized platforms, where investors acquire securities (e.g., debt or equity *tokens*). It requires registration or regulatory exemption and is more suitable for startups at a more mature stage, with traction and a validated business model.

– ***Crowdsourcing***: gathering work or knowledge, not necessarily involving capital contributions or an investment relationship. It is the obtaining of ideas, code, design, technical solutions, product validation, etc.

In the governance field, practices originating from Decentralized Autonomous Organizations (DAOs) can be adapted for traditional startups at two complementary levels. At the technical level, according to Saesen *et al.* (2025), *governance tokens* allow *stakeholders* to vote on strategic decisions, such as profit allocation, election of administrators, and amendments to the corporate charter, with an immutable record on the *blockchain*. At the process level, DAOs have consolidated a set of governance practices – such as formalized proposals, deliberation periods, minimum quorums, leader selection, and auditable records of each decision – that may eventually be absorbed by startups independently of tokenization.

Despite the transformative potential of tokenization, its practical limitations must be acknowledged. Understanding smart contracts by non-technical *stakeholders* can represent a significant challenge, since the code of *smart contracts*, usually written in languages like Solidity, is not intuitive to laypeople (FERTIG; SCHüTZ, 2024). Additionally, implementing and managing *blockchain*-based systems requires preparedness and prudence from all *stakeholders* in both the technological and legal spheres.

2.3 Legal Certainty and Regulatory Landscape

In the regulatory sphere, Brazil has a developing regulatory framework composed of multiple instruments that, taken together, outline the legal treatment of crypto-assets and digital securities offerings, whether tokenized or not. The main regulatory milestones are:

– **Law No. 14,478/2022 (Cryptocurrency Legal Framework)**: establishes general guidelines for the virtual assets market in Brazil, defining responsibilities for virtual asset service providers and granting the Central Bank the authority to regulate and supervise the sector.

– **Decree No. 11,563/2023**: defines the regulatory jurisdiction over crypto-assets in Brazil, assigning to the Central Bank (BCB) supervision of virtual assets used as means of payment, and to the Securities and Exchange Commission (CVM) supervision of those that constitute securities.

– **CVM Resolution No. 88/2022**: regulates electronic collective investment platforms (*crowdfunding*), establishing rules for small business companies to make public offerings of securities with registration exemption, provided that fundraising limits and transparency requirements are met.

– **CVM Guidance Opinion No. 40/2022**: provides guidelines for classifying crypto-assets as securities, guiding case-by-case analysis based on criteria that include the existence of investment, profit expectation, and dependence on the efforts of third parties – criteria that bear resemblance to the U.S. *Howey Test*.

– **CVM Resolution No. 160/2022**: governs public offerings for the distribution of securities, establishing registration and disclosure requirements that apply when crypto-assets are classified as securities.

– **BCB Resolutions No. 519, 520, and 521/2025**: constitute a regulatory milestone, regulating the provision of virtual asset services in Brazil. They detail the authorization, governance, internal controls, and anti-money laundering requirements for virtual asset service providers, completing the framework initiated by the 2022 Legal Framework.

Despite regulatory progress, entrepreneurs still face several factors that create uncertainty in adopting the technology.

First, there is the risk of litigation among partners or collaborators if the solution is not well understood, transparent, and auditable. In the event of disagreements about the distribution of *tokens* or about the rights they represent, the absence of consolidated jurisprudence may make it difficult to predict judicial outcomes.

Second, as noted by (BARRETO, 2022), there is the risk of a cease-and-desist order by the CVM if the distribution is interpreted as an irregular offering of securities. There may also be challenges from the BCB, depending on the nature of the issued asset, in accordance with the division of powers established by Decree No. 11,563/2023.

Finally, equally relevant technical-operational questions arise. What happens if a *stakeholder* is hacked or loses their private key, rendering the *tokens* inaccessible? How should one proceed if a court order requires the redistribution of assets immutably recorded on a public *blockchain*? How should *tokens* be registered in the company's articles of association?

These questions must be addressed before any practical implementation, in order to prevent the adoption of the technology from becoming an operational or legal risk for the nascent company.

Another point to consider is that the scenario changes according to the legal status of the *stakeholders*. It is advisable that they be named as such in the company's articles of association, although in situations involving *crowdsourcing* or occasional investors this may not always be possible. If the startup wishes to proceed along this path, it will need to seek other ways to protect its interests in cases of conflicts, such as the formalization of terms of adherence, non-disclosure agreements, and arbitration clauses.

When *stakeholders* have a CNPJ (i.e., they are legal entities providing services to the *startup*), the relationship tends to be characterized as a contract between companies. This configuration reduces the risk of characterization as an employment relationship or public offering and offers greater contractual flexibility to define the rights represented by the *tokens*. In cooperative models, where the *startup* is organized as a workers' or platform cooperative, the *tokens* may represent the member's participation in the cooperative's results, with backing in cooperative legislation (Law No. 5,764/1971), provided that the corporate structure is consistent with this legal form.

On the other hand, when the recipients are conventional salaried employees, the distribution of *tokens* tied to compensation may be interpreted as part of their salary or as Profit Sharing (*Participação nos Lucros e Resultados – PLR*), which entails labor and social security charges. This modality is therefore the most legally and operationally delicate in the context analyzed.

Additional attention is required regarding the terminology used to describe the rights represented by tokens. Brazilian legal order is particularly sensitive to such nuances (TUCCI, 2021), and the burden of eventually explaining to a court that there was an error can be particularly costly in terms of time and money. Terms such as "dividends", "profit sharing", "profit distribution", "performance bonuses" carry specific legal weight: the first typically refers to the distribution of results in corporations; the second seems more aligned with the PLR and CLT concept, which may support an eventual characterization of an employment or corporate relationship; while the others may be more appropriate depending on the case.

An international reference for assessing whether a given *token* is subject to CVM regulation is the *Howey Test*, a criterion formulated by the U.S. Supreme Court in 1946 and a reference for regulatory bodies worldwide (BSBC Advogados, 2021). The test defines a security as any transaction involving (i) an investment of money, (ii) in a common enterprise, (iii) with an expectation of profit, (iv) derived predominantly from the efforts of third parties.

In Brazil, CVM Guidance Opinion No. 40/2022 makes explicit reference to this test, adopting analogous reasoning but applied autonomously and adapted to the national legal order: the CVM analyzes the economic substance of the transaction, verifying whether there is fundraising from the public with profit expectation based on the efforts of others (BLASCO; BLASCO, 2022). Structuring the *token* in a closed circuit – so that holders are active participants of the company and not mere passive investors waiting for returns – and demonstrating that the token's primary purpose is to organize the startup rather than to promise financial gains, is therefore one of the possible *compliance* strategies to demonstrate good faith and reduce premature regulatory exposure.

To ensure that *tokens* are not subsequently classified as an irregular offering of securities, several *compliance* precautions may be observed together: (i) directing the distribution exclusively to persons who participate directly in the day-to-day operations of the company, such as partners, active collaborators, advisory investors, and service providers with proven operational involvement; (ii) formalizing and recording the relationship through explicit documents (KYC, NDAs, acceptance terms, etc.) that describe the nature of the *tokens*, the rights associated with them, the risks involved, and the absence of any promise of financial return based on third-party efforts; (iii) refraining from any form of public advertising or disclosure of the *tokens*, whether on social networks, institutional websites, or events; (iv) explicitly stating the structural nature of the token, making no promises of appreciation, yield, or financial return; (v) expressly restricting the circulation of *tokens* to a small and identifiable group of persons with a real and active connection to the company, prohibiting their commercialization on secondary markets or trading platforms; and (vi) maintaining detailed and auditable records of all related transactions and interactions.

Even so, depending on the case, registration of the asset with the CVM may be necessary (BARRETO, 2022; BLASCO; BLASCO, 2022). These procedures aim to protect the startup's interests by producing unequivocal evidence of good faith in the event of judicial or administrative challenges from *stakeholders* or third parties.

The ongoing research seeks to integrate this knowledge to propose a practical solution that is technically sound and adherent to current legislation, specifically tailored to the needs of early-stage Brazilian startups.

3 MATERIALS AND METHODS

The methodological path of the research was structured in sequential and complementary stages, some already completed and others planned for the next semester.

3.1 Completed Stages

In-depth bibliographic review

It is worth noting that this research is exploratory and interdisciplinary in nature, situated at the intersection of technology, regulation, and startup management in the Brazilian context. Since this is an emerging field, technical knowledge of *blockchain* was progressively built throughout the research process itself. In this sense, the systematic reading of the book *"Blockchain: The Comprehensive Guide to Blockchain Development, Ethereum, Solidity, and Smart Contracts"* (FERTIG; SCHüTZ, 2024) was fundamental to establishing a technical knowledge base, enabling a structured understanding of the fundamental concepts of the technology, which in turn enabled the subsequent development and analysis stages.

Scientific and/or technical articles and regulatory documents on *blockchain*, smart contracts, asset tokenization, and applicable legislation were selected and analyzed. The main references are listed in the final section and served as the basis for contextualization and the definition of analysis criteria.

Legal certainty analysis and regulatory classification

An analysis of the applicable Brazilian regulatory framework for crypto-assets was conducted, encompassing: Law No. 14,478/2022 (Cryptocurrency Legal Framework), which establishes general guidelines for the virtual assets market; CVM Guidance Opinion No. 40/2022, which applies reasoning analogous to the *Howey Test* autonomously and adapted to the national legal order; CVM Resolutions No. 88/2022 and No. 160/2022; and Decree No. 11,563/2023, which delineates the responsibilities between the CVM and the Central Bank in the regulation of crypto-assets.

Several relevant risk vectors were identified: (i) cease-and-desist proceedings by regulatory bodies for irregular offering of securities; (ii) litigation between parties arising from the absence of consolidated jurisprudence; (iii) risk of employment classification when the recipients are salaried employees; and (iv) technical-operational issues such as loss or compromise of private keys or compliance with court orders concerning immutable records on a *blockchain*. It was also found that the terminology adopted — "dividends", "profit sharing", or "profit distribution" — carries specific legal weight and may influence the regulatory classification to which the company would be subject.

It was concluded that one possible strategy to reduce premature regulatory exposure consists of structuring the token distribution in a closed circuit, directing the tokens exclusively to *active stakeholders* of the company — partners, collaborators with proven operational involvement, advisory investors, and service providers with CNPJ — and not to mere passive investors awaiting returns. This structure, supplemented by compliance procedures such as KYC, signing of explicit documents, prohibition of advertising the crypto-asset and of trading on secondary markets, and maintenance of auditable records, seeks to **protect the startup's interests by producing unequivocal evidence of its good faith in any eventual judicial or administrative challenge**.

Regarding the absence of consolidated jurisprudence, one possible path to mitigate risks is to include arbitration clauses to resolve eventual disputes.

Comparative analysis between platforms

After an initial evaluation of Ethereum, Binance Smart Chain, and Polygon, it was decided to focus the implementation on Polygon (a *sidechain* solution) because this solution maintains full compatibility with Ethereum (EVM), offers significantly lower transaction costs, and data integrity through hash proofs stored on the main Ethereum network.

Development of the smart contract and issuance of the experimental token

The *ProfitToken* contract was implemented in Solidity 0.8.28, adopting the ERC-20 standard due to its widespread adoption, structural simplicity, and compatibility with established ecosystem tools.

Although the ERC-3643 standard is more aligned with *security tokens* – as it incorporates an *on-chain* identity registry, configurable compliance modules, and transfer restrictions based on verified identity – it was decided not to use it at this stage of the research due to its substantially greater implementation complexity. As an alternative, the contract was structured with functionally similar mechanisms, including a *whitelist* system and transfer restrictions, preserving the possibility of future migration to that standard.

The implementation was based on OpenZeppelin libraries, with the goal of using widely audited components and reducing the risk of vulnerabilities associated with fully custom code development.

The contract includes the following functionalities: (i) transfer control through a *whitelist*; (ii) *mint* and *burn* functions restricted to the owner; (iii) emergency pause mechanism; (iv) event emission for audit purposes; and (v) a set of automated tests.

Validation of the smart contract and experimental token

The system was tested in a development environment and subsequently deployed on Polygon's Amoy *testnet*. Tests were conducted for wallet creation, whitelist inclusion, token minting, and token transfer, with verification of the correct functioning of the implemented restrictions.

Construction of the *Argos* prototype

In parallel with the development of the smart contract, the construction of a prototype named *Argos* was initiated, intended for the administrative management of the *token* and for monitoring its transactions.

The prototype is experimental in nature and adopts an open-source model, allowing its use and adaptation for academic or business purposes.

The system architecture includes: (i) an administrative interface based on AdminJS; (ii) a REST backend developed in Node.js/TypeScript; (iii) a PostgreSQL database with Prisma-based modeling; (iv) user identification procedures (KYC); and (v) log recording for audit purposes.

3.2 Future Stages

Implementation of the proportional profit distribution system

Develop and integrate a module responsible for the automated distribution of financial results proportionally to token holders, with structured recording of operations in a database for traceability and audit purposes.

Deepening of legal and technological security analysis

Expand the analysis of regulatory, corporate, and operational risk scenarios, as well as evaluate potential technical vulnerabilities and respective mitigation strategies.

Technical documentation and code release

Prepare detailed technical documentation of the developed system and release the source code in a public repository under a license compatible with free software, ensuring transparency and reproducibility.

Application scenario analysis

Examine possible contexts for using the system in early-stage startups, identifying limitations, adaptation requirements, and improvement opportunities.

3.3 Use of Artificial Intelligence Tools

In accordance with scientific transparency principles, it is declared that artificial intelligence tools – a ubiquitous reality in today's world – were used as support throughout this research in order to enhance the quality of scientific production. Specifically, the following were employed:

- **Claude Sonnet 4.5 and DeepSeek V4 Lite**: for assistance in writing texts, bibliographic review, analysis of regulatory documents, and synthesis of complex information. These tools contributed to the conceptual organization and expository clarity of the report.

- **ChatGPT 5.2 Codex**: for support in generating source code snippets, developing smart contracts in Solidity, and creating artifacts for the functional prototype. The tool accelerated prototyping and enabled iterative testing of functionalities.

All texts and code generated by AI were reviewed, validated, and adapted by the researcher, ensuring adherence to the research objectives, methodological rigor, and compliance with academic standards. The use of these technologies aims to optimize the research process without replacing the critical thinking and authorial responsibility of the researcher.

4 RESULTS

The results achieved to date are predominantly theoretical and exploratory in nature, consistent with the early stage of the investigation. Although a functional prototype has been partially developed, there has been no empirical validation in a real environment, so its technical and operational limitations are acknowledged and discussed in this section.

4.1 Platform Selection: Polygon

After a comparative analysis of Ethereum, Binance Smart Chain, and Polygon (Table 1), and exploratory testing, Polygon was chosen as the implementation platform.

Table 1 – Preliminary comparison between blockchain platforms

Feature	**Ethereum**	**Binance Smart Chain**	**Polygon**
Average cost per transaction	High (variable)	Low	Low
Block speed	15s	3s	2s
Virtual machine	EVM	EVM	EVM
Supported token standards	ERC-20, ERC-3643, etc.	BEP-20 (ERC-20 compatible)	ERC-20, ERC-3643
Documentation	Very complete	Complete	Complete
Community	Large	Large	Large

Fonte: Own elaboration, based on (Ethereum Foundation, 2026b; BNB Chain Community, 2026; Polygon Technology, 2026).

The analysis considered the following aspects of each platform:

Ethereum

Ethereum is the reference network for smart contracts and *security tokens*, offering the most complete documentation, the largest developer community, and the most mature tool ecosystem. Its main obstacle in the context of this research is the high transaction cost (*gas fees*), which can reach tens of dollars during periods of congestion, making frequent use unfeasible for early-stage startups with low-volume financial operations.

Binance Smart Chain

Binance Smart Chain (BSC) offers transaction costs comparable to those of Polygon and adequate block speed, with partial compatibility with the ERC-20 standard via BEP-20. However, it has relevant disadvantages: it is controlled by Binance, a centralized company under regulatory scrutiny in various jurisdictions, which may introduce institutional dependency risks and compliance issues. Additionally, it does not natively support the ERC-3643 (T-REX) standard, which is relevant for *security tokens* with regulated identity and transfer restrictions, and its developer community specialized in smart contracts is smaller than Ethereum's.

Polygon

Polygon is an EVM-compatible sidechain that operates in parallel with Ethereum and uses its own set of validators to achieve consensus (Polygon Technology, 2026). Although it is not a Layer 2 solution in the strict technical sense (like *rollups*), its architecture provides full compatibility with the Ethereum ecosystem, allowing smart contracts developed for the EVM to be deployed without modifications. This feature, combined with reduced transaction costs (fractions of a cent in MATIC), faster block speed than Ethereum (approximately 2 seconds), and support for the ERC-3643 standard for *security tokens* with regulated identity and transfer restrictions (SCHWIETERT; DINIS; Tokeny Solutions, 2021), makes the platform particularly suitable for experimentation with tokenization.

The choice of Polygon was therefore motivated by the combination of accessible cost, full compatibility with Ethereum, and support for the technical standards required for *security tokens* – characteristics that proved most suitable for the current stage of research. It should be noted, however, that this does not represent an exhaustive evaluation of the available *blockchain* platform ecosystem. Other solutions, such as Arbitrum, Optimism, or Base, were not evaluated in detail and may present comparative advantages in different scenarios.

4.2 Development of the *ProfitToken* Smart Contract

The *ProfitToken* smart contract was developed in Solidity 0.8.28, using the audited implementations of the OpenZeppelin library as a foundation. The ERC-20 standard was adopted for its simplicity and broad compatibility with existing tools; although the ERC-3643 standard is more appropriate for *security tokens* by natively incorporating *on-chain* identity registration and compliance modules, its greater complexity was considered premature for the current stage of research. To compensate for this choice, the contract was structured with functionally similar mechanisms, preserving the possibility of future migration.

The main functionalities implemented were:

- ***Whitelist* system**: controls which addresses can send and receive tokens, restricting circulation to the group of authorized *stakeholders* and implementing, in an automated manner, one of the main regulatory safeguards of the model.

- ***Mint* and *burn***: token issuance and destruction functions, restricted to the contract administrator, which allow adjusting the distribution according to the value added by each participant over time.

- **Emergency pause**: mechanism that allows temporarily freezing all transfers in the event of a security incident or operational need.

- **Event logging**: emission of complete events (*AddedToWhitelist*, *TokensMinted*, *TokensBurned*, etc.) that facilitate auditing and synchronization with *off-chain* systems.

The complete source code is available in the project's GitHub repository and is partially presented in Annex A.

4.3 Development of the *Argos* System

The construction of the prototype revealed a finding that, although it seems obvious in retrospect, was not explicitly stated in the initial formulation of the research: *tokens that cannot be traded on secondary markets need to be embedded in a context where they make sense and generate value for their holders*. In the specific case of tokens representing profit rights in startups – the subject of this research – we consider a user-friendly and informative interface to be fundamental, allowing all stakeholders to view balances, track distributions, and understand the associated rights; the token alone does not add perceptible value to the *stakeholders* of an early-stage startup.

This finding motivated the development of the *Argos* system – a free software (GNU GPL v3) prototype or Proof of Concept (PoC) of governance that encapsulates the *ProfitToken* and provides a usability and *compliance* layer on top of the smart contract. The current architecture comprises:

Smart contracts (Solidity + Hardhat): the *ProfitToken* contract developed in Solidity 0.8.28, compiled and tested with the Hardhat framework; deployment scripts for the Polygon Amoy *testnet* and for production networks; an automated test suite covering the main contract functions; and compiled artifacts (ABI and *bytecode*) reused by the *backend* for interaction with the deployed contract.

Backend (Node.js/TypeScript): a REST API for user management, transactions, and interaction with the *blockchain*; Polygon integration via the Viem library; an authentication and authorization system with ADMIN and STAKEHOLDER profiles; and a *blockchain* event listener for automatic synchronization with the database.

Database (PostgreSQL + Prisma ORM): a data model covering user, transaction, document, and audit log entities; an integrated KYC system with support for identity documents; and an event checkpoint for incremental synchronization with the *blockchain*. PostgreSQL was chosen for its robustness and advanced audit features, while Prisma was chosen because it is a database-agnostic ORM, preserving the possibility of future migration to other relational or even NoSQL systems if needed.

Administrative interface (AdminJS, partially developed): a panel for managing *stakeholders*, token issuance, *whitelist* control, transaction history visualization, KYC approval, and document upload.

In functional terms, the system allows a *startup* to register *stakeholders* with identity verification, issue tokens proportionally to the value added by each member, rigorously control circulation through the *whitelist*, and maintain a complete and auditable record of all operations – with the guarantee that data recorded on the *blockchain* is immutable and verifiable by any interested party. The prototype was validated in a development environment with a real *deploy* on the *Polygon Amoy testnet*.

It is important to note that *Argos* is in its early stage of development.

4.4 Compliance Strategies Adopted in the Prototype

The design choices of *Argos* were informed by the regulatory analysis described earlier. The *compliance* model adopted rests on the following pillars:

- **Closed-circuit distribution**: tokens are issued exclusively to active, registered, and verified *stakeholders*, with no public disclosure or fundraising effort directed at the general public.

- **Prohibition of secondary market trading**: the *whitelist* system in the smart contract prevents transfers to unauthorized addresses, technically preventing commercialization on *exchanges* or decentralized platforms.

- **KYC and formal documentation**: all *stakeholders* undergo identity verification and sign documents describing the rights associated with the tokens and the absence of any promise of financial return based on the efforts of third parties.

- **Traceability**: the combined record in a relational database and on the *blockchain* guarantees complete auditability of all operations.

This strategy seeks to rule out the eventual characterization of the model as an irregular offering of securities, without ignoring that legal uncertainty is inherent in a regulatory field still under construction. The analysis of the four criteria of the *Howey Test*, applied in an orientative manner to the proposed model, suggests that the fourth criterion – dependence of profits essentially on the efforts of third parties – tends to be answered negatively when token holders are active participants in the company. However, this analysis does not substitute the individualized legal assessment of each concrete case, which may reach different conclusions depending on the specific circumstances of the *startup* and the evolution of regulatory understanding.

The results presented in the previous sections describe what was built: a functional smart contract, a prototype under development, and a set of technically grounded compliance practices. The following section builds on these deliverables for a second-order analysis – no longer what was done, but what it means, what questions remain unanswered, and what limitations the construction process itself revealed.

5 DISCUSSION

The results obtained to date allow for some preliminary reflections on the feasibility of the proposal, without, however, anticipating conclusions that depend on stages not yet completed. This discussion aims to be candid about what has actually been demonstrated and what remains as a working hypothesis to be verified.

5.1 What Was and Was Not Demonstrated

The main concrete result of this semester is the publication and validation of the *ProfitToken* smart contract and part of the *Argos* system – which operates in a development environment and was validated on the *Polygon Amoy testnet*. This result demonstrates technical feasibility under controlled conditions, but does not answer harder questions: will the system operate reliably in production? Will *stakeholders* without technical knowledge be able to use it? Will real startup founders be willing to adopt a *blockchain*-based solution given the additional layer of complexity, the set of risks, and the uncertainties identified?

Legal feasibility, in turn, is even more difficult to assert. The proposed *compliance* model is well-founded but has not been submitted to evaluation by specialists in corporate or regulatory law, and there is no guarantee that the CVM or BCB would share the same understanding in a concrete case. The absence of consolidated jurisprudence on the subject is simultaneously an opportunity for research originality and a real risk for potential adopters of the solution.

5.2 On the Technical Choice: Polygon and ERC-20

The choice of Polygon proved suitable for the objectives of this stage of research. The minimal transaction costs enabled iterative testing without significant financial impact, and the **EVM compatibility** ensured that the technical knowledge acquired in Solidity and Ethereum ecosystem tools is applicable to other platforms if needed.

The adoption of the ERC-20 standard instead of ERC-3643 was a pragmatic choice that merits reflection. ERC-3643 would have been more semantically appropriate for the proposed use case; however, the substantial implementation complexity – which requires deploying auxiliary identity and compliance contracts in addition to the token itself – would likely have prevented the delivery of a functional prototype this semester, given the conditions under which the research was conducted and the researcher's initial level of technical maturity. The adopted solution – implementing a *whitelist* system on top of ERC-20 – is functionally equivalent for the use case in question, although it does not offer the semantic expressiveness and native regulatory interoperability of ERC-3643. This migration may be addressed in future work.

5.3 The Central Finding: The Token Must Be Embedded in a Context That Gives It Value

One of the most relevant results of this semester is not technical but conceptual: the realization that *tokens that cannot be traded on secondary markets – a necessary condition to avoid problematic regulatory classification – only make sense when embedded in a context that makes them valuable to their holders*. In the specified case, we considered embedding the token in the context of a user-friendly and informative interface allowing all *stakeholders* to view balances, track distributions, and understand the associated rights.

5.4 On the Regulatory Strategy

The outlined *compliance* strategy – closed-circuit distribution, KYC, prohibition of secondary markets, absence of advertising, and careful use of terminology – is plausible and well-founded, but should be read with caution.

First, it relies on an interpretation of the *Howey Test* and CVM Opinion No. 40/2022 that may not be shared by regulators in a concrete case. The boundary between an "active" collaborator and a "passive" investor is not geometrically sharp, and the CVM has discretion to analyze the economic substance of the transaction more broadly.

Second, the strategy does not address all identified risk vectors. Issues such as private key loss by a *stakeholder*, enforcement of court orders over immutable records on a *blockchain*, or the tax implications of distributing tokenized results remain open and will need to be addressed in the next stages – ideally with the support of legal and accounting professionals.

5.5 Potential Strategic Advantages of Tokenization in Early-Stage Companies

Notwithstanding the risks and limitations mapped throughout this research, early adoption of the technology may bring strategic advantages, especially when considering the development horizon of an early-stage *startup*.

Organizing the company by value effectively added. A more operational advantage, this concerns the potential of the technology as an instrument for equitable internal organization. Consider the scenario of three engineers who decide to found a *startup* without significant capital. *Tokens* can be distributed progressively only as each stakeholder works or contributes capital. Thus, the group has an objective and auditable mechanism to quantify and record individual contributions over time. This model is particularly relevant in scenarios common among nascent startups: a founder who contributes predominantly with intellectual capital, another with full-time dedication, and a third who makes occasional financial contributions can have their stakes adjusted in a dynamic, transparent, and contractually grounded manner, without relying on informal renegotiations or traditional equity instruments that require costly corporate amendments. The technology does not solve the human problem of negotiating value among founders, but it provides a recording infrastructure that makes this process more transparent and less susceptible to future disputes.

Tokenized mindset from the start. Building a *token* system in a closed circuit – even if in an experimental and legally cautious manner – requires the *startup* to develop, from the outset, efficient governance and *compliance* procedures: automated *smart contracts*, KYC, transparency, auditable records, etc. This set of routines is not discardable when the company levels up; on the contrary, it may facilitate the transition to more advanced stages of development and regulation.

These advantages do not invalidate the identified risks, nor do they dispense with the necessary legal analysis in each concrete case.

5.6 Identified Limitations and Next Steps

The main limitations of the work carried out so far are:

- The administrative interface of the Argos system is still under development.
- The automated profit distribution functionality – which is the central objective of the research – has not yet been implemented. The current prototype manages tokens but does not perform proportional distribution of financial results.
- The system has not been tested with real users, and usability aspects, especially for *stakeholders* unfamiliar with *blockchain*, have not been evaluated.
- The legal analysis has not been validated by external experts and is exploratory in nature.
- The tax aspects of profit tokenization have not been addressed, and may represent an additional layer of complexity.
- The technical and legal documentation necessary for the solution to be adopted by third parties still needs to be developed.

In the next semester, the priorities will be: (i) implementing the automated profit distribution mechanism, which may involve the use of *stablecoins* or integration with bank transfer systems; (ii) completing the implementation of the administrative interface; (iii) deepening the legal and technological security analysis, preferably with expert support; (iv) conducting tests with users representative of the target audience; and (v) documenting and publishing the code under GPL v3 license, allowing the solution to be evaluated, criticized, and eventually adopted by other startups.

The research is at an early stage, with promising but still preliminary results. The prototype demonstrates that the proposal is technically feasible; the next challenge is to demonstrate that it is legally sound, operationally usable, and genuinely useful for the Brazilian early-stage startup ecosystem.

REFERENCES

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/opiniao-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.; ALZAHRANI, 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 ANNEXES

6.1 Annex A – ProfitToken Contract Code (main excerpts)

```
// 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 ERC-20 token with whitelist, mint, burn, and pause
 */
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 Annex B – Evidence of Contract Deployment on Polygon Amoy

This annex presents the public proof of the *ProfitToken* contract deployment on the *Polygon Amoy* network via the PolygonScan explorer.

Network: Polygon Amoy (*testnet*)

Contract address: <https://amoy.polygonscan.com/address/0x1b5048642BeDe3e361D8653F5219e9dfe8fd1A48>

Token identified in the explorer: ERC-20: Profit Share Token (DIV)

Creation transaction (deploy): <https://amoy.polygonscan.com/tx/0xd1399b9acfe8b53c242be926a3544c4d0dd936b976dc74a0f8c542df987f46b5>

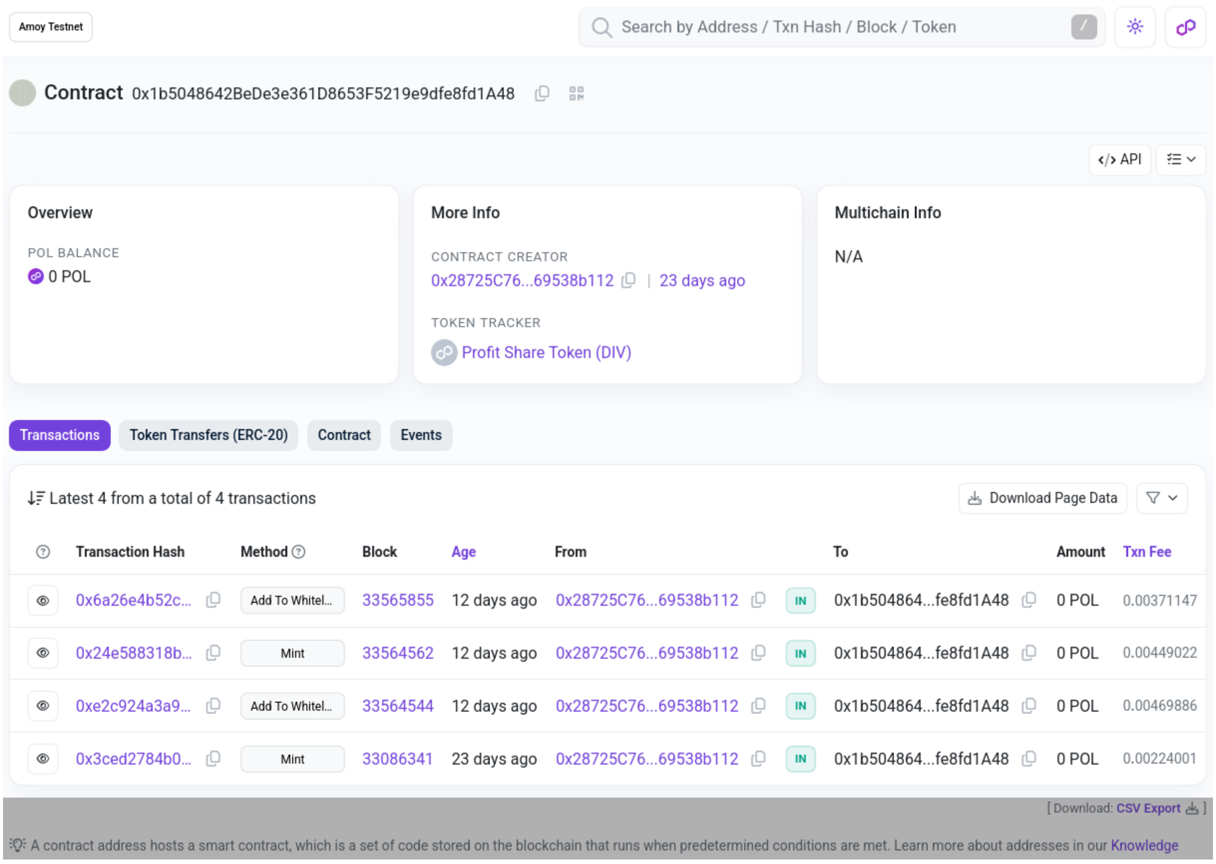

Figure 2 – Confirmation of the *ProfitToken* contract published on the Polygon Amoy network

Fonte: Own elaboration, screenshot from PolygonScan (Amoy Testnet).

Note: As this is a *testnet* environment, the data presented serves as evidence of the technical-operational validation of the deployment and initial testing of the smart contract.

6.3 Annex C – Database Schema of the *Argos* Prototype

Logical diagram (entities and relationships)

```
+------------------+            1:N           +------------------+
|      users       |-------------------------->|   transactions   |
| PK userId        |                           | PK transactionId |
| email (unique)   |                           | FK userId (null) |
| walletAddress(*) |                           | type, amount     |
| role, kycStatus  |                           | txHash, status   |
+------------------+                           +------------------+
         |
         | 1:N
         v
+------------------+
|    documents     |
| PK documentId    |
| FK userId        |
| type, title      |
| fileHash, ipfs   |
+------------------+
         |
         | 1:N
         v
+------------------+
|    audit_logs    |
| PK auditLogId    |
| FK userId (null) |
| action, resource |
| status, metadata |
+------------------+

+--------------------------+
|   event_checkpoints      |
| PK eventCheckpointId     |
| cursorName (unique)      |
| lastBlock, lastLogIndex  |
+--------------------------+

(*) walletAddress is optional, but unique when provided.
```

Brief description of tables

- **users**: main identity and access table. Stores credentials, profile (ADMIN/STAKEHOLDER), KYC data, and account metadata.
- **transactions**: records financial and operational events related to the token (*mint*, *transfer*, *burn*, whitelist changes), including *txHash*, block number, and processing status.
- **documents**: stores documents linked to the user (e.g., KYC, contracts, terms), with file integrity hash and optional support for IPFS reference and *blockchain* anchoring.
- **audit_logs**: audit trail of system actions (who did what, on which resource, and with what result), with support for metadata, IP address, and user agent.
- **event_checkpoints**: technical control table for incremental synchronization of *blockchain* events, storing the last processed block and log index.

6.4 Annex D – Directory Structure of the *Argos* Prototype

This annex describes the folder organization of the *Argos* prototype, based on the root directory `argos/`.

Overview of the directory structure

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

Description of main directories

- **admin**/: administrative layer (panel) of the system. Contains AdminJS configuration, interface components, and database integration for management operations.
- **backend**/: main API of the prototype, implemented in Node.js/TypeScript. Centralizes business rules, authentication/authorization, *blockchain* integration, data persistence, and HTTP routes.
- **smartcontracts**/: smart contracts project (Hardhat/Solidity). Includes the *ProfitToken* source code, deployment scripts, automated tests, and compiled artifacts.
- **.data**/: directory for auxiliary development and demonstration data (e.g., test wallets), used in the local prototype flow.

Note: The structure was organized in a modular format to separate the administrative interface, application logic, and *on-chain* layer, facilitating maintenance and incremental evolution.