Ambisafe

CrypteriumToken Smart Contract Audit by Ambisafe Inc.
November, 2017
Alexey Shendrick, Oleksii Matiiasevych

1. **Introduction.** Crypterium requested that Ambisafe perform an audit of the contracts implementing their token and sale logic. The contracts in question are hosted at: https://etherscan.io/address/0x80a7e048f37a50500351c204cb407766fa3bae7f#code

   Contracts in scope are(and their parents):
   - CrypteriumToken

2. **Disclaimer.** The audit makes no statements or warranties about utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about fitness of the contracts to purpose, or their bugfree status. The audit documentation is for discussion purposes only.

3. **Executive Summary.** Contract functions are well protected from unauthorized access, and don't perform any external calls, effectively eliminating broad variety of problems. Calculations are protected against overflows while at the same time not wasting excess gas. There are 3 core life periods in the contract: before minting is finished, before transfers are allowed, final state. After reaching the final state, no any more tokens can be created, and transfers become freely available. Used compiler(0.4.16) does not have known bugs which might affect contract's logic. Contract fully complies with finalized ERC20 standard. As suggested by the standard, Short Address and Approve-TransferFrom Attack protections are not forced by the contract. Contract is safe to use. Sale starting date constant is set to GMT: Tuesday, October 31, 2017 2:00:00 PM.

4. **Critical Bugs and Vulnerabilities.** No places in code were identified as critical issues.

5. **Line By Line Review.**

   5.1. Lines 81, 97. Note: we agree with commenting out these assertions as they can never be triggered.

Oleksii Matiiasevych,
Solidity Engineer