Proof of Reserves
Audit Report

TAPBIT

Table of Contents

References:
- [**Customer's Website**](#)
- [**Proof of Reserves Methodology**](#)
- [**Proof of Reserves Presentation**](#)

Report details:

- **Report date: Thu Oct 31 2024**
- **Audit date: Thu Oct 31 2024**
- **Approved: Bruno Mogetta**

Executive Summary

The primary objective of this audit is to provide a comprehensive confirmation that Tapbit (hereinafter - Auditee, Tapbit), a leading digital asset exchange, diligently safeguards user liabilities for in-scope digital assets. Through rigorous Proof of Reserve audit procedures, including Proof of Liabilities, Proof of Ownership, Reserves calculation, and Proof of Reserves Assessment, Auditee has demonstrated its commitment to transparency and user trust.

During the meticulous Proof of Reserves process, Tapbit has successfully proved that its holdings provide full coverage for user liabilities, maintaining a remarkable 1:1 ratio for all in-scope assets. This assurance is substantiated by the compelling findings outlined.

Reserves Proofed	
Proof of Liabilities	✓
Proof of Ownership	✓
Reserves Calculation	✓
PoR Assessment	✓

Building Trust Through Proof of Reserves

About Hacken's Proof of Reserves

By implementing the Hacken's Proof of Reserves service, organizations can provide verifiable evidence of their reserve holdings, reassuring customers and stakeholders that their assets are securely held and fully backed. This transparency is essential in establishing trust and differentiating organizations within the crypto industry.

At Hacken, we are focused on verifying an organization's liabilities, such as customer deposits or outstanding loans, to ensure that the liabilities are accurately represented and can be met by the organization's assets.

The purpose of conducting Proof of Reserves audit is to provide transparency and assurance to stakeholders that the organization is operating in a trustworthy and responsible manner. The main objectives of a Proof of Reserves audit include confirming the existence and authenticity of cryptocurrency holdings, verifying the amount of cryptocurrency held matches the amount claimed by the organization.

Proof of Liabilities

Proof of Liabilities involves calculating all liabilities, which are the balances of in-scope assets held by the Auditee users, to form a Client Liability Report. As auditors, we collect the minimum necessary data from client's users to ensure their privacy is safeguarded. This may include a pair of public addresses/balances or UUID/public address/balance, depending on the specific requirements.

Proof of Ownership and Reserve Calculation

Hacken, a trusted third-party Proof of Reserves Assessor, ensures the accuracy of the Total Reserves Balance by verifying ownership of auditee's wallets. This crucial verification process precedes the comparison of the Total Reserves Balance with the Client Liability Report.

To achieve this, Hacken employs secure and verifiable methods like Custom Digital Signatures and "Send-to-Self" Transactions, among other methods, to confirm the ownership of addresses associated with the client's wallets.

- **Custom Digital Signatures** involve exchanging a Hacken-provided custom message, verifying corresponding digital signatures to establish ownership.

- **"Send-to-Self" Transactions**: Hacken provides the auditee with cryptocurrency to send to their own wallet. By inspecting transaction details and matching specific parameters, ownership of the address is confirmed. This meticulous approach ensures the accuracy of the Total Reserves Balance, enabling a comprehensive comparison with the Client Liability Report.

Proof of Reserves audit procedure

1. Preliminary Meetings and Information Flow Understanding

The audit started with a series of meetings aimed at understanding the information flow and the client's asset management methods. These discussions were critical in gaining a comprehensive view of the client's operational structure and the handling of cryptocurrency assets.

2. Supervision and Analysis of Client's Procedures

The client's existing scripts used for compiling their balance sheets were closely supervised. Essential credentials were obtained to facilitate an in-depth analysis. This step was crucial to understand the client's methods for asset compilation and balance reporting.

3. Development of Independent Algorithms for Balance Evaluation

To ensure an independent and unbiased assessment, new scripts were developed by Hacken.

These scripts focused on evaluating the client's available balance and staking, encompassing a range of assets such as cold wallets and hot wallets.

The objective was to cross-verify the client's reported data with an independently sourced dataset.

4. Selection of Clientele for Testing

The client was requested to provide a list of customers to be included in the audit test. For confidentiality purposes, each user associated with our client was assigned a unique user hash. This measure ensured that Hacken could not link any specific balances to identifiable individuals.

5. Procedure for User Data Collection

The client snapshots a list of their users in a specified format. The integrity of the source code was thoroughly verified. Under supervision, the client executed this algorithm to provide the necessary data.

6. Simultaneous Data Retrieval and Comparison

While the client executed the script, Hacken's auditors concurrently ran the independently developed program to ascertain the company's cryptocurrency balances. This step involved a meticulous one-to-one comparison of the assets.

7. Conclusion and Reporting

Upon completing the comparison, conclusions were drawn regarding the accuracy and integrity of the client's reported cryptocurrency reserves. The results of this comprehensive audit provided a clear picture of the client's reserve status, contributing significantly to transparency and trust in their financial reporting.

Proof of Reserves Scope & Findings

Proof of Reserves Audit Scope

Auditee	TAPBIT
Auditee Website	https://www.tapbit.com/
In-scope assets	BTC ETH
In-scope Networks	Bitcoin Ethereum
Number of Liability holders	>45,000

Proof of Reserves Audit Finding

Proof of Liabilities	Hacken's team obtained the total assets of Tapbit liabilities report, including all clients that have at least one non-zero balance of in-scope assets with nominal balances. The dump was inspected as the total Tapbit liabilities report to exclude any duplications of clients' user IDs. The total liabilities balance was summed from all clients' balances of in-scope assets.
Proof of Ownership and Reserves Calculation	Hacken's team obtained from Tapbit management a complete list of all public keys/addresses holding in-scope assets. For each address, Tapbit initiated a small outgoing transaction sending a minimum amount defined by Hacken from each address. Hacken monitored the respective blockchain and verified that the expected outgoing transactions with the defined amounts were received from each of the provided addresses. The fact that Tapbit could initiate outgoing transactions from those addresses conclusively proved their control and ownership over those addresses at the time of this audit.
Data Hash	56e5e75458b8c16715b61cdb8ca36088

Audited wallets

Network	Address
Bitcoin	******************************jsH
Ethereum	**2f5

Collateral ratios

Asset	Collateral Ratio
BTC	>2341%
ETH	>2431%

Team Composition

#	Team Member and Role	Components to review
1	Lead PoR Auditor (Bruno Mogetta) b.mogetta@hacken.io	Audit Supervision, Interview conducting, Results and Recommendations
2	PoR Auditor (Pedro Bustos) p.bustos@hacken.io	Development and maintenance of Hacken's Proof of Reserves and verification tools

Conclusion

Tapbit is dedicated to upholding the highest standards of financial security and ensuring the safety of its users' assets. By conducting regular Proof of Reserves audits, Tapbit reaffirms its commitment to providing a trustworthy and reliable trading platform. Tapbit's efforts towards transparency extend beyond merely creating a system for Proof of Reserves; the company has also committed to engaging an independent auditor, Hacken, for verification of these reserves.

The Hacken team's Proof of Reserves audit, conducted on **Thursday, October 31, 2024**, demonstrates that Tapbit maintains a reserve ratio of **> 100 %**. This finding signifies that Tapbit possesses sufficient reserves to cover its liabilities, thereby bolstering trust and confidence among its users and stakeholders.

This report serves as a testament to the responsible financial management practices employed by Tapbit, as well as the company's dedication to transparency and accountability.