Moniat cryptocurrency imposes tight blockchain security mechanism

Wednesday 19 December, 2018

It has been confirmed that the Moniat cryptocurrency or ERC20 Utility Token runs under a very secure smart contract. Hacken OÜ, an external specialized security consultancy firm, conducted a review and security analysis on the Moniat Smart Contract Code, and published their assessment of its security. The Hacken team scanned the Moniat smart contract for commonly known and more specific vulnerabilities: • Reentrancy • Timestamp Dependence • Gas Limit and Loops • DoS with (Unexpected) Throw • DoS with Block Gas Limit • Transaction-Ordering Dependence • Byte array vulnerabilities • Style guide violation • Transfer forwards all gas • ERC20 API violation • Malicious libraries • Compiler version not fixed • Unchecked external call – Unchecked math • Unsafe type inference • Implicit visibility level.

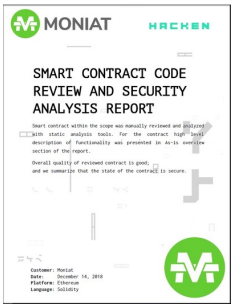
According to the assessment, the Moniat smart contract was confirmed as totally secure. The Hacken team performed analysis of the code functionality, manual audit and automated checks with Mythril, Slither and remix IDE. All the issues found during automated analysis were manually reviewed and the applicable vulnerabilities are presented in the audit overview section. A general overview is presented in the AS-IS section and all the found issues can be found in the audit overview section.

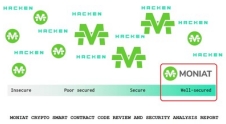
The MAT_Token contract inherits the ERC20 Interface, Owned, SafeMath. The MAT_Token has constructor functions and parameters as follows: The Token symbol is "MAT", the Token name is "Moniat" with 18 decimals and a Total Supply of 20 billion MAT.

The Moniat audit overview found no critical severity vulnerabilities, no high severity vulnerabilities and no medium severity vulnerabilities. The Hacken audit report concluded that the Moniat Smart contract within the scope was manually reviewed and analyzed with static analysis tools. The contract high level description of functionality was presented in the As-is overview section of the report. The audit report contains all found security vulnerabilities and other issues in the reviewed code. The overall quality of the reviewed contract is good, with no serious security impact, and the report summarized that the state of the contract is secure.

Moniat is forked from the Ethereum Blockchain, which uses asymmetric encryption (Public Key Cryptography) to secure the data. Asymmetric encryption uses two keys – public and private – to encrypt the data. The two keys make it impossible to crack the network.

Media:



















Related Sectors:

Business & Finance :: Computing & Telecoms :: Consumer Technology :: Crypto Currency :: Media & Marketing :: Personal Finance ::

Company Contact:

_

Moniat OÜ

E. cryptomoniat@gmail.com
W. https://moniat.com/

Related Keywords:

Moniat :: Cryptocurrency :: erc20 :: Business :: Finance :: Trading :: Money :: Home :: Income :: Profit :: Exchange :: Travel :: Work :: Blockchain :: Security :: Investment ::

Scan Me:

View Online

Additional Assets:

Newsroom: Visit our Newsroom for all the latest stories:
https://www.moniat.pressat.co.uk