

# Deposit to earn rewards



Sign up and deposit to receive up to **17,500 USDT** in bonuses.  
Exclusive for new users only.

Get it now

## Forsage Scam: How to Prevent Forsage Smart Contract Pyramid Schemes?

Original:

<https://www.btcc.com/en-US/academy/research-analysis/forsage-scam-how-to-prevent-forsage-smart-contract-pyramid-schemes>

Eleven people were accused by the U.S. Securities and Exchange Commission (SEC) for their roles in developing and promoting [Forsage](#), the largest and longest-running smart contract-based pyramid scam in history.

Unfortunately, Forsage's alleged ringleader, Lado Okhotnikov, who was last seen in the Republic of Georgia, is still at large. Even though the original Forsage smart contracts have lost much of their appeal, they are still accepting investments, SEC or no SEC.

Preying on the weak and defenseless, Okhotnikov and others like him run smart contract pyramid schemes. How can we strengthen our defenses against them?

### What is Smart Contract Pyramids?

Investment returns in a pyramid scheme are generated by the funds or fees contributed by new investors. They can't last forever because there are a finite number of potential new investors.

In certain ways, a smart contract is ideal for managing a pyramid scheme. The entire back office structure can be automated using code, which makes administration easy for the scammer. Because it is done by code rather than by hand, the pyramid can be promoted as a "honest" Ponzi that is guaranteed to function correctly at all times.

In addition, users have the theoretical ability to perform an audit of this code as it is available to the public.

The perpetrator of a smart contract pyramid scheme can be more anonymous than in a typical pyramid scheme. And although the authorities can shut down a typical pyramid by visiting the office out of which it works, creating it on Ethereum makes it much tougher to stop.

Smart contract pyramids eventually became endemic to Ethereum. A 2019 investigation by a group of Italian researchers cataloged 184 smart contract pyramids in action at the time.

Smallness characterizes the vast majority of these. Forsage, written by Lado Okhotnikov, was the game-changer. In 2020, about \$240 million in transactions would be processed by Forsage's first Ethereum smart contract, x3/x4. At one point, it was second only to the tether contract in terms of activity on Ethereum.

By increasing the price of using Ethereum's gas, Okhotnikov and others like him, who are accused of running pyramid schemes, would be forced to seek refuge on alternative blockchains with lower transaction costs. Okhotnikov established five further Tron and Binance Smart Chain blockchain-based smart contract Ponzi schemes during the subsequent years. Since the introduction of level 2 blockchain systems, or subsidiary blockchains, which have reduced fees, fraudsters have been returning to Ethereum. Okhotnikov has established his newest pyramid, called Meta Force, on the Polygon Network.



[Download App for Android](#)

[Download App for iOS](#)

## A Examination of Forsage

After that, Okhotnikov created another pyramid scheme called Ethereum xGold, which the SEC discovered had been programmed to siphon off some investor money to a wallet that didn't have a matching Forsage ID. This ran counter to what Okhotnikov had said, which was that all money had been returned to investors. Over a thousand ether have been stolen from that address by 2022.

With an astounding 88% failure rate, Meiklejohn et al. report that 1 million Forsage accounts ultimately lost money. Half of all revenue was generated by the top 1,000 users.

Okhotnikov and his cofounders benefited by staking claim to the pinnacle of the organization. According to Meiklejohn et al., the SEC claims they controlled the top five positions in an x3/x4 Forsage pyramid with earnings of 5409 ether (ETH), or more than \$1 million.

Okhotnikov and his associates promoted their schemes extensively across multiple social media platforms. More than 47,000 people have subscribed to Forsage's official YouTube channel since it began focusing on the new Meta Force pyramid. The most watched Forsage video to date has been watched 384,000 times and is in Hindi. This occurs despite the fact that promoting pyramid schemes is explicitly forbidden under YouTube's TOS.

Meiklejohn and her coworkers found that most Forsage victims were located in developing countries including Nigeria, the Philippines, and Venezuela in their paper. This exposes the supposed frauds for what they really are: a means for the wealthy to prey on the weak and defenseless. They must be halted. Nonetheless, how?

## What Can Do to Prevent the Scam?

Since smart contract pyramids are based on immutable distributed ledgers that are immune to censorship, they cannot be targeted at their core or rendered useless by being removed from the

monetary system.

Lex Sokolin, in an article for CoinDesk, has advocated for “white hat” hackers to band together to find flaws in smart contract pyramids and bring them crashing down. It’s an appealing concept, but up to this point, white hat hackers haven’t showed much enthusiasm for hunting pyramids.

Reputational attacks on smart contract Ponzi schemes could be the most effective kind of damage limitation. The charges from the SEC will be helpful in this regard. A potential victim can now consult the opinion of the largest securities regulator in the world when looking into Okhotnikov or one of his “investment” items.

Fortunately, it appears that the SEC’s efforts have paid off. With charges brought against Okhotnikov, the rate of deposits to his newest (alleged) scam, Meta Force, which has already attracted \$42 million, began to decline the following day. A shaken Lado Okhotnikov responded to the SEC’s accusations with slander and defamation on YouTube.

Nonetheless, we needed the SEC to launch its assault far earlier. Securities regulators in Montana and the Philippines both published cease and desist orders early on, which may have prevented some of the damage that might have been done by Okhotnikov’s alleged scams.

There is a clear opportunity for regulators like the SEC to benefit from the openness of blockchain technology. These can be detected as they emerge and their growth tracked, allowing authorities to swiftly put together response teams to deal with them.

Similarly, the SEC could use some like-for-like combat. Internet-based, or “smart,” contract YouTube videos are being used in Ponzi schemes because of their wide audience. Unfortunately, you won’t be able to find the SEC’s charges on YouTube. More people would be likely to learn about Forsage if there was an entertaining film about it, rather than just a curt tweet.

Last but not least, when smart contract Ponzis emerge, prominent blockchain figures like Ethereum’s co-founder Vitalik Buterin and Binance’s CEO Changpeng Zhao should speak out against them. Perhaps they feel that acknowledging the issue would bring unwanted attention to the technology, and hence they would rather not do so. In any case, eliminating these scams as soon as feasible would not only decrease damage to innocent people, but will also limit damage to the long-term reputation of blockchains.