PUBLIC

Security Audit

of STOKR's Smart Contracts

April 29, 2019

Produced for

STOKR

by

CHAINSECURITY

Table Of Content

Foreword

We first and foremost thank STOKR for giving us the opportunity to audit their smart contracts. This documents outlines our methodology, limitations, and results.

– ChainSecurity

Executive Summary

The STOKR smart contracts have been analyzed under different aspects, with a variety of tools for automated security analysis of Ethereum smart contracts.

Overall, we found that STOKR has a well written code and extensive tests with 100% code coverage. CHAINSECURITY did not find major issues. Nonetheless, CHAINSECURITY raised some minor issues and suggestions. These issues were all acknowledged or fixed in a professional manner.

CHAINSECURITY extended the audit after completion on request. The extended review now also includes the post-audit added changes listed below.

- Token destruction now emits an event
- The TokenDistribution event's information was extended
- A function to change the closing time of the crowdsale was added

Audit Overview

Scope of the Audit

The scope of the audit is limited to the following source code files. All of these source code files were received on February 22, 2019.
The corresponding Git commit was: `be93ca797a9096fb3f157fbcefe3dee05214e66c`.
An update has been received on March 21, 2019.
The corresponding Git commit is: `aa0d4dc69087d2d668b921803026644d23c8443c`.
The latest update has been received on April 29, 2019.
The corresponding Git commit is: `9a967af293168dd1d2773336ada11b3534c6031f`.

File	SHA-256 checksum
./crowdsale/MintingCrowdsale.sol	393f81b519b1ebdc7a5fa4b24bd2bcc04f132e1b4bd36a06bd7a28957d1aa254
./crowdsale/RateSourceInterface.sol	d843d7e0a90b554c4f1052d442d4084f4b4996389ef22dafc311eafcbd7bf4b3
./crowdsale/StokrCrowdsaleFactory.sol	ecad6110880c6da853329c83bbcf4e8c8a8fe29fffe68b0cd4b6e86aa43b151e
./crowdsale/StokrCrowdsale.sol	0193b1cb3d39ba4993341b84c32146132c40be7e769d3b70a9ee445ceea47629
./math/SafeMath.sol	e6c93a577ee0942cc0068c3ddc0805023d905338a381d52ea29fa4c0998d4f21
./ownership/Ownable.sol	a1a882a1fc19d439e3ca8dccfba0c4f3f4a6853e2791a316fa872c46d6b60f34
./StokrProjectManager.sol	e79741f4b6db791c0a5182cbfae70db89ccfbc54471738cad74b131f63bbfbfc
./token/ERC20.sol	e497cbc10d77c03b4fa35cfcfd3ec60e56032f75f1a42ba2bf60c5d33c849b6b
./token/MintableToken.sol	879f7201076c62fa8a4e4317f2a4d5e95414b036d4a5869d7d5afe825e17801a
./token/ProfitSharing.sol	8c6fb60080938f0cd5259a25a943d4a2b3b01d5d6d7c1ba347e4ae3377c46c66
./token/StokrTokenFactory.sol	da6704724a713be6e694a96acce6bbcde22a05354c79ede61de6faf2c48ae6fc
./token/StokrToken.sol	b7db6bac950c1a4d3c834bb9efa9302886c10a31350698fe3fd6b5565548adf9
./token/TokenRecoverable.sol	7eca951ef2cda0048052e02eec5bdafa095d1c13e12634f3bf2e5600e54a7971
./whitelist/Whitelisted.sol	cf6e5be5c902b0040429599e922fb30bcadd09fd5174317172b4faa806812214
./whitelist/Whitelist.sol	b102be5d807e47a67ffb1093ba547585a4ae7363fe153dfb71b44134940d4956

Depth of Audit

The scope of the security audit conducted by CHAINSECURITY was restricted to:

- Scan the contracts listed above for generic security issues using automated systems and manually inspect the results.
- Manual audit of the contracts listed above for security issues.

Terminology

For the purpose of this audit, we adopt the following terminology. For security vulnerabilities, we specify the *likelihood*, *impact* and *severity* (inspired by the OWASP risk rating methodology[1]).

Likelihood represents the likelihood of a security vulnerability to be encountered or exploited in the wild.

Impact specifies the technical and business related consequences of an exploit.

Severity is derived based on the likelihood and the impact calculated previously.

[1] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

We categorize the findings into 4 distinct categories, depending on their severities:

- Low: can be considered as less important
-  Medium: should be fixed
-  High: we strongly suggest to fix it before release
-  Critical: needs to be fixed before release

These severities are derived from the likelihood and the impact using the following table, following a standard approach in risk assessment.

	IMPACT		
LIKELIHOOD	**High**	**Medium**	**Low**
High			
Medium			
Low			

During the audit concerns might arise or tools might flag certain security issues. After careful inspection of the potential security impact, we assign the following labels:

- ✓ No Issue: no security impact
- ✓ Fixed: during the course of the audit process, the issue has been addressed technically
- ✓ Addressed: issue addressed otherwise by improving documentation or further specification
- ✓ Acknowledged: issue is meant to be fixed in the future without immediate changes to the code

Findings that are labelled as either ✓ Fixed or ✓ Addressed are resolved and therefore pose no security threat. Their severity is still listed, but just to give the reader a quick overview what kind of issues were found during the audit.

Limitations

Security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a secure smart contract. However, auditing allows to discover vulnerabilities that were overlooked during development and areas where additional security measures are necessary.

In most cases, applications are either fully protected against a certain type of attack, or they lack protection against it completely. Some of the issues may affect the entire smart contract application, while some lack protection only in certain areas. We therefore carry out a source code review trying to determine all locations that need to be fixed. Within the customer-determined timeframe, CHAINSECURITY has performed auditing in order to discover as many vulnerabilities as possible.

System Overview

STOKR is as crowd-investing platform based on smart contracts on the Ethereum blockchain. STOKR enables ventures to create projects and investors to invest into these projects. For this purpose STOKR implemented a system which has built-in features to support investors and ventures. Each project launched on STOKR's platform has a crowdsale contract to manage the sale of a dedicated security token with profit sharing and a global whitelist. Thus, only whitelisted investors can invest.

The profit sharing schemes distributes all deposited profits among the token holders according to their token balance at the time of deposit. A user's profit share is tracked automatically and can be withdrawn at any time using the corresponding function.

The crowdsale has multiple configurable parameters such as an individual purchase cap or start and end times. In case a crowdsale, doesn't reach its defined investment goal, then all investor can obtain a refund. In case of a successful crowdsale, investors can withdraw their tokens after the completion of the crowdsale.

Best Practices in STOKR's project

Projects of good quality follow best practices. In doing so, they make audits more meaningful, by allowing efforts to be focused on subtle and project-specific issues rather than the fulfillment of general guidelines.

Avoiding code duplication is a good example of a good engineering practice which increases the potential of any security audit.

We now list a few points that should be enforced in any good project that aims to be deployed on the Ethereum blockchain. The corresponding box is ticked when STOKR's project fitted the criterion when the audit started.

Hard Requirements

These requirements ensure that the STOKR's project can be audited by CHAINSECURITY.

- ☑ The code is provided as a Git repository to allow the review of future code changes.
- ☑ Code duplication is minimal, or justified and documented.
- ☑ Libraries are properly referred to as package dependencies, including the specific version(s) that are compatible with STOKR's project. No library file is mixed with STOKR's own files.
- ☑ The code compiles with the latest Solidity compiler version. If STOKR uses an older version, the reasons are documented.
- ☑ There are no compiler warnings, or warnings are documented.

Soft Requirements

Although these requirements are not as important as the previous ones, they still help to make the audit more valuable to STOKR.

- ☑ There are migration scripts.
- ☑ There are tests.
- ☑ The tests are related to the migration scripts and a clear separation is made between the two.
- ☑ The tests are easy to run for CHAINSECURITY, using the documentation provided by STOKR.
- ☑ The test coverage is available or can be obtained easily.
- ☑ The output of the build process (including possible flattened files) is not committed to the Git repository.
- ☑ The project only contains audit-related files, or, if not possible, a meaningful separation is made between modules that have to be audited and modules that CHAINSECURITY should assume correct and out of scope.
- ☑ There is no dead code.
- ☑ The code is well documented.
- ☑ The high-level specification is thorough and allow a quick understanding of the project without looking at the code.
- ☑ Both the code documentation and the high-level specification are up to date with respect to the code version CHAINSECURITY audits.
- ☑ There are no getter functions for public variables, or the reason why these getters are in the code is given.
- ☑ Function are grouped together according either to the Solidity guidelines[2], or to their functionality.

[2] https://solidity.readthedocs.io/en/latest/style-guide.html#order-of-functions

Security Issues

This section relates our investigation into securify issues. It is meant to highlight whenever we found specific issues but also mention what vulnerability classes do not appear, if relevant.

Outdated compiler version L ✓ Acknowledged

STOKR's contracts make use of compiler version `0.4.25`, which is an outdated compiler version. Since version `0.4.25` there have been major changes and fixes[3]. As a result, STOKR's code is not compiling with versions above `0.5` due to some breaking changes.

Without an explicit reason, the latest stable compiler version is recommended to be used homogeneously throughout the project.

Likelihood: Low
Impact: Low

Acknowledged: STOKR acknowledged the issue. The reason STOKR provided is that changing the compiler, would result in breaking changes in their development tool chain.

Batch function call may fail L ✓ Acknowledged

`distributeRefunds()` calls the untrusted address `_investor` provided in the function argument. Even though the `transfer()` function is considered safe regarding reentrancy, a malicious address could intentionally make the `transfer()` call fail. As a result, the function `distributeRefunds()` is blocked because the loop cannot be executed anymore. But `distributeRefunds()` is just the "batch" version of `claimRefund()` and therefore the impact is low as each investor can still use `claimRefund()` to get their refund. The same issue occurs in `withdrawProfitShares()`, but again the impact is low as the non-batch version could still be called individually by each investor.

STOKR could consider preventing one failing ETH transfer in the loop from reverting the entire transaction.

Likelihood: Low
Impact: Low

Acknowledged: STOKR acknowledged that they are aware of this issue.

Potential overflow in `setRate()` L ✓ Fixed

STOKR does not use `SafeMath` to verify the new `rate` to be set. This could lead to an overflow in the multiplication part of the check, `newRate < 10 * rate`. If `rate` is near the maximum uint256 value, multiplying by 10 might cause an overflow. This function can only be called by `rateAdmin`, which is set by the owner.

STOKR should consider using `SafeMath.mul()` to prevent overflow.

Likelihood: Low
Impact: Low

Fixed: STOKR solved the problem by adding end enforcing a maximum rate of `uint(-1)/10`.

Adjusting Allowance can lead to front-running L ✓ Fixed

Inside the ERC20 token standard, there is a well-documented[4] issue with front-running when it comes to the `approve` function. When changing a particular allowance from X to Y, where $X \neq 0$ and $Y \neq 0$ using a single transaction, this transaction is susceptible to front-running. The spender of the allowance can send a competing `transferFrom` transaction and therefore transfer $X + Y$ tokens.

[3] https://github.com/ethereum/solidity/releases
[4] https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729

This issue can either be addressed in client applications by performing two transactions, where the first transaction resets the allowance to `0`, or `increaseAllowance` and `decreaseAllowance` functions can be introduced to allow a safe allowance adjustment in a single transaction.

Likelihood: Low
Impact: Medium

Fixed: STOKR solved the issue by adding the two functions `increaseAllowance` and `decreaseAllowance`. STOKR also added a `require()` to check for over- and underflows.

Design Issues

This section lists general recommendations about the design and style of STOKR's project. They highlight possible ways for STOKR to further improve the code.

Functions visbility can be set to external L ✓ Fixed

There are a number of functions declared as `public` when they could also be set to `external`. A non-exhaustive list of these functions is:

- `distributeTokensViaPublicSale()`
- `distributeTokensViaPrivateSale()`
- `addToWhitelist()`
- `removeFromWhitelist()`
- `withdrawProfitShares()`
- `distributeRefunds()`
- `createNewProject()`

Functions with visibility `external` can directly read from `calldata`[5] and do not copy function arguments to memory. Thus, declaring these functions `external` might optimize the gas costs. If and how much gas is saved, depends on the compiler version and the optimization done by the compiler.

Fixed: STOKR fixed the issue by setting the visibility from `public` to `external`.

Failing checks silently continue L ✓ Acknowledged

STOKR uses an `if` in multiple places to perform a check when a `require` would make more sense. For example the second condition in `TokenRecoverable.sol` on line 39.

```
function setTokenRecoverer(address _newTokenRecoverer) public onlyOwner {
  require(_newTokenRecoverer != address(0x0), "New token recoverer is zero");

  if (tokenRecoverer!=address(0x0) && _newTokenRecoverer != tokenRecoverer) {
    emit TokenRecovererChange(_newTokenRecoverer);
  }
  tokenRecoverer = _newTokenRecoverer;
}
```

ChainSecurity sees no reason to allow token recoverer to be updated to a new address if the new address is the same as the current address. STOKR is advised to reevaluate the usage of `if` statements vs throwing an error in such cases as described above.

Acknowledged: STOKR partially solved the problem by only updating the value if it it differs from the current value. However, calling this function to update the value to the same value does still not result in an error.

Crowdsale continues if sold out L ✓ Acknowledged

In case a crowdsale is sold out, it continues until the `hasClosed` condition is fulfilled, which is that the `closingTime` has passed. Up until that time the `finalize` function is not callable. Hence, during this time tokens are not transferable and no deposits can be made even though no more tokens can be purchased.

[5] https://solidity.readthedocs.io/en/v0.5.3/types.html?highlight=external#data-location%7D

Acknowledged: STOKR acknowledged the issue and explained that this behavior is intended.

Remaining tokens might not be purchasable L ✓ Acknowledged

The crowdsale enforces a `tokenPurchaseMinimum` for each token purchase. This can lead to issues towards the end of a crowdsale in case the crowdsale is close to selling out. In particular, it might be impossible to purchase remaining tokens.

As an example let's say that `tokenPurchaseMinimum = 100` and that `tokenRemainingForPublicSale = 80`. Hence, 80 tokens are still for sale. If a buyer tries to purchase 80 tokens, the purchase will fail as it is below the minimum. If a buyer tries to purchase the minimum of 100 tokens, it will fail, because there are only 80 tokens left. Obviously, the impact and likelihood of this issue depend on the choice of the parameters.

Acknowledged: STOKR is aware of this issue and acknowledges it.

Whitelisting of Token Recovery Address is not Enforced L ✓ Fixed

In the documentation, STOKR states that the whitelist defines which addresses "are able to send or receive tokens". This is ensured during regular transfers. However, as part of the `recoverToken` function, tokens can also be transferred and there no whitelist check is performed.

Fixed: STOKR solved the problem by adding the `onlyWhitelisted` modifier to the `recoverTokens` function.

Recommendations / Suggestions

- The function `transferOwnership()` transfers the ownership directly to the address given in the function's argument. In case of a mistake, the ownership will be transferred to some random account and is most likely "lost". Therefore, client could consider using a scheme in which the new owner needs to claim the ownership, to finally get it. This makes sure that at least the account is controlled by some user.
- In `MintingCrowdSale.sol` and `ProfitSharing.sol` STOKR makes use of the fallback function to catch ether sent to the contract and call `buyTokens()`. Since the fallback function is not only called for plain ether transfers (without data) but also when no other function matches, STOKR should check that the data is empty if the fallback function is intended to be used only for the purpose of forwarding ether to `buyTokens()`. Otherwise, callers will not notice if your contract is used incorrectly and functions that do not exist are called[6].
- The storage variable `deploymentBlockNumber` in `StokrProjectManager` is only set once in the constructor. The variable is not used anywhere else. If it is not required urgently by any other interacting contract CHAINSECURITY is not aware of, STOKR could consider removing the variable.
- STOKR might consider using the `indexed` keyword in some logged events. This might make sense to later better search through the events.
- The token contract has a special role called token recoverer. In most places of the code, it is referred to as `tokenRecoverer`. However, there are also multiple occurrences where this role is called `keyRecoverer`. This naming could be harmonized.
- There are different implementations of the ERC20 token standard, but some have started emitting a `Approval` event whenever the token allowance has been changed. In case, STOKR wants to adapt this, an additional `Approval` event could be emitted from the `transferFrom` function.
- In the code, there are two semantically identical getter functions. The two functions `mintingFinished()` and `totalSupplyIsFixed()` both return the value of the variable `totalSupplyIsFixed`. Therefore, one of the two getter functions could be omitted to achieve some gas savings during deployment.

[6] https://consensys.github.io/smart-contract-best-practices/recommendations/#check-data-length-in-fallback-functions

Notes

This section highlights additional remarks about the behaviour of the smart contracts. These are not considered as issues. However, CHAINSECURITY still wants to point them out for completeness and for educational purposes.

Rounding Errors ✓ Acknowledged

(Unsigned) integer divisions generally suffer from rounding errors. The same holds true for divisions inside the EVM. Therefore, the results of arithmetic operations can be imprecise. The effects of these errors can be reduced by ordering arithmetic operations in a numerically stable manner. However, even then minor errors (e.g. in the order of one token wei) can occur.

In the STOKR contracts, any user can call `updateProfitShare(A)` on another user `A` to trigger additional rounding errors and therefore effectively lower the token balance of `A`. Furthermore, the rounding errors during the calculation of profit shares will lead to an accumulated amount of "lost" tokens inside the `ProfitSharing` contract over time. However, CHAINSECURITY expects both of these errors to have a negligible effect due to use of 18 decimals.

Acknowledged: STOKR acknowledged the theoretical possibility, but also correctly pointed out that a potential attacker has no economic incentive to perform such an attack, as it: (i) only incurs a tiny damage on the victim, (ii) incurs gas costs on the attacker, and (iii) does not provide any direct benefit to the attacker.

Disclaimer