PROOF OF RESERVES ASSESSMENT REPORT

Prepared for:

gate.io

May 11, 2020

MOORE

An independent firm associated with Moore Global Network Limited

armanino

A top 25 US-based Public Accounting Firm

PROOF OF RESERVES ASSESSMENT REPORT

May 11th, 2020

TABLE OF CONTENTS

Executive Summary

Armanino LLP was engaged by Gate.io ("Company") to perform a "Proof of Reserves Assessment" ("Proof of Reserves" or "PoR") as of UTC 0:00 on May 4th, 2020. After performing and documenting the Proof of Reserves Assessment procedures, Armanino concluded Gate.io controlled bitcoin ("BTC") in an amount greater than outstanding customer liabilities (included within the Merkle Tree with the Root Hash: 40be27cdbce9c44828ce11105bca7dc8f79d5f08e07cbe7f8ca8e61a62ebb91e). Armanino observed a collateralization ratio of 104% (assets ÷ liabilities). Gate.io bitcoin addresses, exact asset and liabilities amounts are not disclosed in this report to maintain Gate.io privacy. The methods and procedures used to reach our conclusions, as well as the details of those conclusions, is provided in this report for Gate.io management and Gate.io users.

Background

Gate.io

Gate.io is one of the oldest cryptocurrency exchanges, first incorporating in China in 2013, and since expanding across the globe. The Company maintains representatives in China, Singapore, Cayman, and the USA (Virginia). Along with a digital asset trading platform and exchange, Gate.io has also launched its own blockchain (GateChain) with its own token (GateChain Token), and its own wallet software. Gate.io supports over 180 cryptocurrencies, greater than 400 trading pairs and spot, margin, asset management and futures markets for select liquid cryptocurrencies.

Armanino LLP

Armanino LLP is a top 25 US Accounting and Consulting firm, and the largest headquartered in California. Armanino's specialized Blockchain team is comprised of CPA's, attorneys, and consulting professionals, who having been servicing the digital asset industry since 2014.

The Engagement

Armanino LLP was engaged by Gate.io to perform a Proof of Reserves Assessment as of UTC 0:00 on May 4th, 2020. The engagement was performed in accordance with ethics as integrity standards "Statement on Standards for Consulting Services" promulgated by the American Institute of Certified Public Accountants (AICPA). We were not engaged to, and we did not perform, a financial statement audit. We believe the nature and extent of our overall assessment approach, the specific procedures performed, and the evidence collected form an adequate basis for the conclusions we make herein. This report is intended to provide reasonable assurance that Gate.io's BTC reserves are in excess of BTC liabilities as of UTC 0:00 on May 4th, 2020.

Procedures

Armanino performed the following procedures during the course of the assessment:

General

1) Gained an understanding of Gate.io's company background, business model, management, and related relevant details via inquiry with Management, observation and inspection of key documents and media outlets.

2) Gained an understanding of Gate.io's trading platform and underlying system architecture via inquiry with Management, observation with the Gate.io Engineering team, and inspection of Company documentation.

Preparation to Prove Liabilities

3) Assessed the database tables, script used to query the customer database, as well as the logic and parameters used to generate the *Hashed User ID & Balance Report* from Gate.io's production database.

4) Inspected the script used to generate the *Hashed User ID & Balance Report* to determine that the script included logic and operators that would cause it to act as intended (pull a complete and accurate listing of user balances).

5) Inspected the *Hashed User ID & Balance Report* to determine that a test account was included in the listing and that the balance associated with that test account was accurate.

6) Inspected the Gate.io's *Merkle Tree Generator and Verifier* codebase[1] (as of GitHub commit 1a5adef948132544d4850e8d078f40518bbbb4f9) to ensure the code is reasonably reliable for the intended purpose of generating a Merkle Tree from the *Hashed User ID & Balance Report*.

7) Tested the *Merkle Tree Generator and Verifier* codebase (as of commit 1a5adef948132544d4850e8d078f40518bbbb4f9) using test accounts and balances (test users in the Production environment) to ensure the Verifier tool logic functioned as expected.

8) Utilized the Merkle Tree Generator on **TrustExplorer™** to generate a Merkle Tree from the Hashed User ID & Balance Report as of UTC 0:00 on May 4th, 2020 and determined the Root Hash to be 40be27cdbce9c44828ce11105bca7dc8f79d5f08e07cbe7f8ca8e61a62ebb91e.

9) Utilized the Verifier tool on **TrustExplorer™** to test whether the hashed user ID of a known account, combined with the known BTC balance of that user ID, was included in the Merkle Tree

[1] On February 21, 2020, Gate.io published a public, open source code repository for all Gate.io users to view, which included code for the Merkle Tree Generator and the Verifier Tool here: https://github.com/gateio/proof-of-reserves

and determined that our test account was included in the Merkle Tree at Level 23, Position 225082 (calculated Merkle Leaf: 1cd5e76f4741cfa9). [2]

Preparation to Prove Assets

10) Inquired with management to obtain an understanding of the process of receiving customer bitcoins, safely storing customer bitcoins, and sending customer bitcoins outside the exchange when withdrawn by customers ("Custodial Process").

11) Inquired with management to obtain an understanding of the key technical components used in the Custodial Process ("Wallet Infrastructure").

12) Obtained a complete list of Gate.io bitcoin (BTC) addresses deemed in-scope for the purposes of the Proof of Reserves Assessment.

13) For each of the hot and cold wallet addresses obtained, Armanino created a custom message, including (1) a "nonce" or secret, and (2) the hash of the most recent bitcoin block. Thereafter, Armanino then obtained a digital signature of that custom message from Gate.io, and decrypted the message using the relevant public key/s (wallet addresses) to determine that Gate.io signed the message using the private keys for the wallets.

The Proof of Reserves Assessment

14) Observed Gate.io generate the *Hashed User ID & Balance Report* with the appropriate timestamp as of UTC 0:00 on May 4th, 2020 using the same script we assessed in the procedures outlined above, generated the Merkle Tree, and summed the total customer liabilities observed.

15) For each in-scope wallet address, Armanino retrieved the BTC balances as of UTC 0:00 on May 4th, 2020, from the Bitcoin Blockchain, at block height [628806].

16) Armanino reconciled the total liabilities observed via Gate.io's Production customer database to total BTC assets held in the wallets tested above as of UTC 0:00 on May 4th, 2020, and at block height [628806].

[2] Note that Gate.io users with active accounts at the time of the Proof of Reserves Assessment can complete this same test using their own hashed user ID and balance. This allows all users to participate in ensuring the liabilities data provided by Gate.io is complete and accurate.

Conclusions

At the time of the assessment, Armanino LLP confirmed Gate.io customer liabilities on platform across all spot, margin, asset management and futures markets. Armanino also confirmed Gate.io controlled bitcoin in excess of 100% of liabilities (as of block 628806) and was able to exercise the use of the private keys to demonstrate ownership and control at the time of the assessment.

Therefore, as of UTC 0:00 on May 4th, 2020, and as Bitcoin block height 628806, we conclude that Gate.io has bitcoin reserves in excess of customer liabilities. Armanino observed a collateralization ratio of 104% (assets ÷ liabilities).

Appendix I

Further Understanding of Risks and Opportunities

The following table is intended to provide a further understanding of the risks to the conclusions drawn in this report. We believe presenting the risks and opportunities in this way will enable Gate.io customers to obtain a wholistic view of the Proof of Reserves methodology.

Observation		Area of Improvement
Risk Name	**Risk Description**	**Potential Mitigating Action**
PoR Excludes Deposit Addresses	Armanino noted the asset portion of the Proof of Reserves (PoR) did not include *all* addresses owned and controlled by Gate.io, those with material balances that could be used to prove adequate reserves. The PoR excludes user deposit addresses and any other wallets that were not scoped-in during the PoR. Therefore, it is likely that Gate.io holds more bitcoin than noted during the Assessment.	Gate.io may use addresses within a single (or multiple) HD derivation path to derive deposit addresses and provide the Xpub to the assessor.
Unable to Confirm Exclusive Ownership of Keys	It is almost impossible for the assessor to verify that the private keys are *only* owned and controlled by Gate.io. While Armanino gained a general understanding of the wallet structures and control environment, Armanino was not present during key creation and it is possible that keys could have been compromised by another party or borrowed from another party for the purposes of passing the assessment.	Overall this is an inherent risk that is very difficult to address during a PoR assessment. However, a PoR assessee could generate a key/address securely offline in a secure environment under the supervision of an assessor, move funds to the newly created address, and prove control of that address.
Reliance on a 3rd Party Assessor	To place reliance on the assessment, users will have to *trust* that the assessor is performing the assessment in good faith. Users rely on the assessor for providing BTC balances of Gate.io addresses, confirming Gate.io owns those addresses, reviewing the relevant code, and verifying the customer database extract is provided completely and accurately by Gate.io.	To mitigate the risk of an unreliable assessment, the exchange and the user group should ensure the assessor's incentives are aligned and the assessor is a publicly known organization that is responsible for the assessment. Therefore, if the assessor has a reputation "at stake", they are more likely to perform the assessment in good-faith.
Addresses Confirmed as part of the PoR are Kept Private	In order to maintain the privacy and security of Gate.io addresses, Armanino and Gate.io did not release the addresses in-scope for the assessment. Thus, users are unable to verify the BTC balances of the addresses themselves via the blockchain and must rely on the auditor to provide those balances in good faith.	In the future, Zero Knowledge proof schemes may be developed to prove ownership of a specific balance and the BTC balance as of a point in time without disclosing the address itself. However, these potential methodologies are not yet widespread and lack an understandable user experience.

Point in Time Assessment	The assessment is as of a single point in time, and does not assess the BTC balances, other digital asset or fiat balances, nor the overall solvency of Gate.io before or after the assessment date.	The Assessor/Assessee may consider providing PoR assessments on a more frequent basis or develop a "real-time" proof of reserves scheme.
Potential Unaccounted for Liabilities	The scope of the Proof of Reserves Assessment did not include the assessment of liens, encumbrances, or other Company liabilities that may affect the solvency of the Company. Armanino's scope was limited to on-platform liabilities and BTC held within in-scope addresses.	As Proof of Reserves Assessments evolve and become more commonplace, PoR could include an examination of the labilities on the balance sheet, overall Company solvency, and the search for unrecorded liabilities.
Reliance on User Verification	While Armanino performed procedures to gain reasonable comfort over the authenticity of the data provided within the dataset, there is always an inherent possibility of purposeful or accidental inclusions or exclusions that could affect the dataset. In order to confirm all account includes within the dataset are authentic, users must verify their own account balances to ensure they are included within the assessed Merkle Tree.	A new and expanded Proof of Reserves scheme would have to be developed in order to mitigate this inherent risk that does not rely on users performing self-verification.