PROOF OF RESERVES AGREED-UPON PROCEDURES REPORT

Prepared for:

kraken

Management & Platform Clients

January 27, 2022

MOORE

An independent firm associated with Moore Global Network Limited

armanino

A top 25 US-based Public Accounting Firm

PROOF OF RESERVES AGREED-UPON PROCEDURES REPORT

January 27, 2022

TABLE OF CONTENTS

Contents

Executive Summary

Armanino CPA LLP ("Armanino") was engaged by Payward, Inc. ("Kraken" or "Company") to perform a Proof of Reserves ("PoR") agreed-upon procedures ("AUP") as of 11:59PM UTC on December 31, 2021 to demonstrate that, at the time the procedures were performed, Kraken retained custody over a sufficient amount of bitcoin ("BTC"), ether ("ETH"), and staked ether ("staked ETH" or "ETH2") assets (the "In-Kind Assets") to cover client BTC, BTC.M[1] , ETH, and ETH2.S[2] liabilities (the "Client Liabilities") as observed within the database related to Kraken's spot exchange.

Upon performing the agreed-upon procedures, Armanino observed the following findings and results:

Results as of **BTC Block Height:** 716598 | **ETH Block Height:** 13916165 | **ETH2 Epoch:** 88987

Kraken Spot Exchange	Client Liabilities	In-Kind Assets	Collateralization Ratio
BTC	167,891.70 BTC	189,141.56 BTC	**108.25%**
BTC.M	6,838.94 BTC.M		
ETH	2,128,857.51 ETH	2,243,889.19 ETH	**105.40%**
ETH2.S	947,548.48 ETH2.S	947,584.00 Staked ETH	**100.00%**

Armanino also noted all in-scope Kraken spot exchange Client Liabilities were included in the client database extract and aggregated within a Merkle Tree[3] with the Merkle Root Hash:

12f021d4e2b20da9d4e1206b825794e9c410ff71cddb786c7191f08eeead017c

The methods and procedures performed to substantiate these findings are presented within this report and are intended for the use of Kraken Management and the Platform Clients of Kraken.

[1] The BTC.M ticker on the Kraken spot exchange platform represents bitcoin held in custody on behalf of clients by Kraken in separate interest-accruing margin pools and opportunities.

[2] The ETH2.S ticker on the Kraken spot exchange platform represents ether that has been staked on behalf of clients to support the Ethereum 2.0 network upgrade. ETH2.S cannot be un-staked, deposited, or withdrawn until the Ethereum 2.0 network upgrade is complete. ETH2.S represents "principal" ether staked and does not represent rewards earned from staking. A separate ticker, ETH2, represents ether that is earned as staking rewards. See Kraken.com for further details.

[3] 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.

Independent Accountant's Report on Agreed-Upon Procedures

To Kraken Management and Platform Clients of Kraken:

We have performed the procedures enumerated below as of 11:59PM Coordinated Universal Time ("UTC") on December 31, 2021. Management of Payward, Inc. ("Kraken") 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, Kraken retained custody over a sufficient amount of bitcoin ("BTC"), ether ("ETH"), and staked ether ("staked ETH" or "ETH2") assets to cover client BTC, BTC.M, ETH, and ETH2.S liabilities as observed within the database related to Kraken's spot exchange.

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 Kraken and performed by Armanino.
- **Findings & Results:** The results of the procedures performed and a summary of findings.
- **Appendix:** Listing of further understanding of risks and opportunities.

We were engaged by Kraken 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 Kraken. 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 Kraken 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 Kraken Management and Platform Clients of Kraken 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 Armanino CPA LLP ("Armanino") has no responsibility to update the report or findings therein for subsequent points in time.

Armanino

Armanino CPA LLP
San Jose, California

January 27, 2022

Your receipt of this report is subject to the terms of use found here: https://real-time-attest.trustexplorer.io/terms-of-use

Procedures

Armanino performed the following agreed-upon procedures:

General

1) Gain an understanding of Kraken's company background, business model and related relevant details via inquiry with Kraken Management, observation, and inspection of key documents.

Proving Client Account Balance Liabilities on the Kraken Trading Platform

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

3) Observe Kraken Management access the production replica database used to generate the Client Liability Report extract. Observe Kraken Management execute the scripts from Procedure 2 to extract data from the production replica database and note the total balance of BTC, BTC.M, ETH, and ETH2.S and the total number of records from the executed scripts.

4) Observe the extraction of the Client Liability Report with the appropriate parameters (PoR Record ID[4], BTC, BTC.M, ETH, and ETH2.S) from the production replica database and reconcile the total balance of BTC, BTC.M, ETH, and ETH2.S and the total number of records observed in the report extract to the total balance and the total number of records observed in Procedure 3. Confirm Kraken internal accounts were not included within the Client Liability Report extract.

Testing the Merkle Tree Generator & Verifier[5]

5) Utilize the Merkle Tree Generator[6] to aggregate Kraken client data from the Client Liability Report extracted during the assessment and determine the Merkle Root Hash.

6) Randomly select a sample of 10 PoR Record IDs. For each sample, utilize the Verifier Tool on the TrustExplorer: Kraken Proof of Reserves Dashboard[7] to test whether the PoR Record IDs are included within the Merkle Tree. In addition, test one sample 'dummy' account to confirm only valid PoR Record IDs are included within the Merkle Tree.

---

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

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

[6] 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.

[7] 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.

Proving Asset Ownership – BTC & ETH

7) Obtain from Kraken Management a complete list of BTC and ETH addresses holding assets in-scope for the assessment and perform the following procedures:

    a. **Single Signature Addresses:** For each of the in-scope "single-signature" addresses received, obtain a corresponding digital signature generated by Kraken Management with an Armanino-provided custom message. Verify each digital signature is signed by the private key associated with a public address on the listing provided by Kraken Management.

    b. **Multi-Signature Addresses:** For each of the in-scope "multi-signature" addresses received, obtain the underlying addresses utilized to create the multi-signature address and obtain the corresponding digital signatures generated by Kraken Management with an Armanino-provided custom message for each address. Verify each digital signature is signed by the private key associated with a public address utilized to create the multi-signature addresses on the listing provided by Kraken Management. Recreate each multi-signature address on the listing utilizing the underlying public addresses provided by Kraken Management.

Proving Asset Ownership – Staked ETH[8]

8) Obtain from Kraken Management a complete list of ETH2 Validator Public Keys in-scope for the assessment. For each of the Public Keys received, query the Ethereum 2.0 Beacon Chain, and observe the related Withdrawal Credential address(es).

9) Obtain from Kraken Management the Withdrawal Public Key. Confirm the Withdrawal Credential observed in Procedure 8 is derived from the Withdrawal Public Key provided by Kraken Management. For the in-scope Withdrawal Public Key(s), obtain from Kraken Management the corresponding digital signature generated from an Armanino-provided custom message. Verify whether the digital signature provided by Kraken Management was signed using the Armanino-provided custom message and the private key to the Withdrawal Public Key.

Proof of Reserves Assessment

10) Query all BTC, ETH, and staked ETH (the "In-Kind Assets") addresses/keys in scope for the assessment and proven to be custodied by Kraken. Observe and aggregate the BTC, BTC.M, ETH, and ETH2.S balances (the "Client Liabilities") at the specified assessment time.

11) Compare the total liabilities from the Client Liability Report extracted from Kraken's production database to the total assets held in the Kraken custodied addresses tested as of the specified date and time of the assessment time and calculate the collateralization ratio.

[8] See Finding & Results section for background information regarding ETH2 Validator and Withdrawal key pairs.

Findings & Results

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

General

1) Gain an understanding of Kraken's company background, business model and related relevant details via inquiry with Kraken Management, observation, and inspection of key documents.

Results: Armanino inquired with Kraken Management to gain an understanding of the Company's background and business model noting the following:

Kraken is a United States-based cryptocurrency exchange headquartered in San Francisco, California. Through its platform, the Company offers cryptocurrency to fiat trading as well as futures, staking, and over the counter ("OTC") services. The platform is divided into two market exchanges:

- **Kraken Spot Exchange**: For the purchase, sale, and staking of cryptocurrencies using spot and margin transactions.
- **Kraken Futures Exchange**: For trading cryptocurrency futures contracts. As of the report date, futures for bitcoin, ether, litecoin, bitcoin cash, and XRP were available to trade on the futures market.

The scope of the Proof of Reserves assessment includes *only* client liabilities and associated collateral assets on the Kraken *spot* exchange.

As of the report date, Kraken supports over 70 different cryptocurrencies and is available for residents of over 175 countries and in 13 languages. Kraken custodies all assets collateralizing the client liabilities for the Kraken spot exchange and has also received the special purpose depository institution ("SPDI") designation from Wyoming, making Kraken one of the first cryptocurrency exchanges to hold a bank charter.

Proving Client Account Balance Liabilities on the Kraken Trading Platform

Background: Armanino performed procedures to confirm the total client liabilities as of 11:59PM UTC on December 31, 2021. Kraken client liabilities were described by Kraken Management as client claims on assets held in the Kraken spot exchange trading accounts. The client liabilities in scope for the assessment were:

(1) **BTC** – bitcoin held in custody on behalf of clients by Kraken
(2) **BTC.M** – bitcoin held in custody on behalf of clients by Kraken in separate interest-accruing margin pools and opportunities
(3) **ETH** – ether held in custody on behalf of clients by Kraken
(4) **ETH2.S** – ether deposited into the ETH2 deposit contract on behalf of clients by Kraken

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

Results: On January 4, 2022, Armanino met with Kraken'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 the following tables used to derive the client liability balance data:

- **[Table #1]**: Table of the most recent client balances, both for client accounts and Kraken Internal Accounts
- **[Table(s) #2]**: Table(s) of all the historical transactions
- **[Table #3]**: Table of metadata (such as ticker symbol and appropriate decimal places) related to the currencies supported on the exchange platform
- **[Table #4]**: Table of information related to client accounts and identification

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

- **Asset Balance Rollback**: Script to roll back the transactions from the most recent balance data to the specified point in time and arrive at the historical balance (matching the 'as of' date of the Proof of Reserves assessment) using [Table #1] and [Table(s) #2]
- **Exclude Internal Accounts**: Script to exclude Kraken internal accounts with non-custodial balances[9]
- **Filter for Assets**: Script to filter for *only* in scope liability types [BTC, BTC.M, ETH, ETH2.S] using [Table #3]
- **Incorporate PoR Record ID**: Script to include the PoR Record ID related to each client account from [Table #4]
- **Remove Negative Balances**: Script to convert the negative balances to zero[10]

3) Observe Kraken Management access the production replica database used to generate the Client Liability Report extract. Observe Kraken Management execute the scripts from Procedure 2 to extract data from the production replica database and note the total balance of BTC, BTC.M, ETH, and ETH2.S and the total number of records from the executed scripts.

Results: On January 4, 2022, Armanino observed the data engineer access the production replica database and the underlying tables used to generate the Client Liability Report extract.

---

[9] Armanino noted the script excluded specific accounts identified to be Kraken internal accounts that hold non-custodial (i.e., non-client) balances. To gain assurance that the identified accounts were appropriately excluded, Armanino inspected Kraken's record of internal accounts stored separately from the underlying database and noted the accounts excluded in the script reconciled to the accounts with non-custodial balances within Company records.

[10] Armanino noted the negative balances on some client accounts represented balances that are owed to Kraken by the client and are not expected to be collected by Kraken. The client accounts with negative asset balances are not entitled to assets held by Kraken and therefore, do not represent Kraken liabilities. Therefore, Armanino noted that these negative balances should be excluded from the Customer Liability Extract for the purposes of the Proof of Reserves Assessment.

Armanino observed the data engineer execute the scripts observed in Procedure 2 to generate the client liability data within the production replica database and noted the relevant columns [PoR Record ID | BTC | BTC.M | ETH | ETH2.S] and total record count. Armanino then observed the data engineer sum the client liability data within the production replica database and noted the following details:

- **'As of' Time**: 2021-12-31 23:59:59
- **Total Asset Balances**:
    - **BTC**: 167,891.700347194
    - **BTC.M**: 6,838.940879390
    - **ETH**: 2,128,857.50762246
    - **ETH2.S**: 947,548.483001433

4) Observe the extraction of the Client Liability Report with the appropriate parameters (PoR Record ID, BTC, BTC.M, ETH, and ETH2.S) from the production replica database and reconcile the total balance of BTC, BTC.M, ETH, and ETH2.S and the total number of records observed in the report extract to the total balance and the total number of records observed in Procedure 3. Confirm Kraken internal accounts were not included within the Client Liability Report extract.

Results: On January 4, 2022, Armanino observed Kraken's data engineer extract the client liability data from the production replica database. Armanino noted the data was extracted from the production replica database as a csv file and saved to the data engineer's desktop. Subsequently, Armanino observed Kraken's data engineer upload the data extract to a secure file-sharing portal.

Armanino summed the total record count and total asset balances from the Client Liability Report extract, and noted the totals reconciled to the total record count observed in the production replica database.

Additionally, to confirm Kraken non-custodial internal accounts were not included within the Client Liability Report extract, Armanino queried the Client Liability Report extract with the list of Kraken non-custodial internal account PoR Record IDs and confirmed the Kraken non-custodial internal accounts were *not* included within the Client Liability Report extract. Armanino then prepared the Client Liability Report extract for Merkle Tree generation.[11]

[11] In order to protect Kraken Company and client confidentiality, additional supplemental records were added as "padding" to the raw export in order to protect the total record count from being deduced from the Merkle Tree structure. All supplemental records had no balances and do not contribute to the total client liability balances in any way.

Testing the Merkle Tree Generator & Verifier[12]

Background: Armanino utilized a Merkle Tree Generator[13] to aggregate client data extracted from the Kraken database into a single summary hash, the Merkle Root. A Merkle Tree Verifier enables clients to verify client account details were included within the Proof of Reserves Assessment by ensuring each individual client's Merkle Leaf (which is a client's hashed PoR Record ID) can be traced to the Merkle Root.

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

Results: Subsequent to the assessment date, Armanino utilized the Client Liability Report extract provided by Kraken's data engineer as of January 4, 2022. Armanino noted the total record count and asset balances of **[167,891.700347229 BTC | 6,838.94087939 BTC.M | 2,128,857.50762217 ETH | 947,548.483001416 ETH2.S]** observed in Procedures 3 and 4. Armanino then utilized the Merkle Tree Generator to generate a Merkle Tree from the Client Liability Report extracted during the assessment and determined the Root Hash to be:

12f021d4e2b20da9d4e1206b825794e9c410ff71cddb786c7191f08eeead017c

Armanino noted 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 noted from the Client Liability Report.

6) Randomly select a sample of 10 PoR Record IDs. For each sample, utilize the Verifier Tool on the TrustExplorer: Kraken Proof of Reserves Dashboard to test whether the PoR Record IDs are included within the Merkle Tree. In addition, test one sample 'dummy' account to confirm only valid PoR Record IDs are included within the Merkle Tree.

Results: Subsequent to the assessment date, Armanino randomly selected a sample of 10 PoR Record IDs and utilized the Verifier Tool to test whether the PoR Record ID and the balances were included within the Merkle Generator Output. For each sample, Armanino input the PoR Record ID and the [BTC| BTC.M | ETH | ETH2.S] amounts into the Merkle Verifier. Armanino confirmed that all 10 samples were appropriately found within the Merkle Tree.

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

[13] 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.

PoR Record ID	Client Liability Balances				Merkle Leaf Hash Output
	BTC	BTC.M	ETH	ETH2.S	
[Obfuscated PoR Record ID] Sample #1	0.0001840007	0.0	0.377575499	0.0	[Obfuscated Merkle Leaf] Sample #1
[Obfuscated PoR Record ID] Sample #2	0.0145447897	0.0	0.00000548	0.00032	[Obfuscated Merkle Leaf] Sample #2
[Obfuscated PoR Record ID] Sample #3	0.0234804	0.0	0.0	0.0	[Obfuscated Merkle Leaf] Sample #3
[Obfuscated PoR Record ID] Sample #4	0.000002418	0.0	0.00000513	0.0	[Obfuscated Merkle Leaf] Sample #4
[Obfuscated PoR Record ID] Sample #5	0.000004063	0.0	0.06983376	0.0	[Obfuscated Merkle Leaf] Sample #5
[Obfuscated PoR Record ID] Sample #6	0.01387056	0.0	0.0	0.0	[Obfuscated Merkle Leaf] Sample #6
[Obfuscated PoR Record ID] Sample #7	0.04600261	0.0	0.32183	0.0	[Obfuscated Merkle Leaf] Sample #7
[Obfuscated PoR Record ID] Sample #8	0.00408595	0.0	0.0	0.0	[Obfuscated Merkle Leaf] Sample #8
[Obfuscated PoR Record ID] Sample #9	0.23222367	0.0	0.0	0.0	[Obfuscated Merkle Leaf] Sample #9
[Obfuscated PoR Record ID] Sample #10	0.0	0.0	0.175	0.0	[Obfuscated Merkle Leaf] Sample #10

Additionally, Armanino input fictitious account details into the Verifier Tool and noted the dummy account was appropriately not found within the Merkle Tree.

Sample Dummy Account

PoR Record ID	Client Liability Balances				Merkle Leaf Hash Output
	BTC	BTC.M	ETH	ETH2.S	
00000a8cae1693fbdcc54e1b17dc886d9c4a2bc7c5229cb2b6affe62b334f451	N/A	N/A	N/A	N/A	N/A

Proving Asset Ownership – BTC & ETH

Background: To verify that, at the time of assessment, Kraken retained ownership of the bitcoin and ethereum addresses with balances collateralizing the BTC, BTC.M, and ETH client liabilities, Armanino used digital signatures to ensure Kraken was able to sign a custom message provided by Armanino using the associated private keys. Armanino verified whether the digital signature for each address was signed using the Armanino-provided custom message and the private key to the address.

7) Obtain from Kraken Management a complete list of BTC and ETH addresses holding assets in-scope for the assessment and perform the following procedures:

a. **Single Signature Addresses: For each of the in-scope "single-signature" addresses received, obtain a corresponding digital signature generated by Kraken Management with an Armanino-provided custom message. Verify each digital signature is signed by the private key associated with a public address on the listing provided by Kraken Management.**

b. **Multi-Signature Addresses: For each of the in-scope "multi-signature" addresses received, obtain the underlying addresses utilized to create the multi-signature address and obtain the corresponding digital signatures generated by Kraken Management with an Armanino-provided custom message for each address. Verify each digital signature is signed by the private key associated with a public address utilized to create the multi-signature addresses on the listing provided by Kraken Management. Recreate each multi-signature address on the listing utilizing the underlying public addresses provided by Kraken Management.**

Results: On January 21, 2022, Armanino obtained a list of Kraken bitcoin and ethereum addresses holding assets in-scope for the assessment.

Armanino noted the following bitcoin address types and details:

- Native SegWit ("P2WSH") single signature addresses
- Pay to Witness Script Hash Wrapped in P2SH ("P2SH-P2WSH") multi-signature addresses
- Native SegWit ("P2WSH") multi-signature addresses

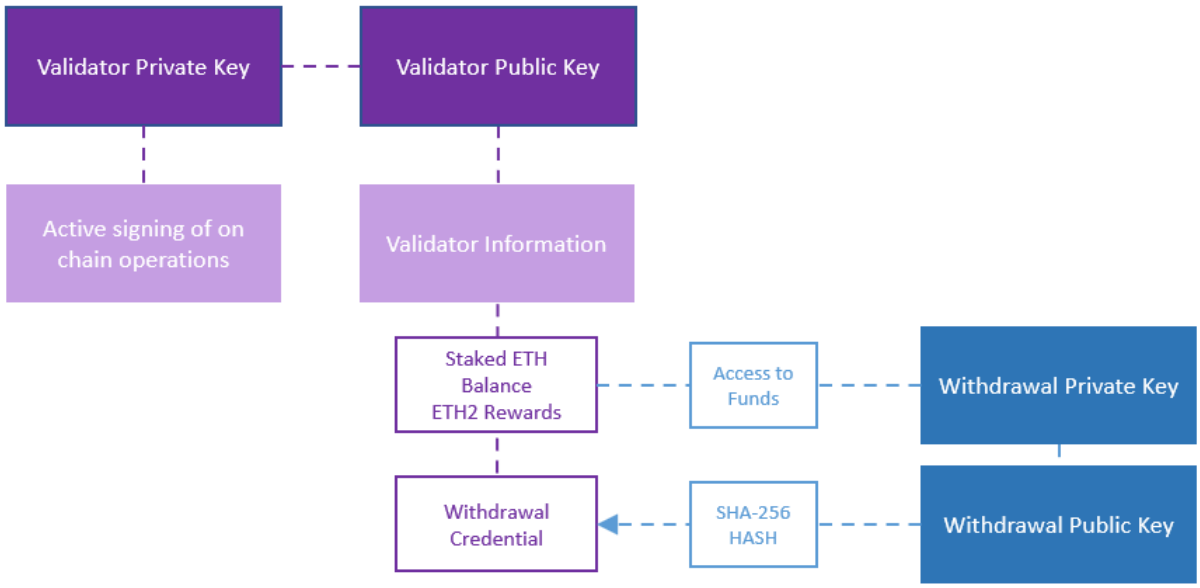
Armanino also noted ethereum single signature addresses.

Single Signature Addresses: For each of the in-scope "single-signature" BTC and ETH addresses received, Armanino obtained a corresponding digital signature generated by Kraken Management with an Armanino-provided custom message. Subsequently, Armanino verified each digital signature was signed successfully by the private key associated with a public address on the listing provided by Kraken Management.

Multi-Signature Addresses: For each of the in-scope "multi-signature" BTC addresses received, Armanino obtained the underlying addresses utilized to create the multi-signature address and obtained the corresponding digital signatures generated by Kraken Management with an Armanino-provided custom message for each address. Subsequently, Armanino verified each digital signature was signed by the private key associated with the public address utilized to create the multi-signature addresses. Armanino also successfully recreated each multi-signature address on the listing utilizing the underlying public addresses provided by Kraken Management.

Proving Asset Ownership – Staked ETH

Background: Kraken provides ETH2 staking services for clients on the Kraken spot exchange. The ETH2.S platform liabilities represent bonded client claims on the ether assets held in the ETH2 deposit contract. The staked ETH assets are locked until the Ethereum 2.0 Beacon Chain upgrade is complete. Armanino noted the following relevant key pairs related to the Ethereum 2.0 Beacon Chain:



There are two relevant key pairs related to each ETH2 Validator Node:

1) Validator Keys: The Validator Public/Private key pair is created initially upon the deposit of ether into the deposit contract.

- **Validator Public Key**: The Validator Public Key is used to retrieve ETH2 Validator information, such as the staked ETH balance as well as the staking rewards. All ETH2 Validators have an associated Withdrawal Credential (see Withdrawal Keys description below), which can also be retrieved using the Validator Public Key.
- **Validator Private Key**: The Validator Private Key is used for active signing of on-chain operations such as block proposals and attestations on the Ethereum 2.0 Beacon Chain.

2) Withdrawal Keys: The Withdrawal Public/Private key pair represents ownership to the staked ETH balance held in the Validator Key.

- **Withdrawal Public Key**: The Withdrawal Public Key is a hash of the Withdrawal Private Key and a pre-image to the Withdrawal Credential. The Withdrawal Public Key also acts as an intermediary step to create the Withdrawal Credential from the Withdrawal Private Key.
- **Withdrawal Credential:** The Withdrawal Credential is the hash of the Withdrawal Public Key that is used as a public identifier to identify who has rights to withdraw funds from a Validator Node.
- **Withdrawal Private Key**: Once the Beacon Chain upgrade is complete, the Withdrawal Private Key can be used for withdrawing the staked ETH funds and rewards from the Validator. Ownership of the Withdrawal Private Key represents ownership of the staked ETH balances and rewards held in the Validator.

Armanino noted all of Kraken's *Validator* Public Keys had the same *Withdrawal Credential*, derived from the same Withdrawal Public Key. Therefore, Armanino noted one Withdrawal Key pair in scope for the assessment. Since ownership of the Withdrawal Private Key represents access to the ETH2 balances held in a Validator, Armanino ensured Kraken retained control of the Withdrawal Private Key for each Validator. To verify that, at the time of the assessment, Kraken retained control of the Withdrawal Private Key for each Validator, Armanino used a digital signature method to ensure Kraken was able to sign a custom message provided by Armanino using the Withdrawal Private Key that was related to *all* Validator Nodes Kraken had staked ETH assets with on behalf of clients. Armanino subsequently verified whether the digital signature was signed using the Armanino-provided custom message and the Withdrawal Private Key.

8) Obtain from Kraken Management a complete list of ETH2 Validator Public Keys in-scope for the assessment. For each of the Public Keys received, query the Ethereum 2.0 Beacon Chain, and observe the related Withdrawal Credential address(es).

Results: Armanino received from Kraken Management a list of ETH2 Validator Public Keys[14] in scope for the assessment and queried the Ethereum 2.0 Beacon Chain for staked ETH balances and associated Withdrawal Credentials. Armanino noted the following details:

- **Total Staked ETH2 Balance**: 947,584.00 ETH
- **Withdrawal Credential**: 0x004f58172d06b6d54c015d688511ad5656450933aff85dac123cd09410a0825c

Armanino verified that the Withdrawal Credential provided by Kraken is associated with all of the Validator Public Keys received.

9) Obtain from Kraken Management the Withdrawal Public Key. Confirm the Withdrawal Credential observed in Procedure 8 is derived from the Withdrawal Public Key provided by Kraken Management. For the in-scope Withdrawal Public Key(s), obtain from Kraken Management the corresponding digital signature generated from an Armanino-provided custom message. Verify whether the digital signature provided by Kraken Management was signed using the Armanino-provided custom message and the private key to the Withdrawal Public Key.

Results: Prior to the assessment date, Armanino obtained the in-scope Withdrawal Public Key from Kraken Management. Armanino confirmed the Withdrawal Credential observed in Procedure 8 was derived from the Withdrawal Public Key provided by Kraken Management by applying the SHA256 hash function to the Withdrawal Public Key and noting the following output:

[14] Armanino included Validator Nodes that had ether (minimum of 32 ether) sent to the Validator Deposit Contract on the Ethereum 1.0 Chain and pending activation on the Ethereum 2.0 Beacon Chain as long as the Validator Nodes were eventually activated. Armanino confirmed all Validators that had ether sent to the Deposit Contract on the Ethereum 1.0 Chain, but not yet eligible and activated as of the assessment cut off time, were subsequently successfully activated. Therefore, the balances of the Validator Nodes provided by Kraken were applicable to include as collateral against the ETH2.S liabilities as of the assessment time.

Hash Input: Withdrawal Public Key:
86e9b1d91219e3c34fac7aaeb831d2a95586e8b7f5b392ccbbe67ed5d3b509b199b798db149ca49d4e42f5c0aa6008f0

Hash Output: Withdrawal Credential:
0e4f58172d06b6d54c015d688511ad5656450933aff85dac123cd09410a0825c

For the Withdrawal Public Key, Armanino obtained from Kraken Management the corresponding digital signature generated from an Armanino-provided custom message and the Withdrawal Private key. Subsequently, Armanino successfully verified that the digital signature provided by Kraken Management was signed by the Withdrawal Private Key associated with the Withdrawal Public Key provided by Kraken Management.

Proof of Reserves Assessment

10) Query all BTC, ETH, and staked ETH (the "In-Kind Assets") addresses/keys in scope for the assessment and proven to be custodied by Kraken. Observe and aggregate the BTC, BTC.M, ETH, and ETH2.S balances (the "Client Liabilities") at the specified assessment time.

Results: Armanino retrieved, from the respective blockchains, the balances of all BTC, ETH and ETH2 addresses/keys in-scope for the assessment and tested in procedures 7-9. Armanino obtained the in-scope asset balances as of 11:59PM UTC on December 31, 2021 and noted the below results:

Asset	Balance	Block Height / Epoch
BTC	189,141.558007517 BTC	716598
ETH	2,243,889.18893071 ETH	13916165
Staked ETH	947,584.00 Staked ETH	88987

11) Compare the total liabilities from the Client Liability Report extracted from Kraken's production database to the total assets held in the Kraken custodied addresses tested as of the specified date and time of the assessment time and calculate the collateralization ratio.

Results: Armanino compared total client liabilities **[167,891.70 BTC | 6,838.94 BTC.M | 2,128,857.51 ETH | 947,548.48 ETH2.S]** from the Client Liability Report extract as of December 31, 2021 from Kraken's production replica database to the total assets **[189,141.56 BTC | 2,243,889.19 ETH | 947,584.00 Staked ETH]** held in the addresses/keys tested in procedures 7-9 and calculated the collateralization ratio as summarized in the Results.

Results

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

1. Armanino noted all records of Kraken spot exchange client liabilities were included in the client database as aggregated in the Merkle Tree with the Merkle Root Hash:

   12f021d4e2b20da9d4e1206b825794e9c410ff71cddb786c7191f08eeead017c

2. Armanino noted Kraken retained custody over a sufficient amount of BTC, ETH, and staked ether Staked ETH assets to cover client BTC, BTC.M, ETH, and ETH2.S liabilities as observed within the database related to Kraken's spot exchange as of 11:59PM UTC December 31, 2021, with the results below:

Results as of **BTC Block Height:** 716598 | **ETH Block Height:** 13916165 | **ETH2 Epoch:** 88987

Kraken Spot Exchange	Client Liabilities	In-Kind Assets	Collateralization Ratio
BTC	167,891.70 BTC	189,141.56 BTC	**108.25%**
BTC.M	6,838.94 BTC.M		
ETH	2,128,857.51 ETH	2,243,889.19 ETH	**105.40%**
ETH2.S	947,548.48 ETH2.S	947,584.00 Staked ETH	**100.00%**

Appendix

Further Understanding of Risks and Opportunities

The following table is intended to provide further context regarding the risks to the findings presented within this report. We believe presenting the risks and opportunities in this way will enable Kraken Platform Clients to further understand and benefit from the findings presented.

Risk Name	Risk Description	Mitigating Action
Point in Time Assessment	The assessment reports balances are as of a single point in time and does not assess the asset and liability balances before or after the assessment date.	The Assessor/Assessee may consider providing Proof of Reserve 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 assets intended to collateralize client liabilities.	As Proof of Reserves assessments evolve and become more commonplace, procedures could be expanded to include an examination of the liabilities on the Company's full balance sheet, overall Company solvency, and an expanded search for unrecorded liabilities.
Reliance on Client Verification	While Armanino performed procedures to gain reasonable comfort over the authenticity of the data provided within the Customer Liability Extract, there exists an inherent possibility of purposeful or accidental inclusions or exclusions that could impact the dataset. In order to confirm all account included within the dataset are authentic, clients 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 clients performing self-verification.
Addresses Confirmed as Part of the Proof of Reserves assessment are Kept Private	In order to maintain the privacy and security of Kraken addresses, Armanino and Kraken did not release the addresses in-scope for the assessment. Thus, clients are unable to verify the balances of the addresses themselves via the blockchain and must rely on the independent assessor to compile and report on the asset portion of the Proof of Reserves Assessment	In the future, Zero Knowledge proof schemes may be developed to prove ownership of a specific balance as of a point in time without disclosing the address itself. However, these potential methodologies are not yet widespread and lack an understandable client experience.
Risk of Ethereum 2.0 Failure	The Ethereum 2.0 upgrade may fail, and Kraken may not be able to fulfill the ETH2.S liabilities.	This is an inherent risk that is extremely difficult (if not impossible) for the independent assessor nor Kraken to mitigate.