HACKEN

MEXC

Proof of Reserves Verification Report

MEXC



Thu November 12 2026

Hacken OU
Parda 4, Kesklinn
Tallinn 10151 Harju Maakond, Eesti
Kesklinna, Estonia

Table of Contents

Table of Contents 1

Executive Summary 2

Building Trust Through Proof of Reserves 3
- About Hacken's Proof of Reserves 3
- Proof of Liabilities 3
- Proof of Ownership and Reserve Calculation 4

Methodology for Proof-of-Reserves Technical Verification of Cryptocurrencies 5
- Preliminary Meetings and Information Flow Understanding 5
- Supervision and Analysis of Client's Procedures 5
- Development of Independent Algorithms for Balance Evaluation 5
- Selection of Clientele for Testing 5
- Procedure for User Data Collection 6
- Simultaneous Data Retrieval and Comparison 6
- Conclusion and Reporting 6

Proof of Reserves Scope & Findings 7
- Proof of Reserves Technical Verification Scope 7
- Proof of Reserves Technical Verification Findings 8
- Verified Wallets 9
- Collateral ratios 11

Team Composition 12

Conclusion 13

Disclaimers 14

References:

- Customer's Website
- Customer's Support Email
- Customer's Support Website
- Proof of Reserves Methodology

Hacken OU
Parda 4, Kesklinn
Tallinn 10151 Harju Maakond, Eesti
Kesklinna, Estonia

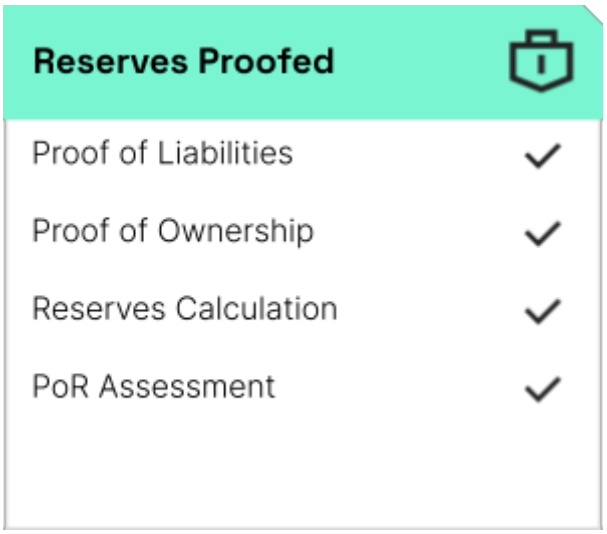
Report details:

- **Report date: Thu November 12, 2026**
- **Technical Verification date: Tue November 10, 2026**
- **Approved: Joaquin Girardi**

Executive Summary

The primary objective of this technical verification is to provide a comprehensive confirmation that MEXC (hereinafter - "MEXC" or the "Verified Entity"), a leading digital asset exchange, diligently safeguards user liabilities for in-scope digital assets. Through rigorous Proof of Reserve procedures, including Proof of Liabilities, Proof of Ownership, Reserves calculation, and Proof of Reserves Technical Verification, the Verified Entity has demonstrated its commitment to transparency and user trust.

During the meticulous Proof of Reserves process, MEXC 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.



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 technical verification 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 technical verification 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 Verified Entity users, to form a Client Liability Report. As technical verification providers, 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 MEXC'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 Verified Entity 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.

Methodology for Proof-of-Reserves Technical Verification of Cryptocurrencies

1. Preliminary Meetings and Information Flow Understanding

The technical verification 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. 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 technical verification, 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 technical verification 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 technical verification providers 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 technical verification provided a clear picture of the client's reserve status, contributing significantly to transparency and trust in their financial reporting.

Hacken OU
Parda 4, Kesklinn
Tallinn 10151 Harju Maakond, Eesti
Kesklinna, Estonia

Proof of Reserves Scope & Findings

Proof of Reserves Technical Verification Scope

Verified Entity	MEXC			
Verified Entity Website	https://www.mexc.com			
In-scope assets	BTC	ETH	USDT	USDC
In-scope Networks	Algorand Aptos Arbitrum Avalanche-C Base Bitcoin BSC	Celo Ethereum Kaia Linea Morph Near Optimism	Plasma Polkadot AH Polygon SEI Solana Sonic Starknet	SUI Ton Tron Unichain XDC ZKSync Lite
Technical Verification type	Proof of Reserves			

Proof of Reserves Technical Verification Findings

Proof of Liabilities	Hacken's team obtained the total assets of MEXC liabilities report which was calculated using all clients' balances greater than 0.00000000 of in-scope assets with nominal balances. Additionally, Hacken conducted an extensive technical verification of the code used to verify the Merkle tree integrity. The Merkle proof validation process was thoroughly examined using the official Merkle proof validation tool. This rigorous verification process, involving a comprehensive code technical verification, reconciliation of user balances, root hash calculations, and Merkle tree validations, has yielded compelling evidence supporting the integrity of the reported balances. While absolute certainty can rarely be attained, Hacken's findings strongly indicate the liabilities report accurately represents the underlying client balances. Liabilities data reflects internal MEXC daily snapshots. Accordingly, the figures provided represent the most recent snapshot available prior to the assessment.
Proof of Ownership and Reserves Calculation	Hacken's team obtained from MEXC management a complete list of all public keys/addresses holding in-scope assets. For each address, MEXC 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 MEXC could initiate outgoing transactions from those addresses conclusively proved their control and ownership over those addresses at the time of this technical verification.
Merkle proofs validator	https://github.com/mexcmerkle/mexc-merkle-proof-of-reserves
Merkle-proof commit hash	9af26ec1d7d65c15136661bc795b5e6cc9b55953

Verified wallets

Network	Address
Algorand	M3IAMWFYEIJWLWFIIOEDFOLGIVMEOB3F4I3CA4BIAHJENHUUSX63APOXXM
Algorand	ZEJPIFQF5MSDOB3YA6OUG4S26FFX64SCTHKDMYCCB26JGG7DC4IPBWQSLQ
Aptos	0xe8ca094fec460329aaccc2a644dc73c5e39f1a2ad6e97f82b6cbdc1a5949b9ea
Arbitrum	0x9b64203878f24eb0cdf55c8c6fa7d08ba0cf77e5
Arbitrum	0xb86f1061E0D79E8319339d5FDbb187D4E7Ad3300
Avalanche-C	0xffb3118124cdaebd9095fa9a479895042018cac2
Base	0x4e3ae00e8323558fa5cac04b152238924aa31b60
Bitcoin	13uZyaPbt4rTwYQ8xWFySVUzWH3pk2P5c7
Bitcoin	17wgJkQ8v66fXTUawQS3sohEfzP4CCD8Xu
Bitcoin	19KYQDpyssRUtpfa4pfAWiNQLeysThd1us
BItcoin	1Ak5Zk6P3Y7AbrdhWHif7GmEJhd6FqAS9J
Bitcoin	1MDVjZdX8QD212pT8Z8EMP7DuFQHKqN3mx
Bitcoin	1NEQFpjSqRMWuHLTrouSbmSgXuJr8zPCN7
Bitcoin	35C2L1pCgwzBHNcDcVL1a5RuoefeWqyjAR
Bitcoin	38RB6AuNgLjPyJqt92wJXoas7ZMYq12gHR
Bitcoin	bc1qnzf53fl4a0lh00p9207c456xkk9fmgdnm6tyky
Bitcoin	bc1qrlsks7xe755m05zfreyjdxn34rypc4lnghtcwc
BSC	0x2e8f79ad740de90dc5f5a9f0d8d9661a60725e64
BSC	0x4982085c9e2f89f2ecb8131eca71afad896e89cb
BSC	0x7354abb551e41bbd9fb32e2e79f44631349119b8
BSC	0x9bb6a22da110c6c9bab745bcaf0ee142ee83af37
BSC	0xa71180a5bfbc0dbd18f7b355e4afa101a319ff6a
Celo	0x9f43427ca3776f00246e8a52b7373ec724b00402
Ethereum	0x0162cd2ba40e23378bf0fd41f919e1be075f025f

Ethereum	0x12C5E4EEEaA20E25847b5453D23246983c512DB7
Ethereum	0x1F7370792a057227024e7a8Cc15b40E3eD171FfC
Ethereum	0x3cc936b795a188f0e246cbb2d74c5bd190aecf18
Ethereum	0x75e89d5979e4f6fba9f97c104c2f0afb3f1dcb88
Ethereum	0x76bf215ADE956642B056B9043e014988941BbdDd
Ethereum	0x9642b23ed1e01df1092b92641051881a322f5d4e
Ethereum	0xBCB302A64ADB7f2C8697e17C1e948f5b058F0e49
Ethereum	0xc411aB12837f63935b71B6c6643d0f7000e55E4b
Ethereum	0xD67f25Ef2399A0C769B1A35634C5Ce77166714dB
Ethereum	0xe4e3ECA65460C14a5245b09fee15a92bA09458b6
Ethereum	0xe8832a868c091263ed190a9f4be304a03895dd91
Ethereum	0xee136c0389733849dd710ac7104e92c6bf497574
Ethereum	0xf016E1D45EF23Bdd414E7A2E4D46E1b34577b508
Ethereum	0xf95334a86d09A6eEc74D69Da344efaca424B13a9
Ethereum	0xc906895C8833481571118F0C59877bFF6bE38aC1
Kaia	0x9dd35021d77c1de5ed50b9d788a2f68903a96b96
Linea	0x4b68038e910941b7438e70a3943dcc4fd543715c
Morph	0x02e78de615f26224b94bba0d34035424396c97a8
Near	423df0a6640e9467769c55a573f15b9ee999dc8970048959c72890abf5cc3a8e
Optimism	0xdf90c9b995a3b10a5b8570a47101e6c6a29eb945
Plasma	0xfa1711c6513b09b13ee8aeef0dff266114b4e97c
Polkadot AH	1NyqRuFPcCXjYneddrmXxKQKSGGTdJSnCQxV3k6Yp2wu6nH
Polygon	0x51e3d44172868acc60d68ca99591ce4230bc75e0
Polygon	0x576b81F0c21EDBc920ad63FeEEB2b0736b018A58
SEI	0x361f9739a4269caf056d936970e19579b1c5935d
Solana	5PAhQiYdLBd6SVdjzBQDxUAEFyDdF5ExNPQfcscnPRj5
Solana	ASTyfSima4LLAdDgoFGkgqoKowG1LZFDr9fAQrg7iaJZ

Sonic	0x680178d61d910736153991660c5710841c440ec7
Starknet	0x069a7818562b608ce8c5d0039e7f6d1c6ee55f36978f633b151858d85c022d2f
SUI	0xc38e308a33c6544657a6c1e3149fc256f0ae71b9546ab0999ee958ad2f15f32
SUI	0xf8b7b95d01ae79756fc3d1bc58675e59a17f07cdafe3d31ea57425adbec2d43f
Ton	UQDYh9Di0cT8QSbnHJcNM6sYlpQAA0rnA7sats7Mgwd344Mm
Tron	TB37WWozkkenGVYWD7Do2N5WT2CedqDktJ
Tron	TEPSrSYPDSQ7yXpMFPq91Fb1QEWpMkRGfn
Unichain	0x4fb80c239ce06d3c8746cf57cbae7e08b8386d8d
XDC	xdcF29f049144467b3dc55e19205c30C1737942F23a
ZKSync Lite	0xb5a6fd438017dbb0a2e5fcdcca715da227582ce4

Collateral ratios

Asset	Collateral Ratio
BTC	>100%
ETH	>100%
USDC	>100%
USDT	>100%

Team Composition

#	Team Member and Role	Components to review
1	Lead PoR provider (Joaquin Girardi) j.girardi@hacken.io	Technical Review Supervision, Interview conducting, Results and Recommendations
2	PoR provider (Vasco Cabral da Camara) v.camara@hacken.io	Development and maintenance of Hacken's Proof of Reserves and verification tools

Conclusion

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

The latest verification, conducted by Hacken on **Tuesday, November 10, 2026**, included a comprehensive review of loan liability accountability and completeness, confirming an in-scope **reserve ratio exceeding 100%** even after considering these obligations. MEXC's diversified asset holdings and robust financial position allowed the platform to maintain full coverage, demonstrating the exchange's resilience and dedication to user fund security.

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

Disclaimers

Hacken Disclaimer

The information given for the assessment has been analyzed based on best industry practices at the time of the writing of this report, with issues or inconsistencies, the details of which are disclosed in this report.

The report contains no statements or warranties on identifying any technical security-related finding.

The report covers the information submitted and reviewed, so it may not be relevant after any modifications.

While this report provides a point-in-time attestation of on-chain assets based on the provided and verified blockchain addresses and data, it should not be considered a comprehensive financial audit of all assets, liabilities, or the organization's overall financial position.

While this report includes a thorough analysis of the provided blockchain addresses and data, point-in-time verification alone should not serve as the sole basis for assessment — conducting multiple independent proof of reserves attestations on a recurring basis is recommended to maintain transparency of on-chain assets over time.

Clarifications

[1] English is the report's original language. The Consultant is not responsible for the accuracy of the translated versions.