Cyberscope

Audit Report

Egochain

February 2024

Repository	https://github.com/EgorasMarket/Egochain-Blockchain
Commit	e4218e0238e45c391d9fd4cdf2d98686eb21234d
Audited by	© cyberscope

Table of Contents

Review

Repository	https://github.com/EgorasMarket/Egochain-Blockchain
Commit	e4218e0238e45c391d9fd4cdf2d98686eb21234d

Audit Updates

Initial Audit	23 Feb 2024

Overview

The Egochain blockchain, as described on its website, is an Evm Compartible Blockchain for Smart Automobiles. It is a public, permissionless Layer 1 blockchain protocol aimed at fast-tracking the global shift to EVs (electric vehicles). It combines Cosmos' rapid transactions and compatibility with Ethereum's developer ecosystem.

Egochain aims to innovate and support the EV technology. Users are rewarded with `EGAX` tokens, which can used for various procedures with the blockchain, such as coverage of EV charging expenses and transaction fees. Lastly, the ecosystem uses the `EGC` token, as well, which serves the role of a debt token.

Audit Scope

The audit scope of the blockchain includes a thorough examination of key areas crucial for functionality and security. The audit primarily concentrates on security vulnerabilities, potential optimizations for performance, code maintainability, and adherence to best coding practices. Additionally, the audit evaluates the robustness of error handling mechanisms, the efficiency of network communication protocols, and the proper use of dependencies and external libraries. Each of these aspects is assessed to ensure the overall reliability and security of Egochain.

Architecture

Egochain is a scalable blockchain that is completely compatible with the Ethereum Virtual Machine. It is built using the Cosmos SDK, in order to achieve benefits, such as high transaction throughput and brief block times. This architecture allows users to perform both Cosmos and EVM formatted transactions and developers to scale EVM dApps cross-chain via IBC.

CLI

Egochain includes an all-in-one command-line interface (CLI). It allows users to run a node, manage wallets and interact with the Egochain network through queries and transactions.

Events

Egochain precompiles emit events when invoked by adding a Log item to the state. This Log structure is composed of several fields: an Address field specifying the precompile's address responsible for the event, Topics for storing event parameters as 32-byte hash indexes, Data for the ABI-encoded event specifics, and BlockNumber indicating the block in which the event occurred. The conversion of event parameters into topics is facilitated by the MakeTopic function.

Gas Usages

The precompiles utilized the RequiredGas function to communicate the necessary gas consumption to go-ethereum, following the conventions set by go-ethereum's native precompiles. This function calculates the gas needed for execution by referencing the standard gas pricing defined within the Cosmos SDK's KVStore.

State management

To monitor state changes, Egochain uses a system of journal logs, which is similar to the go-ethereum journal implementation. Revisions are used to revert the state to a specific point in time, identified by a unique ID and journal index. If an error is encountered, the state reverts to the snapshot captured at the beginning of the transaction. If the transaction is successful, the dirty states are committed to the keeper.

Precompile Vulnerabilities Protection

Egochain precompiles' Run method accepts a readOnly boolean argument which prevents state transitions, when executed via DELEGATECALL, STATICALL, or CALLCODE. Hence, a precompile method that leads to a state transition, determined by the precompiles' IsTransaction method, can only be executed via CALL. Otherwise, the precompile will return an error.

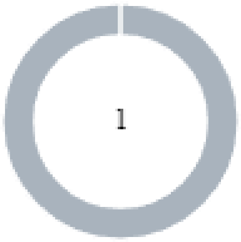
Security and Performance Considerations

Given the nature of the Egochain blockchain, security is paramount. This includes scrutinizing cryptographic implementations, key management, and transaction mechanisms. Performance aspects should also be evaluated, especially in transaction processing and network communication.

Code Quality and Maintainability

Egochain's codebase is reviewed for clarity, maintainability, and adherence to Go's best practices. This includes evaluating the use of modern Go's features, code modularity, and documentation.

Findings Breakdown



●	Critical	0
●	Medium	0
●	Minor / Informative	1

	Severity	Unresolved	Acknowledged	Resolved	Other
●	Critical	0	0	0	0
●	Medium	0	0	0	0
●	Minor / Informative	1	0	0	0

Diagnostics

🔴 Critical 🟠 Medium ● Minor / Informative

Severity	Code	Description	Status
●	TI	Typographical Inconsistencies	Unresolved

TI - Typographical Inconsistencies

Criticality	Minor / Informative
Location	indexer/kv_indexer.go#L60 rpc/backend/blocks.go#L267 rpc/backend/tx_info.go#L355 rpc/types/utils.go#L281
Status	Unresolved

Description

Minor typographical errors were identified across several modules of the project. These inconsistencies, while not impacting the functional integrity of the application or presenting any security vulnerabilities, suggest areas for improvement in terms of code readability. Attention to detail in naming conventions is crucial for maintaining a high standard of code quality, as it enhances the clarity and understanding of the codebase.

```
func TxSucessOrExpectedFailure(res *abci.ResponseDeliverTx) bool {
	return res.Code == 0 || TxExceedBlockGasLimit(res) ||
TxStateDBCommitError(res)
}
```

Recommendation

The correction of these minor typographical errors is recommended, so as to align the blockchain's codebase with best practices for code quality and maintainability.

Summary

The Egochain blockchain is an innovative blockchain on the Cosmos Network. This audit investigates security issues, business logic concerns, potential improvements in performance, and adherence to best coding practices. The codebase review and auditing process revealed no critical findings.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope’s prior written consent. This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment 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 Cyberscope’s position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. 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 Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io