

PayPal Launches PYUSD

Stablecoin: Analysis of Centralized Stablecoins' Smart Contracts



Beosin · Follow

4 min read · Aug 14

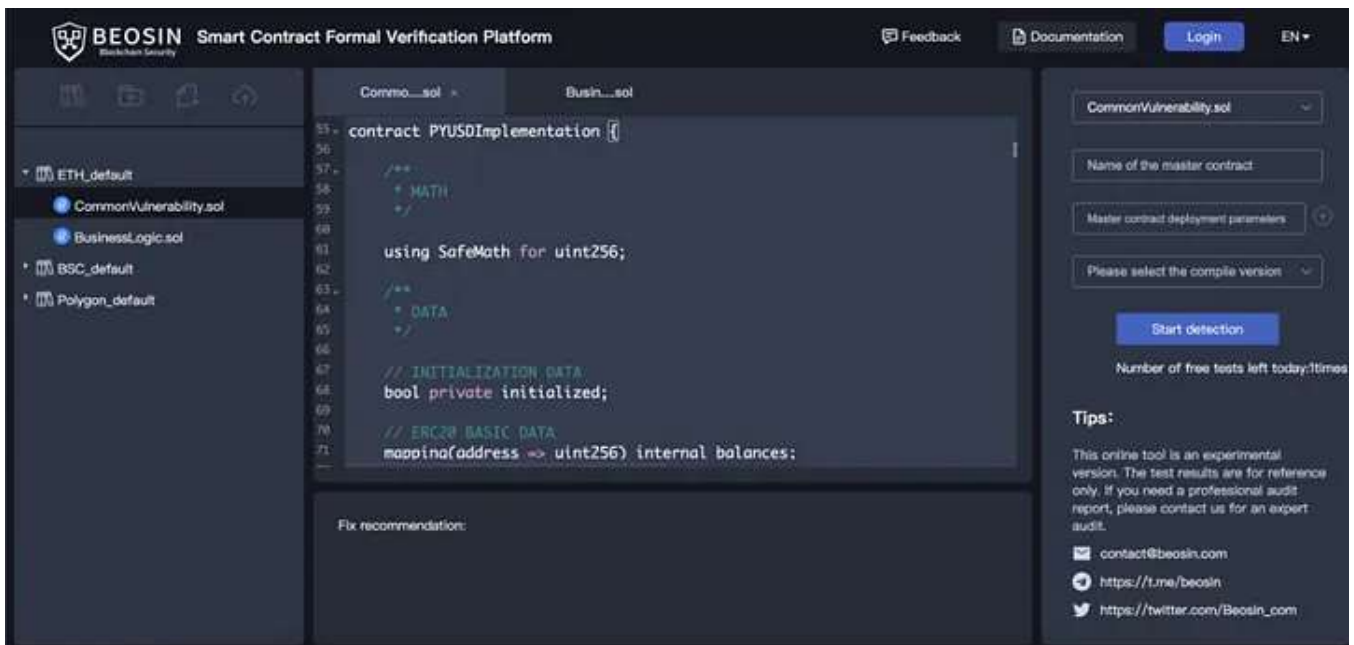


12



On August 7th, payment giant PayPal announced the launch of the PayPal USD (PYUSD) stablecoin. This stablecoin is issued by Paxos and its contract has been deployed on the Ethereum mainnet. Upon inspecting its contract code, it becomes evident that the PYUSD contract code is quite similar to that of USDP, another stablecoin issued by Paxos. The only notable difference is the addition of an external function called “increaseSupply.”

Centralized stablecoins primarily operate by collateralizing with fiat currencies. The stablecoin issuer will stake assets such as fiat currency in a bank account as a reserve for its on-chain stablecoins. This article primarily employs Beosin VaaS to scan stablecoins' smart contracts, examining their logic and uncovering differences among various types of centralized stablecoins.



USDT

1. Potential Fees

USDT employs two variables, namely “basisPointsRate” and “maximumFee,” to define the fees users need to pay to Tether Ltd. when using USDT. The highest fee is set at 50 USDT. Currently, these two variables are both set to 0, indicating that users do not need to pay any additional fees to Tether Ltd. when using USDT.

```

contract BasicToken is Ownable, ERC20Basic {
    using SafeMath for uint;

    mapping(address => uint) public balances;

    uint public basisPointsRate = 0;
    uint public maximumFee = 0;
    ...
}

...

function setParams(uint newBasisPoints, uint newMaxFee) public onlyOwner
{
    require(newBasisPoints < 20);
    require(newMaxFee < 50);

    basisPointsRate = newBasisPoints;
    maximumFee = newMaxFee.mul(10**decimals);


    Params(basisPointsRate, maximumFee);
}

```

Contract Address: <https://etherscan.io/address/0xdac17f958d2ee523a2206206994597c13d831ec7#code>

2. Blacklist:

Tether Ltd. has implemented a blacklist function in the USDT token contract. If an address is added to the blacklist, that address is restricted from invoking the “transfer()” or “transferFrom()” functions to move USDT. Moreover, Tether Ltd. has the capability to use the “destroyBlackFunds()” function, which sets the USDT balance of blacklisted users to 0, thereby countering blacklisted users.



```
function destroyBlackFunds (address _blackListedUser) public onlyOwner
{
    require(isBlackListed[_blackListedUser]);
    uint dirtyFunds = balanceOf(_blackListedUser);
    balances[_blackListedUser] = 0;
    _totalSupply -= dirtyFunds;
    DestroyedBlackFunds(_blackListedUser, dirtyFunds);
}
```

Contract Address: <https://etherscan.io/address/0xdac17f958d2ee523a2206206994597c13d831ec7#code>

USDC

USDC does not impose any fees. Similar to USDT, USDC also employs a blacklist mechanism where addresses on the blacklist are unable to invoke any functions of the USDC contract. However, USDC does not possess a function akin to USDT's "destroyBlackFunds()" function.

```

function approve(address spender, uint256 value)
external override whenNotPaused notBlacklisted(msg.sender)
notBlacklisted(spender) returns (bool)
{ ... }

function transferFrom( address from, address to, uint256
external override whenNotPaused notBlacklisted(msg.sender)
notBlacklisted(from) notBlacklisted(to) returns (bool)
{ ... }

function transfer(address to, uint256 value)
external override whenNotPaused notBlacklisted(msg.sender)
notBlacklisted(to) returns (bool)
{ ... }

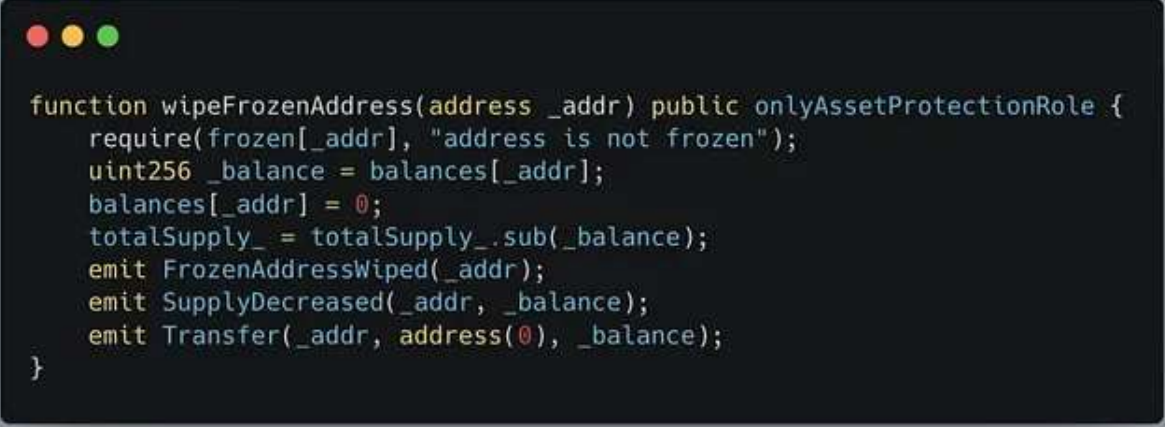
```

All external functions of USDC require that the address is not on the blacklist.

USDP/BUSD/PYUSD

1. Blacklist

The code of USDP, BUSD, and PYUSD is fundamentally similar. Like other centralized stablecoins, they also feature a blacklist functionality, enabling the addition of an address to the “frozen” list to restrict transfers related to USDP and PYUSD. USDP, BUSD, and PYUSD have a function called “wipeFrozenAddress(),” which serves a purpose similar to USDT’s “destroyBlackFunds()” function, resetting the stablecoin balances of addresses in the “frozen” list to 0.



```
function wipeFrozenAddress(address _addr) public onlyAssetProtectionRole {
    require(frozen[_addr], "address is not frozen");
    uint256 _balance = balances[_addr];
    balances[_addr] = 0;
    totalSupply_ = totalSupply_.sub(_balance);
    emit FrozenAddressWiped(_addr);
    emit SupplyDecreased(_addr, _balance);
    emit Transfer(_addr, address(0), _balance);
}
```

<https://etherscan.io/token/0xe17b8aDF8E46b15f3F9aB4Bb9E3b6e31Db09126E#code>

2. Whitelist

USDP, BUSD, and PYUSD introduce the concept of “assetProtectionRole,” akin to a whitelist. Addresses adorned with the “assetProtectionRole” modifier can add an address to the “frozen” list or invoke the “wipeFrozenAddress()” function.

3. Gasless Transfers

USDP, BUSD, and PYUSD further provide two functions: “betaDelegatedTransfer()” and “betaDelegatedTransferBatch()”. These allow users to initiate stablecoin transfers without incurring gas fees, by providing signed information and enabling approved parties to act as proxies for users in the transaction.

```
function betaDelegatedTransfer(
  bytes sig, address to, uint256 value, uint256 fee, uint256 seq, uint256 deadline
) public returns (bool) {
  require(sig.length == 65, "signature should have length 65");
  bytes32 r;
  bytes32 s;
  uint8 v;
  assembly {
    r := mload(add(sig, 32))
    s := mload(add(sig, 64))
    v := byte(0, mload(add(sig, 96)))
  }
  require(_betaDelegatedTransfer(r, s, v, to, value, fee, seq, deadline), "failed transfer");
  return true;
}
```

<https://etherscan.io/token/0xe17b8aDF8E46b15f3F9aB4Bb9E3b6e31Db09126E#code>

Conclusion

Centralized stablecoins adopt blacklist mechanisms to meet regulatory and anti-money laundering requirements. Stablecoins issued by Paxos offer some innovations compared to USDT and USDC. PayPal's deployment of stablecoins on public blockchains will further advance the USD stablecoin market, enabling millions of users to enter the realm of cryptocurrency through the PayPal payment platform.

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, and set up offices in 10+ cities including Hong Kong, Singapore, Tokyo and Miami. 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.

Contact

If you need any blockchain security services, welcome to contact us:

[Official Website](#) [Beosin EagleEye](#) [Twitter](#) [Telegram](#) [Linkedin](#)