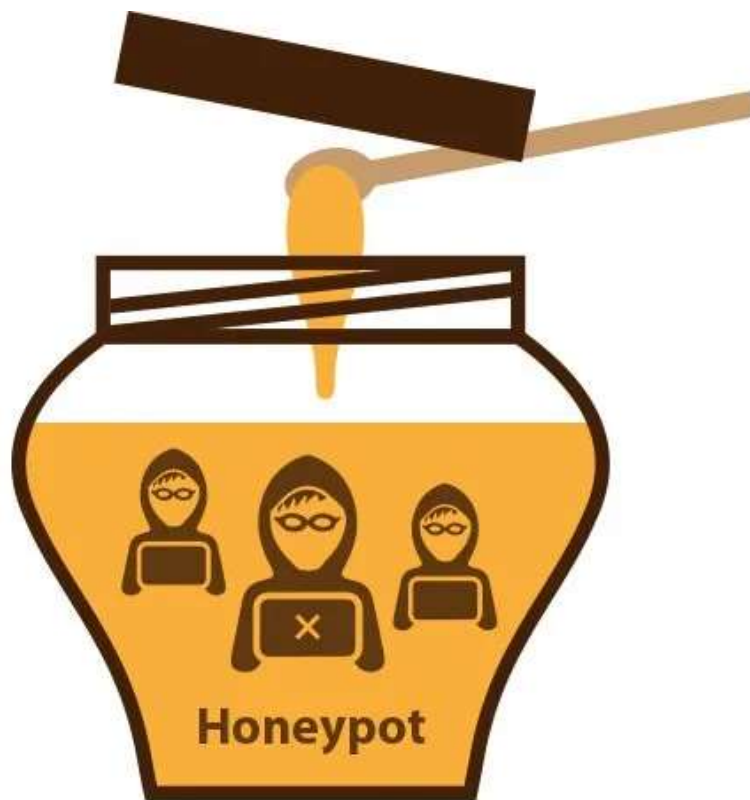


Ape in altcoins but fall into a honeypot. What you should pay attention to in the meme season?





Beosin · [Follow](#)

4 min read · May 10



Recently, the Meme coin fever has pumped various altcoins.

Unaware of what is going on, plenty of people aped in altcoins, but ended up in a honeypot scam and were unable to get their money back. The picture below is a recent victim of honeypot scams who sought help from Beosin.



This happens all the time, and for those who are in FOMO, it's time to calm down and raise your awareness of self-prevention. Let us debunk the tricks of honeypot scams for

you.

What is a honeypot

“Pixiu” is a mythical wild animal in ancient Chinese legend. It can swallow everything (mostly jewelry) and not discharge. So “honeypot”, also called “Pixiu Scam” in Chinese, is used to describe a token that can only be bought but not be sold. Because of the secrecy, even for experienced investors, it is not easy to identify a honeypot scam. Usually the price of a honeypot will rise rapidly. Therefore, people just ape in and are easily deceived. Once you bought it, it can hardly be sold.

Straying into honeypot, why users still increase their positions?

On April 25, 2023, Beosin EagleEye security risk monitoring, alerting and blocking platform found a **counterfeit fraudulent project with the same name as EDU**. The suspected fraudulent project contract address `0x4749a5f83F6F003440cB4B6aD1628d39E900Doc4`. Token owner `0xac150dfd7991622d9f89d505504c572c8eb2282b` buys and sells tokens in EDU pair `0xE3f26c1aDC28f9C85D4B8AB4a995637ad6684862` address and sends tokens to Binance hot wallets, **creating the illusion that there are many people involved (shown in the figure below)**.

 PancakeSwap V2: ED...	OUT	0xac150dfd7991622d...	2,295.08	 Binance-Peg ... (BSC-US...)
0xac150dfd7991622d...	IN	 PancakeSwap V2: ED...	13,986.353322687673635784	 BEP-20: Ope.....pus
 PancakeSwap V2: ED...	OUT	0xac150dfd7991622d...	3,791.03	 Binance-Peg ... (BSC-US...)
0xac150dfd7991622d...	IN	 PancakeSwap V2: ED...	462.171307528039109455	 BEP-20: Ope.....pus
 PancakeSwap V2: ED...	OUT	0xac150dfd7991622d...	129.07	 Binance-Peg ... (BSC-US...)
0xac150dfd7991622d...	IN	 PancakeSwap V2: ED...	2,620.93	 Binance-Peg ... (BSC-US...)
 PancakeSwap V2: ED...	OUT	0xac150dfd7991622d...	9,506.703647229805884449	 BEP-20: Ope.....pus
0xac150dfd7991622d...	IN	 PancakeSwap V2: ED...	2,885.22	 Binance-Peg ... (BSC-US...)
 PancakeSwap V2: ED...	OUT	0xac150dfd7991622d...	10,915.789329475979251736	 BEP-20: Ope.....pus
0xac150dfd7991622d...	IN	 PancakeSwap V2: ED...	973.63	 Binance-Peg ... (BSC-US...)
 PancakeSwap V2: ED...	OUT	0xac150dfd7991622d...	3,795.456646255896015538	 BEP-20: Ope.....pus
0xac150dfd7991622d...	IN	 PancakeSwap V2: ED...	574.243781343303112114	 BEP-20: Ope.....pus
 PancakeSwap V2: ED...	OUT	0xac150dfd7991622d...	145.48	 Binance-Peg ... (BSC-US...)
0xac150dfd7991622d...	IN	 PancakeSwap V2: ED...	11,796.246163211243784773	 BEP-20: Ope.....pus
 PancakeSwap V2: ED...	OUT	0xac150dfd7991622d...	3,064.37	 Binance-Peg ... (BSC-US...)
0xac150dfd7991622d...	IN	 PancakeSwap V2: ED...	13,235.062130239556601353	 BEP-20: Ope.....pus
 PancakeSwap V2: ED...	OUT	0xac150dfd7991622d...	3,619.5	 Binance-Peg ... (BSC-US...)
0xac150dfd7991622d...	IN	 PancakeSwap V2: ED...	1,934.69	 Binance-Peg ... (BSC-US...)

However, because the whitelist address status is not disclosed in the code, the switch function cannot be called twice, and the switch status and whitelist address are controlled by the owner. Users who participate in the project are not able to sell tokens in the default state.

```

92 - function transfer(address _to, uint256 _value) public returns (bool) {
93 -     if(!tokenWhitelist[msg.sender]&&!tokenWhitelist[_to]){
94 -         require(tokenBlacklist[msg.sender] == false);
95 -         require(tokenBlacklist[_to] == false);
96 -
97 -         require(tokenGreylist[msg.sender] == false);
98 -         // require(tokenGreylist[_to] == false);
99 -     }
100 -     if(msg.sender==LP&&ab&&!tokenWhitelist[_to]){
101 -         tokenGreylist[_to] = true;
102 -         emit Gerylist(_to, true);
103 -     }
104 -
105 -     require(_to != address(0));
106 -     require(_to != msg.sender);
107 -     require(_value <= balances[msg.sender]);
108 -     balances[msg.sender] = balances[msg.sender].sub(_value);
109 -     // SafeMath.sub will throw if there is not enough balance.
110 -     balances[_to] = balances[_to].add(_value);
111 -     emit Transfer(msg.sender, _to, _value);
112 -     return true;
113 - }
114 -
115 -
116 - function balanceOf(address _owner) public view returns (uint256 balance) {
117 -     return balances[_owner];
118 - }
119 -
120 - function transferFrom(address _from, address _to, uint256 _value) public returns (bool) {
121 -     if(!tokenWhitelist[_from]&&!tokenWhitelist[_to]){
122 -         require(tokenBlacklist[msg.sender] == false);
123 -         require(tokenBlacklist[_from] == false);
124 -         require(tokenBlacklist[_to] == false);
125 -
126 -         require(tokenGreylist[_from] == false);
127 -     }
128 -
129 -     if(_from==LP&&ab&&!tokenWhitelist[_to]){
130 -         tokenGreylist[_to] = true;
131 -         emit Gerylist(_to, true);
132 -     }
133 -     require(_to != _from);
134 -     require(_to != address(0));
135 -     require(_value <= balances[_from]);
136 -     require(_value <= allowed[_from][msg.sender]);
137 -     balances[_from] = balances[_from].sub(_value);
138 -
139 -
140 -     balances[_to] = balances[_to].add(_value);
141 -     allowed[_from][msg.sender] = allowed[_from][msg.sender].sub(_value);
142 -     emit Transfer(_from, _to, _value);
143 -     return true;
144 - }
145 -

```

At that time, this honeypot scam had already attracted a number of participants, and while Beosin security team was analyzing it, another poor person appeared and continued to buy another 100U, and withdrew 8 BNBs to buy more. At this time, our analysis teammate said, “I feel like he’s going to buy more. ”

Txn Hash	Method	Block	Age	From	To	Value	[Txn Fee]
0xcca8d8ab2dc86b2...	Multicall	27653446	51 secs ago	0xc9744af02e0b7410...	OUT	0.2 BNB	0.000756759
0x48821ca2a5b529cd...	Transfer	27653415	2 mins ago	Binance: Hot Wallet 10	IN	7.90800315 BNB	0.000126
0x3d9069de7a15bb7...	Multicall	27653252	10 mins ago	0xc9744af02e0b7410...	OUT	0.005 BNB	0.000756689
0x4a52e7909ebfc187...	Multicall	27653203	13 mins ago	0xc9744af02e0b7410...	OUT	0.333935919 BNB	0.000756837
0x1eb0e605291445c2...	Multicall	27652996	23 mins ago	0xc9744af02e0b7410...	OUT	0.1 BNB	0.000756601

Sure enough, before the words were finished, this user bought more. He probably felt that the upward trend would continue and then increased his position.

Txn Hash	Method	Block	Age	From	To	Value	[Txn Fee]
0xcca8d8ab2dc86b2...	Multicall	27653446	51 secs ago	0xc9744af02e0b7410...	OUT	0.2 BNB	0.000756759
0x48821ca2a5b529cd...	Transfer	27653415	2 mins ago	Binance: Hot Wallet 10	IN	7.90800315 BNB	0.000126
0x3d9069de7a15bb7...	Multicall	27653252	10 mins ago	0xc9744af02e0b7410...	OUT	0.005 BNB	0.000756689
0x4a52e7909ebfc187...	Multicall	27653203	13 mins ago	0xc9744af02e0b7410...	OUT	0.333935919 BNB	0.000756837
0x1eb0e605291445c2...	Multicall	27652996	23 mins ago	0xc9744af02e0b7410...	OUT	0.1 BNB	0.000756601

This is the mentality of many users who follow suit to buy, but end up in a honeypot.

How to prevent a honeypot?

To prevent crypto scams like honeypot, we summarize the following points to note.

1 Pay attention to cryptos with ultra-high return. Ultra-high return usually means ultra-high risk. In the meme season, pay attention not to be the last buyer.

2 Check the background of a crypto project team, and judge the virtual currency information carefully. There is a lot of inaccurate information and exaggerated propaganda in the virtual currency market, and investors need to maintain a skeptical and prudent attitude and strictly identify the information.

3 Some scams use KOLs to promote themselves. Investors need to maintain a rational judgment and do not follow the trend blindly.

4 Do not believe in “inside information” or “confidential information”. These are usually scams that set traps to lure investors into risky investments.

5 Above all, it is important to enhance your awareness of self-prevention and prudent investment philosophy.

If you want to check how safe a project is, you can enter Beosin EagleEye security risk monitoring, warning and blocking platform, which can monitor the operation status of

the chain, real-time transaction behavior, automatically identify abnormal transactions, comprehensively assess the security operation status of the project, and help users judge the security of a project. **In the News Alerts function, we will also warn some “honeypot” security risks and share safety precaution knowledge with you.**

EagleEye Project Explorer Risk Transactions News Monitor Service Search by Project Name / Token Request a Quote Login Sign Up

Web3 Security Monitor

Security Assessment, Risk Transactions Identification, and Security Sentiment

Assets Monitored **\$396.000B** Project **2605** Chains 4

Blockchain Security Audit Service

Provide professional security audit service for smart contracts & blockchains based on formal verification technology.

[Request a Quote](#)

News Alerts

Risk Alerts

- RT @Beosin_com:** An in-depth Analysis of #zk SNARK Input Aliasing Vulnerabi...
- 3/** Previous attacks: On Apr 28, 2022, Deus Finance was under a \$16M flashloan...
- 2/** After deducting the burn amount, the function updates the approval value ...

Security Monitor

[Learn more>>](#)

Address	Icon	Risk Level
0x6ee7...169e00	👤	High
0x3f19...5061f7	👤	High
0xc6f6...31423c	👤 ⚡	High
0x6670...84a332	👤 ⚡	High
0xd9ba...b3a655	👤	High

Newly Added

Hot Projects

Rank	Project Name	Stars
01	Arbswap-StableSwap	★ ★ ★
02	SyncSwap	★ ★
03	Otter-Airdrop	★ ★ ★
04	Dfans	★ ★ ★
05	Owito Finance	★ ★ ★

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, South Korea, Japan and other 10+ countries. With the mission of “Securing Blockchain Ecosystem”, Beosin provides “All-in-one” blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance. You are welcome to contact us.