HACKEN

BYBIT

Proof of Reserves Audit Report

BYBIT

Thu Dec 19 2024

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 3

Methodology for Proof-of-Reserves Audit of Cryptocurrencies 4
- Preliminary Meetings and Information Flow Understanding 4
- Supervision and Analysis of Client's Procedures 4
- Development of Independent Algorithms for Balance Evaluation 4
- Selection of Clientele for Testing 5
- Procedure for User Data Collection 5
- Simultaneous Data Retrieval and Comparison 5
- Conclusion and Reporting 5

Proof of Reserves Scope & Findings 6
- Proof of Reserves Audit Scope 6
- Proof of Reserves Audit Findings 7
- Audited wallet 8
- Collateral ratios 12

Team Composition 13

Conclusion 13

References:

- Customer's Website
- https://www.bybit.com/app/user/proof-of-reserve
- https://github.com/bybit-exchange/merkle-proof
- Proof of Reserves Methodology
- Proof of Reserves Presentation

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

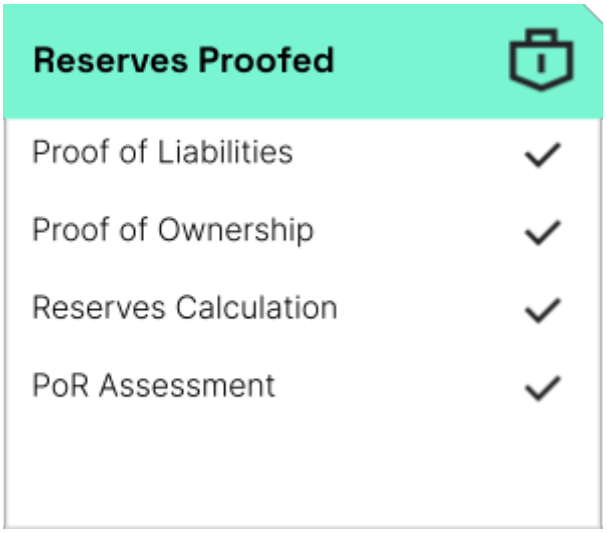
Report details:

- **Report date: Thu Dec 19 2024**
- **Audit date: Thu Dec 12 2024**
- **Approved: Bruno Mogetta**

Executive Summary

The primary objective of this audit is to provide a comprehensive confirmation that ByBit (hereinafter - Auditee, Bybit), 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, Bybit 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.



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

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.

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

Proof of Reserves Scope & Findings

Proof of Reserves Audit Scope

Auditee	BYBIT
Auditee Website	https://www.bybit.com
In-scope assets	AGI, AGLA, APEX, APT, ATOM, AVAX, BEAM, BLUR, BTC, COMP, CRV, DOGE, DOT, DYDX, EOS, ETH, FET, FTM, GALA, IMX, LDO, LINK, LTC, MANA, MNT, OP, PEPE, POL, RENDER, SAND, SHIB, SHRAP, SOL, SUSHI, UNI, USDC, USDE, USDT, WLD, XRP
In-scope Networks	Aptos, Arbitrum, Avalanche-C, Avalanche-X, BASE, Bitcoin, BSC, Celo, Cosmos, Dogecoin, DYDX, EOS, Ethereum, Linea, Fantom, Arbitrum Nova, Kava EVM, Litecoin, Mantle, Manta, Optimism, Polkadot, Polygon, Scroll, Solana, Ton, Tron, XRP Ledger, ZKSync Lite, ZKSync Era
Proof of Reserves Audit type	Proof of Reserves
Number of Liability holders	>59,000,000
Merkle proofs validator	https://github.com/bybit-exchange/merkle-proof
Merkle-proof commit hash	170349cd53549567db0a0185dd7e2f72d4cf04ce

Proof of Reserves Audit Finding

Proof of Liabilities	Hacken's team obtained the total assets of Bybit 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 audit of the code used to generate the Merkle tree and verify its integrity. The team then proceeded to compare the output of the Merkle tree against the liabilities report. The Merkle proof generation and validation process was thoroughly examined using the official Merkle proof validation tool. This rigorous verification process, involving a comprehensive code audit, 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.
Proof of Ownership and Reserves Calculation	Hacken's team obtained from Bybit management a complete list of all public keys/addresses holding in-scope assets. For each address, Bybit 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 Bybit could initiate outgoing transactions from those addresses conclusively proved their control and ownership over those addresses at the time of this audit.
Merkle Tree Root Hash	5eba3e0d9ce473de8d48e9839e309a738ddc3d747a5b71a5b3ca888efc83434a
Merkle proofs validator	https://github.com/bybit-exchange/merkle-proof
Merkle-proof commit hash	170349cd53549567db0a0185dd7e2f72d4cf04ce

Audited wallets

Network	Address
BASE	0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4
Ethereum	0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4
Optimism	0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4
ZKSync Era	0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4
ZKSync Lite	0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4
Ethereum	0x6Bd869be16359f9E26f0608A50497f6Ef122eE3E
Ethereum	0x922fa922da1b0b28d0af5aa274d7326eaa108c3d
Ethereum	0x88a1493366d48225fc3cefbdae9ebb23e323ade3
BSC	0x88a1493366d48225fc3cefbdae9ebb23e323ade3
Mantle	0x88a1493366d48225fc3cefbdae9ebb23e323ade3
BASE	0x88a1493366d48225fc3cefbdae9ebb23e323ade3
Polygon	0x88a1493366d48225fc3cefbdae9ebb23e323ade3
Arbitrum	0x88a1493366d48225fc3cefbdae9ebb23e323ade3
Optimism	0x88a1493366d48225fc3cefbdae9ebb23e323ade3
Avalanche-C	0x88a1493366d48225fc3cefbdae9ebb23e323ade3
Ethereum	0xA7A93fd0a276fc1C0197a5B5623eD117786eeD06
ZKSync Lite	0xA7A93fd0a276fc1C0197a5B5623eD117786eeD06
BASE	0xbaed383ede0e5d9d72430661f3285daa77e9439f
Ethereum	0xbaed383ede0e5d9d72430661f3285daa77e9439f
Ethereum	0xee5B5B923fFcE93A870B3104b7CA09c3db80047A
Arbitrum	0xee5B5B923fFcE93A870B3104b7CA09c3db80047A
Avalanche-C	0xee5B5B923fFcE93A870B3104b7CA09c3db80047A
BASE	0xee5B5B923fFcE93A870B3104b7CA09c3db80047A
BSC	0xee5B5B923fFcE93A870B3104b7CA09c3db80047A
Optimism	0xee5B5B923fFcE93A870B3104b7CA09c3db80047A

Network	Address
Polygon	0xee5B5B923fFcE93A870B3104b7CA09c3db80047A
ZKSync Era	0xee5B5B923fFcE93A870B3104b7CA09c3db80047A
ZKSync Lite	0xee5B5B923fFcE93A870B3104b7CA09c3db80047A
Arbitrum	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Arbitrum Nova	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Avalanche-C	0xf89d7b9c864f589bbF53a82105107622B35EaA40
BSC	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Celo	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Ethereum	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Fantom	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Kava EVM	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Linea	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Manta	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Mantle	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Optimism	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Polygon	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Scroll	0xf89d7b9c864f589bbF53a82105107622B35EaA40
ZKSync Era	0xf89d7b9c864f589bbF53a82105107622B35EaA40
ZKSync Lite	0xf89d7b9c864f589bbF53a82105107622B35EaA40
Manta	0xa6a9f45518881a788e29f82a032f9d400177d2b6
Mantle	0x588846213a30fd36244e0ae0ebb2374516da836c
Aptos	0x84b1675891d370d5de8f169031f9c3116d7add256ecf50a4bc71e3135ddba6e0
Bitcoin	16jVbMCcqq1deKrMB3esL2HPso7kvqUsec
Bitcoin	1GrwDkr33gT6LuumniYjKEGjTLhsL5kmqC
Bitcoin	bc1q2qqqt87kh33s0er58akh7v9cwjgd83z5smh9rp
Bitcoin	bc1qs5vdqkusz4v7qac8ynx0vt9jrekwuupx2fl5udp9jql3sr03z3gsr2mf0f

Network	Address
Bitcoin	bc1qa2eu6p5rl9255e3xz7fcgm6snn4wl5kdfh7zpt05qp5fad9dmsys0qjg0e
Avalanche-X	avax1e6cxrjlmpa0mpk6vpv3dqu9y35jsh7hameh0cg
Polkadot	11yLs2qzU15AhxnH1d7Koqcf83AwutKkDaGbqsJJ6yDWQjc
Polkadot	12nr7GiDrYHzAYT9L8HdeXnMfWcBuYfAXpgfzf3upujeCciz
Cosmos	cosmos17kvae2jckzpkct78yealre3ms2gu28cdmtwsv7
Cosmos	cosmos1pyarvcy2ehrw86rcvfun34gyu2dlunnthvkc83
Solana	42brAgAVNzMBP7aaktPvAmBSPEkehnFQejiZc53EpJFd
Solana	AC5RDfQFmDS1deWZos921JfqscXdByf8BKHs5ACWjtW2
Dogecoin	D94tDRhr4X9Tjgr8MG1Nrd5ARpesPAM7ZB
Dogecoin	DDz1H7AcqPgmKzFEP3pBHW5b1GWuWEoAAP
Litecoin	LKxNtynH2GxLc2oLxUGL6ryckK8JMdP5BR
Litecoin	ltc1qp7cnlxmz8wgc93g0m020ckru2s55t25y3wunf6
Tron	TB1WQmj63bHV9Qmuhp39WABzutphMAetSc
Tron	TB1cPNTPE2yKRbyd5C3hd9KMXgb8HqW1CM
Tron	TKFvdC4UC1vtCoHZgn8eviK34kormXaqJ7
Tron	TQVxjVy2sYt4at45ezD7VG4H6nQZtsua5C
Tron	TS9PDCB6vzLYDCPr5Nas2yzekdr7ot6dxn
Tron	TTH75Z9rfRgzCLNDDYBaR2WjUvuSDRtSMg
Tron	TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa
Tron	TYgFxMvvu2VHFJnxQf8fh1qVAeMfXZJZ3K
EOS	coldcrazycat
EOS	eosdididada3
EOS	kcwo3rimcnqf
XRP Ledger	rMvCasZ9cohYrSZRNYPTZfoaaSUQMfgQ8G
XRP Ledger	raBWjPDjohBGc9dR6ti3DsP9Sn47jirTi3
XRP Ledger	raQxZLtqurEXvH5sgijrif7yXMNwvFRkJN

Network	Address
XRP Ledger	rwBHqnCgNRnk3Kyoc6zon6Wt4Wujj3HNGe
DYDX	dydx10sdnqxvrwe3mhducn6plyewul84edgd47rfnfe
Ton	EQB9Ez10QlyOAN4BVROkTmbm0W0yHnFyCux1eZZeXeKMVV6_
Ton	EQBKHCC8mm-SIPdfHIen840otzpI0i5tyzYw3b54s8ytANhS
Mantle	0xEe6281d94Fed46A90379F2033B6BbdcDa4EF462E
BSC	0x388E52979AC487c6BdaFCC84B251976Cd162790b
Tron	TFbrM6tiw4A3AhFQAyY7u6jYs7m2HFKavU
Tron	TUCS5ToZvL23Q6kKtWUhAGgMfJBwPUZgfu
Tron	TF1yVgYNJYx8AEtKLhjd2YbLJ33uyWu9Eo
Tron	THRKrcUPirR6GU6qvsKAv2M6PUBcwe6ruD
Tron	TMB53f4eYhEhTqkuzKRNDoDNu5Ma5DtMSc
Tron	TTT5cF5aPZjF6FkPJqV4MmnuykMACjDvmb
Fantom	0x88a1493366d48225fc3cefbdae9ebb23e323ade3

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

Collateral ratios

Asset	Collateral Ratio	Asset	Collateral Ratio
AGI	>100%	LDO	>100%
AGLA	>100%	LINK	>100%
APEX	>100%	LTC	>100%
APT	>100%	MANA	>100%
ATOM	>100%	MNT	>100%
AVAX	>100%	OP	>100%
BEAM	>100%	PEPE	>100%
BLUR	>100%	POL	>100%
BTC	>100%	RNDR	>100%
COMP	>100%	SAND	>100%
CRV	>100%	SHIB	>100%
DOGE	>100%	SHRAP	>100%
DOT	>100%	SOL	>100%
DYDX	>100%	SUSHI	>100%
EOS	>100%	UNI	>100%
ETH	>100%	USDC	>100%
FET	>100%	USDE	>100%
FTM	>100%	USDT	>100%
GALA	>100%	WLD	>100%
IMX	>100%	XRP	>100%

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

Bybit 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, Bybit reaffirms its commitment to providing a trustworthy and reliable trading platform. Bybit'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, December 12, 2024**, demonstrates that Bybit maintains a reserve ratio of **> 100 %**. This finding signifies that Bybit 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 Bybit, as well as the company's dedication to transparency and accountability.