



Armor's Labs

ARM Token

Smart Contract Audit

- ARM Audit Summary
- ARM Token Audit
 - Document information
 - Review
 - Audit results
 - Audited target file
 - Vulnerability analysis
 - Vulnerability distribution
 - Summary of audit results
 - Analysis of audit test
 - Test coverage reports
 - Analysis of audit results
 - Re-Entrancy
 - Arithmetic Over/Under Flows
 - Unexpected Ether
 - Delegatecall
 - Default Visibilities
 - Entropy Illusion
 - External Contract Referencing
 - Unsolved TODO comments
 - Short Address/Parameter Attack
 - Unchecked CALL Return Values
 - Race Conditions / Front Running
 - Denial Of Service (DOS)
 - Block Timestamp Manipulation
 - Constructors with Care
 - Uninitialised Storage Pointers
 - Floating Points and Numerical Precision
 - tx.origin Authentication

ARM Audit Summary

Project name : Armors Token

Project address: <https://etherscan.io/address/0xa9ff725189fe00da9c5f27a580dc67fea61e3fb2#code>

Projct target : Token Contract Audit

Test result : The contract basically meets the specifications, the code quality is relatively high.

Audit Info

Audit result : PASSED

Audit NO : 0X201902010006

Audit Team : Armors Labs

ARM Token Audit

The Armors Token team asked us to review and audit their Token contract. We looked at the code and now publish our results.

Here is our assessment and recommendations, in order of importance.

Document information

Name	Auditor	Version	Date
ARM Audit	Rock ,Hosea, Rushairer	1.0.0	2019-02-01

Review

Audit results

No critical or high severity issues were found.

Contracts have the function of freezing accounts, which can prevent abnormal account transactions.

Note that as of the date of publishing, the above review reflects the current understanding of known security patterns as they relate to the ARM Token contract. The above should not be construed as investment advice.

Based on the widely recognized security status of the current underlying blockchain and smart contract, this audit report is valid for 18 months from the date of output.

(Statement: Armors Labs reports only on facts that have occurred or existed before this report is issued and assumes corresponding responsibilities. Armors Labs is not able to determine the security of its smart contracts and is not responsible for any subsequent or existing facts after this report is issued. The security audit analysis and other content of this report are only based on the documents and information provided by the information provider to Armors Labs at the time of issuance of this report (" information provided " for short). Armors Labs postulates that the information provided is not missing, tampered, deleted or hidden. If the information provided is missing, tampered,

deleted, hidden or reflected in a way that is not consistent with the actual situation, Armors Labs shall not be responsible for the losses and adverse effects caused.)

Audited target file

file	md5
arm.sol	841b7905b1cdb28f79ec66bab59e243b

Vulnerability analysis

Vulnerability distribution

vulnerability level	number	proportion
Critical severity	0	0%
High severity	0	0%
Medium severity	0	0%
Low severity	0	0%

Summary of audit results

Vulnerability	status
Re-Entrancy	safe
Arithmetic Over/Under Flows	safe
Unexpected Ether	safe
Delegatecall	safe
Default Visibilities	safe
Entropy Illusion	safe
External Contract Referencing	safe
Short Address/Parameter Attack	safe
Unchecked CALL Return Values	safe
Race Conditions / Front Running	safe
Denial Of Service (DOS)	safe
Block Timestamp Manipulation	safe
Constructors with Care	safe
Uninitialised Storage Pointers	safe
Floating Points and Numerical Precision	safe
tx.origin Authentication	safe

Analysis of audit test

Test coverage reports

```
> scripts/coverage.sh

Starting our own ganache instance
armors-solidity v4.1.13 (core: 4.1.13)
Solidity v0.4.24 (solc-js)
Generating coverage environment
Running: node --max-old-space-size=4096 ./node_modules/.bin/armors-solidity compile --network coverage
(this can take a few seconds)...
Compiling ./contracts/arm.sol...
Compiling ./contracts/mocks/OwnableMock.sol...
Compiling ./contracts/mocks/SafeMathMock.sol...
Writing artifacts to ./build/contracts

Using network 'coverage'.
```

Contract: SafeMath

- `add`
 - ✓ adds correctly (74ms)
 - ✓ throws a revert error on **addition overflow** (52ms)
- `sub`
 - ✓ subtracts correctly (49ms)
 - ✓ throws a revert error if subtraction `result` would be negative (38ms)

Contract: Ownable

- `as an ownable`
 - ✓ should have an owner
 - ✓ changes owner after transfer (130ms)
 - ✓ should prevent non-owners `from` transferring (45ms)
 - ✓ should guard ownership against stuck state (58ms)
 - ✓ loses owner after renouncement (82ms)
 - ✓ should prevent non-owners `from` renouncement

Contract: ArmorsToken

- `total supply`
 - ✓ returns the total amount of tokens
- `balanceOf`
 - when the requested account has no tokens
 - ✓ returns zero
 - when the requested account has some tokens
 - ✓ returns the total amount of tokens
- `transfer`
 - when the recipient is not the zero address
 - when the sender does not have enough balance
 - ✓ throwing
 - when the sender has enough balance
 - ✓ transfers the requested amount (85ms)
 - ✓ emits a transfer event (44ms)
 - when the recipient is the zero address
 - ✓ reverts (39ms)
- `approve`
 - when the spender is not the zero address
 - when the sender has enough balance
 - ✓ emits an approval event (38ms)
 - when there was no approved amount before
 - ✓ approves the requested amount (50ms)
 - when the spender had an approved amount
 - ✓ approves the requested amount and replaces the previous one (48ms)
 - when the sender does not have enough balance

```

✓ emits an approval event
when there was no approved amount before
  ✓ approves the requested amount (48ms)
when the spender had an approved amount
  ✓ approves the requested amount and replaces the previous one (47ms)
when the spender is the zero address
  ✓ emits an approval event (38ms)

```

Events emitted during test:

```

Transfer(from: <indexed>, to: <indexed>, value: 100)
Approval(owner: <indexed>, spender: <indexed>, value: 100)

```

```

transfer from
when the recipient is not the zero address
  when the spender has enough approved balance
    when the owner has enough balance
      ✓ transfers the requested amount (76ms)
      ✓ decreases the spender allowance (54ms)
      ✓ emits a transfer event (48ms)
    when the owner does not have enough balance
      ✓ throwing
  when the spender does not have enough approved balance
    when the owner has enough balance
      ✓ throwing
    when the owner does not have enough balance
      ✓ throwing
when the recipient is the zero address
  ✓ reverts (38ms)
decrease allowance
when the spender is not the zero address
  when the sender has enough balance
    when there was no approved amount before
      ✓ return zero (47ms)
    when the spender had an approved amount
      ✓ emits an approval event (39ms)
      ✓ decreases the spender allowance subtracting the requested amount (58ms)
      ✓ sets the allowance to zero when all allowance is removed (52ms)
      ✓ return zero when more than the full allowance is removed (46ms)
  when the sender does not have enough balance
    when there was no approved amount before
      ✓ return zero (45ms)
  when the spender had an approved amount
    ✓ emits an approval event
    ✓ decreases the spender allowance subtracting the requested amount (51ms)
    ✓ sets the allowance to zero when all allowance is removed (51ms)
    ✓ return zero when more than the full allowance is removed (49ms)
when the spender is the zero address
  ✓ emits an approval event (38ms)

```

Events emitted during test:

```

Transfer(from: <indexed>, to: <indexed>, value: 100)
Approval(owner: <indexed>, spender: <indexed>, value: 0)

```

```

increase allowance
when the spender is not the zero address
  when the sender has enough balance
    ✓ emits an approval event
  when there was no approved amount before
    ✓ approves the requested amount (46ms)
  when the spender had an approved amount

```

```

✓ increases the spender allowance adding the requested amount (45ms)
when the sender does not have enough balance
    ✓ emits an approval event
    when there was no approved amount before
        ✓ approves the requested amount (43ms)
    when the spender had an approved amount
        ✓ increases the spender allowance adding the requested amount (46ms)
when the spender is the zero address
    ✓ emits an approval event (38ms)

```

Events emitted during test:

```

Transfer(from: <indexed>, to: <indexed>, value: 100)
Approval(owner: <indexed>, spender: <indexed>, value: 100)

```

```

Send back eth to msg.sender
✓ reverts (151ms)

```

Contract: Ownable
as an ownable
✓ should have an owner
✓ changes owner after transfer (64ms)
✓ should prevent non-owners from transferring (92ms)
✓ should guard ownership against stuck state

44 passing (8s)
0 failing

File	% Stmt	% Branch	% Funcs	% Lines	Uncovered Lines
contracts/arm.sol	100	100	100	100	
All files	100	100	100	100	

Istanbul coverage reports generated
Cleaning up...

Analysis of audit results

Re-Entrancy

- **Description:**

One of the features of Ethereum smart contracts is the ability to call and utilise code of other external contracts. Contracts also typically handle ether, and as such often send ether to various external user addresses. The operation of calling external contracts, or sending ether to an address, requires the contract to submit an external call. These external calls can be hijacked by attackers whereby they force the contract to execute further code (i.e. through a fallback function), including calls back into itself. Thus the code execution "re-enters" the contract. Attacks of this kind were used in the infamous DAO hack.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Arithmetic Over/Under Flows

- **Description:**

The Ethereum Virtual Machine (EVM) specifies fixed-size data types for integers. This means that an integer variable, only has a certain range of numbers it can represent. A uint8 for example, can only store numbers in the range [0,255]. Trying to store 256 into a uint8 will result in 0. If care is not taken, variables in Solidity can be exploited if user input is unchecked and calculations are performed which result in numbers that lie outside the range of the data type that stores them.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Unexpected Ether

- **Description:**

Typically when ether is sent to a contract, it must execute either the fallback function, or another function described in the contract. There are two exceptions to this, where ether can exist in a contract without having executed any code. Contracts which rely on code execution for every ether sent to the contract can be vulnerable to attacks where ether is forcibly sent to a contract.

- **Detection results:**

PASSED!

- **Security suggestion:** no.

Delegatecall

- **Description:**

The CALL and DELEGATECALL opcodes are useful in allowing Ethereum developers to modularise their code. Standard external message calls to contracts are handled by the CALL opcode whereby code is run in the context of the external contract/function. The DELEGATECALL opcode is identical to the standard message call, except that the code executed at the targeted address is run in the context of the calling contract along with the fact that msg.sender and msg.value remain unchanged. This feature enables the implementation of libraries whereby developers can create reusable code for future contracts.

- **Detection results:**

PASSED!

- **Security suggestion:** no.

Default Visibilities

- **Description:**

Functions in Solidity have visibility specifiers which dictate how functions are allowed to be called. The visibility

determines whether a function can be called externally by users, by other derived contracts, only internally or only externally. There are four visibility specifiers, which are described in detail in the Solidity Docs. Functions default to public allowing users to call them externally. Incorrect use of visibility specifiers can lead to some devastating vulnerabilities in smart contracts as will be discussed in this section.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Entropy Illusion

- **Description:**

All transactions on the Ethereum blockchain are deterministic state transition operations. Meaning that every transaction modifies the global state of the Ethereum ecosystem and it does so in a calculable way with no uncertainty. This ultimately means that inside the blockchain ecosystem there is no source of entropy or randomness. There is no rand() function in Solidity. Achieving decentralised entropy (randomness) is a well established problem and many ideas have been proposed to address this (see for example, RandDAO or using a chain of Hashes as described by Vitalik in this post).

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

External Contract Referencing

- **Description:**

One of the benefits of the Ethereum global computer is the ability to re-use code and interact with contracts already deployed on the network. As a result, a large number of contracts reference external contracts and in general operation use external message calls to interact with these contracts. These external message calls can mask malicious actors intentions in some non-obvious ways, which we will discuss.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Unsolved TODO comments

- **Description:**

Check for Unsolved TODO comments

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Short Address/Parameter Attack

- **Description:**

This attack is not specifically performed on Solidity contracts themselves but on third party applications that may interact with them. I add this attack for completeness and to be aware of how parameters can be manipulated in contracts.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Unchecked CALL Return Values

- **Description:**

There are a number of ways of performing external calls in solidity. Sending ether to external accounts is commonly performed via the transfer() method. However, the send() function can also be used and, for more versatile external calls, the CALL opcode can be directly employed in solidity. The call() and send() functions return a boolean indicating if the call succeeded or failed. Thus these functions have a simple caveat, in that the transaction that executes these functions will not revert if the external call (initialised by call() or send()) fails, rather the call() or send() will simply return false. A common pitfall arises when the return value is not checked, rather the developer expects a revert to occur.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Race Conditions / Front Running

- **Description:**

The combination of external calls to other contracts and the multi-user nature of the underlying blockchain gives rise to a variety of potential Solidity pitfalls whereby users race code execution to obtain unexpected states. Re-Entrancy is one example of such a race condition. In this section we will talk more generally about different kinds of race conditions that can occur on the Ethereum blockchain. There is a variety of good posts on this subject, a few are: Ethereum Wiki - Safety, DASP - Front-Running and the Consensus - Smart Contract Best Practices.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Denial Of Service (DOS)

- **Description:**

This category is very broad, but fundamentally consists of attacks where users can leave the contract inoperable

for a small period of time, or in some cases, permanently. This can trap ether in these contracts forever, as was the case with the Second Parity MultiSig hack

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Block Timestamp Manipulation

- **Description:**

Block timestamps have historically been used for a variety of applications, such as entropy for random numbers (see the Entropy Illusion section for further details), locking funds for periods of time and various state-changing conditional statements that are time-dependent. Miner's have the ability to adjust timestamps slightly which can prove to be quite dangerous if block timestamps are used incorrectly in smart contracts.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Constructors with Care

- **Description:**

Constructors are special functions which often perform critical, privileged tasks when initialising contracts. Before solidity v0.4.22 constructors were defined as functions that had the same name as the contract that contained them. Thus, when a contract name gets changed in development, if the constructor name isn't changed, it becomes a normal, callable function. As you can imagine, this can (and has) lead to some interesting contract hacks.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Uninitialised Storage Pointers

- **Description:**

The EVM stores data either as storage or as memory. Understanding exactly how this is done and the default types for local variables of functions is highly recommended when developing contracts. This is because it is possible to produce vulnerable contracts by inappropriately initialising variables.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Floating Points and Numerical Precision

- **Description:**

As of this writing (Solidity v0.4.24), fixed point or floating point numbers are not supported. This means that floating point representations must be made with the integer types in Solidity. This can lead to errors/vulnerabilities if not implemented correctly.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

tx.origin Authentication

- **Description:**

Solidity has a global variable, tx.origin which traverses the entire call stack and returns the address of the account that originally sent the call (or transaction). Using this variable for authentication in smart contracts leaves the contract vulnerable to a phishing-like attack.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.



armors.io

contact@armors.io

