Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project: (PoS) Wrapped BTC
Website: wbtc.network
Platform: Polygon
Language: Solidity
Date: April 8th, 2025

Table of Contents

Email: audit@EtherAuthority.io

THIS IS A SECURITY AUDIT REPORT DOCUMENT THAT MAY CONTAIN INFORMATION THAT IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

Email: audit@EtherAuthority.io

Introduction

As part of EtherAuthority's community smart contract audit initiatives, the smart contract of the WBTC Token from wbtc.network was audited. The audit was performed using manual analysis and automated software tools. This report presents all the findings regarding the audit performed on April 8th, 2025.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

The UChildERC20 contract is an **upgradeable ERC20 token** designed for **child chains like Polygon**. It supports **native meta-transactions** via **EIP-712** signatures, allowing users to perform actions without directly paying gas. The contract integrates with a root/child token bridge using a **depositor role** to enable **deposits** and **withdrawals** between chains.

Key Features

- **Upgradeable Structure**: Uses an initialize function instead of a constructor for proxy deployments.
- **Native Meta-Transactions**: Implements executeMetaTransaction() using EIP-712 for signature-based transaction execution via relayers.
- **Custom Context**: Uses ContextMixin to correctly identify msgSender() in relayed calls.
- **Child Chain Bridge Support**: Includes deposit() and withdraw() functions, allowing minting and burning on the child chain.
- **Access Control**: Uses AccessControlMixin to manage roles like DEFAULT_ADMIN_ROLE and DEPOSITOR_ROLE.
- **Dynamic Token Info**: Admins can update the token name and domain separator using changeName().

Audit scope

Name	Code Review and Security Analysis Report for (PoS) Wrapped BTC Token Smart Contract
Platform	**Polygon**
File 1	UChildERC20Proxy.sol
File 1 Smart Contract	0x1bfd67037b42cf73acf2047067bd4f2c47d9bfd6
File 2	UChildERC20.sol
File 2 Smart Contract	0x7ffb3d637014488b63fb9858e279385685afc1e2
Audit Date	April 8th, 2025

Email: audit@EtherAuthority.io

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: ● Name: (PoS) Wrapped BTC ● Symbol: WBTC	**YES, This is valid.**
Key Feature ● **Upgradeable ERC20 Token:** ○ Uses an `initialize()` function for deployment via a proxy. ○ Supports dynamic setting of name, symbol, and decimals. ○ Admins can change the token name post-deployment using `changeName()`. ● **Native Meta-Transactions:** ○ Users can sign transactions off-chain and let relayers submit them. ○ Relayers pay gas, users stay gasless. ○ Based on EIP-712 typed data. ○ Ensures replay protection via user-specific `nonces`. ○ Handles `msg.sender` correctly in relayed transactions via `ContextMixin`. ● **Polygon Child Chain Integration:** ○ Compatible with Polygon's PoS bridge architecture. ○ Uses `DEPOSITOR_ROLE` to restrict access to the deposit function.	**YES, This is valid.**

- deposit(): Mints tokens for users when deposits are made from the root chain.
- withdraw(): Burns tokens on the child chain to initiate withdrawal to the root chain.

- **Role-Based Access Control:**
  - Based on `AccessControlMixin`.
  - Roles:
    - DEFAULT_ADMIN_ROLE: Full control (can change name, manage roles).
    - DEPOSITOR_ROLE: Only allowed to call `deposit()`.
  - Protects sensitive functions from unauthorized access.
- **EIP-712 Domain Separation:**
  - Defines a domain separator for secure signature verification.
  - Domain updates automatically when the token name is changed via `changeName()`.
- **msgSender Abstraction:**
  - Custom `_msgSender()` returns the correct user even if the call is made through a relayer (meta-tx).
  - Prevents misuse of `msg.sender` in meta-tx enabled contracts.
- **Utility Functions:**
  - getNonce(address user): Returns the current nonce for a user.
  - executeMetaTransaction(...): Executes a meta-transaction with signature verification.

Audit Summary

According to the standard audit assessment, the Customer's solidity-based smart contract is **“Secured.”** Also, these contracts contain owner control, which does not make them fully decentralized.

We used various tools like Slither, Solhint, and Remix IDE. At the same time, this finding is based on a critical analysis of the manual audit.

All issues found during automated analysis were manually reviewed, and applicable vulnerabilities are presented in the Audit overview section. The general overview is presented in the AS-IS section, and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium, 0 low, and 6 very low-level issues.

Investors' Advice: A Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner-controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Moderated
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Moderated
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Moderated
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Moderated
Gas Optimization	“Out of Gas” Issue	Passed
	High consumption ‘for/while’ loop	Passed
	High consumption ‘storage’ storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage is not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: **PASSED**

Code Quality

This audit scope has 1 smart contract. Smart contracts contain Libraries, Smart contracts, inheritance, and Interfaces. This is a compact and well-written smart contract.

The libraries in (PoS) Wrapped BTC Token are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address, and its properties/methods can be reused many times by other contracts in the WBTC Token.

The EtherAuthority team has no scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are well commented on in the smart contract. Ethereum's NatSpec commenting style is recommended.

Documentation

We were given a WBTC Token smart contract code in the form of a polygonscan web link.

As mentioned above, code parts are well commented on. And the logic is straightforward. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Use of Dependencies

As per our observation, the libraries used in this smart contract infrastructure that is based on well-known industry standard open-source projects.

Apart from libraries, its functions are not used in external smart contract calls.

AS-IS overview

UChildERC20.sol : Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	initialize	external	initializer	No Issue
3	_msgSender	internal	Passed	No Issue
4	changeName	external	Missing Events for Key Actions	Refer Audit Findings
5	deposit	external	No Upper Limit on `deposit()` Minting, Missing Events for Key Actions	Refer Audit Findings
6	withdraw	external	Missing Events for Key Actions, Unrestricted `withdraw()` Function	Refer Audit Findings
7	msgSender	internal	Passed	No Issue
8	executeMetaTransaction	write	`executeMetaTransaction()` Enables Arbitrary Internal Calls	Refer Audit Findings
9	hashMetaTransaction	internal	Passed	No Issue
10	getNonce	read	Passed	No Issue
11	verify	internal	Passed	No Issue
12	_setupContractId	internal	Passed	No Issue
13	only	modifier	Passed	No Issue
14	name	read	Passed	No Issue
15	setName	internal	Passed	No Issue
16	setSymbol	internal	Passed	No Issue
17	symbol	read	Passed	No Issue
18	decimals	read	Passed	No Issue
19	setDecimals	internal	Passed	No Issue
20	totalSupply	read	Passed	No Issue
21	balanceOf	read	Passed	No Issue
22	transfer	write	Passed	No Issue
23	allowance	read	Passed	No Issue
24	approve	write	Passed	No Issue
25	transferFrom	write	Passed	No Issue
26	increaseAllowance	write	Passed	No Issue
27	decreaseAllowance	write	Passed	No Issue
28	_transfer	internal	Passed	No Issue
29	_mint	internal	Passed	No Issue
30	_burn	internal	Passed	No Issue
31	_approve	internal	Passed	No Issue
32	_setupDecimals	internal	Passed	No Issue
33	_beforeTokenTransfer	internal	Passed	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss, etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens being lost
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets, which can't have a significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations, and info statements can't affect smart contract execution and can be ignored.

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

No medium severity vulnerabilities were found.

Low

No low severity vulnerabilities were found.

Very Low / Informational / Best practices:

(1) `executeMetaTransaction()` Enables Arbitrary Internal Calls:

The `functionSignature` in `executeMetaTransaction()` is passed directly to `address(this).call()`. This allows any function on the contract to be invoked, which could be dangerous if there are sensitive functions callable internally.

Resolution: Restrict the callable functions via a whitelist or ensure critical functions are protected from meta-transaction execution. Validate selectors or design a trusted wrapper interface.

(2) No Upper Limit on `deposit()` Minting:

The contract allows minting of arbitrary token amounts on the child chain.

Resolution: While expected for bridged tokens, consider adding sanity checks or use bridge-side rate limiting.

(3) Unused Constants in `ChainConstants`:

`ROOT_CHAIN_ID`, `CHILD_CHAIN_ID`, and their byte equivalents are declared but not

used.

Resolution: Remove unused constants or implement them into EIP-712 domain hashing if intended.

(4) Missing Events for Key Actions:

Functions like `deposit()`, `withdraw()`, and `changeName()` do not emit events.

Resolution: Emit events for tracking off-chain activity and improved transparency.

(5) Unrestricted `withdraw()` Function:

Anyone can call `withdraw()` and burn their tokens. While this seems fine, there's no event emitted or status flag for bridging mechanisms to observe.

Resolution: Emit an event (e.g., `Withdraw(address indexed user, uint256 amount)`) to allow off-chain bridges to track and verify withdrawals.

(6) Hardcoded Chain IDs in `ChainConstants`:

Using hardcoded chain IDs like `1` and `137` may cause confusion or incompatibility if deployed on other networks or testnets.

Resolution: Allow chain ID to be set dynamically during initialization or store them as part of a configuration contract.

Centralization Risk

This smart contract has some functions that can be executed by the Admin (Owner) only. If the admin wallet's private key is compromised, then it creates trouble. The following are Admin functions:

UChildERC20.sol

- changeName: The admin can change the name.

Conclusion

We were given a contract code in the form of a polygonscan web link. We have used all possible tests based on the given objects as files. We observed 6 informational issues in the smart contract, and those issues are not critical. So, **it's good to go for production**.

Since possible test cases can be unlimited for such smart contract protocols, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover the maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

The security state of the reviewed smart contract, based on standard audit procedure scope, is **"Secured".**

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's website to get a high-level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early, even if they are later shown not to represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally, we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation are an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract by the best industry practices at the date of this report, about: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

Because the total number of test cases is unlimited, the audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

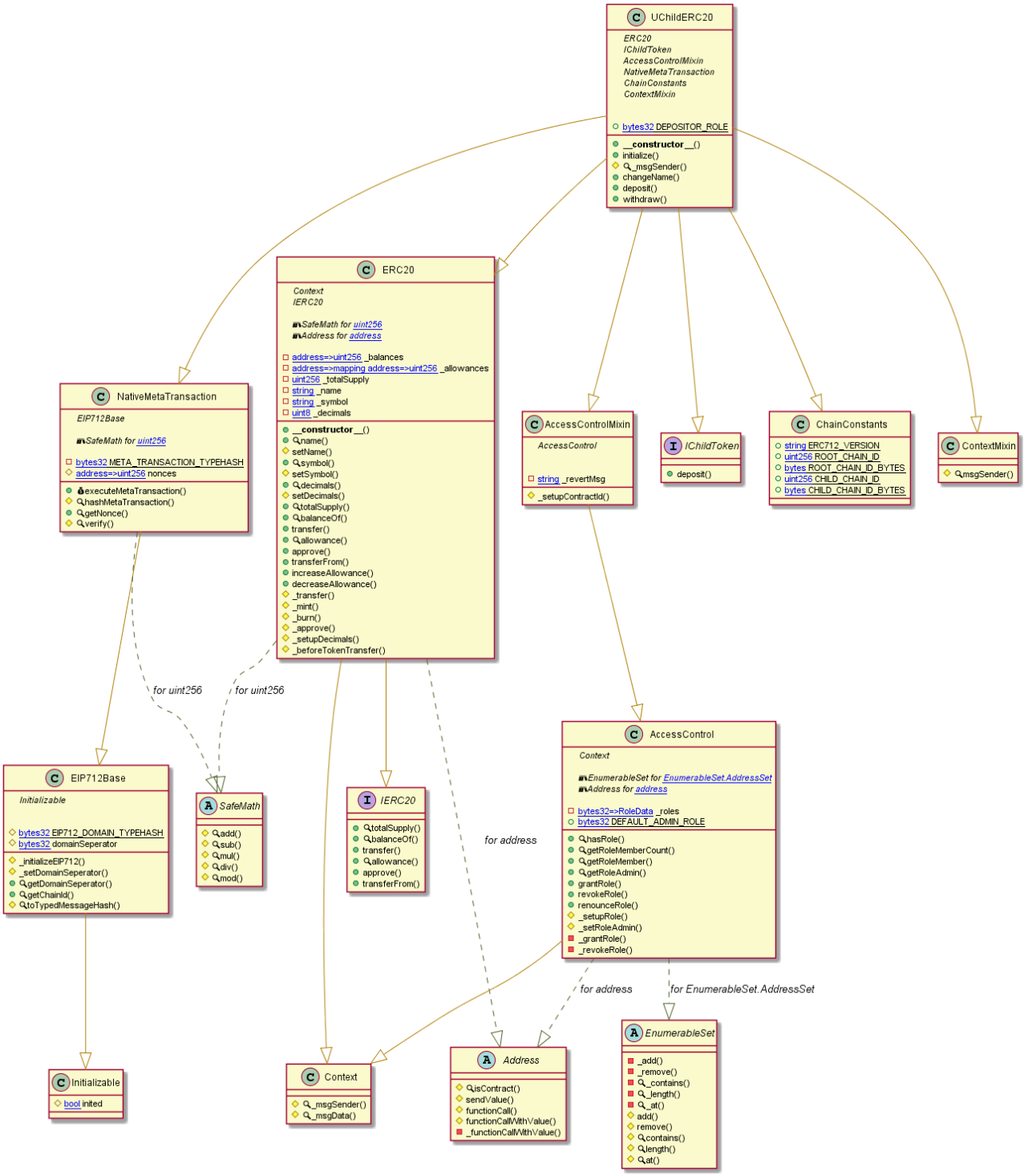
Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can't guarantee explicit security of the audited smart contracts.

Email: audit@EtherAuthority.io

Appendix

Code Flow Diagram - (PoS) Wrapped BTC Token



Slither Results Log

Slither is a Solidity static analysis framework that uses vulnerability detectors, displays contract details, and provides an API for writing custom analyses. It helps developers identify vulnerabilities, improve code comprehension, and prototype custom analyses quickly. The analysis includes a report with warnings and errors, allowing developers to quickly prototype and fix issues.

We did the analysis of the project altogether. Below are the results.

Slither Log >> UChildERC20.sol

```
INFO:Detectors:
Contract locking ether found:
	Contract UChildERC20 (UChildERC20.sol#1488-1564) has payable functions:
	 - NativeMetaTransaction.executeMetaTransaction(address,bytes,bytes32,bytes32,uint8)
(UChildERC20.sol#1361-1395)
	But does not have a function to withdraw the ether
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#contracts-that-lock-ether
INFO:Detectors:
Version constraint 0.6.6 contains known severe issues
(https://solidity.readthedocs.io/en/latest/bugs.html)
	- MissingSideEffectsOnSelectorAccess
	- AbiReencodingHeadOverflowWithStaticArrayCleanup
	- DirtyBytesArrayToStorage
	- NestedCalldataArrayAbiReencodingSizeValidation
	- SignedImmutables
	- ABIDecodeTwoDimensionalArrayMemory
	- KeccakCaching
	- EmptyByteArrayCopy
	- DynamicArrayCleanup
	- MissingEscapingInFormatting
	- ArraySliceDynamicallyEncodedBaseType
	- ImplicitConstructorCallvalueCheck.
It is used by:
	- 0.6.6 (UChildERC20.sol#1214)
	- 0.6.6 (UChildERC20.sol#1234)
	- 0.6.6 (UChildERC20.sol#1242)
	- 0.6.6 (UChildERC20.sol#1256)
	- 0.6.6 (UChildERC20.sol#1332)
	- 0.6.6 (UChildERC20.sol#1438)
	- 0.6.6 (UChildERC20.sol#1452)
```

```
        - 0.6.6 (UChildERC20.sol#1479)
solc-0.6.6 is an outdated solc version. Use a more recent version (at least 0.8.0), if possible.
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Redundant expression "this (UChildERC20.sol#27)" inContext (UChildERC20.sol#21-30)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
executeMetaTransaction(address,bytes,bytes32,bytes32,uint8) should be declared external:
        - NativeMetaTransaction.executeMetaTransaction(address,bytes,bytes32,bytes32,uint8)
(UChildERC20.sol#1361-1395)
Moreover, the following function parameters should change its data location:
functionSignature location should be calldata
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-decl
ared-external
INFO:Slither:UChildERC20.sol analyzed (15 contracts with 93 detectors), 21 result(s) found
```

Solidity Static Analysis

Static code analysis is used to identify many common coding problems before a program is released. It involves examining the code manually or using tools to automate the process. Static code analysis tools can automatically scan the code without executing it.

UChildERC20.sol

```
Gas costs:
Gas requirement of function UChildERC20.initialize is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 1504:4:

Gas costs:
Gas requirement of function UChildERC20.deposit is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 1546:4:

Guard conditions:
Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
Pos: 1392:8:

Delete from dynamic array:
Using "delete" on an array leaves a gap. The length of the array remains the same. If you want to remove the empty position you need to shift items manually and update the "length" property.
Pos: 846:12:
```

Solhint Linter

Solhint Linters are the utility tools that analyze the given source code and report programming errors, bugs, and stylistic errors. For the Solidity language, there are some linter tools available that a developer can use to improve the quality of their Solidity contracts.

UChildERC20.sol

```
Compiler version ^0.6.0 does not satisfy the ^0.5.8 semver
requirement
Pos: 1:8
Code contains empty blocks
Pos: 94:743
Compiler version ^0.6.0 does not satisfy the ^0.5.8 semver
requirement
Pos: 1:750
Explicitly mark visibility of state
Pos: 5:1347
Error message for require is too long
Pos: 9:1373
Avoid to use low level calls.
Pos: 51:1388
Error message for require is too long
Pos: 9:1423\
Compiler version 0.6.6 does not satisfy the ^0.5.8 semver requirement
Pos: 1:1478
Code contains empty blocks
Pos: 40:1497
```

Software analysis result:

This software reported many false positive results, some of which are informational issues. Therefore, those issues can be safely ignored.

Email: audit@EtherAuthority.io