



SOLIDProof
Bring trust into your projects

**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY

Exchange Trade Coin **AUDIT**

SECURITY ASSESSMENT

06. November, 2023

FOR



SolidProof.io



@solidproof_io



Introduction	3
Disclaimer	3
Project Overview	4
Summary	4
Social Medias	4
Audit Summary	5
File Overview	6
Imported packages	6
Components	7
Exposed Functions	7
Capabilities	8
Inheritance Graph	9
Audit Information	10
Vulnerability & Risk Level	10
Auditing Strategy and Techniques Applied	11
Methodology	11
Overall Security	12
Upgradeability	12
Ownership	13
Ownership Privileges	14
Minting tokens	14
Burning tokens	15
Blacklist addresses	16
Fees and Tax	17
Lock User Funds	18
Centralization Privileges	19
Audit Result	21



Introduction

SolidProof.io is a brand of the officially registered company MAKE Network GmbH, based in Germany. We're mainly focused on Blockchain Security such as Smart Contract Audits and KYC verification for project teams.

Solidproof.io assess potential security issues in the smart contracts implementations, review for potential inconsistencies between the code base and the whitepaper/documentation, and provide suggestions for improvement.

Disclaimer

SolidProof.io reports are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc'...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of the security or functionality of the technology we agree to analyze.

Project Overview

Summary

Project Name	Exchange Trade Coin
Website	https://xtc.exchange/
About the project	XTC is a digital platform that aims to provide users with a unique and engaging online gambling and DEX experience. Unlike traditional casinos, XTC combines social interaction with gambling and DEX, creating a dynamic environment where users can enjoy their favorite casino games while also connecting with others. One of the standout features of XTC is its daily yield system, which allows users to earn rewards based on the performance of the casino.
Chain	Binance smart chain
Language	Solidity
Codebase	XTCToken: https://bscscan.com/address/0x9744b01247779c596acfc7e5c6b963eb7e1be7e3#code ICO: https://bscscan.com/address/0xabe281db019b96cf90896227bb4259c4e6991278#code
Commit	N/A
Unit Tests	Not Provided

Social Medias

Telegram	https://t.me/xtcannouncement
Twitter	https://twitter.com/xtcexchange
Facebook	N/A
Instagram	N/A
GitHub	N/A
Reddit	N/A
Medium	N/A
Discord	N/A
YouTube	N/A
TikTok	N/A
LinkedIn	N/A



Audit Summary

Version	Delivery Date	Change Log
v1.0	24. October 2023	<ul style="list-style-type: none">· Layout Project· Automated/ Manual-Security Testing· Summary
v1.2	06. November 2023	<ul style="list-style-type: none">· Reaudit

Note – The following audit report presents a comprehensive security analysis of the smart contract utilized in the project that includes outside manipulation of the contract's functions in a malicious way. This analysis did not include functional testing (or unit testing) of the contract/s logic. We cannot guarantee 100% logical correctness of the contract as we did not functionally test it. This includes internal calculations in the formulae used in the contract.



File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with an SHA-1 Hash.

File Name	SHA-1 Hash
contracts/ICO.sol	9e089e07d15fb622e8f74a9dbcb78f194577be55
contracts/XTC.sol	afee887cbe9f8c0c8339ed987bc73c7b2bec9959

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) be an indication of a changed state or potential vulnerability that was not the subject of this scan.

Imported packages.

Used code from other Frameworks/Smart Contracts.

N/A

Note for Investors: We only audited contracts mentioned in the scope above. All contracts related to the project apart from that are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way. Also, The contract contains the private ICO so please make sure to check and look carefully before investment we are not responsible for any security concerns in the private ICO.



External/Public functions

External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.

State variables

State variables are variables that are stored on the blockchain as part of the contract's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be needed within visibility modifier, such as public, private or internal, which determines the access level of the variable.

Components

 Contracts	 Libraries	 Interfaces	 Abstract
6	4	10	1

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

 Public	 Payable			
108	5			
External	Internal	Private	Pure	View
60	103	7	21	54

StateVariables

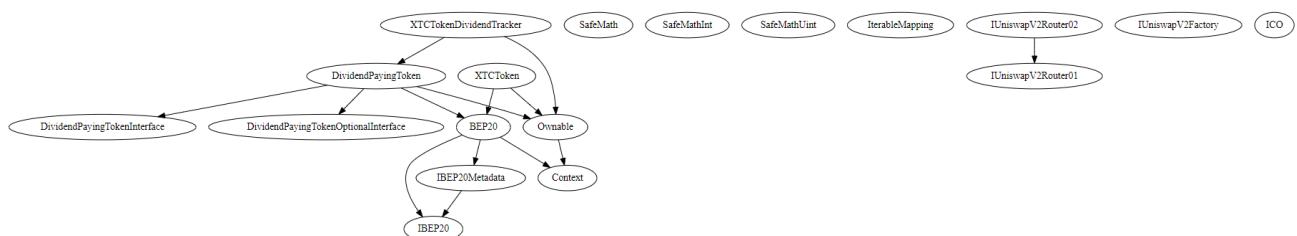
Total	 Public
59	42

Capabilities

Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
0.8.18	-----	Yes		-----
 Transfer s ETH	 Low-Level Calls	 DelegateCa ll	 Uses Hash Function s	 ECRecover
Yes				 New/Create/Create2 yes → NewContract: XTCTokenDivide ndTracker

Inheritance Graph

An inheritance graph is a graphical representation of the inheritance hierarchy among contracts. In object-oriented programming, inheritance is a mechanism that allows one class (or contract, in the case of Solidity) to inherit properties and methods from another class. It shows the relationships between different contracts and how they are related to each other through inheritance.





Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit the vulnerability and the impact of that event on the organization or system. The risk level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 - 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 - 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 - 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 - 1.9	A vulnerability that has informational character but is not affecting any of the code.	An observation that does not determine a level of risk



Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - a. Reviewing the specifications, sources, and instructions provided to SolidProof to ensure we understand the size, scope, and functionality of the smart contract.
 - b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
 - c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.
2. Testing and automated analysis that includes the following:
 - a. Test coverage analysis determines whether test cases cover code and how much code is executed when those test cases are executed.
 - b. Symbolic execution, which is analysing a program to determine what inputs cause each part of a program to execute.
3. Review best practices, i.e., review smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.
4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.



Overall Security Upgradeability

Contract is not an upgradable

 Deployer cannot update the contract with new functionalities.

Description	The contract is not an upgradeable contract. The Deployer is not able to change or add any functionalities to the contract after deploying.
Comment	N/A





Ownership

The ownership is not renounced.

The ownership is not renounced.

Description	<p>The owner has not renounced the ownership that means that the owner retains control over the contract's operations, including the ability to execute functions that may impact the contract's users or stakeholders. This can lead to several potential issues, including:</p> <ul style="list-style-type: none">• Centralizations• The owner has significant control over contract's operations.
Example	N/A
Comment	N/A

Note – *The contract cannot be considered as renounced till it is not deployed or having some functionality that can change the state of the contract.*



Ownership Privileges

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens

Minting tokens refer to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or designated authority, who has the ability to add new tokens to the network's total supply.

Contract owner cannot mint new tokens.

 **The owner cannot mint new tokens.**

Description	The owner is not able to mint new tokens once the contract is deployed.
Comment	N/A



Burning tokens

Burning tokens is the process of permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens	 The owner cannot burn tokens.
Description	The owner is not able burn tokens without any allowances.
Comment	N/A



Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

Contract owner cannot blacklist addresses.

 **The owner cannot blacklist wallets.**

Description	The owner cannot blacklist addresses for transferring of tokens.
Comment	N/A



Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the cost of running the contract, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner cannot set fees more than 25%.



The owner cannot set fees more than 25%.

Description	The owner cannot set fees more than 25%.
Comment	N/A



Lock User Funds

In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When token or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.

Contract owner cannot lock functions.

 The owner cannot lock the contract.

Description	The owner cannot lock funds in the contract.
Comment	N/A



Centralization Privileges

Centralization can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example, if the contract is controlled by a single entity or if certain participants have special permissions or abilities that others do not.

In the project, there are authorities that have access to the following functions:

File	Privileges
XTC.sol	<ul style="list-style-type: none">➤ The owner can update the dividend tracker address.➤ The owner can update the uniswapv2 router address.➤ The owner can exclude the wallets from fees.➤ The owner can exclude multiple wallets from fees at a time.➤ The owner can update the marketing wallet address.➤ The owner can set the automated market pair address after the initial deployment.➤ The owner can update the processing gas fees between 20000 to 50000.➤ The owner can set the claim wait time between 1 hour to 24 hours.➤ The owner can exclude wallets from dividends.➤ The owner can set the max transaction amount of not less than 0.1% of the total supply.➤ The owner enable/disable the swapping.➤ The owner can set any arbitrary value in the minimum swap amount.➤ The owner can set any arbitrary value in the minimum token balance for dividends.➤ There is a burn fee of 1% present in the contract which means 1% of token value will be deducted during each transaction from the user's wallet.➤ The contract contains a total fee of 4% which will deducted from the user's amount after each transaction.
ICO.sol	<ul style="list-style-type: none">➤ The admin can withdraw the XTC amount from the contract.➤ The admin can start ICO only once.➤ Any address can end ICO once the current timestamp



is greater than the end timestamp or the raised amount is greater than the hard-capped value.

- The liquidity of the contract is getting added to the admin wallet.

Recommendations

To avoid potential hacking risks, it is advisable for the client to manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart-contract-based accounts, such as multi-signature wallets.

Here are some suggestions of what the client can do:

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security e.g. Gnosis Safe
- Use of a timelock at least with a latency of e.g. 48-72 hours for awareness of privileged operations
- Introduce a DAO/Governance/Voting module to increase transparency and user involvement
- Consider Renouncing the ownership so that the owner cannot modify any state variables of the contract anymore. Make sure to set up everything before renouncing.



Audit Result

Critical Issues

No critical issues

High Issues

No high issues

Medium Issue

#1 | Liquidity is added to externally owned account.

File	Severity	Location	Status
ICO.sol	Medium	L283-293	Open

Description – The contract's liquidity is automatically added to the 'admin' address, which is not recommended because, in an extreme scenario, this can be used to drain liquidity from the contract.

Alleviation – The contract liquidity is now getting added to the zero address.

#2 | Owner can lock tokens.

File	Severity	Location	Status
XTC.sol	Medium	L916-920	Fixed

Description – The owner can set any arbitrary value in the max transaction, which can lock the tokens for an indefinite period of time which is not recommended. Add a certain threshold where the value cannot be less than that number.

Alleviation – The owner cannot set a maximum transaction amount of not less than 0.1% of the total supply.



Low Issue

#1 | Missing events arithmetic.

File	Severity	Location	Status
XTC.sol	Low	L621-631, L633-640, L655-659, L663-666, L916-920	ACK

Description – Emit all the critical parameter changes.

#2 | Missing Visibility.

File	Severity	Location	Status
XTC.sol	Low	L196	Fixed
ICO.sol	Low	L112, 114, 115	Fixed

Description – It is recommended to add 'public' or 'private' during the initialization of the state variable.

#3 | Local variable shadowing.

File	Severity	Location	Status
XTC.sol	Low	L220-227	Fixed

Description – Rename the component that shadows another component.

#4 | Remove safemath library.

File	Severity	Location	Status
XTC.sol	Low	L66-119	ACK

Description – compiler version above 0.8.0 has the ability to control arithmetic overflow/underflow, it is recommended to remove the unwanted code in order to avoid high gas fees.



#5 | Imprecise arithmetic operation order.

File	Severity	Location	Status
XTC.sol	Low	L329-383	Fixed

Description – It is recommended that the order of arithmetic operations should be multiplied before division in order to avoid any issues.

Alleviation – Functionality is removed from the contract.

Informational Issue

#1 | NatSpec Documentation missing.

File	Severity	Location	Status
XTC.sol	Informational	--	ACK
ICO.sol	Informational	--	ACK

Description – If you started to comment on your code, also comment on all other functions, variables, etc.

Legend for the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.



**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY