Coinsult

Advanced Manual Smart Contract Audit

Project: Game Addict

Website: https://gameaddict.finance/

Low-Risk	Medium-Risk	High-Risk
4 low-risk code issues found	0 medium-risk code issues found	0 high-risk code issues found

Contract Address

0xC7dDE0701DD49be8F5792280DdfCabF64f9dEC14

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

Rank	Address	Quantity (Token)	Percentage
1	0xddd7a4ab2a5cc6af30b42ed1911467faca1beb6d	59,290,000	84.7000%
2	0x6f2aeebf0eb002584c1658b719d4541d8d409e66	10,710,000	15.3000%

Source Code

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

https://bscscan.com/address/0xC7dDE0701DD49be8F5792280DdfCabF64f9dEC14#code

PinkSale generated babytoken

Manual Code Review

In this audit report we will highlight all these issues:

🟢 Low-Risk

4 low-risk code
issues found

🟡 Medium-Risk

0 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.

```
secondsUntilAutoClaimAvailable = nextClaimTime &gt; block.timestamp
? nextClaimTime.sub(block.timestamp)
: 0;
```

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.

Too many digits

Literals with many digits are difficult to read and review.

```
require(
    newValue &gt;= 200000 &amp;&amp; newValue &lt;= 500000,
    &quot;BABYTOKEN: gasForProcessing must be between 200,000 and 500,000&quot;
);
```

Recommendation

Use: Ether suffix, Time suffix, or The scientific notation

Exploit scenario

```
contract MyContract{
    uint 1_ether = 10000000000000000000;
}
```

While `1_ether` looks like `1 ether`, it is `10 ether`. As a result, it's likely to be used incorrectly.

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

No zero address validation for some functions

Detect missing zero address validation.

```
function setMarketingWallet(address payable wallet) external onlyOwner {
    _marketingWalletAddress = wallet;
}
```

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 setTokenRewardsFee(uint256 value) external onlyOwner {
    tokenRewardsFee = value;
    totalFees = tokenRewardsFee.add(liquidityFee).add(marketingFee);
    require(totalFees &amp;lt;= 25, &amp;quot;Total fee is over 25%&amp;quot;);
}

function setLiquiditFee(uint256 value) external onlyOwner {
    liquidityFee = value;
    totalFees = tokenRewardsFee.add(liquidityFee).add(marketingFee);
    require(totalFees &amp;lt;= 25, &amp;quot;Total fee is over 25%&amp;quot;);
}

function setMarketingFee(uint256 value) external onlyOwner {
    marketingFee = value;
    totalFees = tokenRewardsFee.add(liquidityFee).add(marketingFee);
    require(totalFees &amp;lt;= 25, &amp;quot;Total fee is over 25%&amp;quot;);
}
```

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.

Owner privileges

- Owner cannot set fees higher than 25%
- Owner cannot pause trading
- Owner cannot change max transaction amount
- Owner can exclude from fees

Extra notes by the team

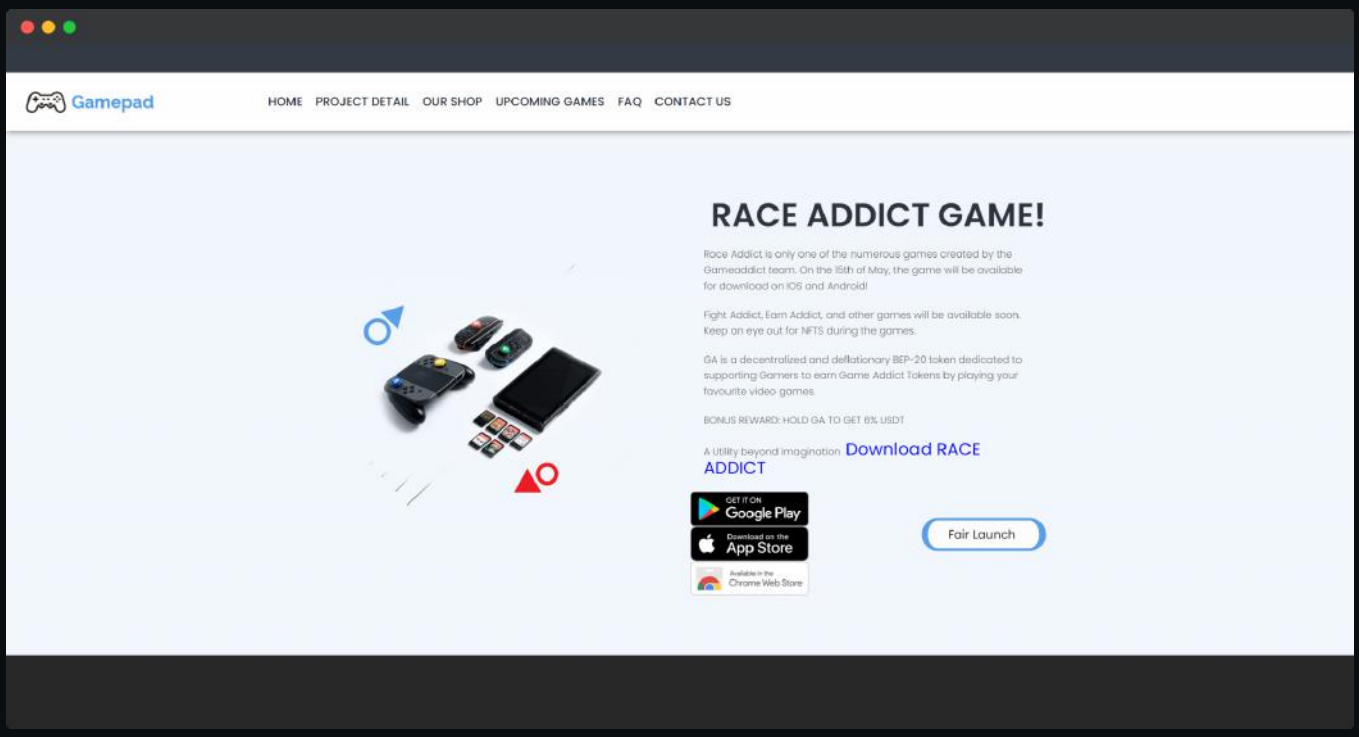
No notes

Contract Snapshot

```
contract BABYTOKEN is ERC20, Ownable, BaseToken {
using SafeMath for uint256;

uint256 public constant VERSION = 1;

IUniswapV2Router02 public uniswapV2Router;
address public uniswapV2Pair;

bool private swapping;

BABYTOKENDividendTracker public dividendTracker;

address public rewardToken;

uint256 public swapTokensAtAmount;

uint256 public tokenRewardsFee;
uint256 public liquidityFee;
uint256 public marketingFee;
uint256 public totalFees;

address public _marketingWalletAddress;

uint256 public gasForProcessing;

// exlcude from fees and max transaction amount
mapping(address =&gt; bool) private _isExcludedFromFees;

// store addresses that a automatic market maker pairs. Any transfer *to* these addresses
// could be subject to a maximum transfer amount
mapping(address =&gt; bool) public automatedMarketMakerPairs;

event UpdateDividendTracker(
    address indexed newAddress,
    address indexed oldAddress
);
```

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.



- Mobile Friendly
- Does not contain jQuery errors
- SSL Secured
- No major spelling errors

Project Overview

Not KYC verified by Coinsult