Smart Contract or Scam Contract? - Ftcyber.com Points Out the Red Flags

When you see the word 'smart contract' in a whitepaper, you should read it as a 'one-way contract' favoring the other party.

BERLIN, GERMANY, September 14, 2022 /EINPresswire.com/ -- According to CheckPoint Research (https://research.checkpoint.com/2022/scammers-are-creating-new-fraudulent-crypto-tokens-and-misconfiguring-smart-contracts-to-steal-funds/), many scammers manipulate tokens' smart contracts — contracts that exist and run automatically as code on the blockchain. Because they are stored on a blockchain, they are public, meaning that anyone can see the terms of the contract and know exactly how it's executed.

> It won't be long before SmartRegulators and SmartLawyers launch SmartLawsuits to notable exchanges", says Timothy Benson, head of investigations at FTCyber"
>
> *Timothy Benson*

Generally, it is misunderstood as a fool-proof contract because it is executed automatically. People don't realize that the automatic execution of contracts at the click of a button can be disastrous. This is especially true if one has put their life savings on the other side of the contract and the counterparty is anonymous. According to recent scam victims, this scenario is what FTCyber.com has found to be the latest wave.

The risks of scam contracts

When investing in cryptocurrency, there's always a risk that anyone could end up being scammed. This is especially true regarding smart contracts, self-executing contracts that live on the blockchain. Because of their nature, it's nearly impossible to alter the smart contract agreement once they've been created. This immutability has been touted as the next great feature for investors. The fact remains that they make a ripe environment for scammers with little upside.

"When you see the word 'smart contract' in a whitepaper, you should read it as a 'one-way contract' favoring the other party. You can also infer that it includes an automatic hand into the contents of your wallet. Would you want a smart contract with your landlord?" asks Timothy

Benson of FTCyber's investigative team.

The most common scams that fall under this category are -

Play-to-Earn (P2E) Smart Contract Games: These games seem like a simple way to make money while enjoying oneself in a casual game. People don't realize the volume of complaints FTCyber and other authorities worldwide are receiving regarding these games. At the click of a button, many people are connecting scammers of P2E games with unlimited access to their wallets. "Playing P2E games is analogous to giving street hustlers the keys to your safe and leaving the room. The volume and scale of scams from these smart contracts are huge. When we track money for our client wallets, we see massive movements of funds being siphoned away to notable players in cryptocurrency.

It won't be long before SmartRegulators and SmartLawyers launch SmartLawsuits to notable exchanges", says Timothy Benson, head of investigations at FTCyber.

Ponzi schemes: A Ponzi scheme is a type of fraud that promises investors high returns in exchange for investment. The problem is that these returns are generated by money from new investors rather than from any actual profit-making activity. Eventually, the scheme will collapse when no new investors are left to provide funds.

Pyramid schemes: Pyramid schemes are similar to Ponzi schemes in that they promise high returns but differ in how they generate those returns. In a pyramid scheme, participants recruit new members into the scheme, who then pay fees to those who recruited them. These fees create the appearance of profits when there is no actual business activity taking place.

Exit scams: An exit scam is when a project team abandons its project and takes all the invested funds. This often happens after an ICO (initial coin offering), when the team behind a project raises money by selling tokens or coins to investors. Once they have raised enough money, they disappear and leave investors with nothing.

Fake ICOs: A fake ICO is another type of scam where false promises of high returns lure investors. In reality, no product or service is being offered, and the only thing investors will end up with is worthless tokens or coins.

Tips on approaching smart contracts

When approaching smart contracts, be sure to consider the following:

Never enter into a smart contract without an audit.
Never believe in no-risk or guaranteed returns.
Approach abstruse smart contracts with extreme caution and distrust; this is a one-sided

agreement. Unless you are sure of the entities in the contract, the addresses are likely anonymous until revealed by FTCyber or law enforcement. Don't take chances.
Never enter into contracts with anonymous or undisclosed entities. Better alone than in bad company.
Never sign a message with a private key as part of joining the contract.
It is important to research and never trust or rely on what is printed in a whitepaper or article. Smart contracts do not legitimize a project but increase risks to the investor.

How can a fund recovery company help in Smart Contracts scams?

The fund recovery process is the best way to help victims get their money back if they have been scammed in this way. These services work by tracking down the hackers and then demanding that they return the money that they have stolen. In many cases, the hackers will agree to this demand because they do not want to risk being caught and arrested. This means that victims can get their money back without going through the legal process."

Apart from this, there are many benefits of using a fund recovery service for Ethereum giveaway scams. First of all, it helps victims to recover stolen funds quickly and without any hassle. Secondly, it puts an end to the fraud, which means that other people will not be scammed in the same way. Finally, it helps to deter future scams by sending a message to the hackers that they will not be able to get away with their crimes.

Peter Thompson
FTCyber.com
+1 917-463-3216
email us here
