Red Flags for Smart Contract Pyramid Schemes in 2021

IC3

Follow

The Initiative for CryptoCurrencies and Contracts (IC3)

--

Listen

Share

by Tyler Kell, Haaroon Yousaf, Sarah Allen, Sarah Meiklejohn, Ari Juels

Have you been offered the chance to earn unlimited passive income in cryptocurrency for life with no risks using a new technology called a smart contract? Congratulations! You may have just encountered a smart contract pyramid scheme.

Pyramid schemes are not a new phenomenon, but they have found a new form in the nascent technology of smart contracts and decentralized, trustless programmable money. In this blog post we identify common characteristics of smart-contract based pyramid schemes that may serve as red flags for further study to determine if a smart-contract based project looks suspicious. Some of these characteristics may not be unique to pyramid schemes or smart-contract pyramid schemes, but some are.

According to the US SEC, "A pyramid scheme is an investment fraud in which new participants' fees are typically used to pay money to existing participants for recruiting new members." Pyramid schemes differ from multi-level-marketing (MLM) schemes, which require that an actual good or service is offered. Pyramid schemes are illegal in the US and in most jurisdictions, while MLMs are legal in some (the US for example) and illegal in others (like China). We identified these aspects of a smart-contract pyramid scheme through our in-depth study of the Forsage pyramid scheme, which was created in early 2020 and is still running today. Since fraud and scamming is so often a cat-and-mouse game between scammers and law enforcement, these characteristics will likely change over time. Therefore, we suggest that these characteristics are most applicable as of this writing, right now, in 2021; however many of these features may be enduring.

Why would a scammer use a smart contract?

Smart contracts are in some ways an ideal medium for pyramid schemes and other scams. Because they run in decentralized, international computer networks, they lack clear jurisdiction and thus cannot easily be dismantled by law enforcement agencies. They can enable quick and geographically distributed payments from a global pool of victims. They seemingly provide privacy protection for their creators in the form of pseudonymous addresses. Finally, as so-called "trustless" applications — with world-readable (byte)code — they present a veneer of trustworthiness to unsuspecting users.

Three Categories of Red Flags for Smart Contract Pyramid Schemes:

1. Language

Our study of pyramid schemes in 2021 turned up a unique set of linguistic choices — jargon — that we believe raise suspicion. These terms are not unique to smart contracts or pyramid schemes, but use of them together can serve as red flags that the project warrants closer inspection. We give a few examples of these terms below.

"Matrix"

Smart contract pyramid schemes may use convoluted structures to organize participants and try to deceive those involved that earnings will not be concentrated at the top of a pyramid structure. The people behind the Forsage pyramid scheme we studied referred to the structure of participants as a "matrix" rather than a pyramid.

"Upline/Downline"

The relationships between participants in a scam may be described using specific language like upline (the person you pay) and downline (the person who pays you) to make the flow of funds less obvious. YouTube promotional videos on Forsage frequently used this jargon, and you can find this jargon defined by the US Federal Trade Commission as a characteristic of "product-based pyramid schemes or recruiting MLM's."

"Passive income"

While some legitimate decentralized finance applications can provide a participant with passive income, these passive income streams are always generated from a clear source, and participants are explicitly told that they are taking on risk. Some examples include lending schemes, or market-making for decentralized exchanges. In these schemes the protocol will describe where passive income is generated as a function of the service it provides, usually by charging fees to some class of participants making use of the service, such as borrowers in a lending scheme. Pyramid schemes, by contrast, may use claims about wealth and passive income to lure hopeful victims into paying money, although these systems do not provide a service to a class of participants that they charge for, nor do they have specific mechanisms for passive income generation- all income comes from new participants buying into the pyramid.

In summary, scammers make claims of perpetual income deriving from relationships between users. The jargon in these schemes serves to formalize and obscure this reality. We might hypothesize as a common thread a basic mapping, as follows in the case of Forsage. There is a pyramid whose maintenance depends upon recruits to furnish ongoing profits. In Forsage communications, the terms used to describe the pyramid is "matrix," recruits are "upline / downline," and profits are "passive income."

2. Promotional Claims

Below are some fraudulent promotional claims we collected while studying the Forsage smart contract pyramid scheme.

"Unhackable"

Claims may rely on the public's lack of knowledge about blockchain technology and modern computer technology to make victims feel secure in the technical properties of the program. Pyramid schemes may claim that the blockchain technology itself makes the pyramid scheme unhackable. Legitimate projects, by contrast, will focus on presenting a security model focusing on the project's application in question and not "the blockchain technology" underlying the application (nor would any serious project ever claim to be "unhackable").

"The contract cannot lose funds"

or "The contract does not store funds"

Technical properties of smart contracts may be used to garner legitimacy for the project. While these claims may sound official, many show a lack of understanding of the true implications of the technical properties they highlight. Also, if a pyramid scheme funnels funds successfully, it will move funds from new users into the wallets of the contract creator, scamming victims without losing funds.

"Scam-proof because the code is viewable"

The code for many smart contracts is open source. However, these contracts can be sufficiently complex to read and understand that one must have an extensive computer science background to follow. Even then, smart contracts may require hours of manual source code review. Thus, scammers can open-source the code of their smart contract and make claims about their transparency while remaining certain that the vast majority of users will not have any hope of understanding the code they published.

"The price of cryptocurrency goes up"

Promises of wealth and success with guaranteed returns in spectacular proportions to the initial buy-in price are used to generate enthusiasm in new recruits in many pyramid schemes (for example Bitconnect and Onecoin). In a cryptocurrency pyramid scheme, victims may be enticed with claims about the spectacular returns found by some cryptocurrency investors. The promoters will highlight success stories and not disclose the volatility of the assets, risks involved, or many people who lose money. Legitimate projects will not make claims about the valuation of the underlying cryptocurrency itself, but rather focus on the function of the project's application.

Targeting of victims in developing countries

Promotion of cryptocurrency pyramid schemes can take advantage of the global nature of cryptocurrency payments to target an international pool of victims. We found that the promoters of the Forsage pyramid scheme actively promoted the scheme to victims in developing economies, including the Philippines and Nigeria.

3. Characteristics of Code

The ultimate source of truth for the actions taken by a smart contract would be its source code. If possible, the best way to identify whether a given smart contract is a pyramid scheme is to just audit the smart contract and see what it does. Unfortunately that is not practical in many situations, and it requires a practitioner skilled in smart contract code.

In some cases, the smart contract code may not be published. If the smart contract code is not published, you may use a decompiler to try to recover the code, or you may monitor the flow of payments and observe that most of the payments funnel up to older users in a pyramid-like fashion.

Auditing the smart contract code itself is much easier by comparison, so if you are lucky enough to have access to a smart contract's code or some decompiled version of the code, keep these ideas in mind when looking at a smart contract for potential tomfoolery:

Registration function

If the entry to the smart contract is one called "register," "signup," "recruit," or something similar, that may be a bad sign, particularly if it's the only callable function, or there are no other meaningful functions. Legitimate applications will take actions and offer some service, so they will likely have a number of state changing functions. Pyramid schemes, by contrast, only exist as a means to funnel money from new participants to old participants, so the only state changing function will be one to recruit new victims into the pyramid.

For instance, in the original Forsage smart contract, the only two functions that were exposed that actually changed the state of the smart contract were called "registrationExt" and "buyNewLevel" — both of which are clearly things that happen in pyramid schemes (that have levels, in a pyramid structure), not legitimate financial applications.

Data structures

Look for data structures that record who participants should pay in the system: "uplines". You might see an array of addresses that maps new users to the target of who should be paid when new registrants enter the system. In Forsage this array was a very complicated set of data structures that would be changed every time a new user registered, and they were called "x3Matrix" and "x6Matrix" — Forsage called the levels of their pyramid matrices.

Look for pyramid scheme jargon in the public codebase. All of the following words could be found in the Forsage codebase that would be associated with a contract devoted to funneling money: "referrer" "matrix" "register" "level" "receiver" "reinvest" "dividends." Again, these jargons may not be exclusive to smart contract pyramid schemes, but with multiple red flags, you may identify one.

Conclusion:

Scammers are utilizing advances in technology, specifically blockchain technology like cryptocurrency and smart contracts, to run international pyramid schemes. We gathered red flags that can be useful in determining if a project may be a pyramid scheme rather than a legitimate blockchain-based application. These warning signs include the language used to describe the project, the way in which it is promoted, and the code that underlies it. For an in-depth look at a specific, currently active scheme, see our paper, "Forsage: Anatomy of a Smart-Contract Pyramid Scheme."