BOULAY

Lindy Labs

Sandclock Holdings d/b/a Lindy Labs

SOC 2 Type 1 Report

for the

Blockchain-Based Smart Contract System

An Independent Service Auditor's Report on the
Suitability of the Design of Controls Relevant to Security

March 31, 2024

AICPA SOC aicpa.org/soc4so SOC for Service Organizations ™

Assurance | Tax | Advisory | Wealth Management
Minneapolis • Naples

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Sandclock Holdings d/b/a Lindy Labs:

Scope

We have examined Sandclock Holdings d/b/a Lindy Labs' ('Lindy Labs' or the 'service organization') accompanying description of its smart contract system found in Section III titled "Description of the Blockchain-Based Smart Contract System" as of March 31, 2024 (description) based on the criteria for a description of a service organization's system set forth in *DC 200*, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria* (description criteria) and the suitability of the design of controls stated in the description as of March 31, 2024 to provide reasonable assurance that Lindy Labs' service commitments and system requirements would be achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100*, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

Lindy Labs uses Heroku (the 'subservice organization') to provide cloud computing and data center hosting services supporting its smart contract system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Lindy Labs, to achieve Lindy Labs' service commitments and system requirements based on the applicable trust services criteria. The description presents Lindy Labs' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lindy Labs' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Lindy Labs, to achieve Lindy Labs' service commitments and system requirements based on the applicable trust services criteria. The description presents Lindy Labs' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Lindy Labs' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Lindy Labs is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Lindy Labs' service commitments and system requirements were achieved. In Section II, Lindy Labs has provided the accompanying assertion titled "Management's Assertion" (assertion) about the description and the suitability of the design of controls stated therein. Lindy Labs is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. the description presents Lindy Labs's smart contract system that was designed and implemented as of March 31, 2024 in accordance with the description criteria .

b. the controls stated in the description were suitably designed as of March 31, 2024, to provide reasonable assurance that Lindy Labs' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization applied the complementary controls assumed in the design of Lindy Labs' controls as of that date.

Restricted Use

This report is intended solely for the information and use of Lindy Labs, user entities of the smart contract system as of March 31, 2024, business partners of Lindy Labs subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, the subservice organization, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Minneapolis, Minnesota
April 15, 2024

SECTION II

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Sandclock Holdings d/b/a Lindy Labs' smart contract system titled "Description of the Blockchain-Based Smart Contract System" as of March 31, 2024 (description) based on the criteria for a description of a service organization's system in *DC 200*, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*. The description is intended to provide report users with information about the smart contract system that may be useful when assessing the risks arising from interactions with the system, particularly information about system controls that Lindy Labs has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100*, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

Lindy Labs uses Heroku (the 'subservice organization') to provide cloud computing and data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Lindy Labs, to achieve Lindy Labs' service commitments and system requirements based on the applicable trust services criteria. The description presents Lindy Labs' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lindy Labs' controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Lindy Labs, to achieve Lindy Labs' service commitments and system requirements based on the applicable trust services criteria. The description presents Lindy Labs' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Lindy Labs' controls.

We confirm, to the best of our knowledge and belief, that:

a. the description presents Lindy Labs' smart contract system that was designed and implemented as of March 31, 2024 in accordance with the description criteria .

b. the controls stated in the description were suitably designed as of March 31, 2024 to provide reasonable assurance that Lindy Labs' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Alexander Hughes
Chief Legal Officer
Sandclock Holdings

SECTION III

DESCRIPTION OF THE BLOCKCHAIN-BASED SMART CONTRACT SYSTEM

DESCRIPTION OF THE BLOCKCHAIN-BASED SMART CONTRACT SYSTEM

Company Background

Sandclock Holdings d/b/a Lindy Labs ('Lindy Labs' or 'the Company') is a technology company that performs blockchain development that, among other things, enables users to save, give, invest, or spend yield generated on stablecoins. The Company began its Sandclock platform as a philanthropy-first project in 2021 and evolved into a generalized wealth management solution. Lindy Labs is a fully remote company based in the Cayman Islands and has approximately 30 employees.

Description of Services Provided

Lindy Labs' blockchain-based smart contract system leverages the security, scalability, and transparency of public blockchain infrastructure to provide optimal user experience and stability. The system consists of three distinct components: Lindy Labs' Sandclock platform includes advanced yield-generating strategies, the Opus platform offers advanced credit solutions, and the research team develops software to modernize legacy systems and provide best-in-class security and efficiency.

Principal Service Commitments and System Requirements

Lindy Labs designs its processes and procedures to meet its objectives for its services. Those objectives are based on the service commitments that Lindy Labs makes to user entities, relevant laws and regulations that govern the provisioning of services, and the financial, operational, and compliance requirements that Lindy Labs has established for the services. Security commitments to user entities are documented and communicated in service agreements as well as in the description of the service offerings provided online.

Security commitments are standardized and include, but are not limited to, the following:

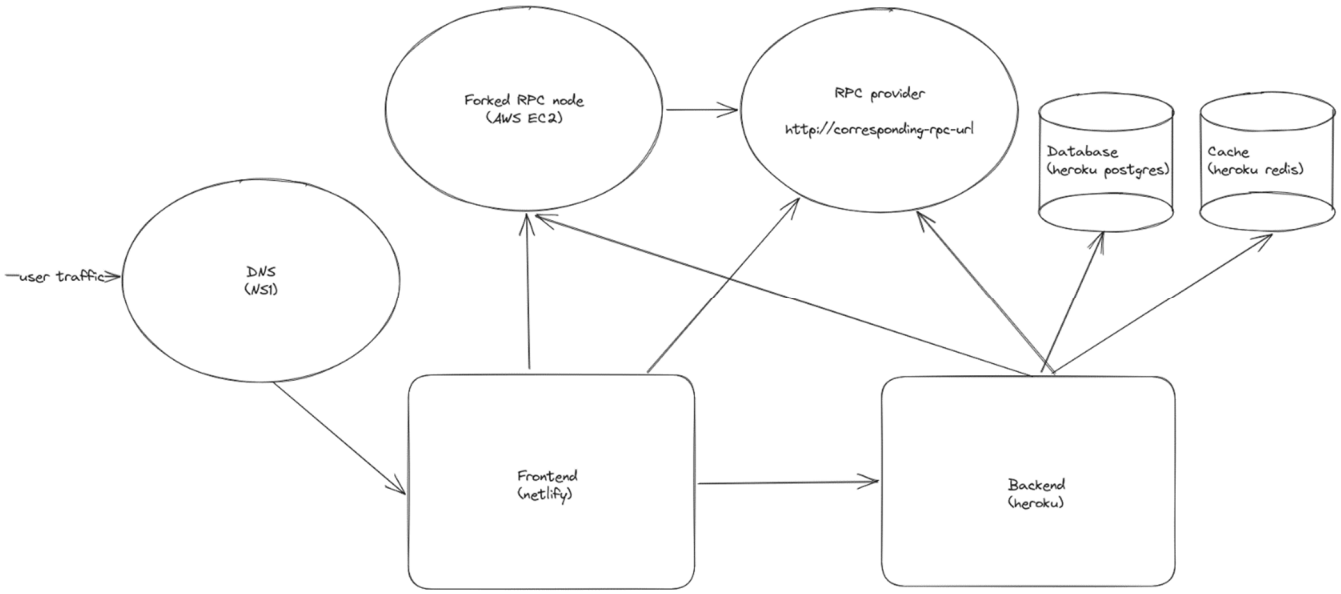
- Restricting access to confidential data to authorized individuals on a need-to-know basis.
- Maintaining industry-standard administrative, physical, and technical measures to protect the security of data from unauthorized access, disclosure, and use.
- Performing routine third-party penetration testing of the system and remediating any identified security vulnerabilities in a timely manner.

Lindy Labs establishes operational requirements that support the achievement of the security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Lindy Labs' organizational policies and procedures, system design documentation, and agreements with user entities. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around system design, development, and operations as well as management of internal business systems and networks. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Blockchain-Based Smart Contract System.

Components of the System

Infrastructure

Lindy Labs uses Heroku to provide cloud computing and data center hosting services supporting its smart contract system. The key infrastructure components are noted in the system diagram and table below.



Component	Purpose
Heroku	Cloud platform for app development
Ethereum Blockchain	Main decentralized database

Software

Primary software used to support the smart contract system include the following:

Software	Purpose
Brownie	Python framework for Ethereum smart contract testing, interaction, and deployment
GitHub	Source code repository and version control system
Google Workspace	Internal collaboration platform and document storage repository
Slack	Internal communication platform
BuildBear	Forked Ethereum sandbox with built-in explorer and faucet
Aegis	Formal verification tool for Cairo
Hevm	Symbolic execution tool for Ethereum Virtual Machine
Notion	Product management, internal documentation, and wiki
Graph Protocol	Decentralized blockchain indexing
Sentry	Open-source error/performance monitoring

Software	Purpose
Datadog	Monitoring and analytics
The Giving Block	Charitable giving API
Open Zeppelin Defender	On-chain monitoring
Tenderly	On-chain simulation and debugging
Foundry	Smart contract development toolchain
Coveralls	Smart contract test coverage report
Slither	Smart contract static analyzer

People

Lindy Labs maintains a staff of approximately 30 employees and contractors across the functional areas of executive management & finance, operations, product, engineering, business development, and legal & compliance.

Executive Management

The executive management team incorporates the following individuals:

- Chief Executive Officer (CEO)
- Chief Operating Officer (COO)
- Chief Strategy Officer (CSO)
- Chief Legal Officer (CFO)

Executive management is responsible for developing and implementing strategic initiatives, making financial plans, addressing legal/regulatory requirements, and overseeing their respective teams.

The CEO oversees the entire organization, ensuring alignment with SOC 2 criteria. The CEO also sets strategic goals, makes financial plans, aligns business operations with security and privacy frameworks, and ensures that the company's activities adhere to legal and ethical standards.

Operations

The COO oversees all day-to-day operational and administrative functions, including partner success, partner program management, program performance analysis, and vendor management. The operations team is responsible for onboarding and manages the configuration of the internal and external components of the organization.

Information Technology, Product Management & Support

The CEO oversees the Product Manager, who in turn oversees engineering, information technology, and information security. The engineering team designs and builds applications, backend infrastructure, data systems, and operational support for system components.

The Product Manager also oversees product strategy, user support, and product design teams. The teams are responsible for end user onboarding, developing best practices and providing support services to customers.

Business Development

The CSO develops and executes strategic initiatives aligned with industry security standards. The CSO is responsible for identifying, developing, and driving key strategic initiatives and ensuring that these strategies are integrated with the company’s overall compliance and security posture. The CSO is also responsible for identifying and cultivating potential strategic partnerships and coordinating and overseeing sales and marketing initiatives.

Legal & Compliance

The CLO oversees all legal, regulatory, and governmental affairs aspects of the Company, ensuring compliance with legal and regulatory requirements. The CLO is also responsible for advising on legal and risk management issues, managing the company's legal affairs, interfacing with lawmakers and state and federal regulators, and ensuring that the Company's operations are in line with the current laws and standards.

Data

Lindy Labs classifies data based on the degree of confidentiality required using the following labels:

- **Company Confidential:** Information collected and used by Lindy Labs to operate the business. Lindy Labs must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information (legal documents, contractual agreements, employee PII, employee salaries, etc.).
- **Customer Confidential:** Information received from customers for processing or storage by Lindy Labs. Lindy Labs must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information (customer operating data, customer PII, etc.).
- **Internal:** Access to internal information is approved by management and is protected from external access (internal memos, design documents, product specifications, correspondences, etc.).
- **Public:** Public information is not confidential and can be made public without any implications for Lindy Labs (press releases, public website, etc.).

Any data file or printed document that is not labeled is considered classified as "Internal" and handled accordingly.

Policies and Procedures

The following security policies and procedures are maintained and updated at least annually by Lindy Labs:

- Acceptable Use
- Access Control
- Backup and Restoration
- Business Continuity and Disaster Recovery
- Change Management
- Corporate Ethics
- Customer Support and SLA
- Data Retention and Disposal
- Incident Management
- Information Classification
- Information Security
- Key Management and Cryptography
- Network Security
- Personnel Security
- Risk Assessment
- Server Security
- Software Development
- Vendor Management
- Vulnerability and Penetration Testing Management
- Workstation and Mobile Device

Lindy Labs employees and contractors are required to acknowledge their understanding of the policies and procedures upon hire.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

Control Environment

Management's Philosophy

Integrity and ethical values are essential elements of management's philosophy and Lindy Labs' control environment. The executive leadership team is responsible for setting the example of ethical conduct at Lindy Labs and communicating expectations across the organization through the Code of Conduct policy.

Security Management

Lindy Labs has a dedicated information security team led by the CLO (who is designated as the Security Officer) and consisting of developers and formal verification engineers. With the title of Security Officer, the CLO is responsible for creating and enforcing security policies and procedures; leading the monitoring, vulnerability management, and incident detection and response initiatives; and tracking and reducing risk organization-wide. The CLO is focused on security policies, audit, enforcement, automation, and remediation.

All Lindy Labs employees are required to attend information security awareness training on an annual basis to ensure that personnel are knowledgeable of risks and controls around cybersecurity and data protection.

Personnel Security

New positions that are posted at Lindy Labs have clearly defined job descriptions and outline the technical and educational requirements the Company is seeking in prospective candidates. Background checks are performed on new employees and contractors prior to their start date. Once employed, personnel are subject to Lindy Labs' procedures around information security. A provisioning ticket is submitted to the IT team requesting that the newly hired employee or contractor obtain the system access necessary to perform their job. Access is granted based on the principle of least privilege.

Physical Security and Environmental Controls

The in-scope systems and infrastructure that support Lindy Labs are hosted in the cloud by Heroku (see *Complementary Subservice Organization Controls* section below). Lindy Labs does not have a physical office and as a result all employees work remotely from their homes.

Logical Security

Lindy Labs uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

Employees sign on to the Lindy Labs production network using internal-only administrative tooling with individual credentials, which includes two-factor authentication. Passwords must conform to defined password standards and are enforced through parameter settings in Lindy Labs. These settings are part of the configuration standards and force users to change passwords at a defined interval and disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts.

All employees accessing the production system are required to use a token-based two-factor authentication system. Customer systems access the Lindy Labs customer portal through the Internet using Secure File Transfer over SSH (SFTP) or HTTPS. In all cases, connections must use protocols that encrypt passwords before they will fully function.

Lindy Labs customers access Lindy Labs services through the Internet using the SSL functionality of their web browser. Users must supply a valid user ID and password with two-factor authentication to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured in the Lindy Labs Heroku console by the administration account.

Change Management

Lindy Labs maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance (QA) testing and user acceptance testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

System Monitoring

Lindy Labs performs system monitoring activities to continuously assess the quality of internal controls over time and ensure that any corrective actions are completed in a timely manner. Examples of system monitoring processes in place include:

- Firewalls – Systems that filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized.
- Vulnerability Scanning – Ongoing process by which infrastructure and software is automatically tested for security weaknesses.
- Patch Management – Ensures infrastructure systems are patched in accordance with vendor-recommended operating system patches.
- Penetration Testing – Web application penetration testing to identify, and subsequently remediate, vulnerabilities that can be exploited by bad actors.

Problem Management

Security incidents and other issues impacting our customers or production operations are managed and tracked using an incident management tool. The COO is responsible for ensuring incidents are properly classified, triaged, resolved, and remediated to avoid repeat occurrences. All prolonged issues that require follow-up are tracked using the Company's ticketing system and are monitored to ensure timely resolution.

Risk Assessment Process

Lindy Labs conducts a risk assessment at least annually. The system risk assessment template enables Lindy Labs to categorize risks to the business, describe their cause and potential impact, and outline mitigation steps to reduce the likelihood and impact. It reviews sensitive data, the codebase, people, production services, physical security, and any additional risks identified by the Company.

Information and Communication Systems

Information and communication are an integral component of Lindy Labs' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Lindy Labs, information is identified, captured, processed, and reported by various information systems as well as through conversations with clients, vendors, regulators, and employees.

Periodic meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Lindy Labs personnel via email.

Monitoring Controls

Lindy Labs performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from Company policies and procedures. Employee activity and adherence to Company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Ongoing Monitoring

Lindy Labs conducts quality assurance monitoring on a regular basis, and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Reporting Deficiencies

Escalation of system events is managed via immediate, direct escalation via dedicated communication channels. Corrective actions are currently documented and communicated in these channels and logged as tickets in Lindy Labs' ticketing system.

Control Objectives and Related Controls

Lindy Labs' control objectives and description of related controls are included in Section IV, "Trust Services Categories, Criteria, and Related Controls Relevant to Security." Although the control objectives and related controls are included in Section IV, they are an integral part of the description of the smart contract system.

Complementary User Entity Controls (CUECs)

Lindy Labs' controls cover only a portion of overall internal control for each user entity of the smart contract system. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by Lindy Labs. Therefore, each user entity's internal control should be evaluated in conjunction with Lindy Labs' controls, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal controls to determine whether the identified CUECs have been implemented and are operating effectively.

Criteria	Control Activity
CC6.1	User entities maintain logical access security to the smart contract system by ensuring unique user IDs, complex passwords and multi-factor authentication are enforced.
CC6.3	User entities restrict access to the smart contract system based on the principle of least privilege.

Complementary Subservice Organization Controls (CSOCs)

Lindy Labs' primary hosting is with Heroku, a subsidiary of Salesforce that provides on-demand cloud computing platforms to individuals, companies, and governments on a paid subscription basis. The technology allows subscribers to have at their disposal a virtual cluster of computers, available all the time, through the Internet.

Lindy Labs' services are designed with the assumption that certain controls will be implemented at Heroku. Such controls are called complementary subservice organization controls. It is not feasible for the service commitments, system requirements, and applicable criteria related to the smart contract system to be achieved solely by Lindy Labs. Therefore, each user entity's internal control must be evaluated in conjunction with Lindy Labs' controls, considering the related CSOCs expected to be implemented at the subservice organization, as described below.

Criteria	Control Activity
CC6.4	• Heroku is responsible for restricting data center access to authorized personnel. • Heroku is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC9.1	• Heroku is responsible for the installation of fire suppression, detection, and environmental monitoring systems at the data centers. • Heroku is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterrupted power supply. • Heroku is responsible for overseeing the regular maintenance of environmental protections at data centers.

Lindy Labs receives and reviews the Heroku SOC 2 Type 2 reports annually. In addition, through its operational activities, Lindy Labs monitors the services performed by Heroku to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Lindy Labs also has communication with the subservice organization to monitor compliance with the service agreement, stay up to date on planned changes at the hosting facility, and communicate any issues or concerns to Heroku management.

System Incidents

There were no identified system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure to the achievement of one or more of those service commitments and system requirements as of March 31, 2024.

Trust Services Criteria Not Applicable

All criteria within the security category were applicable to the smart contract system.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the system is used to provide the service as of March 31, 2024.

SECTION IV

TRUST SERVICES CATEGORIES, CRITERIA, AND RELATED CONTROLS RELEVANT TO SECURITY

SECURITY

Control #	Control Activity Specified by Lindy Labs
Control Environment	
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
CC1.1.1	Lindy Labs has established a Code of Conduct policy that is acknowledged by all new employees and contractors upon hire. This policy outlines expectations the Company has set related to ethics and standards of conduct. Additionally, this policy outlines processes that management has established to evaluate adherence to standards of conduct and address deviations in a timely manner.
CC1.1.2	Lindy Labs has established communication channels that allow employees and contractors to securely and anonymously report issues related to fraud, harassment, and other issues impacting the organization's ethical and integrity requirements.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
CC1.2.1	Lindy Labs has a Board of Directors that is made up of independent leaders with relevant skills and industry expertise, which enables them to provide credible challenge and oversight over management.
CC1.2.2	The Board of Directors meets at least on a quarterly basis to discuss Company performance, strategic and financial objectives, and information security matters.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
CC1.3.1	Lindy Labs maintains an updated organizational chart that establishes structure, reporting lines, and delegation of authority and responsibility across the Company.
CC1.3.2	Lindy Labs' executive leadership team meets at least every other month to discuss operations, issues relating to internal controls, and delivery on key performance metrics.
CC1.3.3	Lindy Labs has an assigned security team that is responsible for the design, implementation, and oversight of the organization's security policies and procedures. The security team communicates important information security events to management in a timely manner.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
CC1.4.1	All positions have a detailed job description that lists qualifications, such as required skills and experience, which candidates must meet in order to be hired by Lindy Labs.
CC1.4.2	Background checks are performed on new hires before their start date, as permitted by local laws. The results are reviewed by Human Resources and appropriate action is taken if deemed necessary.
CC1.4.3	Lindy Labs' executive leadership team meets at least every other month to evaluate its resource requirements to determine whether additional personnel and/or training is necessary.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
CC1.5.1	Lindy Labs maintains formalized performance expectations for each position and uses these expectations as a basis for evaluating the performance of each of its employees. These performance evaluations, which incorporate internal control responsibilities, are completed on an annual basis.

Control #	Control Activity Specified by Lindy Labs
Communication and Information	
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
CC2.1.1	Lindy Labs' mission-critical systems and sensitive information are identified during the annual risk assessment, which includes capturing internal and external sources of data.
CC2.1.2	Lindy Labs maintains an updated network diagram outlining how data is processed and secured.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
CC2.2.1	Lindy Labs maintains updated policies and procedures that outline requirements that employees and contractors must follow as it pertains to conducting themselves appropriately and maintaining security of Company and customer information. These policies and procedures are accessible to all personnel and are acknowledged upon hire.
CC2.2.2	Lindy Labs employees and contractors are required to complete information security training annually.
CC2.2.3	Lindy Labs provides a process for employees and contractors to report potential vulnerabilities, security incidents, and general concerns to management.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
CC2.3.1	Lindy Labs has developed documentation and user guides that describe relevant system components as well as the purpose and design of the system. These documents are made available to both internal and external users and updated as needed.
CC2.3.2	Lindy Labs provides an external-facing support system that allows users to report incidents, complaints, issues, and any other challenges through an appropriate channel. Reported incidents are addressed by the Company's support staff in a timely manner.
Risk Assessment	
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
CC3.1.1	Lindy Labs maintains an updated risk assessment program that describes the processes the Company has in place to identify new business and technical risks and how those risks are mitigated.
CC3.1.2	At least annually, Lindy Labs conducts an assessment on the risks related to blockchain technology, operations, regulatory compliance, finance, and privacy/data security.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
CC3.2.1	At least annually, Lindy Labs performs a risk assessment, which includes the identification of relevant internal and external threats, an analysis of the significance of the risks associated with those threats, a determination of appropriate risk mitigation strategies, and the development or modification of controls consistent with the risk mitigation strategy.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
CC3.3.1	As part of the risk assessment process, management conducts a fraud assessment to evaluate the risks and mitigating controls to prevent and detect fraud.

Control #	Control Activity Specified by Lindy Labs
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
CC3.4.1	As part of the risk assessment process, management identifies and assesses changes that could significantly impact the system of internal control. The assessment includes evaluating changes in blockchain technology, operations, regulatory compliance, finance, and privacy/data security.
Monitoring Activities	
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
CC4.1.1	Lindy Labs conducts ongoing monitoring over internal controls to ensure they are appropriately designed and operating effectively in accordance with baseline requirements. These evaluations are conducted with knowledgeable personnel, integrate with business processes, consider changes in business processes, and vary in frequency based on associated risks.
CC4.1.2	Lindy Labs engages a qualified third-party security firm to conduct code reviews and security assessments of its blockchain platform at least annually. Results are reviewed by management and high priority findings are remediated in a timely manner.
CC4.1.3	Vulnerability scanning is performed on an ongoing basis to identify bugs and security vulnerabilities in operating systems and infrastructure. Issues identified are analyzed and remediated in a timely manner.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and board of directors, as appropriate.	
CC4.2.1	Management assesses the results of ongoing and separate evaluations. Deficiencies are communicated to relevant parties for corrective action, and management tracks whether the deficiencies are remediated in a timely manner.
Control Activities	
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
CC5.1.1	As part of the risk assessment process, management ensures that adequate controls are in place to mitigate the identified risks to an acceptable level. Considerations in the identification and implementation of control activities include entity-specific factors, relevant business processes, incorporating a mix of control activity types (manual, automated, preventive, detective) and segregation of duties.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC5.2.1	Lindy Labs maintains a suite of information technology general controls (ITGCs) to support the achievement of objectives. These ITGCs are identified as part of the annual risk assessment completed by management and cover areas such as technology infrastructure and security management as well as technology acquisition, development, and maintenance.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
CC5.3.1	Lindy Labs maintains updated policies and procedures that incorporate control activities across the organization. These policies and procedures establish requirements pertaining to timely performance of controls, taking corrective action on control deficiencies, and ensuring that competent personnel are accountable for control execution.

Control #	Control Activity Specified by Lindy Labs
Logical and Physical Access Controls	
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	
CC6.1.1	Lindy Labs maintains an updated inventory of information assets within the organization.
CC6.1.2	Access to Lindy Labs' infrastructure and sensitive systems/applications requires complex passwords and multi-factor authentication (MFA).
CC6.1.3	Lindy Labs utilizes Heroku's identity and access management (IAM) tools to securely manage access to Heroku services and resources. IAM enables the Company to create and manage Heroku users/groups and use permissions to allow and deny access to Heroku resources.
CC6.1.4	Lindy Labs maintains active SHA-256 encryption certificates for its web application to ensure secure connections for its users.
CC6.1.5	Lindy Labs utilizes key management tools to create and manage keys and control the use of encryption across its cloud-based environment.
CC6.1.6	Administrative and privileged access rights are restricted to authorized personnel using a role-based access scheme, in accordance with the principle of least privilege.
Please reference *Complementary User Entity Controls (CUECs)* in Section III for additional controls that are to be implemented by user entities.	
CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.2.1	The System Administrator approves system access for newly hired personnel as well as access change requests.
CC6.2.2	System access is removed within 24 hours upon employee or contractor termination.
CC6.2.3	On at least a quarterly basis, HR and the system administrator review access rights for all Lindy Labs personnel to ensure that system access is appropriate. Any access rights that are no longer needed are removed following this review.
CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.3.1	The System Administrator approves system access for newly hired personnel as well as access change requests.
CC6.3.2	System access is removed within 24 hours upon employee or contractor termination.
CC6.3.3	On at least a quarterly basis, HR and the system administrator review access rights for all Lindy Labs personnel to ensure that system access is appropriate. Any access rights that are no longer needed are removed following this review.
Please reference *Complementary User Entity Controls (CUECs)* in Section III for additional controls that are to be implemented by user entities.	
CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
Lindy Labs does not have a physical office, as all employees work remotely. Additionally, Lindy Labs' system is hosted in the cloud through Heroku. Please reference *Complementary Subservice Organization Controls (CSOCs)* in Section III for a list of controls that are to be implemented by the subservice organization.	

Control #	Control Activity Specified by Lindy Labs
CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read and recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.5.1	Lindy Labs maintains a data retention and disposal policy that outlines how long various types of information are to be retained by the Company. Obsolete information systems and databases, as well as electronic and hard-copy files, are disposed of in accordance with this policy.
CC6.5.2	Prior to disposing of obsolete workstations or removable media, the Engineering team ensures that all physical devices are sanitized to remove any confidential information.
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.6.1	Firewall rules are configured to restrict network traffic to approved ports, protocols, and sources.
CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.7.1	Data in-transit is encrypted using transport layer security (TLS) 1.2 protocol or above.
CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
CC6.8.1	Lindy Labs utilizes endpoint protection software to prevent and detect unauthorized or malicious software such as viruses, malware, and ransomware. Alerts, logs, and reports are generated when potential threats are detected.
System Operations	
CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities and (2) susceptibilities to newly discovered vulnerabilities.	
CC7.1.1	Lindy Labs maintains updated baseline configurations for its information systems and system components to reflect the current enterprise architecture.
CC7.1.2	Lindy Labs utilizes a logging system to continuously monitor administrative activities, changes to sensitive data, login attempts, data deletions, and unusual activities at the application and infrastructure level to provide detailed security findings for visibility and remediation.
CC7.1.3	Vulnerability scanning is performed on an ongoing basis to identify bugs and security vulnerabilities in operating systems and infrastructure. Issues identified are analyzed and remediated in a timely manner.
CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
CC7.2.1	Lindy Labs maintains updated detection policies, procedures, and tools to identify anomalies or unusual activity on information systems. Potential security incidents are filtered and analyzed based on established detection measures.
CC7.2.2	Detection tools are periodically analyzed by management for effectiveness and remedial action is taken when necessary.
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
CC7.3.1	Incidents related to security are logged, tracked, and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process.

Control #	Control Activity Specified by Lindy Labs
CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	
CC7.4.1	Lindy Labs maintains an updated incident response program that defines procedures for containing, mitigating, and ending the threats posed by security incidents as well as restoring operations and communicating security incidents and actions taken to affected parties.
CC7.4.2	Lindy Labs follows the incident response program by understanding the nature of the incident, determining a containment strategy, remediating identified vulnerabilities, and communicating remediation activities to appropriate internal and external parties.
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.	
CC7.5.1	Lindy Labs follows the incident response program to restore the affected environment to full operation by rebuilding systems, updating software, installing patches, and/or changing configurations, as needed.
CC7.5.2	Information about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are communicated to appropriate internal and external parties.
CC7.5.3	After an incident has been resolved and appropriate parties have been notified, a postmortem that includes a root cause analysis and lessons learned is completed. Architectural and/or procedures changes are implemented, when possible, to prevent and detect recurrences of similar incidents. This includes conducting additional training to educate personnel on how to prevent future incidents.
Change Management	
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
CC8.1.1	Lindy Labs maintains an updated Change Management Policy that governs the software development lifecycle (SDLC), including (1) authorizing system changes prior to development; (2) designing and developing system changes; (3) documenting and tracking changes prior to implementation; (4) testing and approving system changes; (5) deploying changes to production; (6) evaluating the changes against their objectives; and (7) modifying infrastructure, data, software, and procedures to remediate identified incidents.
CC8.1.2	Lindy Labs uses a version control system to manage source code, documentation, release labeling, and other change management tasks.
CC8.1.3	Changes to application and system infrastructure are developed and tested in a separate development or test environment before implementation.
CC8.1.4	Developers are unable to deploy changes to the production environment without independent code review and approval.
CC8.1.5	Changes to the production environment are communicated to affected internal and external stakeholders.
Risk Mitigation	
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
CC9.1.1	Lindy Labs maintains a captive insurance company to insure against the financial impact of business disruptions, including cyber incidents
CC9.1.2	Lindy Labs maintains an updated business continuity and disaster recovery plan that guides the organization in how to respond and recover from disruptions in networks, systems, and internal operations. This plan is tested on at least an annual basis.
Lindy Labs' system is hosted in the cloud through Heroku. Please reference *Complementary Subservice Organization Controls (CSOCs)* in Section III for a list of controls that are to be implemented by the subservice organization.	

Control #	Control Activity Specified by Lindy Labs
CC9.2: The entity assesses and manages risks associated with vendors and business partners.	
CC9.2.1	Lindy Labs maintains an updated Vendor Management Policy to monitor and ensure service levels and ongoing compliance of existing vendors. The policy outlines roles, responsibilities, and communication protocols around managing vendor relationships and exception handling.
CC9.2.2	Lindy Labs conducts comprehensive vendor due diligence prior to onboarding a new vendor, as well as on an annual basis for existing significant vendors. This includes performing a vendor risk assessment and reviewing the SOC 2 reports, SOC 3 reports, ISO 27001 certifications, and/or responses to information security questionnaires.