Coinsult

Advanced Manual Smart Contract Audit

Project: PyramidPRO

Website: https://pyramidpro.net/

● Low-Risk	● Medium-Risk	● High-Risk
3 low-risk code issues found	1 medium-risk code issues found	0 high-risk code issues found

Contract Address

0xdd6BD55D9BEb898B1C3180C6c03E8668bEf3bCd0

Disclaimer

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

Not available

Source Code

Coinsult was comissioned by PyramidPRO to perform an audit based on the following smart contract:

https://bscscan.com/address/0xdd6bd55d9beb898b1c3180c6c03e8668bef3bcd0#code

Manual Code Review

In this audit report we will highlight all these issues:

🟢 Low-Risk

3 low-risk code issues found

🟡 Medium-Risk

1 medium-risk code issues found

🔴 High-Risk

0 high-risk code issues found

The detailed report continues on the next page...

● **Low-Risk:** Could be fixed, will not bring problems.

Avoid relying on block.timestamp

block.timestamp can be manipulated by miners.

```
function stake (
  uint256 _amount,
  uint256 blockTime,
  bytes memory _adminSignature,
  bytes memory _userSignature
) public {
  bytes32 hashOf = getHash(blockTime, _amount);
  require(_amount = 100 * (10 ** _decimals),  "PyramidPRO: Cannot stake less then 100");
  require(blockTime &gt; block.timestamp &amp;&amp; blockTime &lt; block.timestamp + 5 minutes, &quo
  require(signer == verify(hashOf, _adminSignature), &quot;PyramidPRO: Signer is not admin&quot;);
  require(msg.sender == verify(getEthSignedHash(hashOf), _userSignature), &quot;PyramidPRO: Signer i
```

Recommendation

Do not use `block.timestamp`, now or blockhash as a source of randomness

Exploit scenario

```
contract Game {

    uint reward_determining_number;

    function guessing() external{
      reward_determining_number = uint256(block.blockhash(10000)) % 10;
    }
}
```

Eve is a miner. Eve calls `guessing` and re-orders the block containing the transaction. As a result, Eve wins the game.

🟢 **Low-Risk:** Could be fixed, will not bring problems.

No zero address validation for some functions

Detect missing zero address validation.

```
function changeDevaddress(address _devAddress) public onlyOwner {
  address temp = devAddress;
  devAddress = _devAddress;
  emit singerChanged(temp, _devAddress);
}
```

Recommendation

Check that the new address is not zero.

Exploit scenario

```
contract C {

  modifier onlyAdmin {
    if (msg.sender != owner) throw;
    _;
  }

  function updateOwner(address newOwner) onlyAdmin external {
    owner = newOwner;
  }
}
```

Bob calls `updateOwner` without specifying the `newOwner`, soBob loses ownership of the contract.

● **Low-Risk:** Could be fixed, will not bring problems.

Missing events arithmetic

Detect missing events for critical arithmetic parameters.

```
function mintReward(uint256 amountStaked, uint256 userReward, uint256 devReward) private {
    _mint(msg.sender, userReward);
    _mint(devAddress, devReward);
    _transfer(address(this), msg.sender, amountStaked);
    totalStaked -= amountStaked;
}
```

Recommendation

Emit an event for critical parameter changes.

Exploit scenario

```
contract C {

  modifier onlyAdmin {
    if (msg.sender != owner) throw;
    _;
  }

  function updateOwner(address newOwner) onlyAdmin external {
    owner = newOwner;
  }
}
```

`updateOwner()` has no event, so it is difficult to track off-chain changes in the buy price.

● **Medium-Risk:** Should be fixed, could bring problems.

Owner can mint new tokens

```
function mint(address account, uint256 amount) public onlyOwner returns(bool){
  _mint(account, amount);
  return true;
}
```

Recommendation

No recommendation

Owner privileges

- 🟢 Owner cannot set fees higher than 25%
- 🟢 Owner cannot pause trading
- 🟢 Owner cannot change max transaction amount
- 🔴 Owner can mint new tokens

Extra notes by the team

No notes

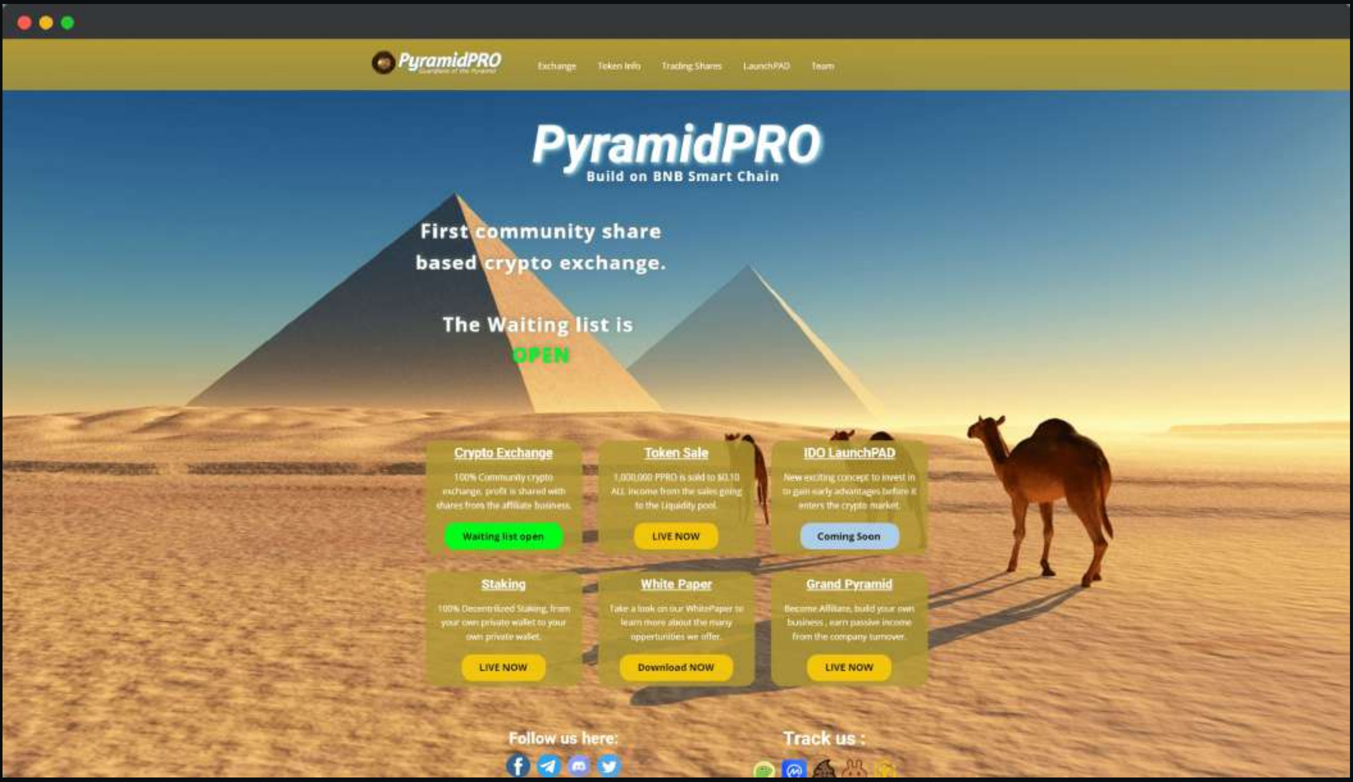
Contract Snapshot

```
contract PyramidPRO is Ownable, Stakeable {

uint private _totalSupply;
uint8 private _decimals;
string private _symbol;
string private _name;
address private devAddress;
address private signer;
uint private MAX_SUPPLY;
uint private rewardSupply;
```

Website Review

Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.



PyramidPRO
Build on BNB Smart Chain

First community share based crypto exchange.

The Waiting list is OPEN

Crypto Exchange
100% Community crypto exchange, profit is shared with shares from the affiliate business.

Token Sale
1,000,000 PPRO is sold to $0.10 ALL income from the sales going to the Liquidity pool.

IDO LaunchPAD
New exciting concept to invest in to gain early advantages before it enters the crypto market.

Staking
100% Decentralized Staking, from your own private wallet to your own private wallet.

White Paper
Take a look on our WhitePaper to learn more about the many oppertunities we offer.

Grand Pyramid
Become Affiliate, build your own business , earn passive income from the company turnover.

● Mobile Friendly

● Does not contain jQuery errors

● SSL Secured

● No major spelling errors

Project Overview

● Not KYC verified by Coinsult