VITAL BLOCK

NODE.JS DEPENDENCIES AUDIT REPORT

@Vital-Block

@VB_Audit

info@vitalblock.org

www.vitalblock.org
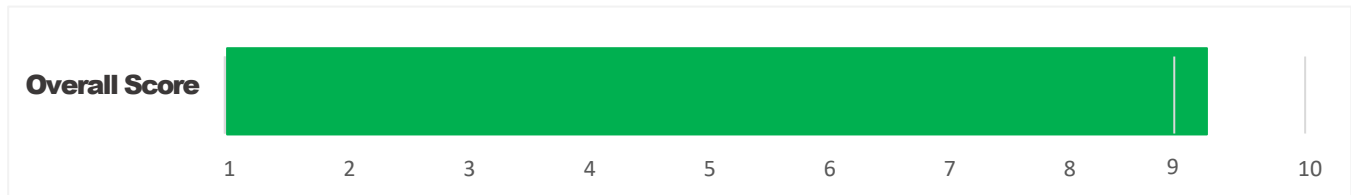
EXECUTIVE SUMMARY

Vital Block has performed the automated and manual analysis of the Node.js code. The code was reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical ! 🔴	Major " 🟠	Medium # 🟡	Minor $ 🟢	Unknown % 🟤
SECURITY	0	0	2	2	0
POPULARITY	0	0	1	2	0
MAINTENANCE	0	0	0	2	1
COMMUNITY	ACTIVE				

BITX - BACKEND Package Health Score **92/100.**

Please note that The Written Node.js Code aren't resistant to exploits, vulnerabilities and/or hacks. and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.

Please note that centralization privileges regardless of their inherited risk status - constitute an elevated impact on npm safety and security.

SCOPE OF WORK

Vital Block was consulted by BitX to conduct the Backend Audit of its Node.js source code. <u>The</u> <u>audit scope of work is strictly limited to mentioned Node.js file only:</u>

```
O Bitx-Backend
```

ℹ️   **Source Code and/or interfaces dependencies are not checked due to being out of scope.**

Verify audited Source code and project file below:

Language
Node.js

Project Name	BITX – BACKEND
License:	MIT
SECURITY	NO KNOWN SECURITY ISSUES

SECURITY CATEGORIES

Quickly assess the security posture of an open source project and its past versions. Further connecting your project with Snyk will offer fix advice and automations that enable security at scale and speed.

Risk Type	Definition
Critical ! 🔴	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
Major " 🟠	These risks are hard to exploit but very important to fix, they carry an elevated risk of Source code manipulation, which can lead to high-risk severity.
Medium # 🟡	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the source code execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor $ 🟢	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Unknown % 🟤	These risks pose uncertain severity to the contract or those who interact with it. They should be fixed immediately to mitigate the risk uncertainty.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.

Dependencies Health Report

DIRECT DEPENDENCIES	PACKAGES GRADED	AVG. SCORE
29	27 / 29	78

Health Check

Healthy ❓	15
Sustainable ❓	5
Need Review ❓	7
Unknown ❓	2

15 packages are healthy

@nestjs/platform-express

Package Health Score	98 / 100

WEEKLY DOWNLOADS	1,675,343
LAST RELEASE	6 days ago
LICENSE	MIT
CONTRIBUTORS	390
VULNERABILITIES	0 C 0 H 0 M 0 L

mongoose

Package Health Score	97 / 100

WEEKLY DOWNLOADS	1,960,330
LAST RELEASE	3 days ago
LICENSE	MIT
CONTRIBUTORS	410
VULNERABILITIES	0 C 0 H 0 M 0 L

15 **Packages are healthy**

@nestjs/core

| | Package Health Score | | | **95 / 100** |

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
2,242,628	6 days ago	MIT	390	0 C 0 H 0 M 0 L

axios

| | Package Health Score | | | **95 / 100** |

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
41,208,112	2 months ago	MIT	400	0 C 0 H 0 M 0 L

rxjs

| | Package Health Score | | | **95 / 100** |

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
43,477,640	2 months ago	Apache-2.0	430	0 C 0 H 0 M 0 L

15 Packages are healthy

dotenv

| Package Health Score | 94 / 100 |

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
31,849,813	22 days ago	BSD-2-Clause	70	0 C 0 H 0 M 0 L

zod

| Package Health Score | 93 / 100 |

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
4,226,029	4 months ago	MIT	240	0 C 0 H 0 M 0 L

tape

| Package Health Score | 92 / 100 |

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
535,423	7 days ago	MIT	100	0 C 0 H 0 M 0 L

15 Packages are healthy

@nestjs/mongoose

Package Health Score   **89 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
270,620	24 days ago	MIT	30	0 C 0 H 0 M 0 L

@nestjs/schedule

Package Health Score   **89 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
527,823	22 days ago	MIT	30	0 C 0 H 0 M 0 L

bitcoinjs-lib

Package Health Score   **89 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
95,200	1 month ago	MIT	90	0 C 0 H 0 M 0 L

15 **packages are healthy**

---

rimraf

Package Health Score   **88 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
76,739,562	2 months ago	ISC	30	0 C 0 H 0 M 0 L

@nestjs/axios

Package Health Score   **86 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
995,847	24 days ago	MIT	10	0 C 0 H 0 M 0 L

---

tiny-secp256k1

Package Health Score   **86 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
118,357	10 days ago	MIT	20	0 C 0 H 0 M 0 L

5 packages are Sustainable

Health Check

Healthy ❓	15
Sustainable ❓	5
Need Review ❓	7
Unknown ❓	2

5 packages are sustainable

bip32

Package Health Score **79 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
148,865	4 months ago	MIT	8	C H M L

crypto-js

Package Health Score **79 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
5,151,784	2 years ago	MIT	30	C H M L

web3

Package Health Score **74 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
464,455	12 days ago	LGPL-3.0	250	C H M 1 L

get-random-values

Package Health Score **71 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
83,372	3 months ago	MIT	4	C H M L

reflect-metadata

Package Health Score **70 / 100**

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
6,420,778	4 years ago	Apache-2.0	4	C H M L

7 packages need review

Dependencies Health Report

[↓] Test another package.json   ⬿ Share Results

DIRECT DEPENDENCIES	PACKAGES GRADED	AVG. SCORE
29	27 / 29	78

🛡 **web3** has a vulnerability in its latest version.

Health Check

Healthy ❷	15
Sustainable ❷	5
Need Review ❷	7
Unknown ❷	2

7 packages need review

bs58

		Package Health Score	68 / 100

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
998,605	1 year ago	MIT	6	

ecpair

		Package Health Score	61 / 100
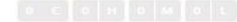
WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
19,120	10 months ago	MIT	2	

@cmdcode/crypto-utils

		Package Health Score	50 / 100

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
1,534	1 day ago	CC-BY-1.0	-	

crypto

		Package Health Score	50 / 100

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
667,705	6 years ago	ISC	1	

text-encoder

		Package Health Score	45 / 100

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
4,770	5 years ago	ISC	2	

tap-spec

		Package Health Score	44 / 100

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
22,091	5 years ago	MIT	8	

bs64

		Package Health Score	34 / 100

WEEKLY DOWNLOADS	LAST RELEASE	LICENSE	CONTRIBUTORS	VULNERABILITIES
5	10 years ago	-	-	

2 unknown packages

Dependencies Health Report

Test another package.json Share Results

DIRECT DEPENDENCIES	PACKAGES GRADED	AVG. SCORE
29	27 / 29	78

web3 has a vulnerability in its latest version.

Health Check

Healthy ❷	15
Sustainable ❷	5
Need Review ❷	7
Unknown ❷	2

2 unknown packages

@cmdcode/buff-utils	PENDING... ❷

@cmdcode/keylink	PENDING... ❷

FZT-01 PACKAGE OVERFLOW

Category	Severity ●	Location	Status
Inconsistency	Informational	@nestjs/platform-express	Acknowledged

Description

In **jest ,** the following equation is used inside an unchecked block

```
    "test:watch": "jest --watch",
  "test:cov": "jest --coverage",
  "test:debug": "node --inspect-brk -r tsconfig-paths/register -r ts-node/register node_modules/.bin/jest --runInBand",
  "test:e2e": "jest --config ./test/jest-e2e.json"
},
```

The function jest () does not have the override specifier. It should be noted that since -- > a function that overrides only a single interface function does not require the override specifier (see doc). However, all other instances of this in the code base contain the override specifier.

Recommendation

We recommend either checking and Ensure you're using the healthiest npm packages

FZT-02 SECURITY OVERFLOW

Category	Severity ●	Location	Status
Dependencies Health	Informational	nest-cli.json	Acknowledged

Inside Code

```json
{
  "collection": "@nestjs/schematics",
  «SourceRoot": "src"
}
```

FZT-03 SECURITY OVERFLOW

Category	Severity ●	Location	Status
Dependencies Health	Informational	@nestjs/core	Acknowledged

Start Code

```
"format": "prettier --write \"src/**/*.ts\" \"test/**/*.ts\"",
    "start": "nest start",
    "start:dev": "nest start --watch",
    "start:debug": "nest start --debug --watch",
    "start:prod": "node dist/main",
    "lint": "eslint \"{src,apps,libs,test}/**/*.ts\" --fix",
    "test": "jest"
```

Security NO KNOWN SECURITY ISSUES ?
All security vulnerabilities belong to **production dependencies** of direct and indirect packages.

SECURITY AND LICENSE RISK FOR SIGNIFICANT VERSIONS   All Versions

Version		Vulnerabilities	License Risk
10.0.5	07/2023	0 C 0 H 0 M 0 L	0 H 0 M 0 L
9.4.3	06/2023 POPULAR	0 C 0 H 0 M 0 L	0 H 0 M 0 L
8.4.7	06/2022	0 C 0 H 0 M 0 L	0 H 0 M 0 L
7.6.18	06/2021	0 C 0 H 0 M 0 L	0 H 0 M 0 L
7.5.5	11/2020	0 C 0 H 0 M 0 L	0 H 0 M 0 L

LICENSE MIT

SECURITY POLICY Yes

FZT-03 POSSIBLE OVERFLOW

Category	Severity ●	Location	Status
Dependencies Health	Informational	/npm-package/axios	Acknowledged

> **If you use require for importing, only default export is available:**

```
axios({ method: self.componentConfig["method"], url: self.componentConfig["action_path"],
data: self.componentConfig["data"], headers: { 'X-CSRF-Token':
document.getElementsByName("csrf-token")[0].getAttribute('content') }
```

INHERITANCE GRAPH

```
BitX-Backend      nest-cli      package      package-lock      tsconfig.build      tsconfig
      |                                            |
      v                                            v
    BitX                                         BitX
```
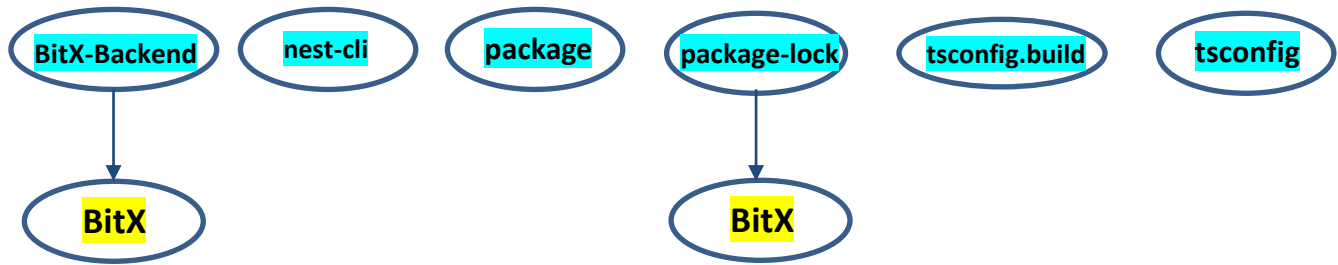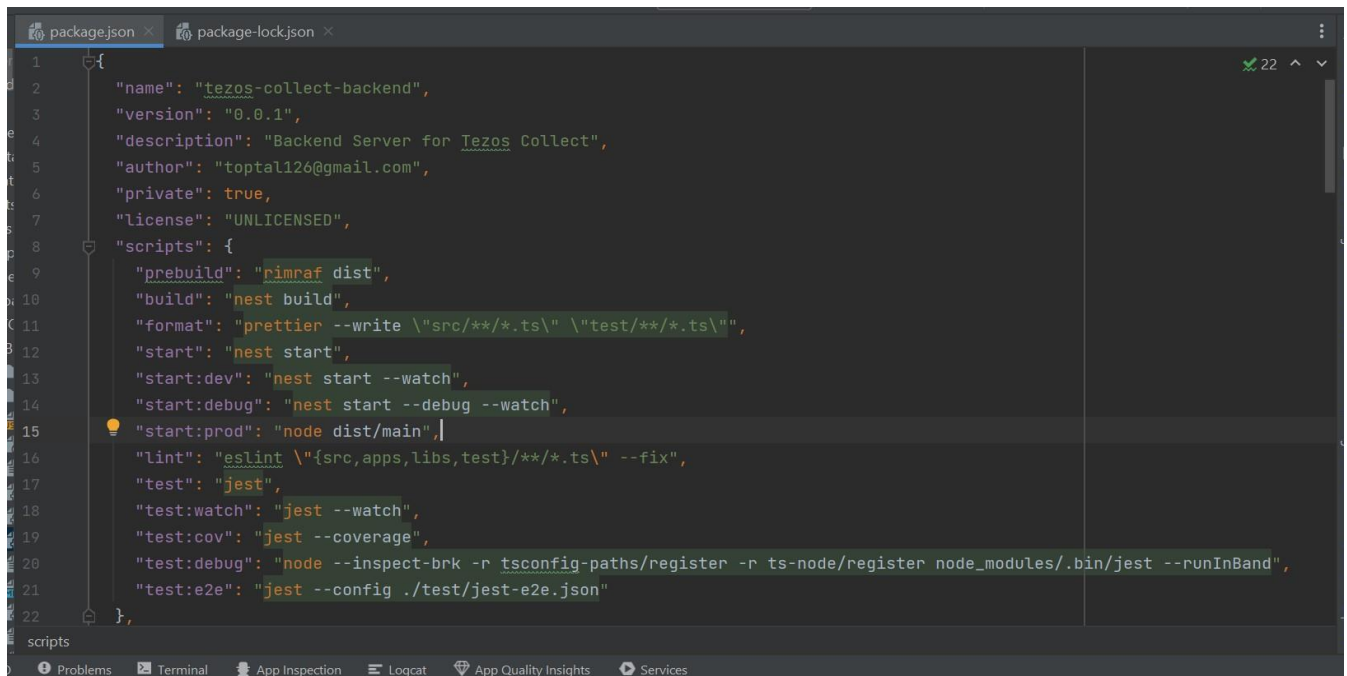
Identifier	Definition	Severity
CEN-16	Node.js Source Code privileges of BitX	Minor $ 🟩

Vulnerability 0 : No important security issue detected.
Threat level: Non

```
📄 package.json ×    📄 package-lock.json ×                                                    ⋮
  1   {                                                                               ✓ 22 ∧ ∨
  2     "name": "tezos-collect-backend",
  3     "version": "0.0.1",
  4     "description": "Backend Server for Tezos Collect",
  5     "author": "toptal126@gmail.com",
  6     "private": true,
  7     "license": "UNLICENSED",
  8     "scripts": {
  9       "prebuild": "rimraf dist",
 10       "build": "nest build",
 11       "format": "prettier --write \"src/**/*.ts\" \"test/**/*.ts\"",
 12       "start": "nest start",
 13       "start:dev": "nest start --watch",
 14       "start:debug": "nest start --debug --watch",
 15       "start:prod": "node dist/main",
 16       "lint": "eslint \"{src,apps,libs,test}/**/*.ts\" --fix",
 17       "test": "jest",
 18       "test:watch": "jest --watch",
 19       "test:cov": "jest --coverage",
 20       "test:debug": "node --inspect-brk -r tsconfig-paths/register -r ts-node/register node_modules/.bin/jest --runInBand",
 21       "test:e2e": "jest --config ./test/jest-e2e.json"
 22     },
 scripts
 ⓘ Problems   ⌷ Terminal   🖊 App Inspection   ≡ Logcat   🛡 App Quality Insights   ● Services
```

RECOMMENDATION

Project stakeholders should be consulted during the initial asset distribution process.

RECOMMENDATION

Align the team with a shared definition of clean code. Meet the defined standards every time with continuous feedback on code and a clear go/no-go quality gate in pull requests..

ALLEVIATION

BitX project team understands the centralization risk. Some functions are provided privileged access to ensure a good runtime behaviour in the project.

Identifier	Definition	Severity
COD-18	Third Party Dependencies	Minor 🟢

The Source Code Node.js is interacting with third party protocols, protections code. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised, and exploited. Moreover, upgrades in third parties can create severe impacts, e.g., change code source, deprecation of previous routers, etc.

RECOMMENDATION

Inspect and validate third party dependencies regularly, and mitigate severe impacts whenever necessary.

DISCLAIMERS

Vital Block provides the easy-to-understand audit of Node.js, JavaScript and Raw source codes (commonly known as smart contracts).

The Node.js Source code for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without Vital Block prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way

to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SOURCE CODE, OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THERE OF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, VITAL BLOCK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, VITAL BLOCK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, VITAL BLOCK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SOURCE CODES, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT'S OR ANY OTHER INDIVIDUAL'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. Vital Block does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.

LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than Vital Block. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites and social accounts owners. You agree that Vital block Security is not responsible for the content or operation of such websites and social accounts and that Vital Block shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.

ABOUT VITAL BLOCK

Vital Block provides intelligent blockchain Security Solutions. We provide solidity and Raw Code Review, testing, and auditing services. We have Partnered with 15+ Crypto Launchpads, audited 150+ smart contracts, and analyzed 400,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Aptos, Oasis, etc.

Vital Block is Dedicated to Making Defi & Web3 A Safer Place. We are Powered by Security engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 5 core members, and 4+ casual contributors.

Website: https://Vitalblock.org

Email: info@vitalblock.org

GitHub: https://github.com/vital-block

Twitter: https://twitter.com/VB_Audit

Telegram (Engineering): https://t.me/vital_block

Telegram (Onboarding): https://t.me/vitalblock_cmo

vital-block

info@vitalblock.org

www.Vitalblock.org

Vital Block Dedicated to Securing Public and Private Blockchain Ecosystem