AdEx Network

ADX Token Contract Audit

July 2020

Table of contents

Summary

Forkway LTD was engaged in security auditing of the new ADX token contract. AdEx is a blockchain software development company that provides products answering on significant needs in the advertising industry.

This security review is focused on code quality and functionality, addressing not only potential security issues but also readability, transparency and intent.

We reviewed the contracts manually, as well as through automated tools. We reviewed the JS tests that the AdEx team provided.

Scope of audit

Commit: 6e408e75397ecec9c6c642731de71e1903ae1d6f

Files: ADXToken.sol

Contracts:

- ADXToken
- ADXSupplyController
- ADXFlashLoans

Auditor: Stas Oskin, stas@forkway.co

Dependencies such as SafeERC20 and SafeMath have been covered in previous protocol audits, namely the Sigma Prime Audit.

Disclaimer

Forkway LTD holds no responsibility for the findings in this security audit. We do not provide any guarantees or warranties related to the function of the smart contract system.

Conclusion

The reviewed smart contract system is simple (130 LoC as of commit 6e408e75397ecec9c6c642731de71e1903ae1d6f) and features three well isolated contracts. It follows good coding standards and practices, with no readability issues.

During the report, we discovered several observations and minor issues related to the new functionality and the changes from the old token contract. **All were quickly addressed by the AdEx team in a satisfactory manner.**

The ADXToken contract **does not** include upgradability, pausability, built-in fees, locked tokens, ERC777 or any other features that we consider being vectors of risk in an ERC20 contract.

Observations

We noticed a few items that while not being security issues, still stand out as important differences from the previous contract, which is deployed at https://etherscan.io/token/0x4470BB87d77b963A013DB939BE332f927f2b992e.

New monetary policy

The previous contract was restricted to 100M ADX while the new system is restricted to 150M by the supply controller. The extra 50M tokens can be minted by AdEx's governance addresses.

We recommend transparently communicating this policy change to ADX token holders, explaining why it's needed.

AdEx team comment: The extra 50M tokens are intended to be distributed over at least 2 years. Our estimation is that we will distribute 5-10M every year. The purpose of this distribution is to incentivize staking, similar to how Compound distributes COMP to incentivize lending. The distribution method is based on OUTPACE payment channels and is similar to the current distribution method implemented here: https://github.com/AdExNetwork/adex-validator/blob/master/scripts/distribute-rewards.js. Most importantly, the new policies and their purpose will be announced in early August.

Status: ✔Resolved

Governance through AdEx's multisig

The ADXSupplyController relies on governance addresses. The AdEx team informed us that their multisig (0x23c2c34f38ce66ccc10e71e9bb2a06532d52c5e9) will be used for this purpose.

The governance addresses have two levels of privilege:

- Mint: allows them to mint tokens, up to the supply cap (150M)
- All: allows them to add other governance addresses and change the supply controller

AdEx team comment: This is necessary in order to upgrade to a more decentralized governance system in the future. Furthermore, it enables us to act quickly in the beginning in order to migrate the staking pools and initialize the flash loans pool. The multisig is 3/5, with all the signers using HW wallets - 3 of them are team members and 2 are advisors. In early future,

we intend to replace the governance by multisig to a governance by DAO (please keep confidential).

Status: ✔Resolved

Lack of vesting features

While the previous contract had vesting features built in, the new ADXToken contract does not.

AdEx team comment: This feature can be still implemented by an external contract in a much safer way. The built-in grant feature (taken from OpenZeppelin) had a method called revokeTokenGrant, which enabled tricking exchanges by granting them vested tokens and then revoking the grant. This was easy to work around, but we decided to drop the feature for increased security.

Status: ✔Resolved

Flash loans and ADXFlashLoans

The ADXFlashLoans contract provides the ability to get flash loans on-chain. This is not related to or dependent on either ADXToken or ADXSupplyController. Furthermore, it can be used with any ERC20 token. **As such, we believe it should be moved from ADXToken.sol** to another source file.

It is also worth noting that ADXFlashLoans requires ADX to be deposited to it in order to function. With no fees, incentives and ability to withdraw implemented, sending ADX tokens to this contract is essentially burning them.

AdEx team comment: We agree with the observations. We are going to move ADXFlashLoans to a separate source file. As for the incentive - we have set aside 5M of the newly minted ADX for the flash loans - it's part of the newly planned monetary policy (tokenomics). It's important to point out in the final report that we will not be deploying the flash loans feature immediately at the new token contract launch.

Status: ✔Resolved in commit ed1802f751ffe2162e9db538cc6e491b49d2a0cb, branch new-token-audit

Issues

Migrating staked tokens

Severity: Medium

We understand that a core part of the AdEx system is the Staking contract (G0 audit).

As of the time of writing, there are 5641215.9971 ADX staked with AdEx's on their staking portal here: https://staking.adex.network/

We asked the AdEx team how will the migration affect these staked tokens, as being in a contract there won't be possible to call swap on them, and their owners must initial unbonding and wait for it to complete. Having said that, it's important to point out that swap is **not time restricted**, and it will be always possible to perform it. As such, it's possible that stakers request unbond, wait for it to mature (30 days), call swap and then bond again.

However, **this is disadvantageous to stakers**, as they will lose the new staking rewards while they are waiting for the unbond to mature, due to AdEx stopping calculating rewards as soon as unbonding starts.

Recommendation: We recommend that AdEx team modifies the reward distribution system to enable sending rewards to stakers waiting for unbond to complete, or that they present a plan of migrating the Staking contract.

AdEx team comment: We are going to auto-migrate the stakers automatically. The way this is going to work is by fully slashing the old pool, then creating a new Staking contract that auto-initializes all the previous bonds in it's constructor, and depositing the equivalent amount of the new token on the contract. Stakers won't lose anything and won't have to do anything. This is going to be revealed in the next token migration announcement in early August.

Status: ✔Resolved

Governance operator can lock themselves out of SupplyController

Severity: Low

In the ADXSupplyController contract, a governance address may call setGovernance to remove their own privileges. This is intended behavior, but if there are no other governance addresses set, the ADXSupplyController will remain without governance and as such with no ability to mint or be changed.

Recommendation: We recommend that the AdEx team disallows a governance address from removing its own privilege.

AdEx team comment: this is intended behavior, as we need to be able to step down control when the DAO governance transition has completed. We realize that we need to be careful with how we call setGovernance in order to avoid getting locked out.

Status: ✔Resolved

mint() can be called before previous token holders have swapped, leading to a higher total supply once all old tokens have been swapped

Severity: Low

The ADXSupplyController provides a mint() function which allows the governance (currently controlled by the AdEx team) to mint new tokens, up to 150M total supply (line 36). However, initially, before holders of the previous token have called swap(), the totalSupply of the token is actually 0.

This allows for the hypothetical scenario of:

- AdEx deploys the new contracts
- AdEx immediately mints 150M after 10 August (up to the ADXSupplyController restriction)
- all token holders swap, minting another 100M in the process
- total supply is now 250M

We are downgrading this to *low* severity as only the AdEx team can take advantage of this, and it will be a public knowledge if they really do this. Nonetheless, we strongly recommend that it's corrected.

Recommendation: introduce stronger time locks that only allow the team to mint up to 50M until one month from the migration, allowing time for holders to upgrade their tokens in the meantime before unlocking the full "up to 150M" mint ability.

AdEx team comment: we agree with this observation, and we will implement the recommendation before deploying; we will proceed in the following way: deploy contracts, mint 5M for the flash loan pool, mint ~5M for the staking pool, mint 5M for rewards; then announce the token upgrade UI and encourage everyone to upgrade

Status: ✔**Resolved** in commit c718f62ac464a8dc11d8179544c702c49b7cc53f