Revista de Contabilidade e Organizações
www.rco.usp.br

DOI: http://dx.doi.org/10.11606/issn.1982-6486.rco.2025.230807

Journal of Accounting and Organizations
www.rco.usp.br

Red Flags in Play-to-Earn Crypto Games: Proposal and Testing of a Checklist Based on Ponzi Scheme

Sinais de Alerta em Cripto Jogos: Proposta e Teste de uma Lista de Verificação com Base em Esquemas Ponzi

Rodrigo Barbosa de Almeida[a], Rafael Sousa Lima[b], Paulo Vitor Souza de Souza[c]

[a] *Centro Universitário de Brasília – Brazil*
[b] *Universidade de Brasília – Brazil*
[a] *Universidade Federal do Paraná – Brazil*

Keywords
Blockchain.
Cryptocurrencies.
Crypto games.
Red flags.
Fraud.

Abstract

Play-to-earn crypto games represent a growing niche in the blockchain ecosystem, combining entertainment and financial investment but also raising concerns about potential fraud. This study aims to assess to what extent it is possible to detect red flags resembling those commonly associated with Ponzi schemes in play-to-earn crypto games, through the proposal and empirical testing of an original checklist. A literature review was conducted to identify red flags present in traditional schemes and cryptocurrencies. These red flags were validated by digital forensic experts as a possible criminal checklist. The proposed checklist was empirically tested against a sample of six play-to-earn crypto games (both active and discontinued projects), selected based on user activity and availability of historical data. The findings suggest that game mechanics, token value, and withdrawal difficulty are the most important aspects in assessing the risks of Ponzi schemes in crypto games. On the other hand, webpages, tokenomics, and utility of the token and NFTs are less relevant for risk assessment. This study is innovative in its specific focus on identifying red flags in Ponzi schemes within the play-to-earn gaming market, a recent and underexplored area, thus filling a gap in previous research on cryptocurrencies. In this exploratory study, the literature review was limited by the lack of research regarding Ponzi schemes in crypto games. The identification of red flags associated with schemes in crypto games can provide insights for investors and users, aiding the prevention of participation in fraudulent schemes, thereby contributing to the reduction of these acts stemming from large-scale globalization.

Palavras-chave
Blockchain.
Criptomoedas.
Cripto jogos.
Red flags.
Fraude.

Resumo

Os jogos play-to-earn em blockchain representam um nicho em expansão, que une entretenimento e investimento financeiro, mas que também suscita preocupações quanto a fraudes. Este estudo visa avaliar em que medida é possível sinais de alerta que se assemelham às características comumente associadas aos esquemas Ponzi em jogos de criptomoedas no modelo play-to-earn, por meio da proposição e da testagem empírica de um checklist inédito. Foi realizada uma revisão de literatura para identificar sinais de alerta presentes em esquemas tradicionais e em criptomoedas. Esses sinais de alerta foram validados por especialistas em forense digital como uma possível lista de verificação criminal. O checklist proposto foi testado empiricamente em uma amostra de seis jogos play-to-earn (ativos e descontinuados), selecionados com base em sua atividade de usuários e na disponibilidade de dados históricos. Os resultados sugerem que a mecânica do jogo, o valor do token e a dificuldade de saque são os aspectos mais importantes na avaliação dos riscos de esquemas Ponzi em jogos de criptomoedas. Por outro lado, páginas da web, tokenomics e a utilidade dos tokens e NFTs são menos relevantes para a avaliação de risco. Este estudo é pioneiro em seu foco específico na identificação de sinais de alerta em esquemas Ponzi no mercado de jogos play-to-earn, uma área recente e pouco explorada, preenchendo assim uma lacuna nas pesquisas anteriores sobre criptomoedas. Neste estudo exploratório, a revisão de literatura foi limitada pela escassez de pesquisas sobre esquemas Ponzi em jogos de criptomoedas. A identificação de red flags associados a esquemas em jogos de criptomoedas pode oferecer insights para investidores e usuários, ajudando a evitar a participação em esquemas fraudulentos e contribuindo para a redução desses atos provenientes da globalização em larga escala.

Article information
Received: 30 de dezembro de 2024
Approved: 18 de setembro de 2025
Published: 29 de setembro 2025
Responsible editor: Prof. Flávia Zóboli Dalmácio

Practical implications

The findings of this study contribute directly to strengthening regulatory practices and developing risk assessment tools in cryptocurrency for businesses, markets, and governments. The proposed checklist can aid regulators, investors, and developers in identifying fraudulent schemes in play-to-earn games, contributing to risk awareness and fostering more informed decision-making in this emerging market.

Corresponding author: Tel. +55 (41) 3360-4362
E-mail: paulovsouza@ufpr.br; rafaellima1515@gmail.com; rodrigobarbosaderalmeida@gmail.com
Av. Prefeito Lothário Meissner, 632 – Jardim Botânico, Curitiba - PR, 80210-170, Brazil.

1 INTRODUCTION

The rise of blockchain technology in the digital era has drawn the attention of malicious actors exploring new opportunities to gain advantages through old fraudulent schemes, but under a new guise. Due to the increasing global adoption of cryptocurrencies, Ponzi fraudsters can be increasingly seen using this technology to lure victims (Dupuis et al., 2023; Heyman, 2023).

A Ponzi deceives investors with promises of extraordinary returns with little or no risk (Frankel, 2012; Nataraj-Hansen, 2024). In cryptocurrencies, such schemes gain complexity as tokens and NFTs simulate value while depending on continuous user inflows to remain viable (Heyman, 2023; Botha et al., 2023). It is a long-known criminal masterpiece, complicated in appearance yet still in use, which has shaped not only the financial world but also the legal and social aspects of society (Yuspin & Fadhlulloh, 2022).

The identification of a Ponzi scheme involves recognizing certain characteristics commonly observed in these crimes, which can be investigated through the so-called red flags. Generally, red flags represent alerts or signals observed in frauds and are considered important mechanisms that assist in detecting potential new frauds (Dal Magro & Cunha, 2017).

Although recognizing fraud signs is a key defense (Dias, 2016), the literature on “red flags” is concentrated in traditional financial and corporate contexts, where even established indicators can fail to predict major scandals (Carvalho and Silva, 2024). In auditing, studies focus on using red flags to assess risk (Munteanu et al., 2024) and identify recurrent, though variable, fraud indicators (du Toit, 2024). Other research highlights behavioral dimensions, showing that professional skepticism improves detection (Ramadhany et al., 2025) and that specific behavioral patterns can characterize financial fraud (Sandhu, 2022).

Taken together, these studies confirm the relevance of red flags as a methodological tool for detecting fraud but also reveal a gap: the application of this approach to emerging environments such as blockchain-based play-to-earn games has been little explored. Addressing this gap is essential, given the economic and social impact of these games and the risks associated with their rapid growth and limited regulation.

Previous work has shown that red flags can protect victims from fraudulent schemes (Frankel, 2012). Building on this for the crypto market, Heyman (2023) developed a red flag checklist for Ponzi schemes and validated it against the Mirror Trading International (MTI) case, where 88% of the flags were present. Our research adopts Heyman's checklist methodology but adapts and extends it to the play-to-earn gaming context. We incorporate determinants critical for this niche but not central to Heyman’s work, such as game mechanics, token/NFT utility, and smart contract auditing.

However, with the increasing popularity of cryptocurrencies and the expansion of financial markets, new forms of investment have emerged, now seen in the entertainment sector. The gaming industry seized the opportunity with the play-to-earn games, i.e., games that create their own currencies and tokens, rewarding players (Wang et al., 2021b; Vidal-Tomás, 2022).

Wang et al. (2021a) assert that due to the complexity of this new technology and the lack of supervision, the increasing popularity of blockchain applications has attracted a considerable amount of fraud. The number of occurrences of pyramid or Ponzi scheme-based crimes shows that criminals have begun to exploit this new market. The social scenario is aggravated when investors who enter the game later may have little chance of obtaining returns (Delfabbro et al., 2022).

This study addresses the urgent need to protect investors from fraudulent schemes in the emerging play-to-earn (P2E) gaming market. Theoretically, it contributes to fraud detection literature by extending the concept of 'red flags' from traditional finance and cryptocurrencies (Heyman, 2023; Bartoletti et al., 2021; Frankel, 2012) to the unique context of P2E games, where financialization intersects with game mechanics. Practically, the research provides an innovative checklist for regulators, investors, and developers to assess project risks. This tool helps prevent the significant financial losses and erosion of trust in blockchain applications often caused by fraudulent or unsustainable projects.

Thus, this research aims to answer the following question: What red flags based on traditional Ponzi schemes are commonly employed in play-to-earn crypto games? Therefore, this research aims to assess to what extent it was possible to detect red flags resembling those associated with Ponzi schemes in play-to-earn crypto games, through the proposal and testing of a novel checklist specifically designed for this context.

The detection of financial fraud has become necessary to ensure the smooth operation of the market and safeguard investors' interests (Li et al., 2024). Several studies have approached the topic in the realm of cryptocurrencies. Heyman (2023) researched red flags in cryptocurrencies and provided a checklist for their verification. Bartoletti et al. (2021) conducted extensive literature reviews on cryptocurrency fraud. Thus, there are already research efforts toward identifying Ponzi schemes in cryptocurrencies, capturing red flags.

This study provides a red flag checklist for the underexplored play-to-earn crypto games market. Our use of the term "Ponzi scheme" is purely analytical, focusing on identifying structural indicators without making legal accusations against projects or developers. The contribution is twofold: adapting a fraud detection framework to a novel context (theoretical) and providing a decision-making tool for stakeholders, including players, developers, and regulators (practical).

2 LITERATURE REVIEW

2.1 Ponzi schemes and fraud red flags

Security fraud involves deceiving investors with false statements for illicit gain (Benson, 2009). The archetypal example is the Ponzi scheme, originating from Charles Ponzi's early 20th-century enterprise. He promised exceptionally high returns, using capital from new investors to pay earlier ones, creating an illusion of success. Such schemes are inherently unsustainable as they depend entirely on attracting new money rather than generating legitimate profits. They are therefore destined to collapse once the inflow of new capital ceases (Benson, 2009; Frankel, 2012; Cres, 2014).

In a traditional Ponzi scheme model, the funds used to fulfill obligations to initial investors are derived from new investors, whose continuous engagement is essential for the scheme to persist (SEC, 2013). In other words, the mechanism involves using resources from new investors to compensate the previous ones, with the fraudsters sustaining the scam's survival by continuously attracting new victims (Zheng et al., 2023). Nevertheless, difficulty in recruiting new investors, large withdrawals, or numerous complaints cause the scheme to collapse (Fu et al., 2022).

Ponzi schemes constitute an investment scam that facilitates profit generation from a commodity but depends on enrolling additional sales agents (victims) to market the product and recruit further sales agents (additional victims), rather than relying on the product's intrinsic value (Nataraj-Hansen, 2024).

The rapid advancement of information technology, while beneficial, has also introduced significant challenges. It has complicated the authentication of electronic data in legal proceedings (Yang & Feng, 2021) and facilitated illegal trading through modern communication platforms (Nelson & Ramirez, 2022). This digital landscape empowers fraudsters, whose crimes are often underreported, making losses difficult to assess and fostering a cycle of impunity (Dal Magro & Cunha, 2017). Consequently, this impunity, combined with technological innovation, creates opportunities for more sophisticated fraudulent schemes, especially in emerging environments like blockchain-based cryptocurrencies (Heyman, 2023).

2.2 Cryptocurrencies, blockchain and NFTs

The blockchain became globally popular following the creation of the cryptocurrency Bitcoin (Nakamoto, 2008). The term "blockchain" arises from the system of encryption in interconnected blocks, which can be applied in various sectors, as it enables the distributed recording of transactions in a shared and secure manner (Drescher, 2017). Bitcoin is traded on a decentralized network that allows for the reliable transfer of digital money without a banking or governmental intermediary, which would typically incur fees and taxes (Kadoo & Sodi, 2023).

The second generation of blockchain, emerging in 2014, introduced "smart contracts". These are self-executing programs that automatically enforce the rules and conditions of a digital agreement, enabling a wide range of applications (Zou et al., 2021). Their value is often derived from properties such as scarcity and uniqueness (Drescher, 2017). One of the innovations based on the second generation of blockchain technology that has impacted intellectual property is called non-fungible tokens (NFTs). NFTs are stored in smart contracts, which are executed when predetermined conditions are met (Sakiz & Gencer, 2021).

NFTs are the foundation for many crypto games, which support a business model where users earn rewards while playing (play-to-earn) (Scholten et al., 2019). This type of crypto game incentivizes players to perform actions related to the game's performance or progress so that they can receive rewards in cryptocurrencies

or NFTs, which can be used within the game, exchanged for other cryptocurrencies, or sold on external markets, including for fiat currency (Vidal-Tomás, 2022).

2.3 Play-to-earn games and red flags

Play-to-earn games have become more appealing with the advent of GameFi (derived from Game Finance), a term that refers to the use of blockchain technology to create game-based economies, ensuring ownership and trading of in-game virtual assets, player compensation, and some forms of passive income investment (Kiong, 2022).

While high returns are a primary motivation in crypto games (Tavares et al., 2023), a sustainable in-game economy is crucial to balance supply/demand and prevent unfair wealth concentration (Jiang & Liu, 2021). Unsustainable economic models or promises of unrealistic returns are themselves "red flags", signals that help detect and prevent potential fraud (Yücel, 2013; Dias, 2016; Dal Magro & Cunha, 2017; Nascimento & Rech, 2022). Therefore, identifying these indicators is critical to avoid Ponzi schemes in blockchain projects (Botha et al., 2023; Heyman, 2023).

Red flags in blockchain projects span from presentation to technical security. Poor-quality websites, superficial white papers, and low team credibility with shallow social media engagement are key warnings (An & An, 2019; Kshetri, 2022). Due diligence should include assessing the team, community interaction, and token history (Bhujel & Rahulamathavan, 2022; Heyman, 2023). Financial alerts include unsustainably high returns and withdrawal difficulties (Botha et al., 2023; Heyman, 2023). Finally, a lack of third-party code audits is a major technical flaw, especially in the gaming community where it is a standard for reliability (Gunay & Kaskaloglu, 2022).

The literature highlights several red flags common to Ponzi schemes. These include: promising high returns with little risk; using high-pressure sales tactics (Cres, 2014; Lewis, 2015); lacking transparency with unverifiable or overly complex business strategies (Frankel, 2012; Lewis, 2015; SEC, 2023); operating without regulatory oversight or audits (Frankel, 2012; Lewis, 2015); and creating difficulties with payments or withdrawals (SEC, 2013). The use of celebrity endorsements is also a frequent warning sign (Cres, 2014).

In summary, while the literature offers extensive discussion on red flags in financial fraud and cryptocurrencies, little attention has been given to their manifestation in play-to-earn games. This gap justifies the development of a specific checklist adapted to this context, which represents the main contribution of this study.

3 RESEARCH DESIGN

3.1 Proposal of a checklist for crypto games

To address a gap in the literature, we developed a checklist for identifying Ponzi-like red flags in crypto games. The proposed 10-item checklist, detailed in Appendix 1, was constructed by adapting known red flags from traditional Ponzi and blockchain literature to the peculiarities of crypto games and NFTs. To mitigate subjectivity, this initial model was then refined based on a consultation with five Brazilian experts in forensic computer science, whose feedback guided the inclusion, exclusion, and final description of each item.

The checklist is an academic tool for identifying potential risk patterns, not for definitively classifying projects as fraudulent or making legal judgments. Its validation was exploratory, based on a restricted consultation with digital forensic specialists, as broader methods were infeasible due to the scarcity of qualified experts in this niche field. While this approach suits the study's exploratory objectives, it also highlights an opportunity for future research to expand the validation with a larger and more diverse sample.

To ensure replicability, each determinant was operationalized using observable criteria, with the full methodology detailed in Table 1. For example, "Token Value" was evaluated based on significant price drops (>80%), "Website" quality on its design and security, and "Social Media" on engagement patterns. This systematic coding drew upon descriptive evidence from white papers, official websites, smart contract audits, and user feedback, applying a consistent logic to all determinants to guide the analysis and facilitate replication.

Table 1
Criteria for Operationalization

Determinant (*Red Flag*)	Observable Criteria / Coding Rule
Token Value	Drop >80% from peak value; extreme volatility not correlated with market benchmarks.
Website	Low-quality design; absence of HTTPS; lack of basic information (team, tokenomics, gameplay).
Social Media	Low engagement; suspicious/promotional comments; inactivity or deleted channels.
White Paper	Absence of document; poor writing; unrealistic promises of returns.
Development Team	Profiles absent, unverifiable, or lacking blockchain/game development experience.
Token and NFT Utility	No clear use cases; lack of trading market; low liquidity.
Game Mechanics	Minimal interactivity; repetitive tasks; lack of skill-based rewards.
Tokenomics	Unclear rules; absence of burning/scarcity mechanisms; disproportionate allocations.
Withdrawal Difficulty	Delays or limits reported in forums/social media; opaque payment processes.
Smart Contract Audit	No external audit report; unknown certifier; lack of updates in code repository.

3.2 Data collection and analysis

To assess the crypto games against the checklist, data were collected from diverse sources. These included official project materials such as websites, white papers, and smart contracts, alongside external platforms providing historical token data and social media channels (YouTube, X, Telegram, Discord). The Wayback Machine was used as needed to access pages that were unavailable or altered during the collection period, ensuring comprehensive data gathering.

The data collection focuses on identifying the presence of the determinants from Table 1 in each evaluated crypto game. As a means of supporting this process and continuing the construction of an appropriate proposal, a working framework was developed with detailed procedures that served as a step-by-step guide for evaluating each red flag.

The target population was crypto games, defined as blockchain-based games that convey the hope of financial returns to their users. The delimited sample consisted of six crypto game projects. The selection criterion for four games was the average number of users during 2021, choosing the largest ones, as the number of users tends to reflect the projects' reach. This information was obtained from a query made to the FootPrint Analytics website.

In addition to these four projects, two were included that, at the time of the query, had inactive web pages, indicating the termination of the project. This measure aimed to better understand the application of the determinant-based approach and capture its effectiveness since the termination of the project may indicate different characteristics from the other active projects selected.

We selected 2021 as our reference period as it was the historical peak for the play-to-earn market, a year of “unprecedented expansion” for crypto gaming tokens (Vidal-Tomás, 2022). Industry data confirms this, with venture capital funding exceeding USD 4 billion and over 1.4 million daily active wallets connected to blockchain games (DappRadar, 2021). This unparalleled growth makes 2021 the ideal year for evaluating the subsequent persistence or discontinuation of projects.

The chosen projects are listed in Table 2, with the data collection period between April 9, 2023, and May 13, 2023. For the analysis of historical token values, the period from the first available quote until December 30, 2022, was considered. For the volume analysis, the daily average in December 2022 was considered. In cases of unavailable website data on the collection dates, such as for terminated projects, efforts were made to obtain the last saved content from the Wayback Machine service.

For ethical and methodological reasons, the projects analyzed in this study are anonymized (coded as Project A, Project B, etc.). The intention is not to accuse specific developers of fraudulent behavior, but rather to highlight patterns of risk that resemble red flags commonly associated with Ponzi schemes.

Table 2
Selected Projects for Data Collection

Project	Average Number of Users	Website Address	Active Website
Project A	106,703	[link removed for anonymization]	Yes
Project B	68,098	[link removed for anonymization]	Yes
Project C	65,453	[link removed for anonymization]	Yes
Project D	58,167	[link removed for anonymization]	Yes
Project E	4,934	[link removed for anonymization]	No
Project F	2,419	[link removed for anonymization]	No

Notes: For ethical reasons, the names and direct addresses of the projects are omitted and replaced with neutral identifiers (Project A–F).
Source: Authors.

For this exploratory study, we selected a purposive sample of six play-to-earn crypto games. This size is not intended for statistical generalization but is adequate for identifying patterns and testing the proposed checklist, an approach supported by exploratory research principles (Eisenhardt, 1989; Yin, 2018). Selection criteria included: (i) market relevance in 2021; (ii) historical data availability; and (iii) a mix of ongoing and discontinued projects to ensure variation for comparative analysis while maintaining analytical depth

4 RESEARCH RESULTS

4.1 Project A

As noted in Table 3, Project A exhibited red flags regarding the token value, development team, and game mechanics. The significant drop in token value (99.6%) compared to its launch price is noteworthy, suggesting potential shortcomings in the project's ability to maintain its value. Given its limited gameplay and lack of appeal particularly due to the absence of player interaction, it is surprising that the project remained active with a significant financial transaction volume in token trading. This observation could stem from either an ongoing project development phase or may reflect characteristics consistent with risks observed in Ponzi-like schemes.

Table 3
Analysis of Data: Project A.

Red Flag	**Source**	**Analysis**	**Observations**
Token Value	[link removed for anonymization]	*Red Flag*	-99.6% of the initial value
Website	[link removed for anonymization]	Ok	-
Social Media	Twitter: [removed for anonymization] Instagram: [removed for anonymization]	Ok	-
White Paper	[link removed for anonymization]	Ok	-
Development Team	[link removed for anonymization]	*Red Flag*	Team is not identifiable
Token and NFT Utility	*White Paper* and Websites	Ok	-
Game Mechanics	*White Paper* and Websites	*Red Flag*	Insufficient documentation and non-engaging or attractive gameplay, not requiring skill.
Tokenomics	*White Paper*	Ok	
Withdrawal Difficulty	*White Paper* and Websites	Ok	-
Smart Contract Audit	[link removed for anonymization]	Ok	-

This result illustrates how, despite the extreme depreciation of the token and the weak gameplay mechanics, the project remained active with relevant trading volume. According to Frankel (2012) and Cres (2014), financial schemes may persist temporarily due to continuous inflows of new participants, even when the underlying product lacks intrinsic value. The persistence of Project A, therefore, signals a potential misalignment between economic fundamentals and investor behavior, consistent with Ponzi-like dynamics described in the literature.

4.2 Project B

The findings regarding the Project B platform (Table 4) indicate that the project did not exhibit significant red flags. However, it is noteworthy that the token value experienced a period of significant appreciation followed by a significant drop from its peak value, although it still shows appreciation compared to its initial value. The game offered differentiated gameplay compared to others, and it is a project with a substantial track record in the market, still maintaining a considerable trading volume.

Table 4
Analysis of Data: Project B.

Red Flag	**Source**	**Analysis**	**Observations**
Token Value	[link removed for anonymization]	Ok	-
Website	[link removed for anonymization]	Ok	-
Social Media	Discord: [removed for anonymization] Twitter: [removed for anonymization]	Ok	-
White Paper	[link removed for anonymization]	Ok	-
Development Team	*White Paper*	Ok	-
Token and NFT Utility	*White Paper* and Websites	Ok	-
Game Mechanics	*White Paper*, Youtube, App	Ok	-
Tokenomics	*White Paper*	Ok	-
Withdrawal Difficulty	*White Paper* and Websites	Ok	-
Smart Contract Audit	[link removed for anonymization]	Ok	-

Unlike Project A, which revealed fundamental weaknesses in token value and gameplay, Project B maintained a stronger market position, despite volatility linked to external shocks such as hacker attacks. This reinforces Heyman's (2023) argument that technological risks and security breaches can generate vulnerabilities that resemble financial fraud patterns, even in projects with more elaborate mechanics. Practically, this suggests that resilience in gameplay design does not eliminate risks if the surrounding infrastructure remains exposed to external threats.

4.3 Project C

Project C (Table 5) exhibited red flags regarding the token value and game mechanics. The token value plummeted by 90.7% compared to its launch quotation, and the gameplay was not deemed engaging or attractive, particularly due to the absence of player-versus-player battles, which adversely impacts user retention and acquisition. The project's continued activity, akin to the first project evaluated, is surprising and may be attributed to either being a game still in development or signaling an ongoing Ponzi scheme.

Table 5
Analysis of Data: Project C.

Red Flag	**Source**	**Analysis**	**Observations**
Token Value	[link removed for anonymization]	*Red Flag*	-90.7% of the initial value
Website	[link removed for anonymization]	Ok	-
Social Media	Discord: [removed for anonymization] Twitter: [removed for anonymization] Telegram: [removed for anonymization] Facebook: [removed for anonymization]	Ok	-
White Paper	[link removed for anonymization]	Ok	-
Development Team	*White paper*	Ok	-

Red Flag	Source	Analysis	Observations
Token and NFT Utility	*White Paper* and Websites	Ok	-
Game Mechanics	*White Paper* and Websites	*Red Flag*	Gameplay is neither engaging nor attractive.
Tokenomics	[link removed for anonymization]	Ok	-
Withdrawal Difficulty	*White paper* e Internet	Ok	-
Smart Contract Audit	[link removed for anonymization]	Ok	-

Similar to Project A, Project C presented a severe token devaluation, but with additional weaknesses in gameplay attractiveness. The absence of competitive mechanisms, such as player-versus-player dynamics, aligns with Tavares et al. (2023), who stress that sustainable engagement is central to balancing supply and demand in play-to-earn economies. The coexistence of strong token depreciation and poor mechanics reinforces the red flags noted by Dias (2016) and Nascimento and Rech (2022), where lack of user retention mechanisms increases the risk of collapse once financial incentives lose appeal.

4.4 Project D

During the data collection of the Project D (Table 6), it was discovered that the original crypto game had been terminated, and the current page seemed to represent a sort of second version. Therefore, for analytical purposes, the project was deemed inactive, and the Wayback Machine service was utilized with content saved on December 27, 2022, the last available date with information from the previous project version. Its token (ETERNAL) had its initial quotation recorded on September 13, 2021.

Table 6
Analysis of Data: Project D.

Red Flag	Source	Analysis	Observations
Token Value	[link removed for anonymization]	*Red Flag*	-86.8% of the initial value.
Website	[link removed for anonymization]	Ok	-
Social Media	Discord: [removed for anonymization] Twitter: [removed for anonymization] Telegram: [removed for anonymization] Instagram: [removed for anonymization]	*Red Flag*	Game ended and a second version was released with new currency.
White Paper	[link removed for anonymization]	Ok	-
Development Team	*White Paper*	*Red Flag*	Team not clearly identified.
Token and NFT Utility	*White Paper*	Ok	-
Game Mechanics	*White Paper* and Websites	*Red Flag*	Gameplay is not engaging or attractive.
Tokenomics	*White Paper*	Ok	-
Withdrawal Difficulty	Websites	*Red Flag*	Reports of barriers to withdrawing.
Smart Contract Audit	[removed for anonymization]	Ok	-

Project D exhibited five of the ten potential red flags. A key indicator was an 86.8% decline in its token value, a drop whose magnitude and persistence align with warnings in the literature (Botha et al., 2023; Heyman, 2023). This collapse was explained by another flag identified on social media: an announcement that the game had ended and would be rebooted with a new token. The other red flags were: an unidentified development team, which reduces accountability (Bhujel & Rahulamathavan, 2022); unattractive game mechanics that hinder user retention (Tavares et al., 2023); and reported difficulties with withdrawing funds, a strong indicator of Ponzi-like schemes (SEC, 2013; Frankel, 2012). As per our methodology, these findings are interpreted as potential risk patterns, not as a definitive classification of the project.

Project D's comparison with other cases reveals key risk interactions. Its diverse vulnerabilities, particularly withdrawal difficulties, a critical Ponzi red flag (SEC, 2013), distinguished it from Project C. Unlike the more resilient Project B, Project D demonstrates how combining these withdrawal barriers with an anonymous development team fatally erodes user confidence (An & An, 2019; Kshetri, 2022). This underscores the importance of triangulating economic, informational, and operational determinants in risk assessment.

4.5 Project E

Among the two selected projects with inactive pages, the first to have data collected was Project E (Table 7). The webpage of Project E project communicated the termination of activities. Before presenting the red flags, it is worth noting that this project exhibited a distinctive configuration compared to others in the sample. Unlike projects that issued their own tokens, Project E remunerated players using the token of a cryptocurrency exchange (an intermediary). This structural difference influenced the way economic incentives were organized and partially mitigated issues of liquidity, which were frequent in other cases.

Table 7
Analysis of Data: Project E.

Red Flag	**Source**	**Analysis**	**Observations**
Token Value	[link removed for anonymization]	*Red Flag*	-80.1% of the initial value
Website	[link removed for anonymization]	Ok	-
Social Media	YouTube: [removed for anonymization] Twitter: [removed for anonymization] Telegram: [removed for anonymization] Instagram:[removed for anonymization]	*Red Flag*	Pages deleted or without content
White Paper	[link removed for anonymization]	*Red Flag*	High return promise.
Development Team	Página não disponível	*Red Flag*	Unidentified team.
Token and NFT Utility	*White paper*	Ok	-
Game Mechanics	*White Paper* and Websites	*Red Flag*	Gameplay based solely on luck.
Tokenomics	*White paper*	Ok	-
Withdrawal Difficulty	Websites	Ok*	-
Smart Contract Audit	Not located	*Red Flag*	-

Note: (*) Paid with a token from a cryptocurrency intermediary that is still active. Source: Authors.

Project E terminated its activities entirely, accumulating six red flags. Two were particularly salient: its white paper explicitly promised high returns, a classic Ponzi scheme indicator (Frankel, 2012; Cres, 2014), and its gameplay was superficial, based only on chance. Interestingly, unlike other terminated projects, Project E did not exhibit withdrawal difficulties because it used an intermediary token instead of its own currency. This observation is significant, as it reinforces that withdrawal barriers are not the only critical determinant of fraud risk and that unrealistic promises of return can, by themselves, signal an unsustainable project (Botha et al., 2023).

4.6 Project F

Finally, data from the Project F project were collected (Table 8). Project F exhibited five red flags, and its characteristics (a lifespan of less than three months and abrupt abandonment) are indicative of a “Rug Pull”. This aligns with literature defining Rug Pulls as schemes where developers suddenly withdraw liquidity, leaving investors with worthless tokens (Heyman, 2023; Botha et al., 2023). The specific red flags included a 99.9% token value collapse, deleted social media, an unidentified team, and withdrawal difficulties. In the play-to-earn context, the complete absence of gameplay was particularly telling, indicating the project's sustainability was never based on user engagement but solely on financial speculation.

Table 8
Analysis of Data: Project F.

Red Flag	Source	Analysis	Observations
Token Value	[link removed for anonymization]	*Red Flag*	-99.9% of the initial value.
Website	[link removed for anonymization]	Ok	-
Social Media	Telegram: [removed for anonymization] Discord: [removed for anonymization] Twitter: [removed for anonymization]	*Red Flag*	Deleted networks. High return promises.
White Paper	[link removed for anonymization]	Ok	-
Development Team	[link removed for anonymization]	*Red Flag*	Partially identified.
Token and NFT Utility	*White Paper* and Websites	Ok	-
Game Mechanics	*White Paper* and Websites	*Red Flag*	Gameplay is neither engaging nor attractive.
Tokenomics	*White Paper*	Ok	
Withdrawal Difficulty	Websites	*Red Flag*	Reports on social media of difficulty withdrawing.
Smart Contract Audit	[link removed for anonymization]	Ok	-

Project F's rapid collapse in under three months, combined with red flags like extreme token depreciation, deleted social media, and anonymous developers, is characteristic of a "Rug Pull" scheme (Zheng et al., 2023). Unlike Project E's gradual decline, Project F's abrupt failure represents a sharper form of opportunistic behavior, reinforcing the concern that technology provides new channels for fraud (Yang & Feng, 2021). From a practical standpoint, this case underscores the critical need for early detection of cumulative red flags, as such accelerated collapses leave investors with no time to react.

4.7 Discussion

The presence of red flags in several projects suggests that users and investors should proceed with caution and assess risks when considering investments in the crypto games market, as cautioned by Hujel and Rahulamathavan (2022). The redder flags, the greater the risk of the project being involved in a Ponzi scheme, and the analysis should consider assigning different weights to each determinant for each scenario. Appendix 2 presents an organized summary of the red flags verified in the six crypto games analyzed and shows that, overall, the most frequent red flags (including discontinued games) are related to token value and game mechanics, which suggests they are important warnings of Ponzi schemes, as proposed by An and An (2019) and Bhujel and Rahulamathavan (2022).

While token value volatility in cryptocurrencies complicates risk analysis, metrics like transaction volume remain useful. Project A exemplified this: its high transaction volume, despite a low token price, was combined with other red flags, poor gameplay, an anonymous team, and flawed audits. This accumulation of signals indicated a high risk of discontinuation with Ponzi-like characteristics, potentially harming over 100,000 users. In contrast, Project C showed fewer red flags (only token value and game mechanics). Thus, despite also having a devalued token, its overall risk of being a Ponzi scheme was considered lower.

With respect to the game mechanics, the understanding was reached that this variable should be evaluated specially. Gameplay, discussed by authors such as Jesus et al. (2022), proved to be a fundamental characteristic of crypto games because it is often the most sought after by users, even outweighing financial returns, as seen in the Project B (the most popular). Thus, observing this red flag in some analyzed projects indicated a distortion of the entertainment purpose of the games, amplifying the risks related to token value and other determinants.

In Appendix 2 it is noted that the red flags webpage, tokenomics, and utility of the token and NFT did not show any occurrence, even in the discontinued projects. This outcome may suggest that these indicators are not useful in detecting fraud in crypto games, contrary to what An and An (2019) argued.

The "withdrawal difficulty" red flag warrants special attention. Though less frequent in our sample than in traditional Ponzi schemes (observed in only two inactive projects), its importance is high. This lower frequency is likely due to automated systems in active projects, which mask withdrawal issues until the project is already

collapsing, a pattern consistent with traditional fraud (SEC, 2013). Since this flag directly impacts investor returns (Tavares et al., 2023), it serves as a necessary, albeit often late-stage, indicator in risk assessment.

The red flags identified in the inactive crypto games, issues with token value, social media, white papers, the development team, game mechanics, and smart contract audits, show a clear parallel to traditional Ponzi schemes. Withdrawal difficulty was also common, except for Project E, which lacked a native token. This strong correspondence suggests these projects may have been terminated for being Ponzi-like schemes, though other hypotheses cannot be ruled out.

Although withdrawal restrictions are often cited in literature as one of the main characteristics of Ponzi schemes, in the context of crypto games these should be seen as red flags to be analyzed in combination with other determinants, rather than as definitive proof of fraudulent intent. Considering all the foregoing, Table 9 was compiled, consolidating the research's main findings and presenting the importance of the selected red flags for assessing the risk of Ponzi schemes in crypto games.

Table 9
Risks assessment of Ponzi schemes in crypto games.

Red Flag	**Occurrences**	**Risk Assessment**
Game Mechanics	5/6 (83%)	High
Token Value	5/6 (83%)	High
Development Team	4/6 (67%)	Moderate
Social Media	3/6 (50%)	Moderate
Smart Contract Audit	2/6 (33%)	Moderate
Withdrawal Difficulty	2/6 (33%)	High
White Paper	1/6 (17%)	Moderate
Website	0/6 (0%)	Low
Tokenomics	0/6 (0%)	Low
Token and NFT Utility	0/6 (0%)	Low

It is important to emphasize that the presence of red flags, due to their subjective nature, is not a guarantee of fraud, as Yücel (2013) explained, or that a particular crypto game is a Ponzi scheme. Red flags and other important data should be analyzed in context, along with other relevant information about the project, to determine the likelihood of fraud. Similarly, the absence of red flags should not be assumed as an unconditional green light for any investment.

The findings for the active projects reinforce those red flags must be analyzed holistically and in context (Cres, 2014; Dias, 2016). For example, Project B's lack of red flags does not guarantee it is risk-free. In contrast, Projects A and C, while still active, present warning signs that indicate potential risk to investors. This illustrates that a project's risk profile depends on the combined analysis of signals, rather than the mere presence or absence of individual flags.

5 FINAL CONSIDERATIONS

This study was conducted to assess to what extent it is possible to detect red flags resembling those commonly associated with Ponzi schemes in play-to-earn crypto games, through the proposal and empirical testing of an original checklist. A literature review was conducted to identify red flags present in traditional schemes and cryptocurrencies. These red flags were validated by digital forensic experts as a potential checklist for criminal detection. The checklist was tested against a sample of six crypto games whose data were available on the internet.

Of the ten proposed determinants for Ponzi-like schemes in crypto games, seven were identified in our analysis. Based on the operational criteria detailed in Table 2, three determinants emerged as most relevant for risk assessment: token value, game mechanics, and withdrawal difficulty. These consistently met the established red flag thresholds across multiple projects. Conversely, webpage presence, tokenomics, and token/NFT utility were classified as less important due to their greater variability and weaker alignment with the defined criteria.

The study revealed that token value, although presumed to be highly volatile, contains relevant signals regarding transaction volume and frequency, especially when high transaction volume is observed alongside the token's low value. When this scenario is combined with low gameplay appeal, lack of information about the development team, flaws in smart contract audits, and other red flags, it indicates high risks that a crypto game may be discontinued suggesting resemblance to characteristics often associated with Ponzi-like structures.

This study offers a dual contribution by filling a theoretical gap and providing practical implications for several stakeholders. Theoretically, it adapts traditional fraud detection concepts to the nascent play-to-earn domain. Practically, it offers a framework to help investors identify potential Ponzi schemes and avoid losses, highlighting that monitoring liquidity dynamics, not just token price, is a crucial risk signal. For policymakers, our findings underscore the need for stricter regulation and supervision. For researchers, this study provides a foundation for refining methodologies and expanding knowledge on fraud in crypto games. This work is presented as an academic tool to inform on potential risks, not as a definitive legal classification. In addition to regulatory concerns, the social and economic importance of this topic is evident, as fraudulent crypto games can cause significant harm to thousands of users worldwide, reinforcing the urgency and necessity of studies such as this.

This study has limitations inherent to its exploratory design, notably the subjective nature of the analysis and a checklist validation restricted to a small expert group. Consequently, the methodology should be viewed as an instrument to aid in risk assessment, not as a definitive legal classification of fraud. Future research could build upon these findings to enhance robustness and generalizability. Key opportunities include: broadening the checklist's validation with more experts or statistical techniques (e.g., factor analysis); adopting quantitative approaches to analyze historical token value and user data; and conducting focused studies on specific determinants to reinforce the concept of red flag-based fraud identification.

REFERENCES

An, J., & An, E. (2019). What an investor wants; What an investor needs: Identifying deceptive projects on blockchain market. ICIS 2019 Proceedings.

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: analysis and perspectives. Ieee Access, 9, 148353-148373. https://doi.org/10.1109/ACCESS.2021.3123894

Benson, S. S. (2009). Recognizing the red flags of a Ponzi scheme. The CPA Journal, 79(6), 18.

Bhujel, S., & Rahulamathavan, Y. (2022). A survey: Security, transparency, and scalability issues of nft's and its marketplaces. Sensors, 22(22), 8833. https://doi.org/10.3390/s22228833

Botha, J., Botha, D. P., & Leenen, L. (2023). An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020. In ICCWS 2023 18th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited. 18(1), 36–48. https://doi.org/10.34190/iccws.18.1.1087

Carvalho, R. P. D., & Silva, A. H. C. (2024). A Irrelevância dos Indicadores Econômico-Financeiros como Red Flags para Detecção de Fraudes em Demonstrações Financeiras: O Caso Americanas SA. Pensar Contábil, 25(88), 12-19.

Cotler, B. (2023). Tokenized and Non-tokenized Assets: Legal Considerations. The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges, 249-263. https://doi.org/10.1108/978-1-80455-320-620221017

Cres, F. (2014). Esquema Ponzi: Como Tirar Dinheiro dos Incautos. Portuguese Edition ed. Armada Press.

Cross, C. (2017). Anatomy of a Ponzi Scheme: Scams Past and Present. Slice Publishing Mystery and Thriller Books.

Dal Magro, C. B., & Cunha, P. R. D. (2017). Red flags in detecting credit cooperative fraud: the perceptions of internal auditors. Revista Brasileira de Gestao de Negocios, 19, 469-491. https://doi.org/10.7819/rbgn.v19i65.2918

DappRadar. (2021). Blockchain game report 2021. DappRadar. https://dappradar.com/blog/bga-blockchain-game-report-2021

Delfabbro, P., Delic, A., & King, D. L. (2022). Understanding the mechanics and consumer risks associated with play-to-earn (P2E) gaming. Journal of Behavioral Addictions, 11(3), 716-726. https://doi.org/10.1556/2006.2022.00066

Dias, S. (2016). Caracterização e Identificação de Esquemas Ponzi. Dissertação. (Mestrado em Auditoria) - Lisboa: Instituto Superior de Contabilidade e Administração de Lisboa.

Drescher, D. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps. Berkeley, CA: Apress.

Dupuis, D., Smith, D., & Gleason, K. (2023). Old frauds with a new sauce: digital assets and space transition. Journal of Financial Crime, 30(1), 205-220. https://doi.org/10.1108/JFC-11-2021-0242

du Toit, E. (2024). The red flags of financial statement fraud: a case study. Journal of Financial Crime, 31(2), 311-321. https://doi.org/10.1108/JFC-02-2023-0028

Eisenhardt, K. M. (1989). Building theories from case study research. Academy of Management Review, 14(4), 532–550. https://doi.org/10.2307/258557

Frankel, T. (2012). The Ponzi Scheme Puzzle: A History and Analysis of Con Artists and Victims. New York: Oxford University Press.

Fu, S., Wang, Q., Yu, J., & Chen, S. (2022). FTX collapse: a Ponzi story. arXiv preprint arXiv:2212.09436. http://arxiv.org/abs/2212.09436

Gunay, S., & Kaskaloglu, K. (2022). Does utilizing smart contracts induce a financial connectedness between Ethereum and non-fungible tokens? Research in International Business and Finance, 63, 101773. https://doi.org/10.1016/j.ribaf.2022.101773

Heyman, C. E. (2023). A red flag checklist for cryptocurrency Ponzi schemes. Journal of Financial Crime, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JFC-05-2023-0118

Jesus, S. B., Austria, D., Marcelo, D. R., Ocampo, C., Tibudan, A. J., & Tus, J. (2022). Play-to-Earn: A qualitative analysis of the experiences and challenges faced by axie infinity online gamers amidst the COVID-19 pandemic. International Journal of Psychology and Counseling, 1(12), 291-424.

Jiang, X. J., & Liu, X. F. (2021). Cryptokitties transaction network analysis: The rise and fall of the first blockchain game mania. Frontiers in Physics, 9, 57. https://doi.org/10.3389/fphy.2021.631665

Kadoo, S., & Sodi, K. (2023). An Analysis of Cryptocurrency, Bitcoin and the Future. International Journal of Advanced Research in Science, Communication and Technology, 3(3), 287–292. https://doi.org/10.48175/IJARSCT-8157

Kshetri, N. (2022). Scams, frauds, and crimes in the nonfungible token market. Computer, 55(4), 60-64. https://doi.org/10.1109/MC.2022.3144763

Kiong, L. V. (2022). Metaverse Made Easy: A Beginner's Guide to the Metaverse: Everything you need to know about Metaverse, NFT and GameFi. Liew Voon Kiong.

Lewis, M. K. (2015). Understanding Ponzi Schemes: Can Better Financial Regulation Prevent Investors from Being Defrauded? Edward Elgar Publishing.

Munteanu, V., Zuca, M. R., Horaicu, A., Florea, L. A., Poenaru, C. E., & Anghel, G. (2024). Auditing the risk of financial fraud using the red flags technique. Applied Sciences, 14(2), 757. https://doi.org/10.3390/app14020757

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review. https://bitcoin.org/bitcoin.pdf

Nascimento, M. R., & Rech, I. J. Contribuições de Red Flags para Detecção de Fraudes Corporativas. Management in Perspective, 2(1), 112–138. https://doi.org/10.14393/MIP-v2n1-2021-66006

Ramadhany, A. A., Erlina, E., Sadalia, I., & Fachrudin, K. A. (2025). Enhancing Fraud Detection Performance: The Interplay of Red Flag Awareness, Self-Efficacy, and Professional Skepticism. Journal of Risk and Financial Management, 18(6), 301. https://doi.org/10.3390/jrfm18060301

Sakız, B., & Gencer, A. H. (2021, August). Blockchain beyond cryptocurrency: non-fungible tokens. In International Conference on Eurasian Economies (pp. 154-161). https://www.avekon.org/?p=/conf/13/paperdetail&id=2527

Sandhu, N. (2022). Red flag behaviors in financial services frauds: a mixed-methods study. Journal of Financial Regulation and Compliance, 30(2), 167-195. https://doi.org/10.1108/JFRC-01-2021-0005

Scholten, O. J., Hughes, N. G. J., Deterding, S., Drachen, A., Walker, J. A., & Zendle, D. (2019, October). Ethereum crypto-games: Mechanics, prevalence, and gambling similarities. In Proceedings of the annual symposium on computer-human interaction in play (pp. 379-389). https://dl.acm.org/doi/10.1145/3311350.3347178

SEC. (2013). Ponzi Schemes Using Virtual Currencies. Available at https://www.sec.gov/investor/alerts/ia_virtualcurrencies

SEC. (2023). Ponzi Scheme | Investor.gov. Available at https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme

Tavares, R., Sousa, J. P., Maganinho, B., & Gomes, J. P. (2023). Gamers' Reaction to the Use of NFT in AAA Video Games. Procedia Computer Science, 219, 606-613. https://doi.org/10.1016/j.procs.2023.01.329

Vidal-Tomás, D. (2022). The new crypto niche: NFTs, play-to-earn, and metaverse tokens. Finance Research Letters, 47, 102742. https://doi.org/10.1016/j.frl.2022.102742

Wang, L., Cheng, H., Zheng, Z., Yang, A., & Zhu, X. (2021a). Ponzi scheme detection via oversampling-based Long Short-Term Memory for smart contracts. Knowledge-Based Systems, 228, 107312.

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447. Available at http://arxiv.org/abs/2105.07447

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). Sage Publications.

Yücel, E. (2013). Effectiveness Of Red Flags in Detecting Fraudulent Financial Reporting: An Application In Turkey. Journal of Accounting & Finance, (60). Available at https://search.ebscohost.com/login.aspx?direct=true&db=bsx&AN=90619644&lang=pt-br&site=eds-live

Yuspin, W., & Fadhlulloh, Q. H. (2022). Ponzi Scheme: Risk and Regulation in Indonesia. International Journal of Social Science Research and Review, 5(10), 339-345. https://doi.org/10.47814/ijssrr.v5i10.599

Zheng, Z., Chen, W., Zhong, Z., Chen, Z., & Lu, Y. (2023). Securing the ethereum from smart ponzi schemes: Identification using static features. ACM Transactions on Software Engineering and Methodology, 32(5), 1-28. https://doi.org/10.1145/3571847

Zou W. et al. (2019) Smart contract development: Challenges and opportunities. IEEE Transactions on Software Engineering, 47(10), 2084-2106. https://doi.org/10.1109/TSE.2019.2942301

How to cite this paper

Almeida, R. B., Lima, R. S & Souza, P. V. S. (2025). Red Flags in Play-to-Earn Crypto Games: Proposal and Testing of a Checklist Based on Ponzi Scheme. *Revista de Contabilidade e Organizações*, 19:e230807. DOI: http://dx.doi.org/10.11606/issn.1982-6486. rco.2025.230807