armanino

PROOF OF RESERVES Agreed-Upon Procedures Report

Prepared for:

Gate.io

Management & Platform Users

October 28, 2022

MOORE

An independent firm associated with Moore Global Network Limited

armanino

A top 20 US-based Public Accounting Firm

Independent Accountant's Report on Agreed-Upon Procedures

To Gate.io Management and Platform Clients of Gate.io:

We have performed the procedures enumerated below as of 00:00AM Coordinated Universal Time ("UTC") on October 19, 2022. Management of Gate Global, Corp ("Gate.io") has agreed to and acknowledged that the procedures performed are appropriate to meet the intended purpose of demonstrating that, at the time the procedures were performed, Gate.io retained custody over a sufficient amount of the in-kind assets to cover the in-scope client liabilities as observed within the database related to Gate.io's exchange platform.

This report may not be suitable for any other purpose. The procedures performed may not address all the items of interest to a user of this report and may not meet the needs of all users of this report and, as such, users are responsible for determining whether the procedures performed are appropriate for their purposes.

The procedures and the associated findings are set forth in the attached sections:

- **Procedures:** Listing of all procedures requested by Gate.io and performed by Armanino.
- **Findings & Results:** The results of the procedures performed by Armanino.

We were engaged by Gate.io to perform this agreed-upon procedures engagement and conducted our engagement in accordance with attestation standards established by the American Institute of Certified Public Accountants. We were not engaged to and did not conduct an examination or review engagement, the objective of which would be the expression of an opinion or conclusion, respectively, related to the platform account liabilities and asset balances represented by Gate.io. Accordingly, we do not express such an opinion or conclusion. Had we performed additional procedures, other matters might have come to our attention that would have been reported.

We are required to be independent of Gate.io and to meet our ethical responsibilities in accordance with the relevant ethical requirements related to our agreed-upon procedures engagement.

This report is intended solely for the information and use of Gate.io Management and Platform Clients of Gate.io and is not intended to be and should not be used by anyone other than these specified parties. The practitioner's report is as of a specified point in time and we have no responsibility to update the report or findings therein for subsequent points in time.

Armanino CPA LLP
San Jose, California
October 28, 2022

Procedures

General

1) Obtain an overview of Gate.io's company background, business model and supported features via inquiry with Gate.io Management and inspection of Gate.io's website, www.gate.io.

2) Obtain a list of Client Liabilities and In-Kind Assets in scope for the Proof of Reserves assessment from Gate.io Management.

Proving Client Account Balance Liabilities on the Gate.io Platform

3) Inspect the scripts used by Gate.io Management to pull client and balance data from the underlying database to ensure the logic and parameters are designed to pull a complete and accurate listing of client liabilities (excluding identified Gate.io internal accounts) with the in-scope assets.

4) Observe Gate.io Management execute the scripts from Procedure 3 to extract data from the production database and observe the total balance of the in-scope client liabilities from the executed scripts.

5) Observe Gate.io Management open the generated Client Liability Report from the production database with the output fields Hashed UID[1] and the in-scope client liabilities. Obtain the Client Liability Report from Gate.io Management and reconcile the total balance of the in-scope client liabilities observed in the report extract to the total balance observed in Procedure 4. Confirm Gate.io internal accounts identified by Management were not included within the Client Liability Report extract.

Utilizing the Merkle Tree Generator & Verifier[2]

6) Utilize the Merkle Tree Generator to aggregate Gate.io client data from the Client Liability Report extracted during the assessment and determine the Merkle Root Hash.

7) Randomly select a sample of 10 Hashed UIDs. For each sample, utilize the Verifier Tool on the TrustExplorer: Gate.io Proof of Reserves Dashboard[3] to cryptographically test whether the Hashed UIDs are included within the Merkle Tree. In addition, cryptographically test one sample 'dummy' account to confirm only valid Hashed UIDs are included within the Merkle Tree.

---

[1] 'Hashed UID,' or 'Hashed User ID,' refers to an individual client's record included within the Proof of Reserves assessment.

[2] FAQ on the Merkle Tree can be found here: https://proof-of-reserves.trustexplorer.io/faq.

[3] TrustExplorer is Armanino's proprietary blockchain-enabled assurance technology suite designed to increase trust for participants in the digital asset industry. Proof of Reserves, one of TrustExplorer's flagship solutions, is a report and client verification portal that enables digital asset platforms to prove the assets held on behalf of the clients. The Gate.io Proof of Reserves webpage can be found here: https://proof-of-reserves.trustexplorer.io/clients/gate.io.

Proving Asset Ownership – BTC & ETH

8) Obtain from Gate.io Management a complete list of all addresses holding bitcoin and ether assets in-scope for the assessment. Provide Gate.io Management a specific amount of cryptocurrency to execute a "send-to-self" transaction for each of the addresses. Receive a corresponding transaction hash from Gate.io Management for a "send-to-self" transaction completed for each address. Inspect the transaction details on the corresponding blockchain and observe the amount, timestamp, and "sending" address match the specific parameters communicated.

Proof of Reserves Assessment

9) Query balances for all asset addresses in scope and demonstrated to be controlled by Gate.io Management as of the date of the assessment.

10) Compare the total liabilities from the Client Liability Report extracted from Gate.io's production database as observed within Procedure 5 to the total assets controlled by the Gate.io custodied addresses (the "In-Kind Assets") as of the specified date and time of the assessment and calculate the collateralization ratio based on the mapping provided by Gate.io Management.

Findings & Results

Armanino completed the agreed-upon procedures as outlined above with the following findings and results:

General

1) Obtain an overview of Gate.io's company background, business model and supported features via inquiry with Gate.io Management and inspection of Gate.io's website, www.gate.io.

Results: Armanino inquired with Gate.io Management to gain an understanding of the Company's background and business model recording the following:

Gate.io is a global cryptocurrency exchange headquartered in the Panama. Through its platform, the Company offers cryptocurrency to fiat trading as well as futures, staking, derivatives, futures, over the counter ("OTC") services and more. The platform is divided into two market exchanges:

- **Gate.io Trade Exchange**: For the purchase, sale, and staking of cryptocurrencies using spot and margin transactions.
- **Gate.io Derivative Exchange**: For trading perpetual futures contracts, termed futures contracts, options, and more.

The scope of the Proof of Reserves assessment includes client liabilities and associated collateral assets on both the Gate.io 'Trade' and 'Derivative' exchanges.

As of the assessment date, Gate.io supports over 1,500 different cryptocurrencies and over 2,700 trading pairs. Gate.io custodies all assets collateralizing the client liabilities for the Gate.io spot exchange. The wider Gate.io ecosystem includes its native GateChain blockchain, HipoDeFi, NFT Magic Box, Wallet.io, and Gate Ventures.

2) Obtain a list of Client Liabilities and In-Kind Assets in scope for the Proof of Reserves assessment from Gate.io Management.

Armanino obtained from Gate.io management the full list of in-scope client liabilities as of 00:00AM UTC on October 19, 2022. Gate.io client liabilities and sub-liability types were described by Gate.io Management as client claims on assets held in the Gate.io accounts. All sub-liabilities balances are summed by asset denomination and presented within the overall liability balance for each In-Scope Client Liability. The client liabilities in scope for the assessment were:

In-Scope Client Liabilities for PoR as of Time of Assessment

Liability	Sub-Liability Type	Description
Bitcoin ("BTC") & Ether ("ETH")	Spot	Accounts that enable users to buy and sell cryptocurrencies for immediate delivery in the market on a specified date
	Margin	Accounts trading on margin denominated in USD or USDT
	Auto Invest	Accounts that automatically purchase cryptocurrency at predetermined intervals
	Cross Margin	Accounts whereby excess margin from a trader's margin account is transferred to another one of their margin accounts to satisfy maintenance margin requirements
	Structured Financial	Accounts that have been generated access to prepackaged investments that include assets linked to interest and derivatives
	Lending (ZM Lend & ZM Lend (Borrow))	Accounts that have lent out or borrowed tokens counterparties in return for receiving or paying interest
	Liquidity Mining (LD Swap)	Accounts participating in "liquidity mining" opportunities facilitated by Gate.io
	BTC-Settled Swap Futures (BTC-only)	Accounts of USD-denominated futures positions that are settled in BTC

Armanino then obtained from Gate.io Management the in-scope in-kind asset balances as of 00:00AM UTC on October 19, 2022. Gate.io in-kind assets were described by Gate.io Management as assets held on behalf of platform customers. The in-kind assets in scope for the assessment were:

In-Kind Assets for PoR as of Time of Assessment

Asset	Description
BTC	Bitcoin controlled by Gate.io
ETH	Ether controlled by Gate.io

Proving Client Account Balance Liabilities on the Gate.io Platform

3) Inspect the scripts used by Gate.io Management to pull client and balance data from the underlying database to ensure the logic and parameters are designed to pull a complete and accurate listing of client liabilities (excluding identified Gate.io internal accounts) with the in-scope assets.

Results: On October 18, 2022, Armanino met with Gate.io's data engineer to gain an understanding of the scripts and tables used to extract client liability balance data for the Client Liability Report extract used within the Proof of Reserves Assessment.

Armanino observed **7** databases for which data was extracted from for the purposes of the Proof of Reserves assessment. Armanino then observed **9** tables for which database information was compiled to derive the client liability balance data.

Armanino then inspected the scripts used to extract data from the observed databases and tables to compile the data into the Client Liability Report extract used for the Proof of Reserves assessment. Armanino observed the following **key functions used in the scripts** to compile the Client Liability Report:

- **Extract Point in Time Balances**: Script to extract balances as of a specified point-in-time (matching the 'as of' date of the Proof of Reserves assessment).
- **Exclude Internal Accounts**: Script to exclude Gate.io internal accounts with non-custodial balances. Armanino observed the script excluded **4** specific accounts identified by Gate.io Management to be Gate.io internal accounts that hold non-custodial (i.e., non-client) balances.
- **Filter for In-Scope Liabilities**: Script to index and filter for *only* in scope liability types.
- **Incorporate Hashed UID**: Script to generate a Hashed User ID from an 'original' User ID for each client account.

4) Observe Gate.io Management execute the scripts from Procedure 3 to extract data from the production database and observe the total balance of the in-scope client liabilities from the executed scripts.

Results: On October 19, 2022, Armanino observed Gate.io's data engineer execute the scripts observed in Procedure 3 to generate the client liability data from the production database and observed the aggregate liability balances within the terminal window.

Using unixtime.org, Armanino converted the Unix Timestamp of 1666137600 observed in the terminal window and observed the "human-readable" date on unixtime.org to be 00:00AM UTC October 19, 2022.

5) Observe Gate.io Management open the generated Client Liability Report from the production database with the output fields Hashed UID[4] and the in-scope client liabilities. Obtain the Client Liability Report from Gate.io Management and reconcile the total balance of the in-scope client liabilities observed in the report extract to the total balance observed in Procedure 4. Confirm Gate.io internal accounts identified by Management were not included within the Client Liability Report extract.

Results: On October 19, 2022, Armanino observed Gate.io's data engineer extract the client liability data from the production database with parameters including the Hashed UID and Gate.io account platform balances for the in-scope liabilities, as observed within Procedure 2. Armanino observed the data engineer perform a checksum on the Customer Liability Extract file and observed the checksum output to be **087d6348228e74e7e317846213462fe9**. Armanino obtained the customer liability extract and executed a checksum and observed a matching output.

Armanino summed the total asset balances from the Client Liability Report extract, and confirmed the totals reconciled to the total asset balances observed in the terminal during the observation with Gate.io Management.

Additionally, to confirm the 4 non-custodial internal accounts were not included within the Client Liability Report extract, Armanino generated "dummy" Hashed UIDs using the User IDs of the internal accounts excluded within the query and the 'hashlib.sha256' library provided by Gate.io Management. Armanino

[4] 'Hashed UID,' or 'Hashed User ID' refers to an individual client's record included within the Proof of Reserves assessment.

then queried the Client Liability Report extract with the list of "dummy" non-custodial internal account Hashed UIDs and confirmed the non-custodial internal accounts were *not* included within the Client Liability Report extract.

Utilizing the Merkle Tree Generator & Verifier[5]

6) Utilize the Merkle Tree Generator to aggregate Gate.io client data from the Client Liability Report extracted during the assessment and determine the Merkle Root Hash.

Results: Armanino then prepared the Client Liability Report extract for Merkle Tree generation.[6] Subsequent to the assessment date, Armanino utilized the Client Liability Report extract provided by Gate.io's data engineer as of 00:00AM UTC October 19, 2022.

A Merkle Tree Verifier enables clients to cryptographically verify client account details were included within the Proof of Reserves Assessment by cryptographically linking each individual client's Merkle Leaf (which is a client's Hashed UID) to the Merkle Root. The Merkle Root is an aggregation of all client liability account balances in scope for the Proof of Reserve Assessment truncated into a single summary hash.

Armanino then utilized the Merkle Tree Generator[7] to generate a Merkle Tree from the Client Liability Report extracted during the assessment and determined the Root Hash to be:

da68c9a0e25a08f39d5d93122da1c03a5d75b254d35bdc1c7469e587b21fb8c4

Armanino confirmed the additional informational outputs generated from the Merkle Tree Generator, such as total record count and asset balances, reconciled to the total record count and asset balances from the Client Liability Report.

7) Randomly select a sample of 10 Hashed UIDs. For each sample, utilize the Verifier Tool on the TrustExplorer: Gate.io Proof of Reserves Dashboard[8] to cryptographically test whether the Hashed UIDs are included within the Merkle Tree. In addition, cryptographically test one sample 'dummy' account to confirm only valid Hashed UIDs are included within the Merkle Tree.

---

[5] FAQ on the Merkle Tree can be found here: https://proof-of-reserves.trustexplorer.io/faq.

[6] To create a "symmetrical" Merkle Tree, additional supplemental records were added as "padding" to the raw export. All supplemental records had no balances and do not contribute to the total client liability balances in any way. A "symmetrical" Merkle Tree is a Merkle Tree that has a number of records that adheres to the formula, 2^(x).

[7] The source code for the Merkle Tree Generator and Verifier has been open-sourced and is available for inspection here: https://github.com/armaninollp/proof-of-reserves-merkle-tree-tool.

[8] TrustExplorer is Armanino's proprietary blockchain-enabled assurance technology suite designed to increase trust for participants in the digital asset industry. Proof of Reserves, one of TrustExplorer's flagship solutions, is a report and client verification portal that enables digital asset platforms to prove the assets held on behalf of the clients. The Kraken Proof of Reserves webpage can be found here: https://proof-of-reserves.trustexplorer.io/clients/kraken.

Results: Subsequent to the assessment date, Armanino randomly selected a sample of 10 Hashed UIDs and utilized the Verifier Tool to cryptographically test whether the Hashed UID and the balances were included within the Merkle Generator Output. For each sample, Armanino input the Hashed UID and the in-scope liability amounts into the Merkle Verifier. Armanino confirmed that all 10 samples were found within the Merkle Tree. Additionally, Armanino input fictitious account details into the Verifier Tool and confirmed the dummy account was not found within the Merkle Tree.

Proving Asset Ownership – BTC & ETH

8) Obtain from Gate.io Management a complete list of all addresses holding bitcoin and ether assets in-scope for the assessment. Provide Gate.io Management a specific amount of cryptocurrency to execute a "send-to-self" transaction for each of the addresses. Receive a corresponding transaction hash from Gate.io Management for a "send-to-self" transaction completed for each address. Inspect the transaction details on the corresponding blockchain and observe the amount, timestamp, and "sending" address match the specific parameters communicated.

Results: On October 20, 2022, Armanino obtained a list of Gate.io addresses holding bitcoin and ether assets in-scope for the assessment.

For each in-scope address received, Armanino provided Gate.io Management a specific amount of cryptocurrency to execute a "send-to-self" transaction. After receiving the transaction hash, Armanino inspected transaction details on the corresponding blockchain, noting the amount, timestamp, and "sending" address matched the specific parameters communicated.

Proof of Reserves Assessment

9) Query balances for all asset addresses in scope and demonstrated to be controlled by Gate.io Management as of the date of the assessment.

Results: Armanino retrieved, from the respective blockchains, the balances of all addresses in-scope for the assessment and tested in Procedure 8. Armanino obtained the in-scope asset balances as of 00:00AM UTC on October 19, 2022.

10) Compare the total liabilities from the Client Liability Report extracted from Gate.io's production database as observed within Procedure 5 to the total assets controlled by the Gate.io custodied addresses (the "In-Kind Assets") as of the specified date and time of the assessment and calculate the collateralization ratio based on the mapping provided by Gate.io Management.

Armanino confirmed all in-scope records of Gate.io trade and derivative exchange client liabilities were included in the client database as aggregated in the Merkle Tree with the Merkle Root Hash:

da68c9a0e25a08f39d5d93122da1c03a5d75b254d35bdc1c7469e587b21fb8c4

Armanino confirmed Gate.io retained control over in-kind assets in excess of client liabilities as observed within the database related to Gate.io's trade and derivative exchanges as of 00:00AM UTC October 19, 2022, with the results below:

Results as of:
BTC Block Height: **759290** | ETH Block Height: **15778435**

	Chains of Underlying Assets	Collateralization Ratio
BTC	**Bitcoin**	**107.79%**
ETH	**Ethereum**	**104.45%**