Behind A Crypto Scam Case

Extract Information About Ponzi Schema With OSINT Methods

HADESS

WWW.HADESS.IO

TABLE OF CONTENTS

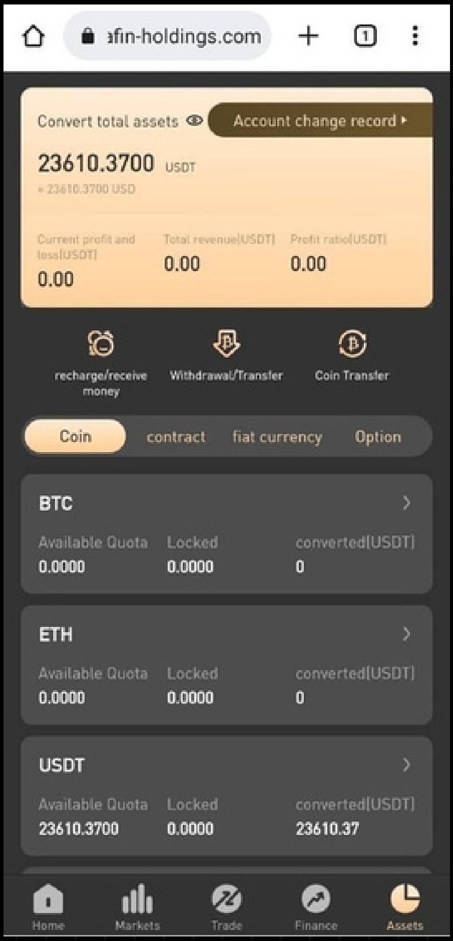
FOREWARD

Scams and fraudulent activities have been prevalent throughout human history, and with the advent of the internet and digital technologies, these scams have taken on new forms and have become even more sophisticated. To combat these scams, it's important to use a variety of techniques and tools to uncover the individuals and organizations behind them. One such technique is Open Source Intelligence (OSINT), which involves gathering and analyzing publicly available information from various sources.

In this guide, we will explore how to use OSINT methods to find the individuals or organizations behind a scam scenario. We will cover various sources of information, including social media, online forums, and blockchain explorers, and we will provide step-by-step instructions on how to use these sources to gather and analyze information. We will also discuss the importance of verifying the authenticity of the information and the potential legal and ethical considerations involved in conducting OSINT investigations.

By using these OSINT methods, we can shine a light on the individuals and organizations behind scams, and help protect ourselves and others from falling victim to their fraudulent activities. Let's get started.

Case Review



Convert total assets

23610.3700 USDT

≈ 23610.3700 USD

Current profit and loss[USDT]	Total revenue[USDT]	Profit ratio[USDT]
0.00	0.00	0.00

BTC

Available Quota	Locked	converted[USDT]
0.0000	0.0000	0

ETH

Available Quota	Locked	converted[USDT]
0.0000	0.0000	0

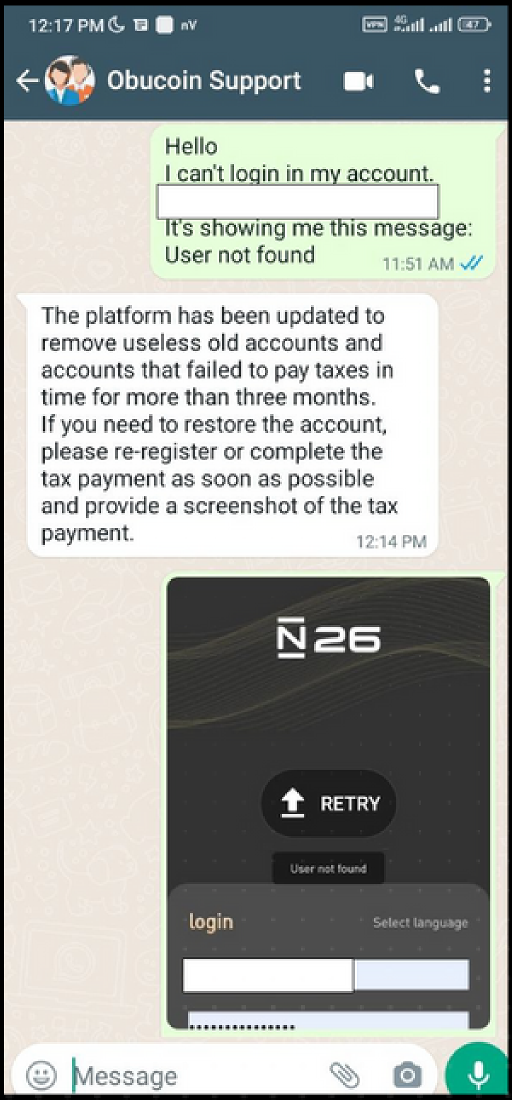
USDT

Available Quota	Locked	converted[USDT]
23610.3700	0.0000	23610.37

Integrafin Holdings is a fake crypto site that lures people into depositing funds with the promise of huge profits before scamming victims out of their crypto.

Would-be investors are contacted through platforms such as WhatsApp and Telegram and persuaded to create an account on the site and deposit the USDT stablecoin

However, once the alleged profits start to stack up and the victim comes to withdraw their funds they're told they need to pay a 'commission' or 'release fee' to do so.

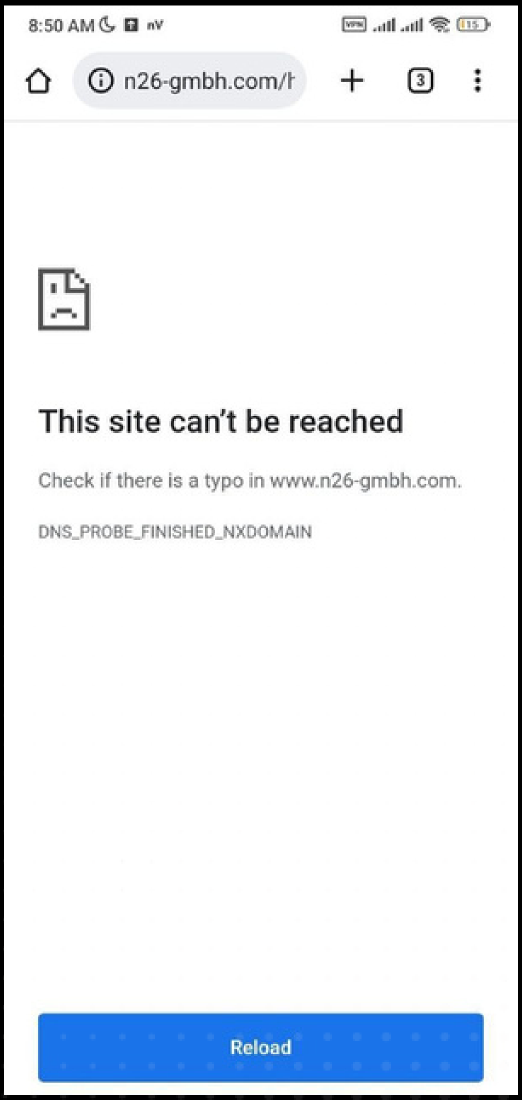


12:17 PM

Obucoin Support

Hello
I can't login in my account.
It's showing me this message:
User not found 11:51 AM

The platform has been updated to remove useless old accounts and accounts that failed to pay taxes in time for more than three months.
If you need to restore the account, please re-register or complete the tax payment as soon as possible and provide a screenshot of the tax payment. 12:14 PM



8:50 AM

n26-gmbh.com/t

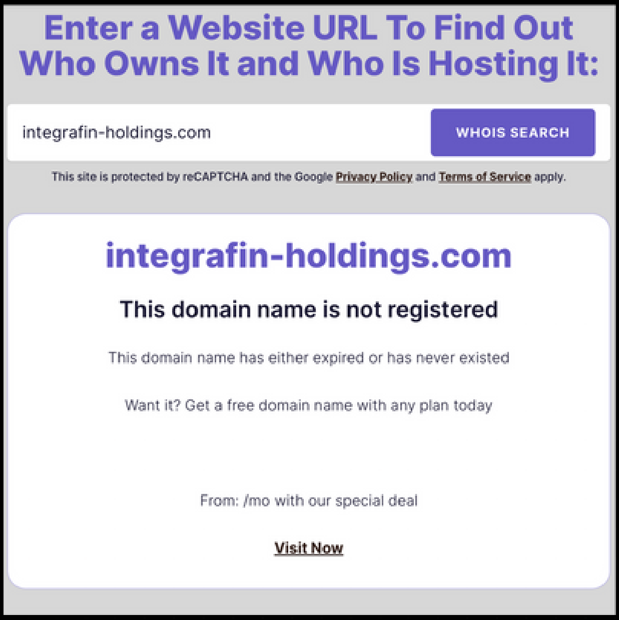
This site can't be reached

Check if there is a typo in www.n26-gmbh.com.

DNS_PROBE_FINISHED_NXDOMAIN

Integrafin-holdings.com

https://digital.com/best-web-hosting/who-is/#search=integrafin-holdings.com



Enter a Website URL To Find Out Who Owns It and Who Is Hosting It:

integrafin-holdings.com

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

integrafin-holdings.com

This domain name is not registered

This domain name has either expired or has never existed

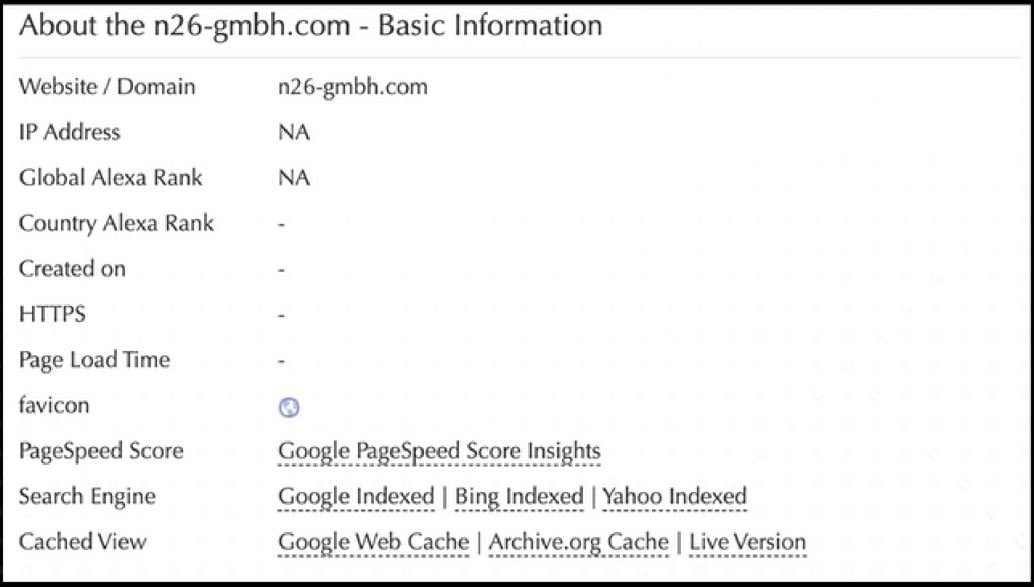
Want it? Get a free domain name with any plan today

From: /mo with our special deal

Visit Now

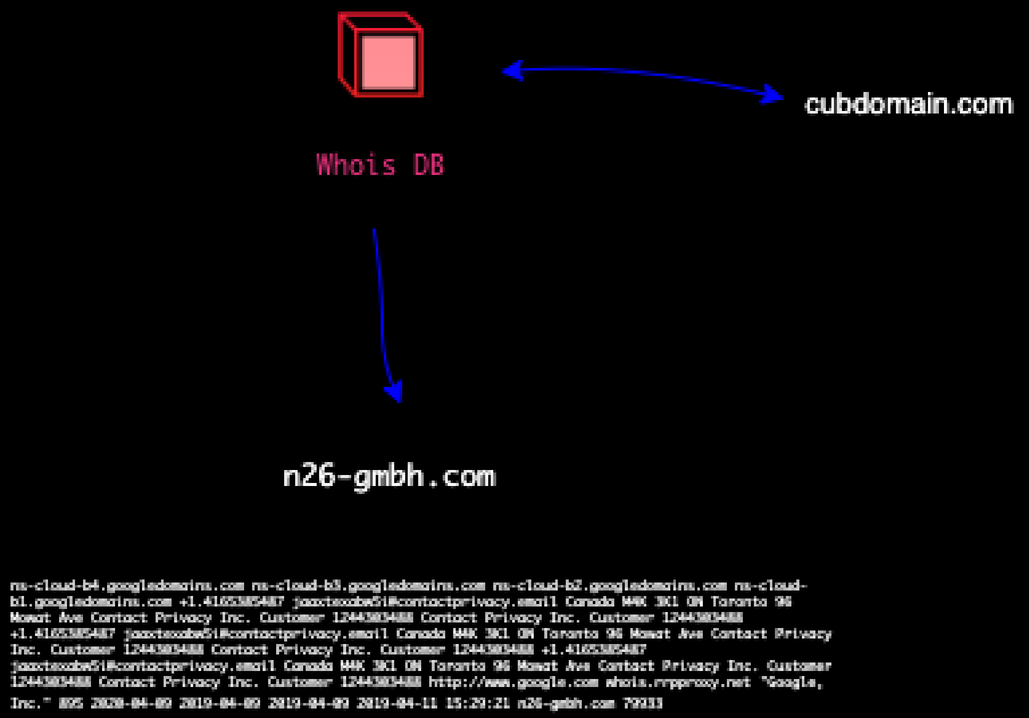
https://www.cubdomain.com/domains-registered-by-date/2019-04-11/16

https://www.cubdomain.com/site/n26-gmbh.com



About the n26-gmbh.com - Basic Information

Website / Domain	n26-gmbh.com
IP Address	NA
Global Alexa Rank	NA
Country Alexa Rank	-
Created on	-
HTTPS	-
Page Load Time	-
favicon	🌐
PageSpeed Score	Google PageSpeed Score Insights
Search Engine	Google Indexed | Bing Indexed | Yahoo Indexed
Cached View	Google Web Cache | Archive.org Cache | Live Version

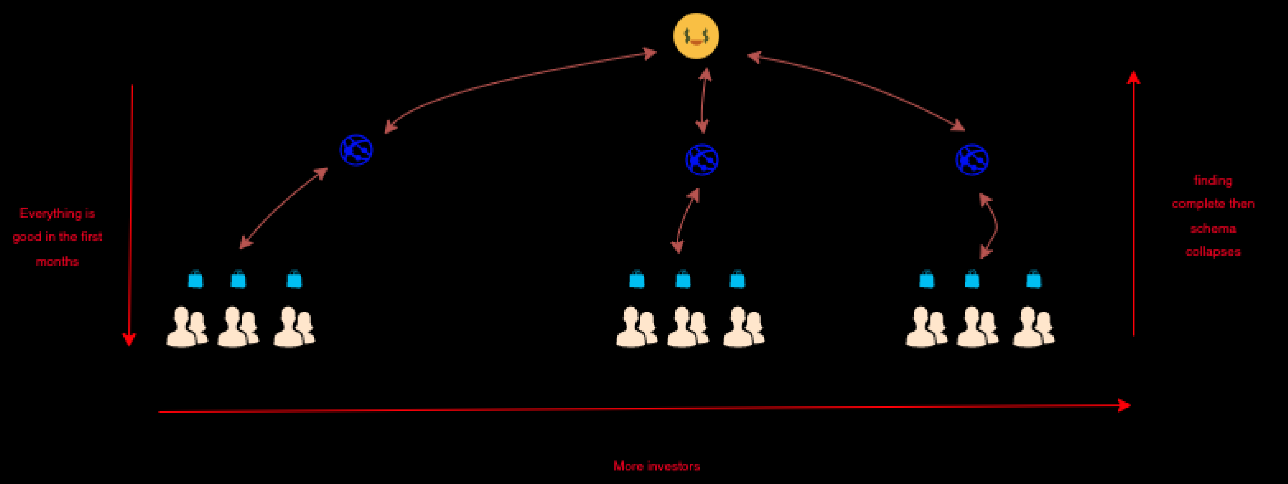


```
ns-cloud-b4.googledomains.com ns-cloud-b3.googledomains.com ns-cloud-b2.googledomains.com ns-cloud-
b1.googledomains.com +1.4165385487 jaaxtexabw5i@contactprivacy.email Canada M4K 3K1 ON Toronto 96
Mowat Ave Contact Privacy Inc. Customer 1244303488 Contact Privacy Inc. Customer 1244303488
+1.4165385487 jaaxtexabw5i@contactprivacy.email Canada M4K 3K1 ON Toronto 96 Mowat Ave Contact Privacy
Inc. Customer 1244303488 Contact Privacy Inc. Customer 1244303488 +1.4165385487
jaaxtexabw5i@contactprivacy.email Canada M4K 3K1 ON Toronto 96 Mowat Ave Contact Privacy Inc. Customer
1244303488 Contact Privacy Inc. Customer 1244303488 http://www.google.com whois.rrpproxy.net "Google,
Inc." 895 2020-04-09 2019-04-09 2019-04-09 2019-04-11 15:29:21 n26-gmbh.com 79933
```

Whois/2019-04-11.zip/full-database.csv included breached whois record

79933 n26-gmbh.com 2019-04-11 15:29:21 2019-04-09 2019-04-09 2020-04-09 895 "Google, Inc." whois.rrpproxy.net http://www.google.com Contact Privacy Inc. Customer 1244303488 Contact Privacy Inc. Customer 1244303488 96 Mowat Ave Toronto ON M4K 3K1 Canada jaaxtexabw5i@contactprivacy.email +1.4165385487 Contact Privacy Inc. Customer 1244303488 Contact Privacy Inc. Customer 1244303488 96 Mowat Ave Toronto ON M4K 3K1 Canada jaaxtexabw5i@contactprivacy.email +1.4165385487 Contact Privacy Inc. Customer 1244303488 Contact Privacy Inc. Customer 1244303488 96 Mowat Ave Toronto ON M4K 3K1 Canada jaaxtexabw5i@contactprivacy.email +1.4165385487   ns-cloud-b1.googledomains.com ns-cloud-b2.googledomains.com ns-cloud-b3.googledomains.com ns-cloud-b4.googledomains.com clientTransferProhibited

Ponzi


Everything is good in the first months
finding complete then schema collapses
More investors

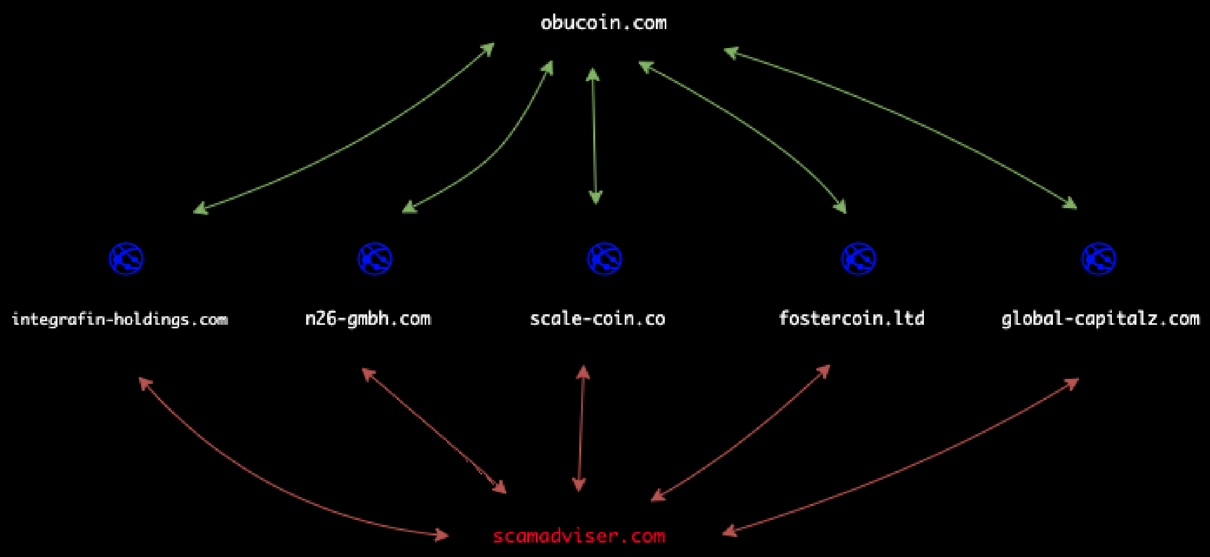
A Ponzi scheme is a fraudulent investment scheme in which returns are paid to earlier investors using the capital provided by newer investors, rather than from profits earned through legitimate business activities. The scheme relies on the constant recruitment of new investors to pay off the returns promised to earlier investors.

The fraudster behind the Ponzi scheme typically promises high returns in a short period of time, often with little or no risk. They may use tactics such as fancy brochures, websites, or presentations to lure in potential investors. Once investors start to receive returns on their investment, they may be encouraged to invest even more money, and may even be incentivized to recruit others to invest in the scheme.

However, as more and more investors join the scheme, it becomes increasingly difficult for the fraudster to keep up with the promised returns. Eventually, the scheme will collapse when there are not enough new investors to pay off the returns promised to earlier investors, and many people will lose their money.

Ponzi schemes are illegal in most countries, and those who run them can face criminal charges and significant fines. It's important to be cautious and do your due diligence before investing in any opportunity that promises high returns with little or no risk.

check with scamadviser.com:



Fake Bitcoin Transaction

A fake Bitcoin transaction is a type of scam in which someone pretends to send Bitcoin to another person, but in reality, no actual Bitcoin is sent or received. This scam is often used to trick people into sending money or goods before they receive the promised Bitcoin payment.

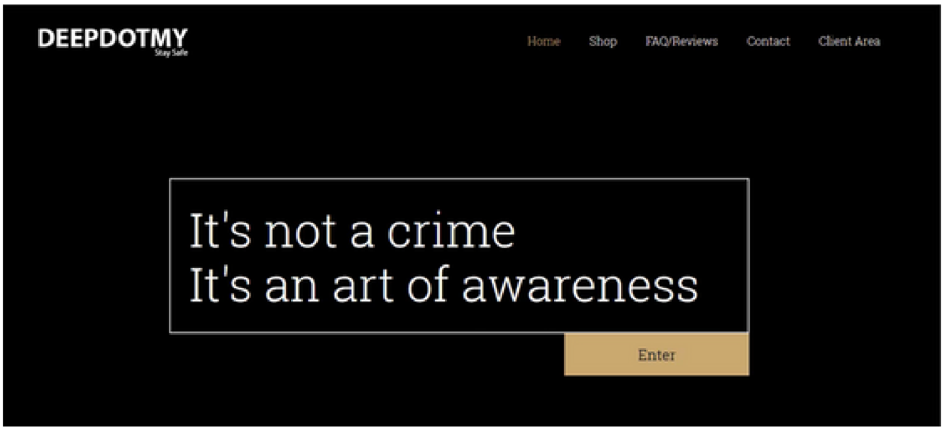
In a fake Bitcoin transaction, the scammer typically creates a fake transaction record using a blockchain explorer or other tool that allows them to manipulate the transaction data. They may alter the sender or recipient address, the amount of Bitcoin sent, or other details of the transaction to make it appear as though Bitcoin has been sent from one address to another.

The scammer may then send a screenshot or other proof of the fake transaction to the victim, along with instructions on how to send the promised Bitcoin payment. Once the victim sends the payment, the scammer disappears, leaving the victim with no way to recover their lost Bitcoin or money.

To create a fake Bitcoin transaction, a scammer may use a tool such as a blockchain explorer or a software program that allows them to modify the transaction data before it is broadcast to the network. They may alter the recipient address, the amount of Bitcoin being sent, or other details of the transaction in such a way as to make it appear legitimate.

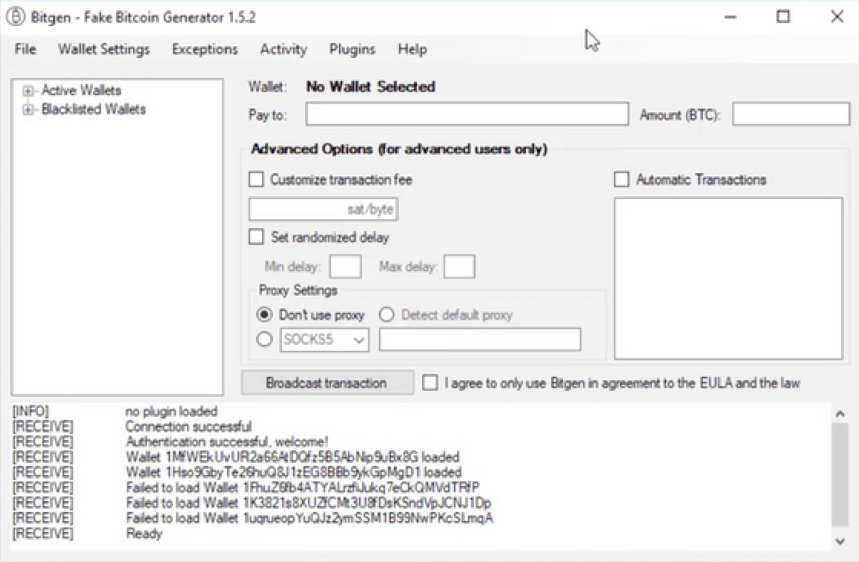
Popular seller:

Price: 500 GBP



DEEPDOTMY
Stay Safe

It's not a crime
It's an art of awareness



Bitgen - Fake Bitcoin Generator 1.5.2

Wallet: No Wallet Selected

Pay to:

Amount (BTC):

Advanced Options (for advanced users only)

□ Customize transaction fee

sat/byte

□ Set randomized delay

Min delay: Max delay:

□ Automatic Transactions

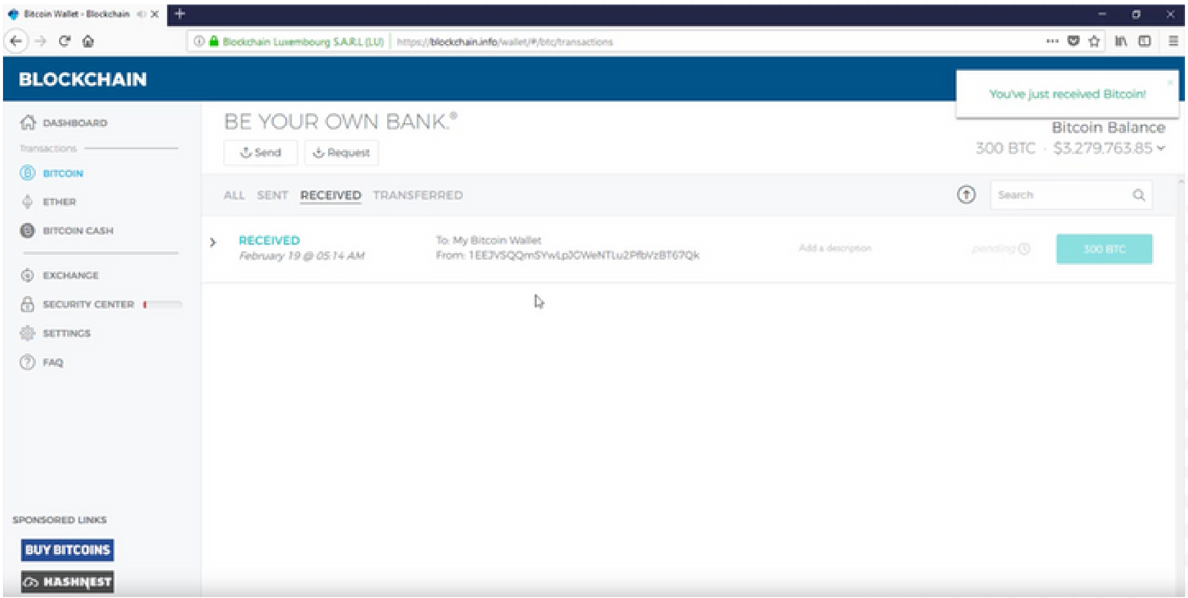
Proxy Settings

● Don't use proxy ○ Detect default proxy

○ SOCKS5

□ I agree to only use Bitgen in agreement to the EULA and the law

```
[INFO]          no plugin loaded
[RECEIVE]       Connection successful
[RECEIVE]       Authentication successful, welcome!
[RECEIVE]       Wallet 1MfWEkUvUR2a66AtDQfz5B5AbNip9uBx8G loaded
[RECEIVE]       Wallet 1Hso9GbyTe26huQ8J1zEG8BBb9ykGpMgD1 loaded
[RECEIVE]       Failed to load Wallet 1FhuZ6fb4ATYALrzfiJukq7eCkQMVdTRfP
[RECEIVE]       Failed to load Wallet 1K3821s8XUZfCMt3U8fDsKSndVpJCNJ1Dp
[RECEIVE]       Failed to load Wallet 1uqrueopYuQJz2ymSSM1B99NwPKcSLmqA
[RECEIVE]       Ready
```



Bitcoin Wallet - Blockchain

Blockchain Luxembourg S.A.R.L (LU) https://blockchain.info/wallet/#/btc/transactions

BLOCKCHAIN

You've just received Bitcoin!

BE YOUR OWN BANK.®

Bitcoin Balance
300 BTC · $3,279,763.85

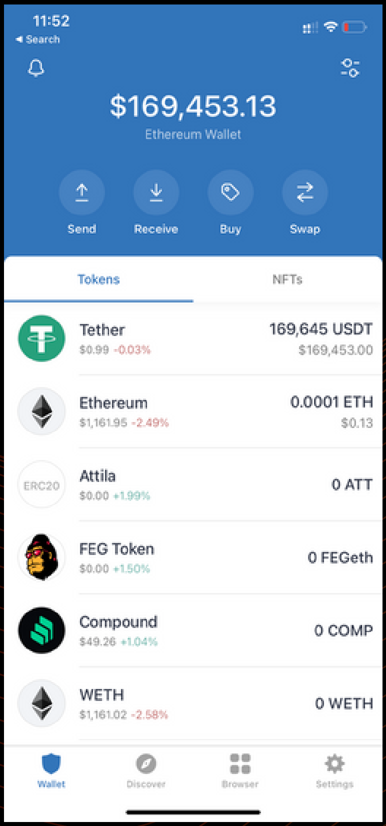
RECEIVED
February 19 @ 05:14 AM
To: My Bitcoin Wallet
From: 1EEJVSQQmSYwLpJGWeNTLu2PfbVzBT67Qk
Add a description
pending
300 BTC

Scam Smart Contract

A scam smart contract is a type of fraudulent code that is deployed on a blockchain platform, such as Ethereum. The code is designed to trick users into sending cryptocurrency to the contract address, with the promise of receiving a greater amount of cryptocurrency in return. However, the contract is programmed to execute in such a way that the scammer ends up with all the cryptocurrency, leaving the victim with nothing.

There are several types of scam smart contracts, including:

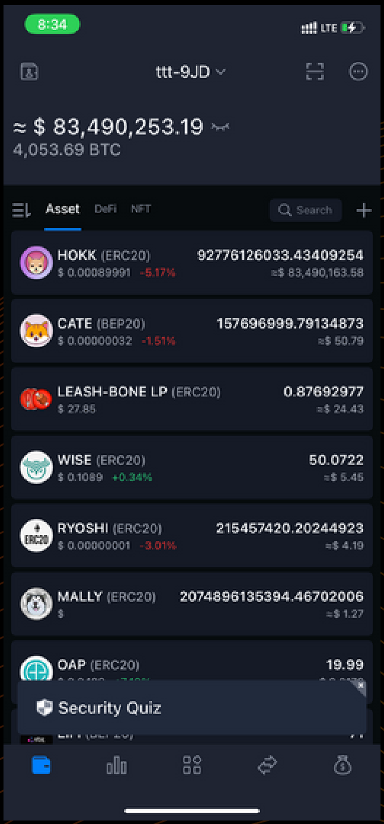
1. Ponzi schemes: These contracts promise high returns to early investors by paying them out of the funds invested by later investors. However, the contract eventually collapses when there are not enough new investors to pay off earlier investors, and most people end up losing their money.
2. Fake ICOs: Scammers may create smart contracts that appear to be associated with a legitimate Initial Coin Offering (ICO), but are actually designed to steal funds from unsuspecting investors. The scammers may use fake websites, social media accounts, and whitepapers to make the ICO appear legitimate, but in reality, the funds are being sent directly to the scammer's wallet.
3. Token scams: Scammers may create smart contracts that claim to offer a new cryptocurrency or token that is guaranteed to increase in value. However, in most cases, the tokens are worthless and the scammer simply takes the investor's money.
4. Phishing scams: Scammers may create smart contracts that mimic legitimate contracts in order to trick users into sending their cryptocurrency to the wrong address. They may use social engineering tactics to convince users to click on a link or download a file that contains the scam contract.



11:52
◂ Search

$169,453.13
Ethereum Wallet

Tether $0.99 -0.03% 169,645 USDT $169,453.00
Ethereum $1,161.95 -2.49% 0.0001 ETH $0.13
Attila $0.00 +1.99% 0 ATT
FEG Token $0.00 +1.50% 0 FEGeth
Compound $49.26 +1.04% 0 COMP
WETH $1,161.02 -2.58% 0 WETH

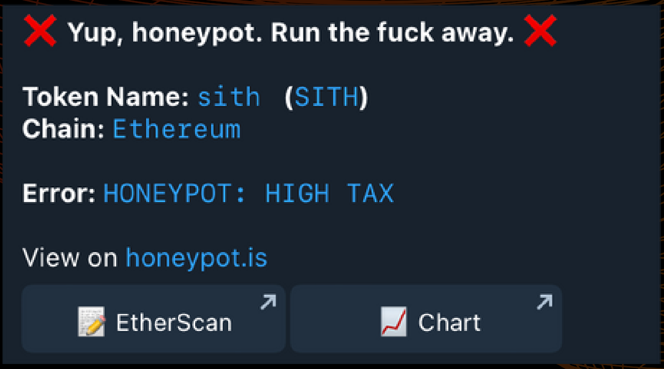


8:34
ttt-9JD

≈ $ 83,490,253.19
4,053.69 BTC

HOKK (ERC20) $ 0.00089991 -5.17% 92776126033.43409254 ≈$ 83,490,163.58
CATE (BEP20) $ 0.00000032 -1.51% 157696999.79134873 ≈$ 50.79
LEASH-BONE LP (ERC20) $ 27.85 0.87692977 ≈$ 24.43
WISE (ERC20) $ 0.1089 +0.34% 50.0722 ≈$ 5.45
RYOSHI (ERC20) $ 0.00000001 -3.01% 215457420.20244923 ≈$ 4.19
MALLY (ERC20) $ 2074896135394.46702006 ≈$ 1.27
OAP (ERC20) 19.99

https://t.me/honeypotis



❌ Yup, honeypot. Run the fuck away. ❌

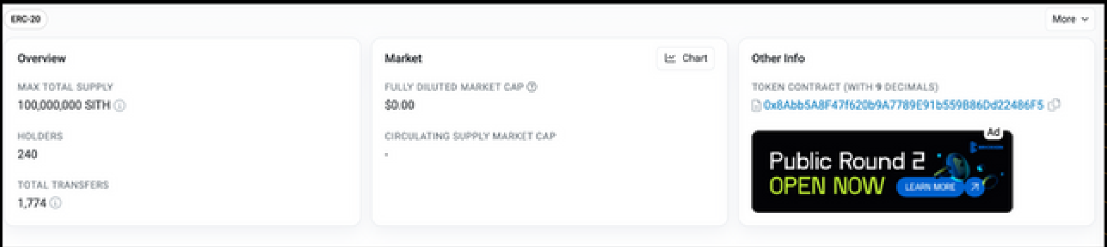
Token Name: sith (SITH)
Chain: Ethereum

Error: HONEYPOT: HIGH TAX

View on honeypot.is

Token Contract

https://etherscan.io/token/0x8Abb5A8F47f620b9A7789E91b559B86Dd22486F5



ERC-20

More

Overview

MAX TOTAL SUPPLY
100,000,000 SITH

HOLDERS
240

TOTAL TRANSFERS
1,774

Market

Chart

FULLY DILUTED MARKET CAP
$0.00

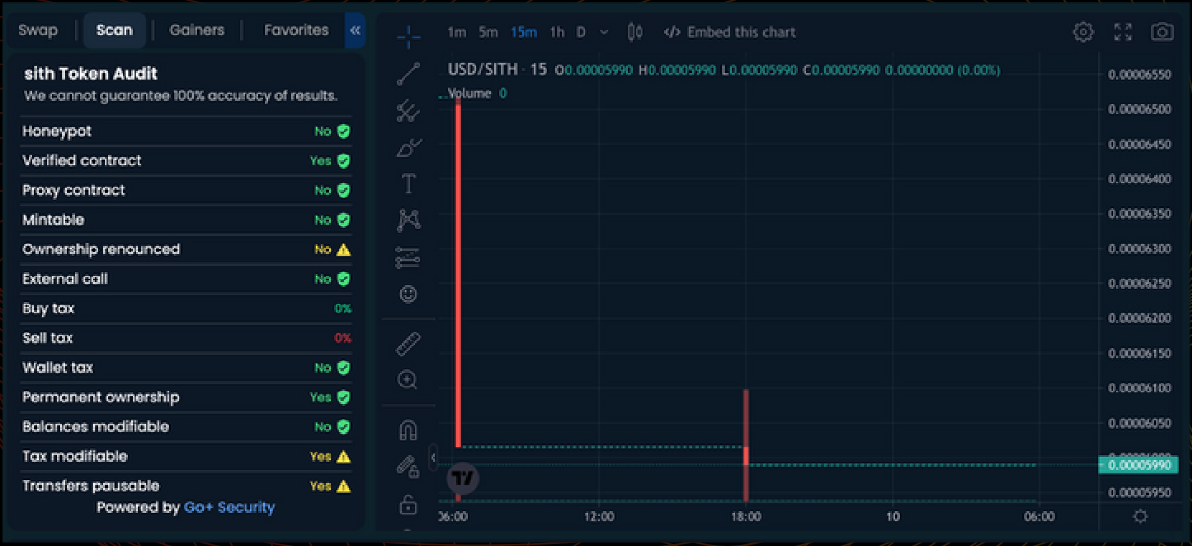
CIRCULATING SUPPLY MARKET CAP
-

Other Info

TOKEN CONTRACT (WITH 9 DECIMALS)
0x8Abb5A8F47f620b9A7789E91b559B86Dd22486F5

sith Token Audit

https://dexcheck.io/app/eth/chart/0x610eb827e7677d8b71a1a240b931d675386b76ca



USD/SITH · 15 O0.00005990 H0.00005990 L0.00005990 C0.00005990 0.00000000 (0.00%)

sith Token Audit

We cannot guarantee 100% accuracy of results.

Honeypot	No ✓
Verified contract	Yes ✓
Proxy contract	No ✓
Mintable	No ✓
Ownership renounced	No ⚠
External call	No ✓
Buy tax	0%
Sell tax	0%
Wallet tax	No ✓
Permanent ownership	Yes ✓
Balances modifiable	No ✓
Tax modifiable	Yes ⚠
Transfers pausable	Yes ⚠

Powered by Go+ Security

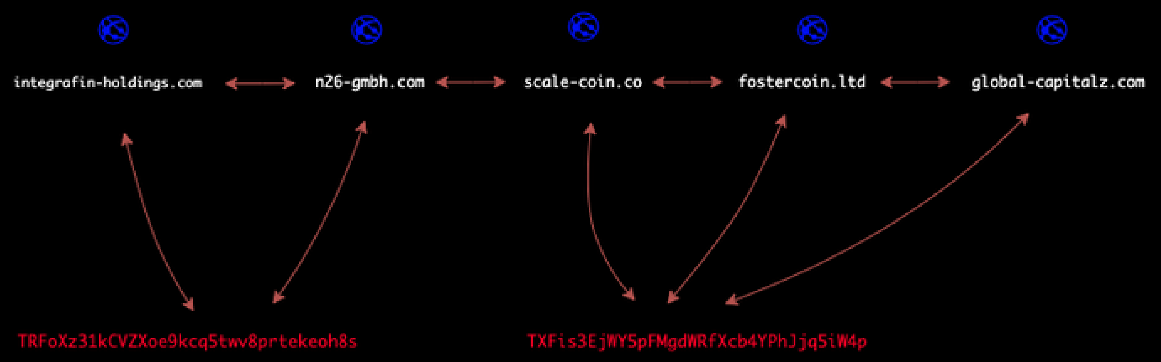
Contract Source Code

In this contract, the owner can set the tax fee, which is a percentage of the value sent to the payTax() function. The contract automatically deducts the tax fee from the amount sent and sends it to the owner's address. The amount of tax collected is tracked in the totalCollected variable.

The owner can also withdraw the tax collected by calling the withdrawTax() function, which sends the entire amount collected to the owner's address.

```
pragma solidity ^0.8.0;

contract AutoWithdrawTax {
  address public owner;
  uint256 public taxFee;
  uint256 public totalCollected;

  constructor(uint256 _taxFee) {
    owner = msg.sender;
    taxFee = _taxFee;
  }

  function payTax() public payable {
    uint256 fee = msg.value * taxFee / 100;
    uint256 amount = msg.value - fee;
    totalCollected += fee;
    payable(owner).transfer(amount);
  }

  function setTaxFee(uint256 _taxFee) public {
    require(msg.sender == owner, "Only the owner can set the tax fee");
    taxFee = _taxFee;
  }

  function withdrawTax() public {
    require(msg.sender == owner, "Only the owner can withdraw the tax");
    uint256 amount = totalCollected;
    totalCollected = 0;
    payable(owner).transfer(amount);
  }
}
```

https://etherscan.io/address/0x8Abb5A8F47f620b9A7789E91b559B86Dd22486F5#code



Auto Checker + Auto Withdraw

"Auto checker" and "auto withdraw" are terms commonly used in cryptocurrency scams, particularly those involving phishing or fraudulently obtaining access to a user's cryptocurrency wallet.

In this context, "auto checker" refers to a software tool that is used to automatically monitor and scan a victim's cryptocurrency wallet or exchange account. The goal of the auto checker is to identify when the victim's wallet or exchange account has received a new deposit, allowing the scammer to quickly move in and steal the deposited cryptocurrency.

Similarly, "auto withdraw" refers to a software tool that is used to automatically transfer the stolen cryptocurrency out of the victim's wallet or exchange account and into the scammer's own wallet or exchange account.

Both of these tools are designed to automate the theft process and make it more efficient for the scammer. If you come across any offers or services that involve "auto checker" or "auto withdraw," it is likely a scam and should be avoided. It's always important to be cautious and do your research before trusting anyone with your cryptocurrency.

On of the famous software called “etherborrow”

https://medium.com/jelly-market/how-to-get-infura-api-key-e7d552dd396f

Infura is a web3 API service that provides a gateway to access Ethereum and IPFS networks. It allows developers to connect to Ethereum nodes without running their own node, providing a scalable and reliable infrastructure to build decentralized applications.

To use Infura to check a wallet balance in code, you will need to follow these steps:

1. Sign up for a free Infura account at https://infura.io/register.
2. Create a new project and generate an API key.
3. Install the web3.js library in your project by running npm install web3.
4. In your code, initialize a new web3 instance with the Infura endpoint URL and API key, like so:

```
const Web3 = require('web3');
const infuraEndpoint = 'https://mainnet.infura.io/v3/YOUR-PROJECT-ID';
const web3 = new Web3(new Web3.providers.HttpProvider(infuraEndpoint));
```

Replace YOUR-PROJECT-ID with your Infura project ID.

1. Use the web3.eth.getBalance() method to get the balance of a wallet address, like so:

```
const address = '0x123...'; // replace with the wallet address you want to check
web3.eth.getBalance(address, (error, balance) => {
  console.log(web3.utils.fromWei(balance, 'ether')); // convert balance from wei to ether and log to console
});
```

Replace 0x123... with the wallet address you want to check. The web3.utils.fromWei() method is used to convert the balance from wei to ether.

HADESS.IO