Choice Coin v2
Security Audit

July 2022

Table of Contents

I. Overview

Choice Coin v1 introduced Decentralized Decisions, a globally secure voting platform on the Algorand blockchain. Still, more development was needed to continuing growing DAO participation on Algorand. Participation is critical for DAOs because participation drives use, decentralization, and legal compliance. Thus, there was a need for a platform that consistently and constantly rewards users for participation in governance processes.

The underlying problem addresses is how to create a streamlined and self-sustaining system for decentralized governance. The solution, Choice Coin v2, builds on Choice Coin's Decentralized Decisions software to provide an integrated and continuously live web application for DAO governance. The web application allows users to make a proposal or participate in DAO voting globally and at any time. The purpose for Choice Coin v2 is to build a governance platform for DAOs on the Algorand blockchain.

This Security Audit was prepared by the core development team for Choice Coin v2. The purpose for this audit is to ensure the application is secure prior to the MainNet launch on the Algorand blockchain. The software is mostly written in the Algorand JavaScript-SDK, uses the React application framework, and leverages the existing security infrastructure within the Algorand blockchain. We developed a three-step methodology to audit the software for security.

First, the methodology calls for simplifying and synchronizing the software to its fundamental functional elements. Second, the methods include creating a software file tree to showcase the file structure and repository organization, as well as a software audit to describe all files. Third, the methodology includes technical analysis of the entire software stack with discussion of dependencies and potential risks.

II. Software Audit

MVP	README.md package.json .gtignore		
	rewards	.env.example .gitignore README.md config.js package.json rewards.js	
	public	manifest.json background.svg favicon.ico index.html	
	src	App.js Index.js	
		assets	choice-logo.png compliance-logo.png copy-to-dashboard.png disconnect-logo.png interchain-logo.png voting-logo.png
		components	**election**	Election.js ElectionCard.js ElectionList.js SearchBar.js
			navbar	BottomNavigationBar.js MenuBar.js Settings.js TopNavigationBar.js
			propose	propose.js
		pages	Landing.js MainPage.js VoteAndProposalLinkPage.js CompliancePage.js ConverterPage.js
		statics	AlertModal.js WalletConfirmation.js
		store	reducers.js stores.js
		styles	electionlist.css index.css landing.css reset.css

Files	Description
MVP	
Package.json	Contains dependencies and libraries for web app.
.gitignore	Ignore node modules.
README.md	Description file.
public	The front-end formatting integrated with JavaScript logic for web development.
src	Source file for code for web application.
rewards	Code for voting rewards.
public	
Background.svg	Background image for application.
favicon.ico	Image icon for Choice logo.
index.html	Root HTML designed to improve search engine performance.
manifest.json	Helps to improve offline development and performance from react.
src	
assets	Contains logos and icons for the web app.
components	Different functional elements of the website.
pages	Web design and frontend for the applications.
statics	The logic for user connection to the Algorand network.
store	Database storage and management for the website.
styles	Design and css styling for the website.
App.js	Imports files and connects main components and pages.
index.js	Imports application for indexing using react.
assets	
choice-logo.png	Choice Coin logo.
compliance-logo.png	Compliance logo.
copy-to-dashboard.png	Copy logo.
disconnect-logo.png	Disconnect logo.
interchain-logo.png	Interchain logo.
voting-logo.png	Voting logo.
components	
election	Contains the cards and logic for votes.
navbar	Contains the navigation bar and settings.
propose	The proposal component of the website.
election	
Election.js	Voting logic for multi-vote functionality.
ElectionCard.js	This is the card for each vote.
ElectionList.js	The main voting function with Algorand integration.
SearchBar.js	Search for current votes.
navbar	
BottomNavigationBar.js	Bottom navigation for mobile view.
MenuBar.js	Toggle bar that includes external social links.
Settings.js	Wallet disconnect function.

TopNavigationBar.js	Algorand wallet connect functionality and icons.
propose	
Propose.js	Software for proposal processing.
pages	
CompliancePage.js	Landing page for compliance software.
ConverterPage.js	Landing page for interchain converter software.
Landing.js	Landing page for web application.
MainPage.js	The main web page for the application.
VoteAndProposalLinkPage.js	Page for proposal and voting software.
statics	
AlertModal.js	Pop up modal for the wallet connectivity.
WalletConfirmation.js	Wallet confirmation pop up.
store	
Reducers.js	Contains data state logic and management.
Stores.js	Data storage software.
styles	
Electionlist.css	Formatting for voting pages.
Index.css	Formatting for main pages.
Landing.css	Formatting for landing pages.
Reset.css	Base formatting.
rewards	
.env.example	Example file with variables.
.gitignore	Ignore node modules.
README.md	Description file.
config.js	Network connection and configuration file.
package.json	Dependencies for software.
rewards.js	Main reward script for software execution.

III. Infrastructure

The Choice Coin v1 model was widely successful using Decentralized Decisions. In total, the model hosted six votes – four of which were for Choice Coin DAO governance, one for AlgoCharts governance, and one for Yieldly governance. Thus, the software was successfully deployed for both internal and external governance operations. However, there was certainly room for improvement in the software. For example, one issue with the architecture is that it was severed for hosting purposes on two separate platforms, Heroku and Netifly.

Choice Coin v2 solved problems existing in the Decentralized Decisions software by consolidating and simplifying architectures and code. For example, the entirety of Choice Coin v2 is hosted on Heroku. The software runs on the domain decentralized-decisions.app which was purchased on GoDaddy. Additionally, the architecture and code base were simplified, allowing v2 model to scale and support multiple votes to run at once on the web application. In turn, this will allow for more volume to flow through the software for both Choice Coin DAO votes and external votes as well.

Choice Coin v2 leverages the existing software infrastructure of the Algorand blockchain. Algorand is a proof-of-stake blockchain, which evolved to improve security and efficiency compared to existing proof-of-work blockchains.[1] One problem with proof-of-work blockchains is they require large scale electricity computation to validate transactions across a network.[2] Algorand solves this problem, requiring minimal computation to validate global transactions using zero-knowledge proofs.[3] The proof-of-stake mechanism incorporates the timestamp signature used in proof-of-work blockchains,[4] but validates transactions faster and more securely with post-quantum cryptography. The Choice Coin v2 software continues building on the existing consensus architecture within the Algorand blockchain.[5]

[1] Yossi Gilad, et al., Algorand: Scaling Byzantine Agreements for Cryptocurrencies, 53 (2017).
[2] Liana Badea, The Environmental and Economic Impact of Bitcoin (March 2021), DOI:10.1109/ACCESS.2021.3068636. *See also* Lucas Girard, Environmental Impacts of Cryptocurrency Mining (2018).
[3] Jing Chen, Silvio Micali, Algorand 4 (2017), arXiv:1607.01341. ("The amount of computation required is minimal.")
[4] Scott J. Shackelford, Steve Myers, Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace, 19 Yale J. L. & Tech. 334, 351 (2017).
[5] Yossi Gilad, et al., Algorand: Scaling Byzantine Agreements for Cryptocurrencies (2017).

IV. Technical Analysis

DAO participants need a mechanism by which they govern rules, software development, and growth strategy. In fact, Choice Coin v1 was able to meet this demand for two Partners in addition to the Choice Coin DAO itself, Yieldly and AlgoCharts. Choice Coin v2 allows any DAO to make a proposal to generate a vote on the Algorand blockchain.

One of the hardest problems for decentralized governance software is developing and way to allow anyone to make a proposal for a new vote. Choice Coin v2 tackles this problem with a new design for decentralized voting. To automate proposal generation, the Choice Coin DAO developed a new governance gateway called Tita. The Tita design was incorporated into the v2 model and allows for anyone to make a proposal for a vote.

Proposals are backbone for decentralized governance. Without a distributed process by which organizations can improve, DAOs become centralized, stagnant, and unstable. The approval process balances the need for decentralization and quality control – which is necessary to avoid vulgarity, criminal activity, or otherwise inappropriate proposals. After being approved, votes made available to public on Decentralized Decisions for a public vote.

The main two security risks include private keys being compromised and passwords being comprised for hosting services. The core development team has developed a procedure to minimize these risks. The procedure includes protocols for account creation, password protection, and private key transfer. The goal is to minimize exposure to keys and passwords and refrain from any online storage.

The core development team decided against automating the creation of addresses and private keys, which would have included storage in a private MongoDB database. The team elected against this option due to vulnerabilities associated with online storage. As such, the new addresses will be created manually, and their associated private keys will be managed in an offline database. In sum, Choice Coin v2 is a more secure, scalable, and systematic DAO voting machine.