



Proof of Reserves Audit Report

WhiteBIT



Wed Nov 20 2024


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	11
Findings	12
Team Composition	13
Conclusion	14

References:

- [Customer’s Website](#)
 - [Proof of Reserves Methodology](#)
 - [Proof of Reserves Presentation](#)
-


Report details:

- **Report date: Wed Nov 20 2024**
- **Audit date: Mon Nov 18 2024**
- 

Executive Summary

The primary objective of this audit is to provide a comprehensive confirmation that WhiteBIT (hereinafter - Auditee, WhiteBIT), 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, WhiteBIT 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 Prooved 	
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	WhiteBIT				
Auditee Website	https://whitebit.com/				
In-scope assets	100X	DGD	IEOS	PAWG	STRI
	2XDN	DIGEX	IHC	PAWS	STRM
	3CS	DOGE	INRT	PAWZ	SUPERBID
	ACED	DOGES	JNB	PGALA	SWAPP
	ACOIN	DOGIRA	JULD	PGPAY	SXI
	ADA	DOT	KATANA	PHTF	TABOO
	AE	DOV	KEY	PIR	TERN
	AGIX	EARNX	KISHIMOTO	PKRFI	TLW
	AMLT	ELAN	KLAY	PLA	TOMI
	AQGT	ELONONE	KLEE	POLY	TOMOE
	AQN	EMPIRE	KOCJ	POODL	TORG
	ARV	EOS	KOJI	PPT	TREEP
	ASS	ESHK	KTLYO	PRT	TRIBE
	ATOM	ETC	KUPP	PSI	TRUXTR
	AVAX	ETH	LADYS	PTOY	TRX
	AWG	ETHW	LEND	PUNDIX	TT
	AWX	EVX	LIBFX	PWC	TWA
	BCH	EXRD	LID	PYE	TYC
	BDCC	FJB	LIEN	WARK	ULT
	BERRY	FLIX	LIFE	QBIT	UNI
	BFIRE	FLOWOLD	LINK	QTECH	USDC
	BHT	FLT	LOFI	QUA	USDP
	BITCCA	FMA	LOKA	R	USDT
	BLCT	FME	LOOM	RAK	USM
	BLVR	FNT	LOT	RAPTOR	UTED
	BLXM	FOF	LOTTO	RARE	VERI
	BNB	FOGE	LTC	REAL	VIDYA
	BNOX	FORTH	LUFFY	REM	VLT
	BOBC	FOY	MATIC	REP	VNDC



BREW	FROGE	MBOX	REQ	VNLA
BSBT	FROGEX	MDX	RNDR	VOLT
BTC	FSAFE	MEDI	ROX	WBT
BUBO	FTM	MEFA	RPZX	WBTC
CAP	FTT	MELLO	RX	WCOM
CBUCKS	FUN	MEXC	SAFU	WLD
CDL	FUTURE	MIR	SANSHU	WLONG
CELO	GAL	MIRAI	SATT	WNXM
CENT	GAME	MNDAO	SFC	WORLD
CFXQ	GAPT	MNDOGE	SGC	WOZX
CLG	GARI	MNE	SHARK	WSBT
COP	GBC	MNTG	SHIB	WTC
COPTER	GMC	MONEY	SIL	XCUR
CPIE	GRUMPY	MTP	SL	XEMX
CRT	GSMT	MYL	SLAM	XLM
CRYPT	GULF	NCAT	SLT	XNR
CT	HAPPY	NCDT	SMARS	XRDOGE
CUC	HDX	NEAR	SMI	XRP
CUR	HMETA	NEEO	SNB	YFFC
CVA	HMR	NOOFT	SOL	ZAMZAM
CXRBN	HNZO	NTK	SOLO	ZIL
CYCE	HODL	NVZN	SRM	ZZZ
DAA	HOGL	OCEAN	SRO	
DEEZ	HOKK	OCTA	SSLX	
DEF	HPPOT	ORFANO	STARK	
DEFO	ICHI	PAND	STON	



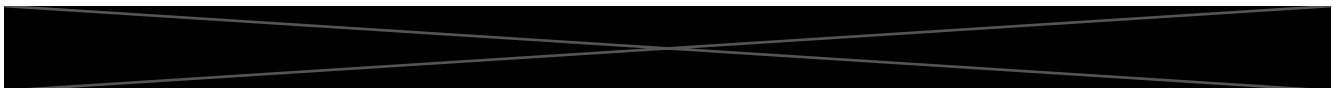
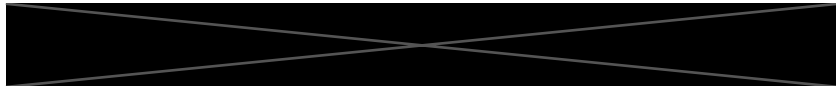
In-scope Networks

Arbitrum	Dogecoin	Polygon
Avalanche	Ethereum	Ripple
Bitcoin	Ethereum Classic	Solana
Bitcoin Cash	Ethereum PoW	Stellar
BSC	Fantom	Tron
Cardano	Klaytn	Whitechain
Celo	Litecoin	
Cosmos	Optimism	

**Proof of Reserves
Audit type**

Proof of Reserves

**Number of Liability
holders**





Proof of Reserves Audit Finding

Proof of Liabilities Hacken’s team obtained the total assets of WhiteBIT liabilities report, including all clients’ balances greater than 0.00000000 of in-scope assets with nominal 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 WhiteBIT management a complete list of all public keys/addresses holding in-scope assets. For each address, WhiteBIT 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 WhiteBIT 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 6e3f24d953cc7592cbfb1f5d1abae5cdaf1bc87008df5d
a047e0c83c970a9741ab064b98ae46aeb4c4c00ed605
d1999b194fe034256b27ddef67944dddafa03b9



Audited wallets

Network	Address
Bitcoin	
Ethereum	
Polygon	
Litecoin	
Bitcoin Cash	
Tron	
Whitechain	
BSC	
Dogecoin	
Stellar	
Ripple	
Cosmos	
Solana	
Cardano	
Celo	
Ethereum PoW	
Avalanche	
Optimism	
Klaytn	
Ethereum Classic	
Arbitrum	
Fantom	



Collateral ratios

Asset	Collateral Ratio	Asset	Collateral Ratio
BTC*	507%	USDT*	108%
WBT*	100%	USDC*	205%
ETH*	269%	SOL*	101%

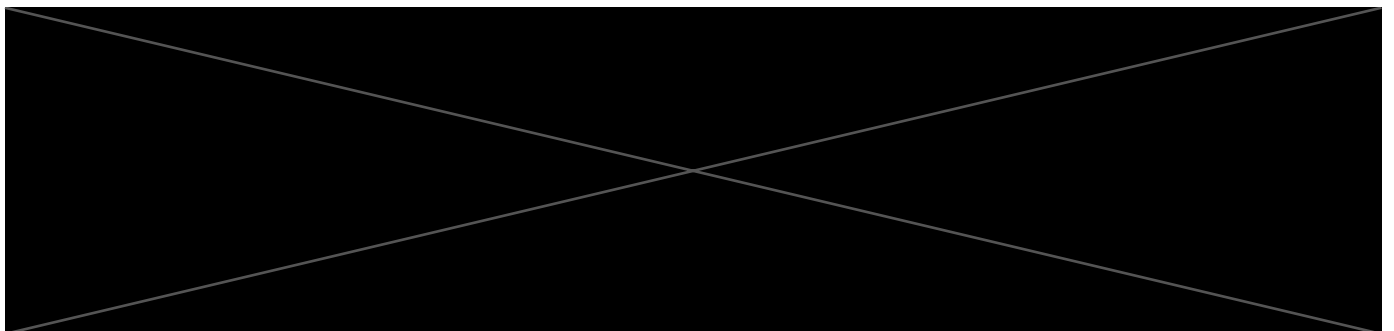
These tokens represent the following percentage of reserves and liabilities:

Percentage of Total Reserves	Percentage of Total Liabilities
>90%	>90%

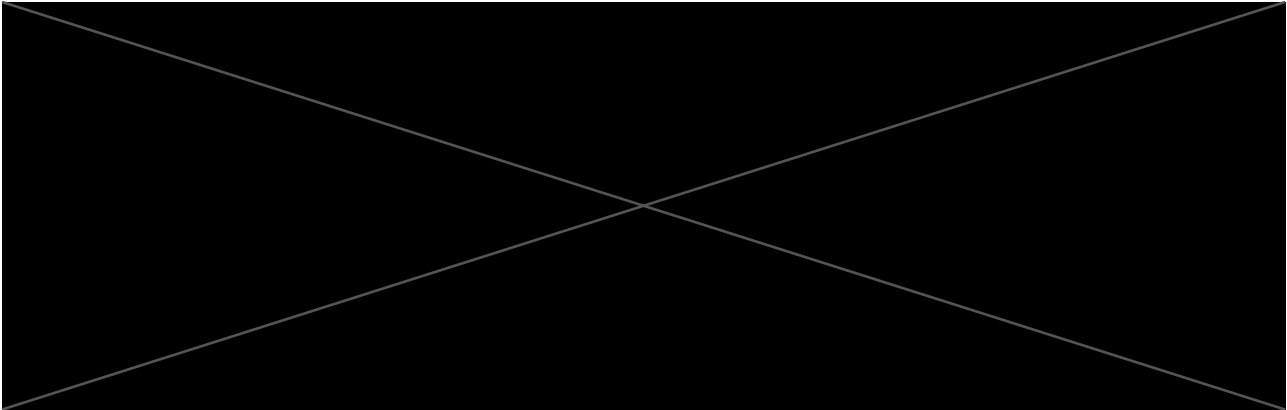
* The surplus balance of these tokens is large enough to cover all the outstanding balances of every other token in the scope of this audit.

Total Collateral Ratio

238%



Team Composition



Conclusion

WhiteBIT 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, WhiteBIT reaffirms its commitment to providing a trustworthy and reliable trading platform. WhiteBIT'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 **Mon, Nov 18, 2024**, demonstrates that WhiteBIT maintains a reserve ratio of **238 %**. This finding signifies that WhiteBIT 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 WhiteBIT, as well as the company's dedication to transparency and accountability.