A Case Study on The HyperFund Fraud: A $1.7 Billion Crypto Ponzi Scheme

Krishna Damarla

College of Graduate and Professional Studies

Trine University

FIN 5063: Corporate Finance

Mr. Daniel Sabol

March 30, 2025

Table of Contents

Summary

This paper discusses HyperFund, a fraudulent investment platform based on cryptocurrency which served as a pyramid scheme from 2020 to 2022 (U.S. Securities and Exchange Commission, 2024). Through an analysis of Securities and Exchange Commission filings, court documents, and journalism insights, this study shows how the founders of HyperFund deceived investors through false promises while operating a Ponzi. The scheme collapsed in 2022, resulting in a total loss of USD 1.7 billion for investors. This study also describes the mechanism of the scheme, key victims, gaps in cryptocurrency regulations and the importance of independent financial whistleblowers. Finally, it ends with lessons learned and recommendations to investors and regulators.

Introduction

Background of HyperFund

HyperFund launched in June 2020 as a cryptocurrency investment platform promising extraordinary returns. The platform claimed to generate profits through cryptocurrency mining operations and decentralized finance strategies (U.S. Securities and Exchange Commission, 2024). It is marketed through multi-level marketing techniques, zoom conference calls and social media influencers. Investigations revealed these business operations were completely fictitious. The platform operated for nearly two years before collapsing in early 2022 when investor withdrawals overwhelmed the scheme's ability to recruit new participants (U.S. District Court, 2024).

Purpose of the Report

This study provides a comprehensive analysis of HyperFund's fraudulent operations, with a key focus on three aspects. First, it examines the mechanisms through which the scheme deceived investors. Second, it analyzes the social and regulatory factors that enabled the scheme to persist. Finally, it evaluates the consequences for both investors and the broader cryptocurrency market. The findings aim to educate both policymakers and investors about the risks of such fraudulent schemes (Higgins, 2023).

Mechanics of the Fraud

Pyramid Scheme Structure

HyperFund operated as a pyramid scheme, though it employed cryptocurrency to obscure its operations. The platform required new investors to purchase membership packages with promised returns of up to 300%. These returns were generated through the continuous recruitment of new investors rather than legal businesses. This scheme incorporated multi-level marketing elements, offering additional bonuses for participants who recruited others into the program. This created exponential growth in the early stages but guaranteed eventual collapse when new recruitment inevitably slowed (Financial Crimes Enforcement Network, 2024).

False Promises and Marketing Tactics

The platform's marketing materials made several fraudulent claims to attract investors. For instance, HyperFund advertised partnerships with Fortune 500 firms and cryptocurrency mining operations, but neither of them existed. Social media posts and videos with complex jargon created an illusion of legitimacy. The scheme mainly aimed at cryptocurrency enthusiasts with limited financial knowledge, highlighting the transformation potential of decentralized finance while simultaneously covering the lack of underlying business processes (CCN, 2024).

Use of Cryptocurrency to Evade Detection

HyperFund implemented several concepts of cryptocurrency to avoid regulatory scrutiny. All transactions happened in cryptocurrencies such as Tether and Bitcoin, allowing the scheme to bypass traditional banking regulations. The platform handled fiat conversions by offshoring to shell companies in jurisdictions with weak financial regulations. This international structure delayed regulatory response and complicated enforcement efforts. Further, the pseudonymous nature of blockchain transactions made it difficult for investors to trace fund flows and verify the platform's underlying business activities (Mishkin & Eakins, 2018).

Key Figures

Founder's Role

As the alleged founder of HyperFund, Sam Lee (Xue Lee), the Australian blockchain entrepreneur established the platform's basic structure and recruited investors. He was accused with conspiracy to commit fraud for operating crypto investment schemes in the US (Guardian, 2024).

Court documents describe Lee as an architect of the fraudulent HyperFund business model of the “pyramid and Ponzi scheme”, designing the tiered membership system and compensation plan. Lee leveraged his prior involvement in legitimate cryptocurrency projects to establish credibility. Despite clear warnings of the scheme's instability, Lee continued promoting HyperFund until its collapse. As of 2024, Lee is charged with several civil and criminal cases, including wire and securities fraud (U.S. District Court, 2024).

Promoter's Guilty Plea

Brenda Chunga served as one of HyperFund's most active promoters under the pseudonym "Bitcoin Beautee." Chung has gained thousands of investors via social media, and in-person events and received millions of dollars in commissions. In January 2024, Jung was convicted of committing securities fraud and wire fraud. Her plea includes continuous investigation and significant financial fines. This case shows how influential promoters can greatly expand the range of coverage and enhance the damage of financial fraud.

SEC and DOJ Charges

The Securities & Exchange Commission (SEC) complaint includes numerous violations of laws on securities, including an unregistered proposal, sale of securities and fraudulent distortion of investment returns. The Department of Justice (DOJ) parallelly charged criminal cases on conspiracy and wire fraud. These actions represent one of the most significant enforcement efforts against a cryptocurrency-based pyramid scheme. The case continues to develop as authorities work to identify additional participants and restore assets for victims.

Whistleblowers and Early Detection

Independent New Zealand researcher Danny de Hek emerged as the earliest and most consistent critic of HyperFund. Through his YouTube channel beginning in 2021, de Hek published detailed analyses exposing the scheme's mathematical impossibilities (Segal, 2022). His work identified several red flags including inconsistent return calculations, lack of mining verification, and suspicious payment delays. Despite limited subscribers to his YouTube channel, de Hek's persistent warnings eventually gained traction among cryptocurrency communities and media outlets.

The New York Times brought mainstream attention to HyperFund's fraud through a November 2022 investigative report (de Hek, 2021). The article synthesized de Hek's findings with additional research, revealing the scheme's rebranding tactics and fabricated leadership. Journalists traced connections between HyperFund and other fraudulent cryptocurrency projects, demonstrating a pattern of deception. This reporting significantly increased pressure on regulators to act, though formal charges would not come for another fourteen months.

Regulatory Delays in Response

The extended timeline between initial warnings and official action shows systemic problems in cryptocurrency regulation. Various factors contributed to this delay, including jurisdictional complexities, restricted regulatory resources, and technical problems of blockchain-based fraud (CBS News, 2021) investigations. This HyperFund case echoes historical patterns observed in traditional financial frauds, where regulators often try to catch up with innovative technologies and schemes until significant damage has already occurred.

Network of Related Frauds

HyperVerse

Following HyperFund's collapse, investigators uncovered its connections to HyperVerse, a subsequent venture using identical fraudulent tactics. Most remarkably, HyperVerse invented a fictitious CEO named "Steven Reece Lewis," complete with fabricated credentials and AI-generated publicity photos. This elaborate deception included a professionally produced launch video featuring paid actors posing as enthusiastic employees. Creating entirely fictional executives demonstrates how sophisticated cryptocurrency frauds have become in manufacturing false legitimacy. These tactics successfully attracted additional investment despite HyperFund's recent collapse, showing how rebranding can extend fraudulent operations (Segal, 2022).

Bitcoin Blockchain Global

Further investigation revealed ties between HyperFund and Bitcoin Blockchain Global (BBG), an Australian cryptocurrency platform that collapsed in 2023 with $58 million in losses. Court documents show Sam Lee served as an advisor to BBG while operating HyperFund, suggesting a pattern of fraudulent activities across multiple platforms. The BBG case shared key characteristics with HyperFund, including promises of guaranteed returns from nonexistent mining operations and reliance on continuous new investment to sustain payouts. This connection highlights how operators of financial fraud frequently rebrand themselves to evade detection.

HyperCapital

The web of related entities included HyperCapital, which operated as a shadowy investment arm handling HyperFund's finances. Forensic accounting revealed that HyperCapital used new investor funds to pay existing debts rather than generate legitimate returns. This created a complex financial shell game where funds moved between entities to create the illusion of profitability. The operation maintained separate accounting systems for internal tracking versus investor reporting, deliberately obscuring the complete lack of revenue generation. Such sophisticated financial engineering demonstrates how modern frauds exploit both technological and regulatory grey areas.

Impact and Consequences

The human cost of HyperFund's collapse became tragically clear as victim impact statements poured in during legal proceedings. Investor losses ranged from savings to life-changing sums, with severe consequences for retirees who invested their pensions (U.S. District Court, 2024). A total of $1.7 billion loss is one of the largest cryptocurrency frauds in history, affecting more than a million investors around the world. Recovery efforts have proven to be difficult due to the international nature of the scheme and the difficulties of tracking cryptocurrency transactions, with less than 5% of funds being reclaimed for victims as of 2024.

Scandals such as HyperFund starkly damaged public trust in cryptocurrency markets. A 2023 Pew Research study found that 32% of Americans cited fraud concerns as their main reason for avoiding cryptocurrency investments, up from 21% before HyperFund's collapse. This distrust is creating collateral damage for legitimate blockchain projects. The case has become a frequently cited example in cryptocurrency policy and regulation debates, with proponents of stricter supervision using it to demonstrate potential damage from insufficient consumer protections.

In response to HyperFund and similar cases, regulators have made several reforms. SEC now requires cryptocurrency projects to undergo third-party reserve audits and maintain transparent accounting practices (SEC, 2023). These rules aim to prevent the type of obfuscation HyperFund played. Also, international collaboration between financial regulators has increased, with data-sharing agreements designed to quickly detect cross-border frauds. Although these measures represent progress, critics argue they remain reactive rather than preventative, focusing on the need for more fundamental modifications in how cryptocurrency markets are controlled.

Lessons & Recommendations

The HyperFund case offers three important lessons. One, it demonstrates how the technical complexity of blockchain can be taken as an advantage to confuse investors and evade oversight. Two, it reveals the vulnerability of decentralized financing to affinity fraud, where scammers exploit shared interests and identities to strengthen trust. Three, it stresses the key role of independent researchers where traditional oversight mechanisms are often behind innovation. These insights suggest both technological solutions and social awareness campaigns are required to protect investors in cryptocurrency markets and to counter psychological manipulation tactics.

For Regulators

Regulators should prioritize three key reforms based on HyperFund's lessons. First, they must establish real-time cryptocurrency monitoring systems using blockchain analytics tools to detect suspicious patterns. Second, international coordination mechanisms need strengthening to prevent jurisdictional arbitrage by fraudsters. Third, whistleblower reward programs should be expanded to encourage early exposure of fraudulent schemes. These measures would help close the current gap between fraud innovation and regulatory response, potentially preventing future schemes from reaching HyperFund's scale.

For Investors

Cryptocurrency investors can use several evidence-based practices such as verifying business registration, checking for third-party audits, and researching principals' backgrounds to protect themselves. Investors must maintain healthy scepticism on guaranteed returns, remembering that if an opportunity seems too good to be true, it probably is. The most important thing is investors should avoid any opportunity emphasizing returns over product value, the hallmark of pyramid schemes. Such preventive measures are vital in cryptocurrency markets where regulatory protections remain incomplete.

Conclusion

The HyperFund case emphasizes important lessons for cryptocurrency markets and financial regulation. As evidenced by its $1.7 billion collapse, even mature investors remain vulnerable to Ponzi schemes disguised as innovative blockchain projects (CBS News, 2021). This fraud highlights the need for systemic reforms mandating transparency in digital asset markets, aggressive regulatory pursuit of cross-border crypto crimes and investor vigilance against unrealistic returns. Blockchain technology provides transformative potential. However, HyperFund demonstrates how human factors like greed and deception continue to threaten financial systems. Future protection requires a combination of technological solutions with enhanced investor education and global regulatory coordination to detect and prevent similar schemes (MIT OpenCourseWare, 2024). These measures may help balance innovation with accountability in evolving digital finance ecosystems.

References

CBS News. (2021). 60 Minutes archive: The man who figured out Madoff's Ponzi scheme. YouTube. https://www.youtube.com/watch?v=3wUJesUik5A

CCN. (2024). HyperFund owners accused of fraud in $1.7B pyramid scheme. https://www.ccn.com/news/hyperfund-owners-accused-fraud-pyramid-scheme/

de Hek, D. (2024). Sam Lee breaks his silence: HyperVerse scandal takes another turn. LinkedIn. https://www.linkedin.com/pulse/sam-lee-breaks-his-silence-hyperverse-scandal-takes-another-de-hek-afmjc/

Financial Crimes Enforcement Network. (2024). Annual report on cryptocurrency fraud trends. U.S. Department of the Treasury.

The Guardian. (2024). Australian Sam Lee charged with conspiracy to commit in US for role in Ponzi scheme. https://www.theguardian.com/technology/2024/jan/30/australian-sam-lee-charged-with-conspiracy-to-commit-in-us-for-role-in-ponzi-scheme

Higgins, R. C. (2023). Analysis for financial management (13th ed.). McGraw-Hill Education. https://www.mheducation.com/highered/product/Analysis-for-Financial-Management-Higgins.html

Mishkin, F. S., & Eakins, S. G. (2018). Financial markets and institutions (9th ed.). Pearson.

MIT OpenCourseWare. (2024). Lecture 4: The financial market. YouTube. https://www.youtube.com/watch?v=b5H8D_wD2AY

Segal, D. (2022). The crypto Ponzi scheme avenger. The New York Times. https://www.nytimes.com/2022/11/11/business/crypto-ponzi-scheme-hyperfund.html

U.S. Department of Justice. (2024). Court filings related to HyperFund case. https://www.justice.gov/criminal/case/hyperfund-and-associated-cases

U.S. Securities and Exchange Commission. (2024). SEC charges founder of $1.7 billion "HyperFund" crypto pyramid scheme. https://www.sec.gov/newsroom/press-releases/2024-11