ICAI Dubai Chapter – Emerging Standards of Auditing
Hyatt Regency, Tuesday, May 23, 2023

Auditing Proof of Reserves in Crypto Exchange: Issues, Challenges & Way Forward

Presented by:
Vinod Kashyap

Agenda

Preamble

01

Proof of Reserves

02

Issues & Challenges

03

Auditing Standards & Guidance

04

Way Forward

05

Preamble

Crypto Jargon

Cryptocurrency Exchange

Cryptocurrency exchanges are privately –owned platforms that facilitate the trading of cryptocurrencies for other crypto assets , including digital and fiat currencies and NFTs.

Proof of Reserves

Proof of Reserves (PoR) is an independent audit conducted by a third party which seeks to ensure that a custodian holds the assets it claims to on behalf of its clients. This auditor takes an anonymized snapshot of all balances held and aggregates them into a Merkle Tree - a privacy-friendly data structure that encapsulates all client balances.

The idea behind publication of Proof of Reserves to the public and in particular the customers of crypto exchange is that cryptocurrency held on deposit matches up with users balances.

Proof of Liabilities

Proof of Liabilities (PoL) is a scheme designed to let companies that accept monetary deposits from consumers (e.g. Bitcoin exchanges, gambling websites, online Bitcoin wallets, etc.) prove their total amount of deposits (their liabilities) without compromising the privacy of individual users.

Proof of Solvency

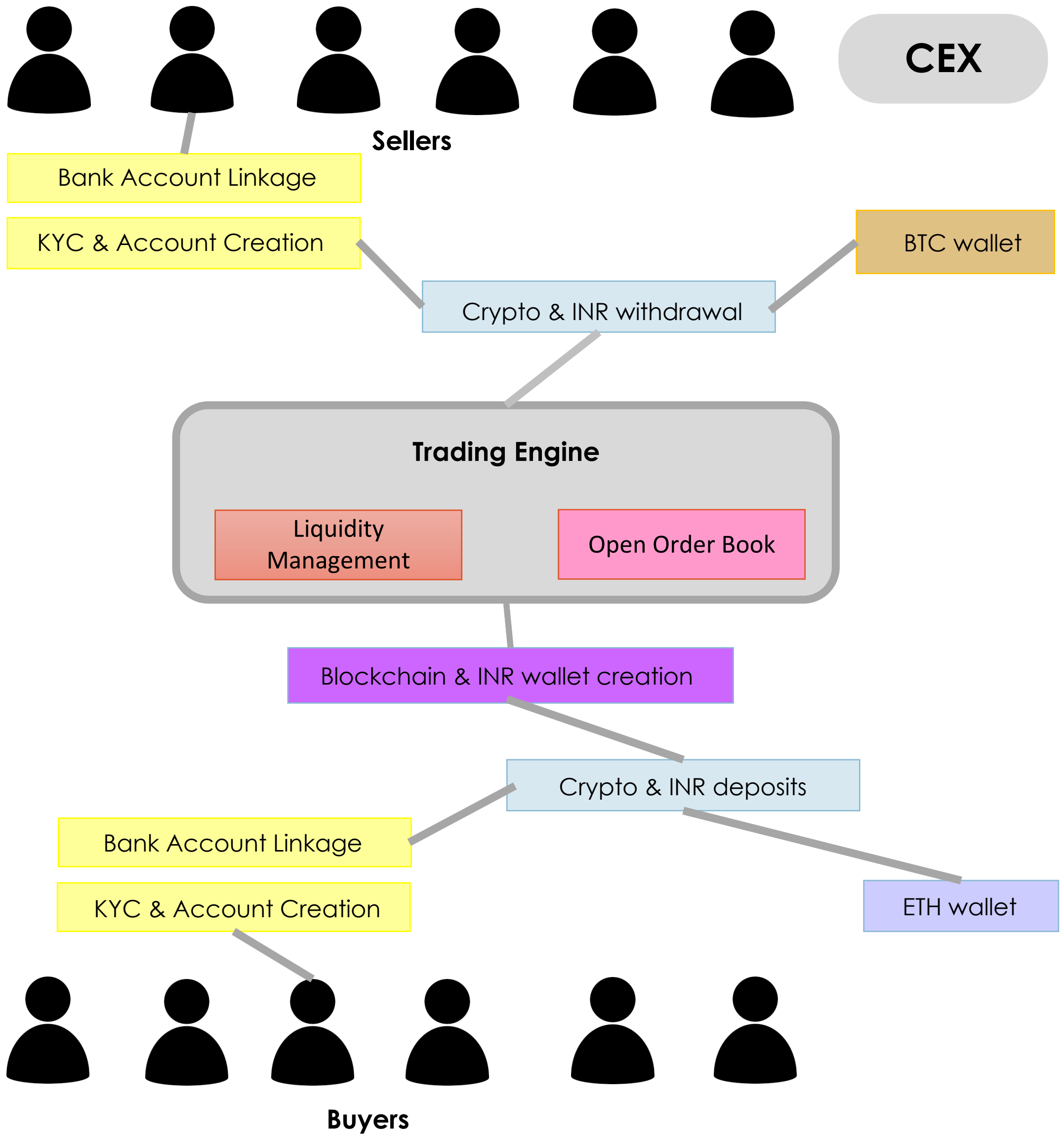
Proof of Solvency = Proof of Reserves + Proof of Liabilities

Crypto Jargon Cont..

Merkel Tree

In cryptography or computer science, a hash tree or Merkle tree is a tree in which every "leaf" (node) is labelled with the cryptographic hash of a data block, and every node that is not a leaf (called a branch, inner node, or innode) is labelled with the cryptographic hash of the labels of its child nodes. A hash tree allows efficient and secure verification of the contents of a large data structure.

Types of Crypto Exchanges



CEX

Sellers

Bank Account Linkage

KYC & Account Creation

BTC wallet

Crypto & INR withdrawal

Trading Engine

Liquidity Management

Open Order Book

Blockchain & INR wallet creation

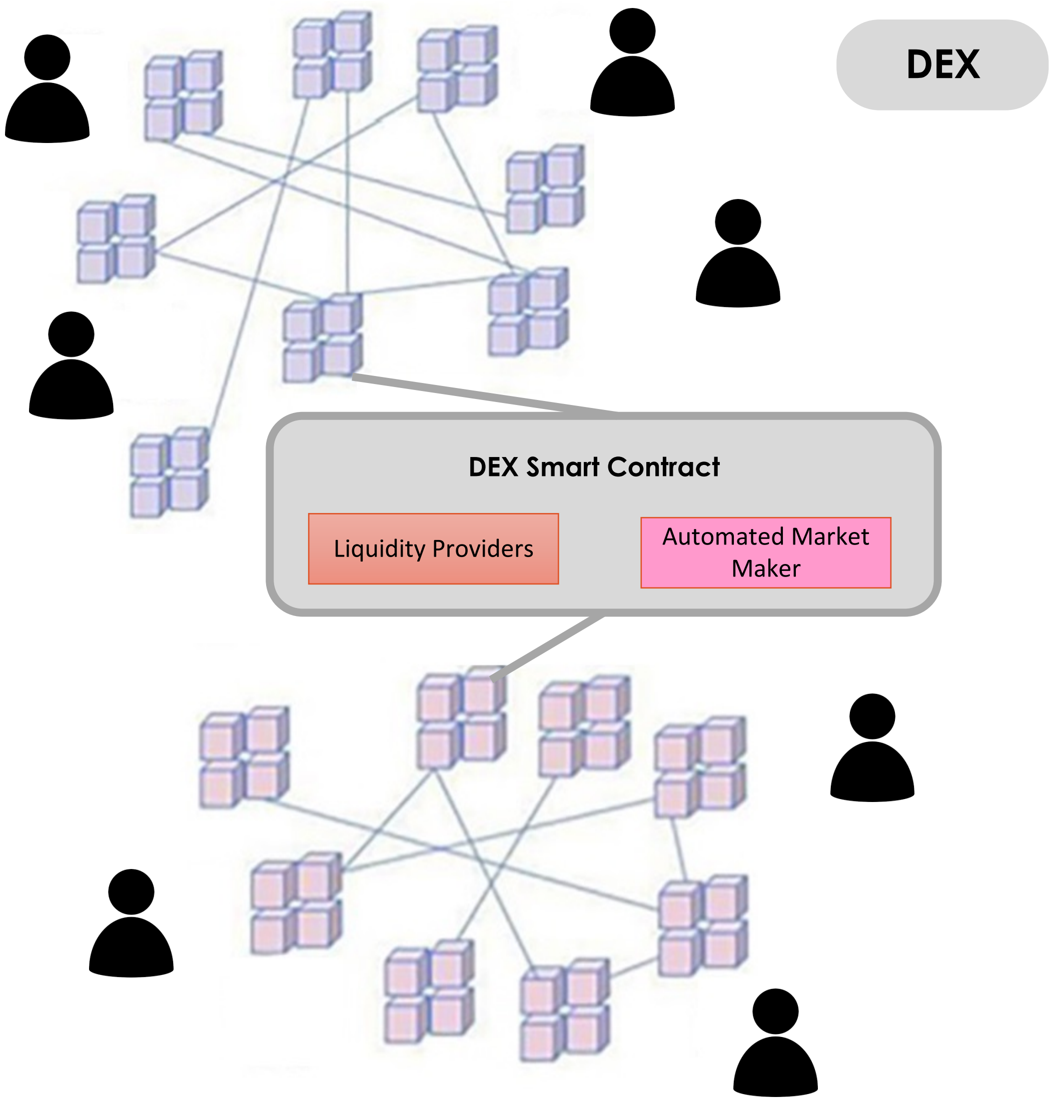
Crypto & INR deposits

Bank Account Linkage

KYC & Account Creation

ETH wallet

Buyers



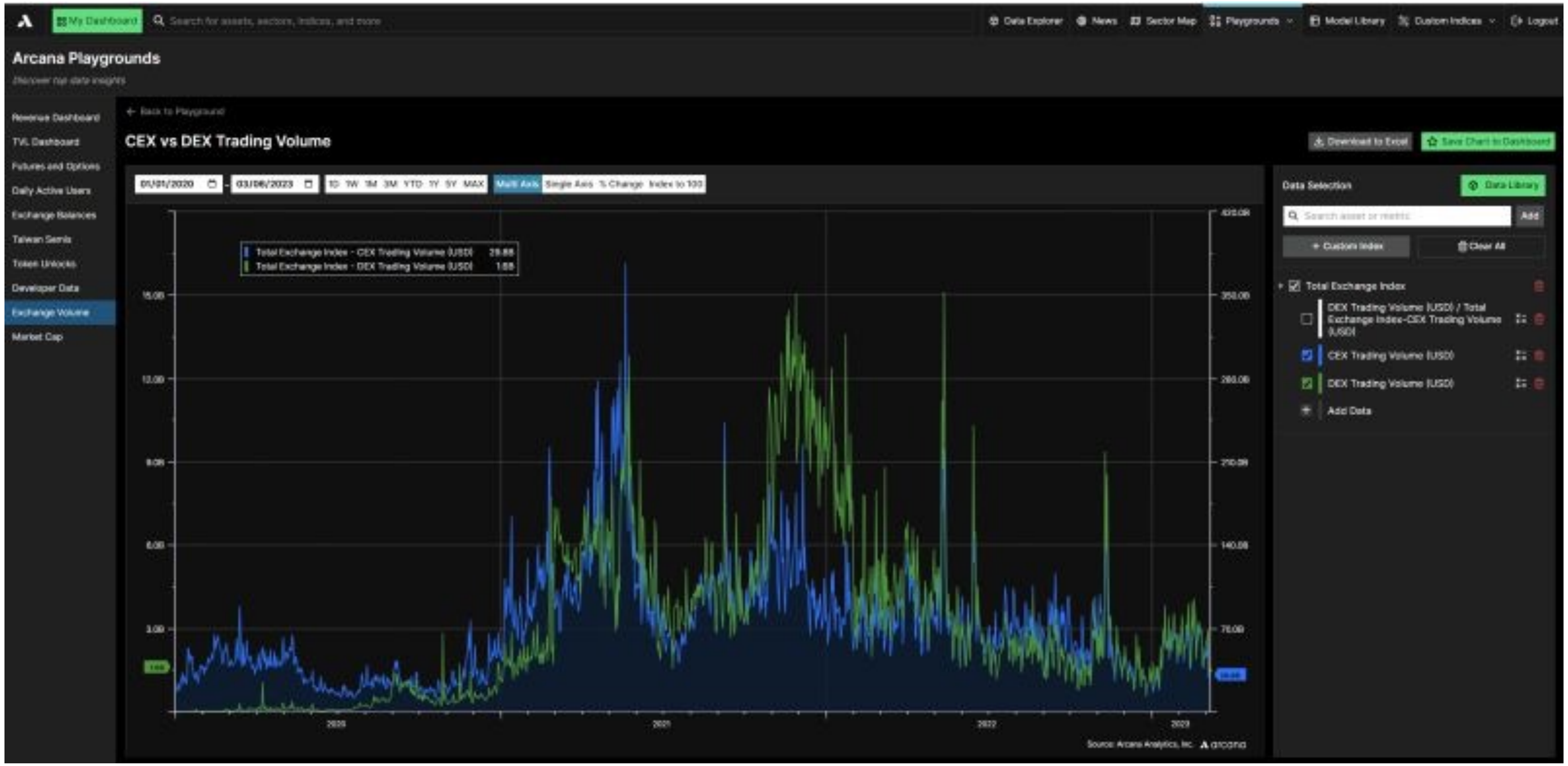
DEX

DEX Smart Contract

Liquidity Providers

Automated Market Maker

CEX Vs. DEX



Arcana Playgrounds

Discover top data insights

CEX vs DEX Trading Volume

01/01/2020 – 03/06/2023

Multi Axis

Total Exchange Index - CEX Trading Volume (USD) 29.8B

Total Exchange Index - DEX Trading Volume (USD) 1.0B

Data Selection

☑ Total Exchange Index

□ DEX Trading Volume (USD) / Total Exchange Index-CEX Trading Volume (USD)

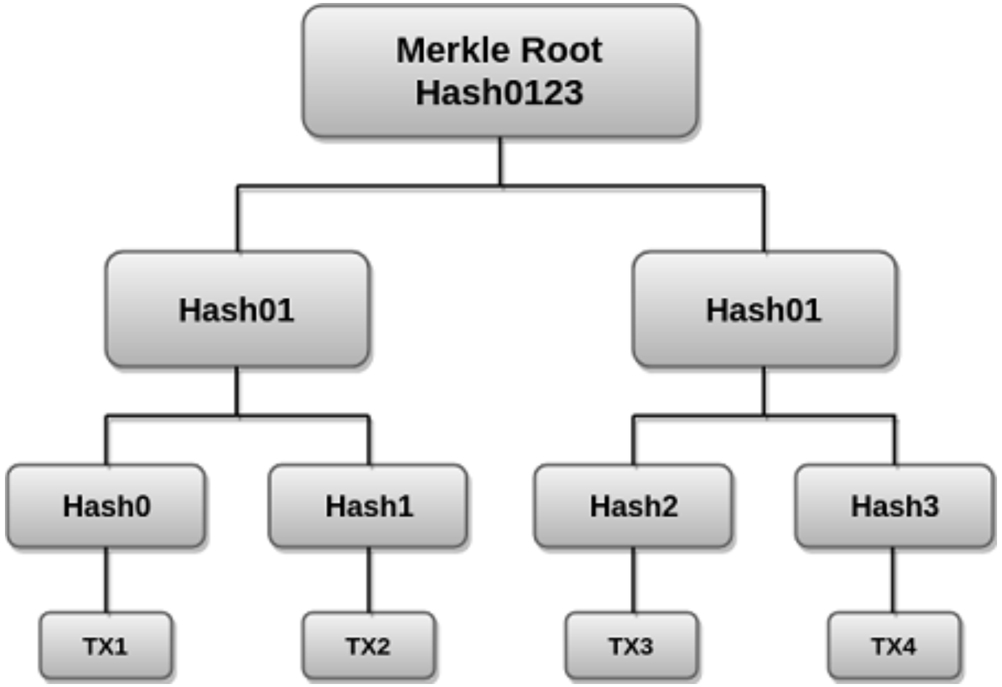
☑ CEX Trading Volume (USD)

☑ DEX Trading Volume (USD)

Source: Arcana Analytics, Inc.

- Centralized Exchange (CEX) aggregated trading volume in blue (right hand side axis)
- Decentralized Exchange (DEX) aggregated trading volume in green (Left hand side axis)
- CEX are 95%% of aggregated trading volume and DEX are only 5%
- The largest exchanges are still CEX

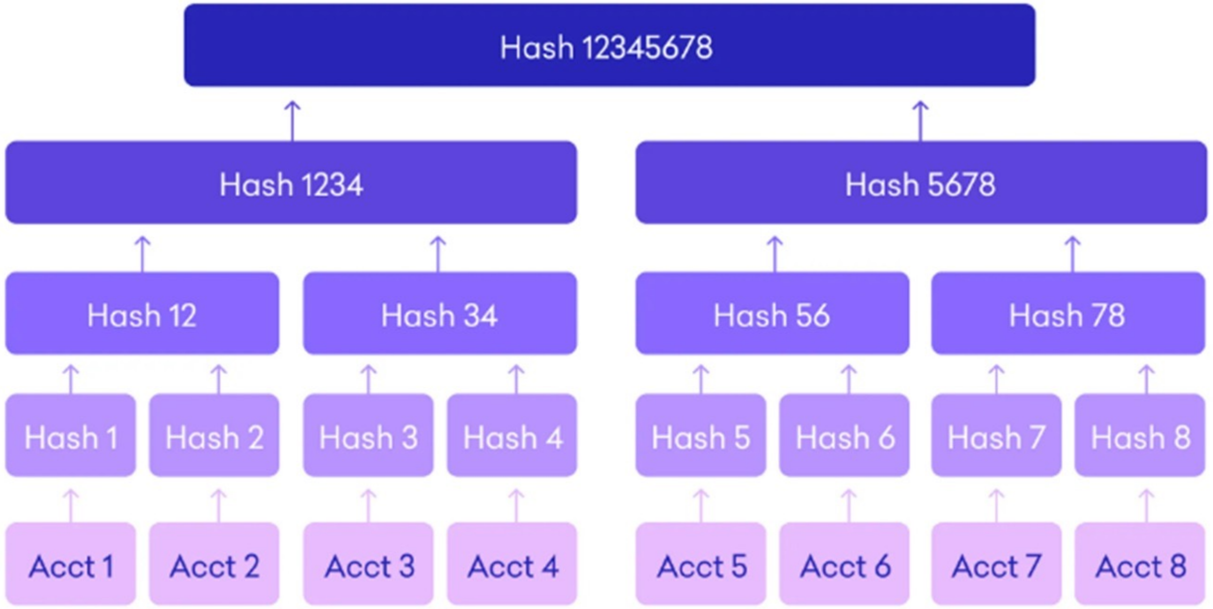
Merkel Tree



- In cryptography or computer science, a hash tree or Merkle tree is a tree in which every "leaf" (node) is labelled with the cryptographic hash of a data block, and every node that is not a leaf (called a branch, inner node, or innode) is labelled with the cryptographic hash of the labels of its child nodes. A hash tree allows efficient and secure verification of the contents of a large data structure.

- It is a mathematical data structure composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure. Merkle Tree is also known as Hash Tree.

Auditing Proof of Reserves on Merkel Tree



- The data of all the balances held is taken by the third party in the form of a Merkle tree
- A Merkle root is then obtained, which uniquely identifies and sums up the balances of all the accounts taken
- These balances are then verified on public blockchains where assets are held using the digital signatures provided by the exchange
- The data of the balances and the details of the assets on the public blockchains are verified. These numbers should balance, thus ensuring consistency
- Systems will also be set up for customers to check if the assets they hold are verified
- Any changes in data will affect the Merkel root indicating possible tampering with assets

Crypto Exchange & Investors

Investors use exchange to trade dollars for crypto

Investors have little to no assurance over reserves custody

Audit methods, formal report, investors participate in proving reserves

Proof of Reserves

Proof-of-Reserves

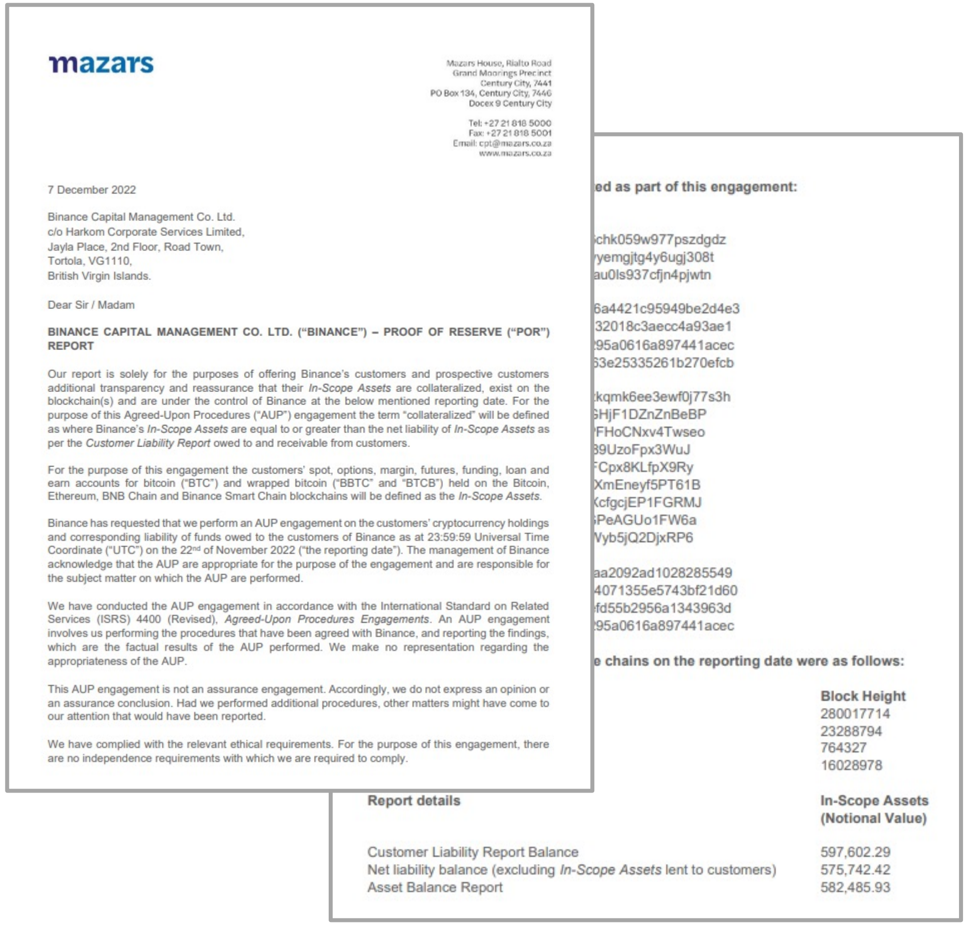
Proof of reserves is supposed to instill some added trust, but they aren’t complete audits and don’t necessarily provide a full picture of a company’s financials, such as total liabilities (deposits) owed back to clients and other types of debt. Nor do they assess the quality of a crypto exchange’s controls.

Audit Reports on Proof of Reserves

Crypto Exchange

- **Binance Capital Management Co Ltd. –** Agreed Upon Procedures (AUP) Report under ISRS 4400 (Mazars)
- **FTX Trading Ltd. –** Attestation report not available. Clean audit opinions as on December 31, 2021 and 2020.(Prager Metis LLP & Armanino LLP)
- **Karken -** Agreed Upon Procedures (AUP) Report under auditing standards issued by AICPA (Armanino)

Binance



mazars

Mazars House, Rialto Road
Grand Moorings Precinct
Century City, 7441
PO Box 134, Century City, 7446
Docex 9 Century City

Tel: +27 21 818 5000
Fax: +27 21 818 5001
Email: cpt@mazars.co.za
www.mazars.co.za

7 December 2022

Binance Capital Management Co. Ltd.
c/o Harkom Corporate Services Limited,
Jayla Place, 2nd Floor, Road Town,
Tortola, VG1110,
British Virgin Islands.

Dear Sir / Madam

BINANCE CAPITAL MANAGEMENT CO. LTD. ("BINANCE") – PROOF OF RESERVE ("POR") REPORT

Our report is solely for the purposes of offering Binance's customers and prospective customers additional transparency and reassurance that their *In-Scope Assets* are collateralized, exist on the blockchain(s) and are under the control of Binance at the below mentioned reporting date. For the purpose of this Agreed-Upon Procedures ("AUP") engagement the term "collateralized" will be defined as where Binance's *In-Scope Assets* are equal to or greater than the net liability of *In-Scope Assets* as per the *Customer Liability Report* owed to and receivable from customers.

For the purpose of this engagement the customers' spot, options, margin, futures, funding, loan and earn accounts for bitcoin ("BTC") and wrapped bitcoin ("BBTC" and "BTCB") held on the Bitcoin, Ethereum, BNB Chain and Binance Smart Chain blockchains will be defined as the *In-Scope Assets*.

Binance has requested that we perform an AUP engagement on the customers' cryptocurrency holdings and corresponding liability of funds owed to the customers of Binance as at 23:59:59 Universal Time Coordinate ("UTC") on the 22nd of November 2022 ("the reporting date"). The management of Binance acknowledge that the AUP are appropriate for the purpose of the engagement and are responsible for the subject matter on which the AUP are performed.

We have conducted the AUP engagement in accordance with the International Standard on Related Services (ISRS) 4400 (Revised), *Agreed-Upon Procedures Engagements*. An AUP engagement involves us performing the procedures that have been agreed with Binance, and reporting the findings, which are the factual results of the AUP performed. We make no representation regarding the appropriateness of the AUP.

This AUP engagement is not an assurance engagement. Accordingly, we do not express an opinion or an assurance conclusion. Had we performed additional procedures, other matters might have come to our attention that would have been reported.

We have complied with the relevant ethical requirements. For the purpose of this engagement, there are no independence requirements with which we are required to comply.

ed as part of this engagement:

chk059w977pszdgdz
yemgjtg4y6ugj308t
au0ls937cfjn4pjwtn

6a4421c95949be2d4e3
32018c3aecc4a93ae1
95a0616a897441acec
3e25335261b270efcb

kqmk6ee3ewf0j77s3h
HjF1DZnZnBeBP
FHoCNxv4Twseo
9UzoFpx3WuJ
Cpx8KLfpX9Ry
XmEneyf5PT61B
cfgcjEP1FGRMJ
PeAGUo1FW6a
Vyb5jQ2DjxRP6

aa2092ad1028285549
4071355e5743bf21d60
fd55b2956a1343963d
95a0616a897441acec

e chains on the reporting date were as follows:

Block Height
280017714
23288794
764327
16028978

Report details	**In-Scope Assets (Notional Value)**
Customer Liability Report Balance	597,602.29
Net liability balance (excluding *In-Scope Assets* lent to customers)	575,742.42
Asset Balance Report	582,485.93

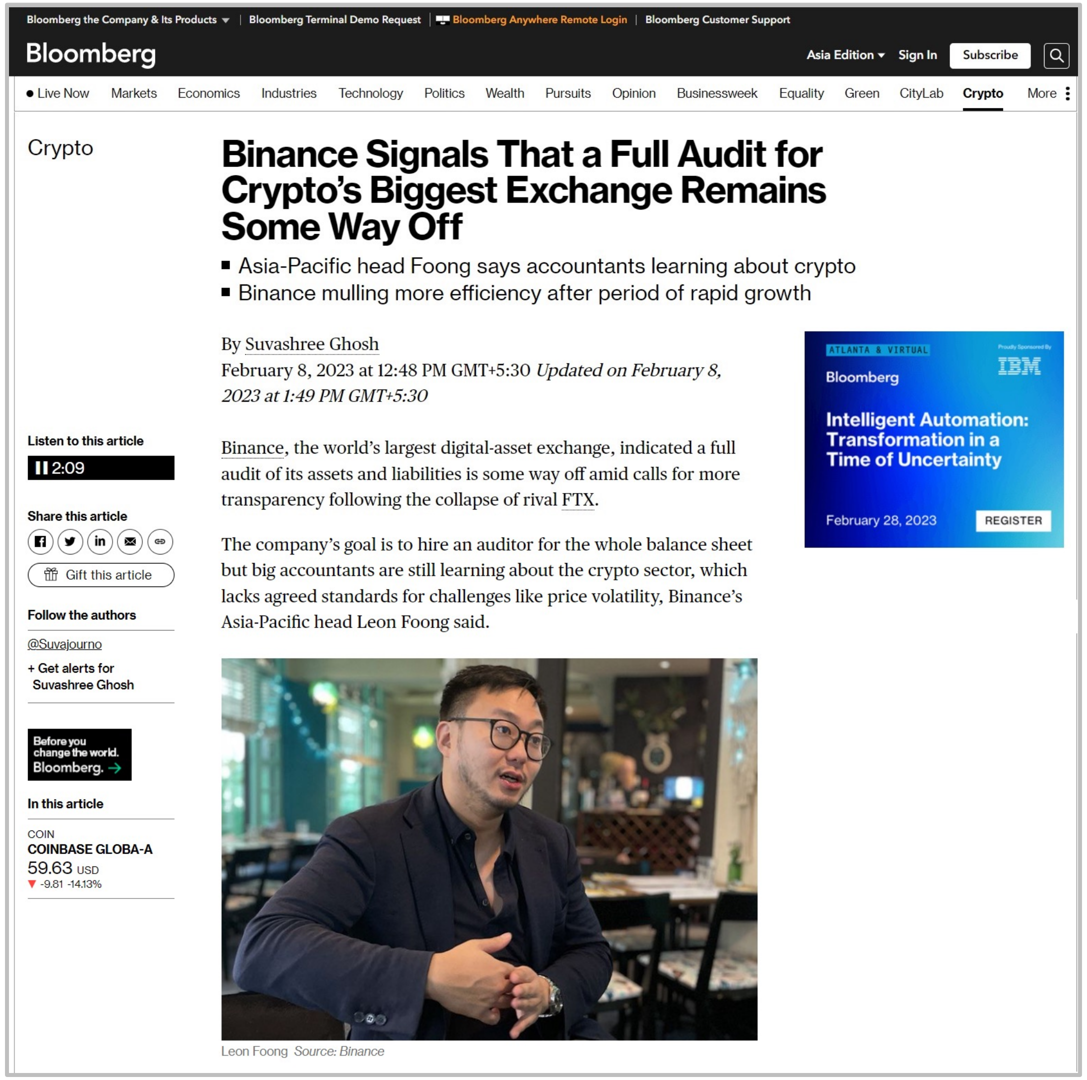
Facts

- Agreed Upon Procedures (AUP)Report under ISRS 4400 issued by IAASB
- Obtained "Assets Balance Reports" and "Public Key Addresses" from Management and verified the same.
- Verified movement of funds at "Public Key Addresses" using Private Key
- Obtained "Customer Liability Report" from the database
- Checked completeness of data and for any duplicate customer Ids

Red Flags 🚩

- Limitations of an Agreed Upon Procedures (AUP) Report
- Exchange financial position
- Existence & effectiveness of internal controls
- Binance Accounts have never been audited

Binance Cont..



Crypto

Binance Signals That a Full Audit for Crypto's Biggest Exchange Remains Some Way Off

- Asia-Pacific head Foong says accountants learning about crypto
- Binance mulling more efficiency after period of rapid growth

By Suvashree Ghosh
February 8, 2023 at 12:48 PM GMT+5:30 *Updated on February 8, 2023 at 1:49 PM GMT+5:30*

Binance, the world's largest digital-asset exchange, indicated a full audit of its assets and liabilities is some way off amid calls for more transparency following the collapse of rival FTX.

The company's goal is to hire an auditor for the whole balance sheet but big accountants are still learning about the crypto sector, which lacks agreed standards for challenges like price volatility, Binance's Asia-Pacific head Leon Foong said.

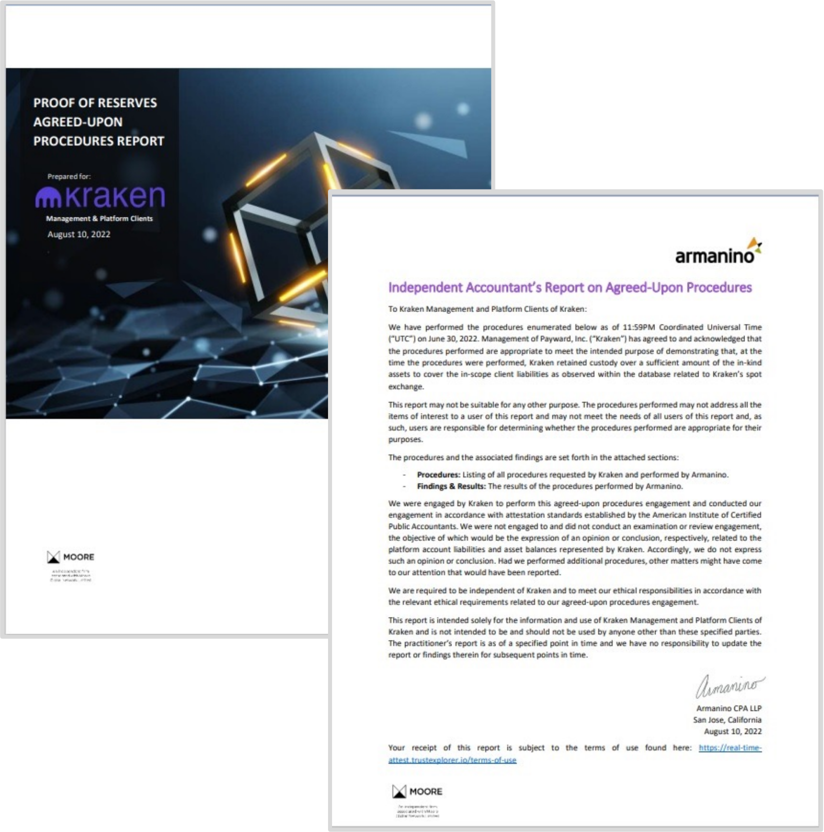
Leon Foong *Source: Binance*

Before you change the world. Bloomberg.

ATLANTA & VIRTUAL
Bloomberg
IBM
Intelligent Automation: Transformation in a Time of Uncertainty
February 28, 2023
REGISTER

More skeletons may come out of the cupboard when audit is done…

Kraken



PROOF OF RESERVES
AGREED-UPON
PROCEDURES REPORT

Prepared for:

kraken

Management & Platform Clients

August 10, 2022

MOORE

armanino

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 June 30, 2022. 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 the in-kind assets to cover the in-scope client 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 by Armanino.

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 we have no responsibility to update the report or findings therein for subsequent points in time.

Armanino

Armanino CPA LLP
San Jose, California
August 10, 2022

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

MOORE

Facts

- Agreed Upon Procedures (AUP)Report issued under auditing standards issued by AICPA (SSAE – 19)
- Obtained an overview of the company back ground, business model & supported features
- Obtained a list of customer liabilities and in-kind assets from management
- Utilized Merkel Tree generator and verifier

Red Flags 🚩

- Real Time Attestation . No auditor involvement in AUP Report preparation.
- Limitations of an Agreed Upon Procedures (AUP) Report.
- Financial position of crypto exchange not known.
- Existence & effectiveness of internal controls

Audit Reports on Proof-of-Reserves Cont...

Stable Coins

- **Teether Holdings Limited -** Audit Report of Consolidated Reserves under ISAE 3000 (BDO)
- **Circle Internet Financial Inc. -** Attestation Report on Reserves Account under auditing standards issued by AICPA (Grand Thornton)
- **Techteyx Ltd. (TrueUSD) –** Attestation report on TrueUSD holding under auditing standards issued by AICPA (Armanino LLP)
- **Mek Global Ltd. (KuCoin) -** AUP Report on Proof of Reserves under ISRS 4400 (Mazars)

Teether Holdings Limited.

Tether Holdings Limited

INDEPENDENT AUDITORS' REPORT ON THE
CONSOLIDATED RESERVES REPORT

AMZ/FMT/fbs - RC134792022BD0803

BDO

allow holders to transact and settle transactions in a rapid
, and may be verified by the sender and the recipient. The
novating rapidly. Accordingly, any users of digital assets,
roup, should first inform themselves of the general risks and
g as to evolving legal and regulatory requirements. Users of
selves with the risk disclosures, as they may be changed and

hese matters.

v attention to the Management's Key Accounting Policies
asis of accounting. The CRR is prepared by management of
purposes. As a result, the CRR may not be suitable for another

d the corresponding consolidated total assets and consolidated
ctivity prior to and after this time and date was not considered
described above. In addition, we have not performed any
nce on the financial or non-financial activity on dates or times

agement of the Group for additional information only, and this
ope of our assurance engagement and, accordingly, we do not
e on it. Our responsibility is to read the other information in
her the other information is materially inconsistent with the
rse of the engagement, or otherwise appears to be materially

BDO Italia S.p.A.
Andrea Mezzadra
Partner

Tether Holdings Limited | Independent Auditors' Report

Page. 3 of 3

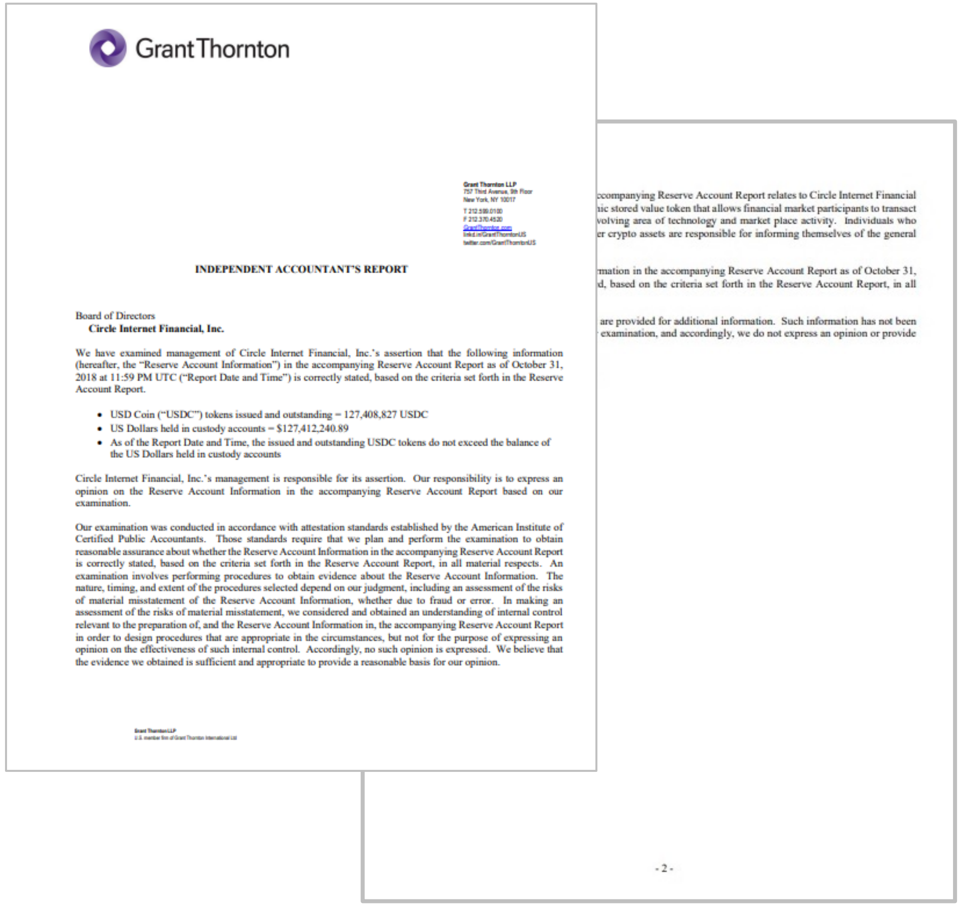
Facts

- Teether (USDT) has the largest market capitalization among fiat-backed Stablecoins
- Central Banks don't have any technical solution of monitoring liabilities of fiat-backed Stablecoins and the assets that back them
- Teether issues audit report on its consolidated reserve account to show that it's liabilities are 100% covered by its reserves and assets
- Teether shared Audit Report on Consolidated Reserve Account in accordance with ISAE 3000. (Revised). – "Assurance Engagements Other than Audit c eview of Historical Financial Information" issued by IAASB

Red Flags

- Audit Report is based upon Consolidated Reserves Account prepared by the management NOT extracted from an audited financial statement
- Teether has never published its audited financial statements in the last 5 years triggering existential fears over the $68 Bn Stablecoins dependability and bonafide.
- ISAE 3000 may not be suitable for audit of Consolidated Reserves.

Circle Internet Financial Inc.



GrantThornton

Grant Thornton LLP
757 Third Avenue, 9th Floor
New York, NY 10017

T 212.599.0100
F 212.370.4520
GrantThornton.com
linkd.in/GrantThorntonUS
twitter.com/GrantThorntonUS

INDEPENDENT ACCOUNTANT'S REPORT

Board of Directors
Circle Internet Financial, Inc.

We have examined management of Circle Internet Financial, Inc.'s assertion that the following information (hereafter, the "Reserve Account Information") in the accompanying Reserve Account Report as of October 31, 2018 at 11:59 PM UTC ("Report Date and Time") is correctly stated, based on the criteria set forth in the Reserve Account Report.

- USD Coin ("USDC") tokens issued and outstanding = 127,408,827 USDC
- US Dollars held in custody accounts = $127,412,240.89
- As of the Report Date and Time, the issued and outstanding USDC tokens do not exceed the balance of the US Dollars held in custody accounts

Circle Internet Financial, Inc.'s management is responsible for its assertion. Our responsibility is to express an opinion on the Reserve Account Information in the accompanying Reserve Account Report based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether the Reserve Account Information in the accompanying Reserve Account Report is correctly stated, based on the criteria set forth in the Reserve Account Report, in all material respects. An examination involves performing procedures to obtain evidence about the Reserve Account Information. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of the Reserve Account Information, whether due to fraud or error. In making an assessment of the risks of material misstatement, we considered and obtained an understanding of internal control relevant to the preparation of, and the Reserve Account Information in, the accompanying Reserve Account Report in order to design procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of such internal control. Accordingly, no such opinion is expressed. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Grant Thornton LLP
U.S. member firm of Grant Thornton International Ltd

ccompanying Reserve Account Report relates to Circle Internet Financial
nic stored value token that allows financial market participants to transact
volving area of technology and market place activity. Individuals who
er crypto assets are responsible for informing themselves of the general

rmation in the accompanying Reserve Account Report as of October 31,
d, based on the criteria set forth in the Reserve Account Report, in all

are provided for additional information. Such information has not been
examination, and accordingly, we do not express an opinion or provide

- 2 -

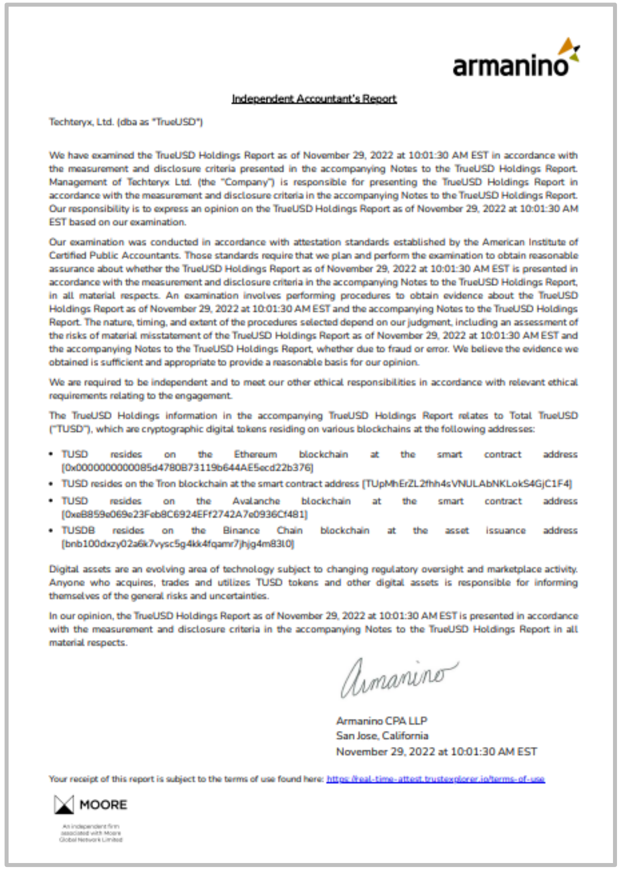
Facts

- Attestation Report on Reserve Account in accordance with Attestation Standards issued by AICPA.
- The Practitioners used the words "correctly stated" in expression of opinion in their reports for the months from October 2018 to December 2021.

Red Flags

- The use of words "correctly stated" amounts to providing "Absolute Assurance" on Reserve Account.
- "Absolute Assurance is not attainable because of the nature of audit evidence and characteristics of the fraud" – AICPA SAS No 82
- AICPA suggests the use of words "fairly stated" in expression of opinion – SSAE 18

TrueUSD



armanino

Independent Accountant's Report

Techteryx, Ltd. (dba as "TrueUSD")

We have examined the TrueUSD Holdings Report as of November 29, 2022 at 10:01:30 AM EST in accordance with the measurement and disclosure criteria presented in the accompanying Notes to the TrueUSD Holdings Report. Management of Techteryx Ltd. (the "Company") is responsible for presenting the TrueUSD Holdings Report in accordance with the measurement and disclosure criteria in the accompanying Notes to the TrueUSD Holdings Report. Our responsibility is to express an opinion on the TrueUSD Holdings Report as of November 29, 2022 at 10:01:30 AM EST based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether the TrueUSD Holdings Report as of November 29, 2022 at 10:01:30 AM EST is presented in accordance with the measurement and disclosure criteria in the accompanying Notes to the TrueUSD Holdings Report, in all material respects. An examination involves performing procedures to obtain evidence about the TrueUSD Holdings Report as of November 29, 2022 at 10:01:30 AM EST and the accompanying Notes to the TrueUSD Holdings Report. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of the TrueUSD Holdings Report as of November 29, 2022 at 10:01:30 AM EST and the accompanying Notes to the TrueUSD Holdings Report, whether due to fraud or error. We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

The TrueUSD Holdings information in the accompanying TrueUSD Holdings Report relates to Total TrueUSD ("TUSD"), which are cryptographic digital tokens residing on various blockchains at the following addresses:

- TUSD resides on the Ethereum blockchain at the smart contract address [0x0000000000085d4780B73119b644AE5ecd22b376]
- TUSD resides on the Tron blockchain at the smart contract address [TUpMhErZL2fhh4sVNULAbNKLokS4GjC1F4]
- TUSD resides on the Avalanche blockchain at the smart contract address [0xeB859e069e23Feb8C6924EFf2742A7e0936Cf481]
- TUSDB resides on the Binance Chain blockchain at the asset issuance address [bnb100dxzy02a6k7vysc5g4kk4fqamr7jhjg4m83l0]

Digital assets are an evolving area of technology subject to changing regulatory oversight and marketplace activity. Anyone who acquires, trades and utilizes TUSD tokens and other digital assets is responsible for informing themselves of the general risks and uncertainties.

In our opinion, the TrueUSD Holdings Report as of November 29, 2022 at 10:01:30 AM EST is presented in accordance with the measurement and disclosure criteria in the accompanying Notes to the TrueUSD Holdings Report in all material respects.

Armanino

Armanino CPA LLP
San Jose, California
November 29, 2022 at 10:01:30 AM EST

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

MOORE

An independent firm
associated with Moore
Global Network Limited

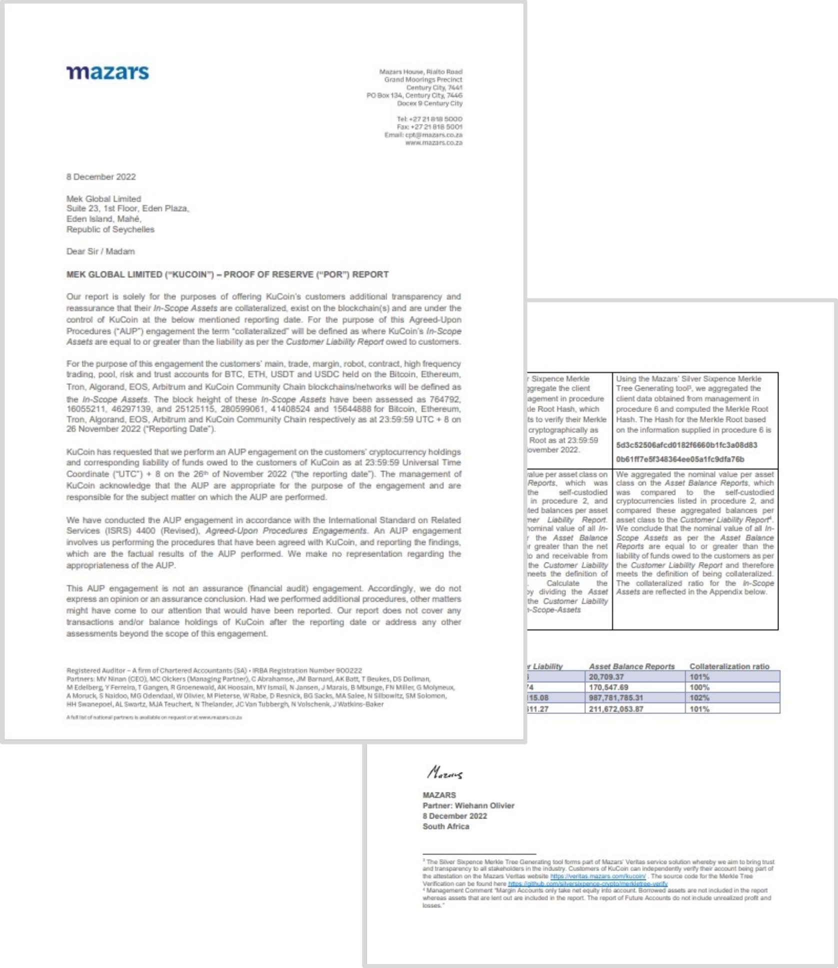
Facts

- Independent Accountant's Report on TrueUSD Holdings report in accordance with Attestation Standards issued by AICPA.

Red Flags

- Report generated by computer system without any involvement of the Practitioner in the audit process.

KuCoin



mazars

Mazars House, Rialto Road
Grand Moorings Precinct
Century City, 7441
PO Box 134, Century City, 7446
Docex 9 Century City

Tel: +27 21 818 5000
Fax: +27 21 818 5001
Email: cpt@mazars.co.za
www.mazars.co.za

8 December 2022

Mek Global Limited
Suite 23, 1st Floor, Eden Plaza,
Eden Island, Mahé,
Republic of Seychelles

Dear Sir / Madam

MEK GLOBAL LIMITED ("KUCOIN") – PROOF OF RESERVE ("POR") REPORT

Our report is solely for the purposes of offering KuCoin's customers additional transparency and reassurance that their *In-Scope Assets* are collateralized, exist on the blockchain(s) and are under the control of KuCoin at the below mentioned reporting date. For the purpose of this Agreed-Upon Procedures ("AUP") engagement the term "collateralized" will be defined as where KuCoin's *In-Scope Assets* are equal to or greater than the liability as per the *Customer Liability Report* owed to customers.

For the purpose of this engagement the customers' main, trade, margin, robot, contract, high frequency trading, pool, risk and trust accounts for BTC, ETH, USDT and USDC held on the Bitcoin, Ethereum, Tron, Algorand, EOS, Arbitrum and KuCoin Community Chain blockchains/networks will be defined as the *In-Scope Assets*. The block height of these *In-Scope Assets* have been assessed as 764792, 16055211, 46297139, and 25125115, 280599061, 41408524 and 15644888 for Bitcoin, Ethereum, Tron, Algorand, EOS, Arbitrum and KuCoin Community Chain respectively as at 23:59:59 UTC + 8 on 26 November 2022 ("Reporting Date").

KuCoin has requested that we perform an AUP engagement on the customers' cryptocurrency holdings and corresponding liability of funds owed to the customers of KuCoin as at 23:59:59 Universal Time Coordinate ("UTC") + 8 on the 26th of November 2022 ("the reporting date"). The management of KuCoin acknowledge that the AUP are appropriate for the purpose of the engagement and are responsible for the subject matter on which the AUP are performed.

We have conducted the AUP engagement in accordance with the International Standard on Related Services (ISRS) 4400 (Revised), *Agreed-Upon Procedures Engagements*. An AUP engagement involves us performing the procedures that have been agreed with KuCoin, and reporting the findings, which are the factual results of the AUP performed. We make no representation regarding the appropriateness of the AUP.

This AUP engagement is not an assurance (financial audit) engagement. Accordingly, we do not express an opinion or an assurance conclusion. Had we performed additional procedures, other matters might have come to our attention that would have been reported. Our report does not cover any transactions and/or balance holdings of KuCoin after the reporting date or address any other assessments beyond the scope of this engagement.

Registered Auditor – A firm of Chartered Accountants (SA) • IRBA Registration Number 900222
Partners: MV Ninan (CEO), MC Olckers (Managing Partner), C Abrahamse, JM Barnard, AK Batt, T Beukes, DS Dollman, M Edelberg, Y Ferreira, T Gangen, R Groenewald, AK Hoosain, MY Ismail, N Jansen, J Marais, B Mbunge, FN Miller, G Molyneux, A Moruck, S Naidoo, MG Odendaal, W Olivier, M Pieterse, W Rabe, D Resnick, BG Sacks, MA Salee, N Silbowitz, SM Solomon, HH Swanepoel, AL Swartz, MJA Teuchert, N Thelander, JC Van Tubbergh, N Volschenk, J Watkins-Baker

A full list of national partners is available on request or at www.mazars.co.za

r Sixpence Merkle ggregate the client agement in procedure kle Root Hash, which ts to verify their Merkle cryptographically as Root as at 23:59:59 ovember 2022.	Using the Mazars' Silver Sixpence Merkle Tree Generating tool[3], we aggregated the client data obtained from management in procedure 6 and computed the Merkle Root Hash. The Hash for the Merkle Root based on the information supplied in procedure 6 is **5d3c52506afcd0182f6660b1fc3a08d83** **0b61ff7e5f348364ee05a1fc9dfa76b**
alue per asset class on *Reports*, which was the self-custodied in procedure 2, and ted balances per asset *ner Liability Report*. nominal value of all *In-* r the *Asset Balance* r greater than the net o and receivable from the *Customer Liability* neets the definition of . Calculate the y dividing the *Asset* the *Customer Liability* *n-Scope-Assets*	We aggregated the nominal value per asset class on the *Asset Balance Reports*, which was compared to the self-custodied cryptocurrencies listed in procedure 2, and compared these aggregated balances per asset class to the *Customer Liability Report*[4]. We conclude that the nominal value of all *In-Scope Assets* as per the *Asset Balance Reports* are equal to or greater than the liability of funds owed to the customers as per the *Customer Liability Report* and therefore meets the definition of being collateralized. The collateralized ratio for the *In-Scope Assets* are reflected in the Appendix below.

r Liability	*Asset Balance Reports*	Collateralization ratio
3	20,709.37	101%
74	170,547.69	100%
15.08	987,781,785.31	102%
11.27	211,672,053.87	101%

Mazars

MAZARS
Partner: Wiehann Olivier
8 December 2022
South Africa

[3] The Silver Sixpence Merkle Tree Generating tool forms part of Mazars' Veritas service solution whereby we aim to bring trust and transparency to all stakeholders in the industry. Customers of KuCoin can independently verify their account being part of the attestation on the Mazars Veritas website https://veritas.mazars.com/kucoin/ . The source code for the Merkle Tree Verification can be found here https://github.com/silversixpence-crypto/merkletree-verify

[4] Management Comment "Margin Accounts only take net equity into account. Borrowed assets are not included in the report whereas assets that are lent out are included in the report. The report of Future Accounts do not include unrealized profit and losses."

Facts

- Agreed Upon Procedures (AUP) Report on Proof of Reserves in accordance with ISRS 4400 (Revised) issued by IAASB.

Red Flags

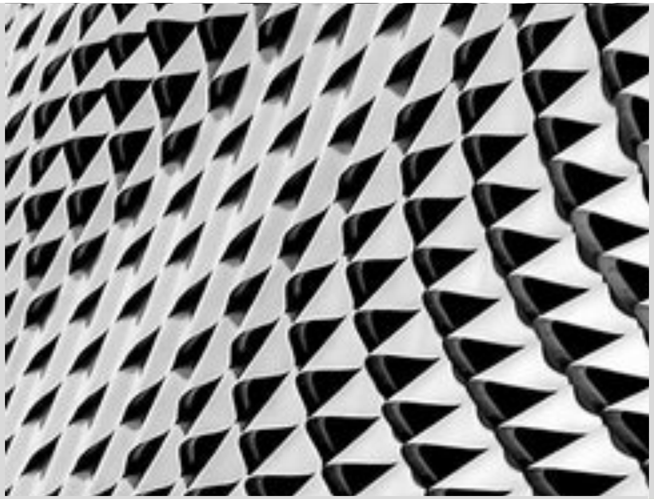
- Limitations of an Agreed Upon Procedures (AUP) Report
- Financial position of entity not considered
- Existence & effectiveness of internal controls

Issues & Challenges

What could go wrong?

2

Crypto Exchange may have material contingent liability.

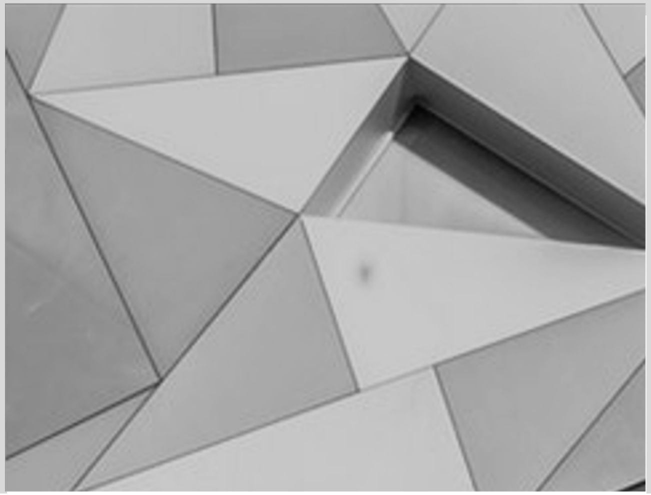


4

Crypto Exchange may not have exclusive control over the Private Keys.

1

Crypto Exchange may have material liabilities other than “outstanding balance due to it’s customers.



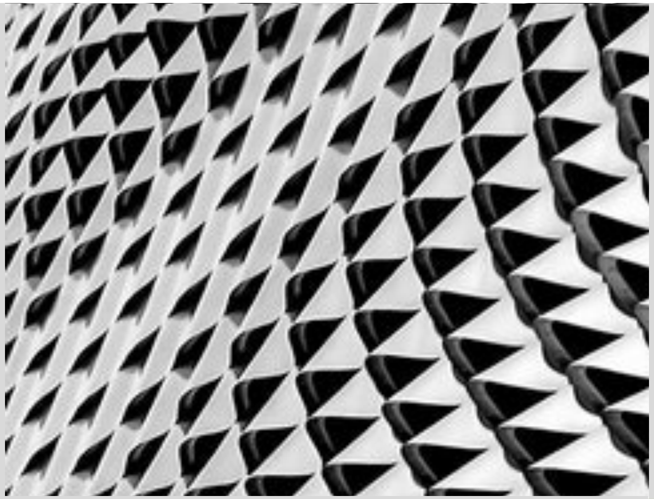
3

Crypto Exchange may have material off-chain assets or real world assets.

Issues & Challenges Cont..

6

Crypto Exchange may manipulate the facts since the correctness of verified balances is only valid during the time of audit.

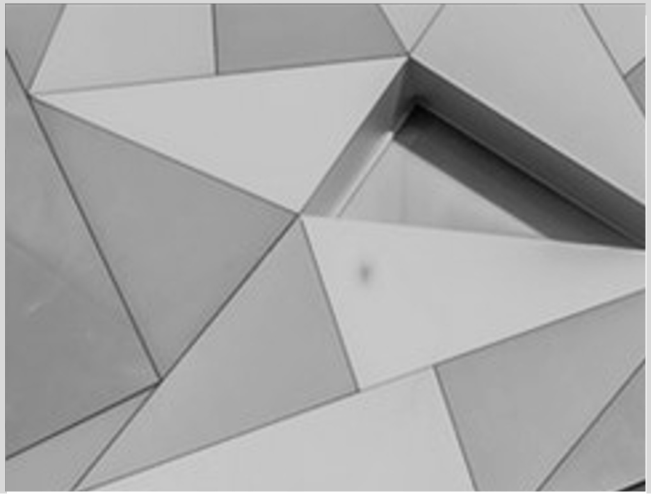


8

Crypto exchange could borrow funds to show it’s reserves are in excess of liabilities.

5

A fraudulent audit result may be produced by a third party auditor in collaboration with the custodian under consideration.



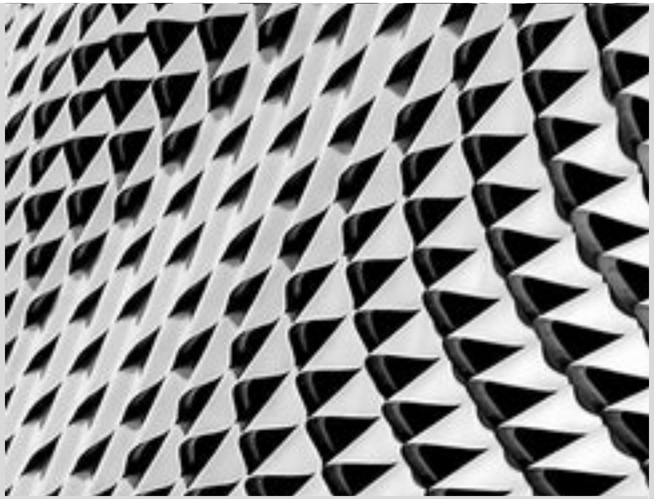
7

The legitimacy of audit can be impacted by the loss of Private Keys or users funds.

Issues & Challenges Cont..

10

Crypto Exchange might be involved in shadow banking.

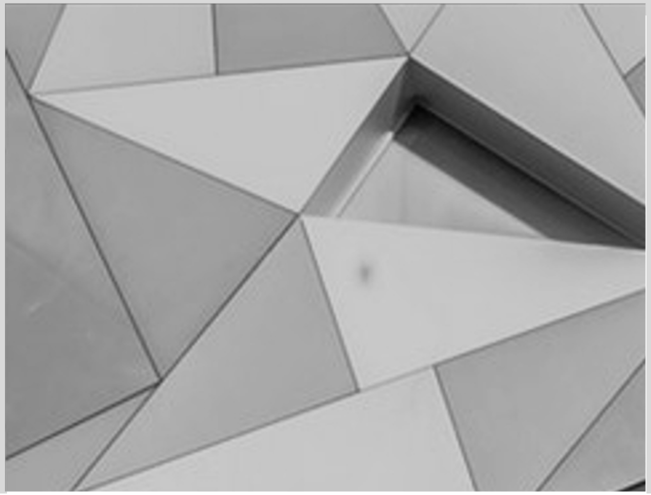


12

Crypto exchange may not have strong finances

9

Correctness of audit of Proof of Reserves depends upon the auditors competence.

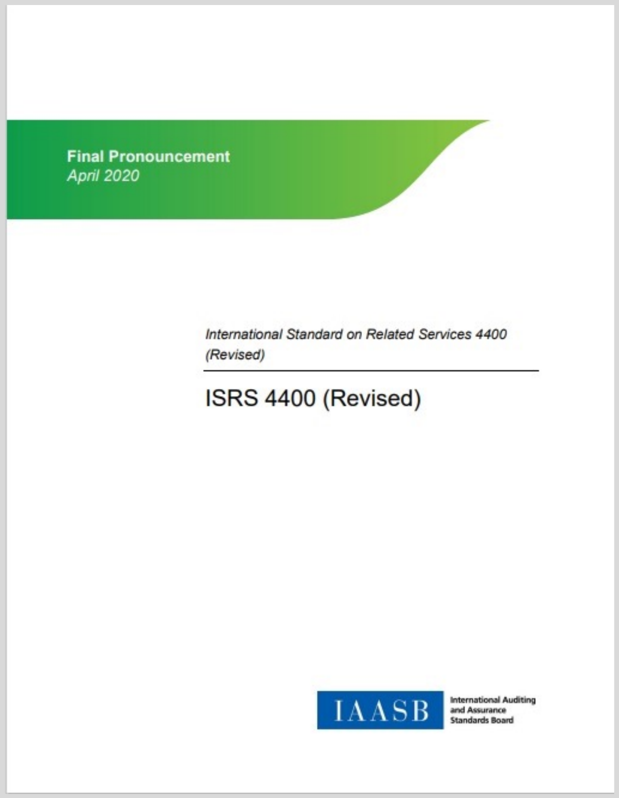


11

Internal Controls may not be effective in crypto exchange

Auditing Standards & Guidance

Auditing Standards



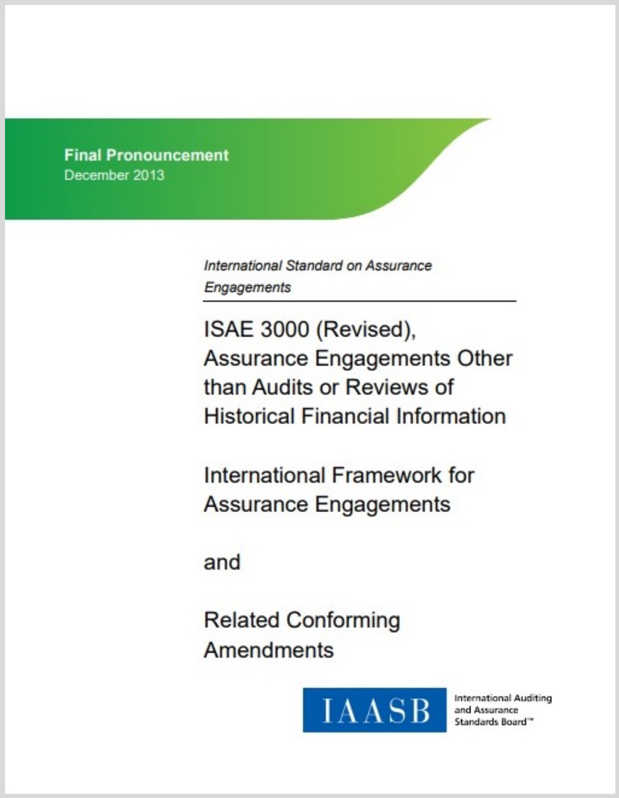
Final Pronouncement
April 2020

International Standard on Related Services 4400 (Revised)

ISRS 4400 (Revised)

IAASB International Auditing and Assurance Standards Board

Agreed Upon Procedures Engagements



Final Pronouncement
December 2013

International Standard on Assurance Engagements

ISAE 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information

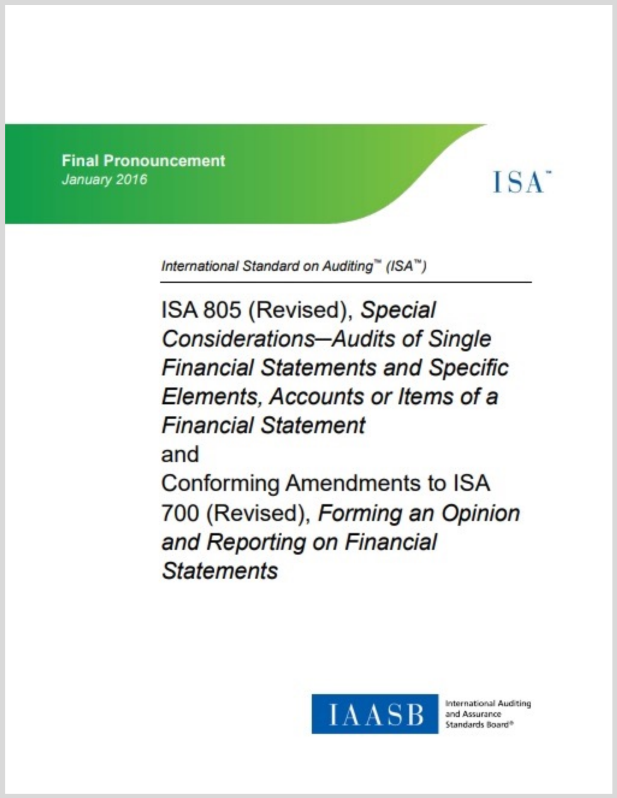
International Framework for Assurance Engagements

and

Related Conforming Amendments

IAASB International Auditing and Assurance Standards Board™

Assurance Engagements Other than Audits or Reviews of Historical Financial Information



Final Pronouncement
January 2016

ISA™

International Standard on Auditing™ (ISA™)

ISA 805 (Revised), *Special Considerations—Audits of Single Financial Statements and Specific Elements, Accounts or Items of a Financial Statement*
and
Conforming Amendments to ISA 700 (Revised), *Forming an Opinion and Reporting on Financial Statements*

IAASB International Auditing and Assurance Standards Board®

Special Considerations – Audit of Single Financial Statements and Specific Elements, Accounts or Items of a Financial Statement

Guidance

No Guidance

- AICPA - Proof of Reserves Working Group is developing guidance on audit of Proof of Reserves

Way Forward

Approach to Auditing Proof of Reserves

01

Risk Assessment

Auditor should make a risk assessment of crypto exchange as per risk assessment framework followed in the country. Viz: COSO -2013 Framework, ISA 315 , Turnboil in UK etc.

02

Evaluation of Internal Controls

Auditor should evaluate the internal controls implemented by the crypto exchange to address the related risks.

03

Complete Financial Statement Audit

Auditor should audit the complete financial statement of crypto exchange and not just on-chain assets and customers liabilities.

04

Verification of on-chain & off-chain

Auditor should verify both on-chain and off-chain assets appearing in the financial statement of crypto exchange.

05

Exclusive Control Over Private Keys

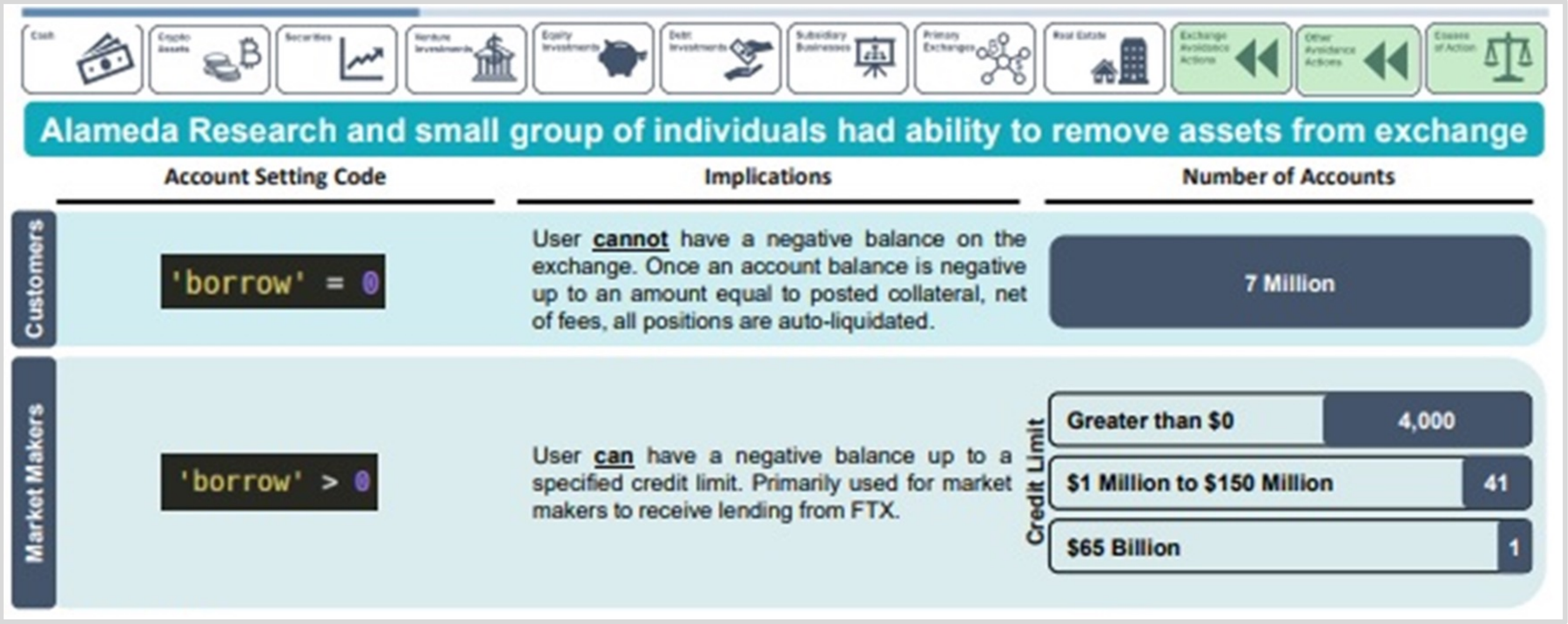
Auditor should verify if the crypto exchange has exclusive control over the Private Keys relating to on-chain crypto assets.

06

Compliance with ISA 805

Audit should comply with the requirements of ISA 805 (Revised) "Special Considerations – Audit of Single Financial Statements and Specific Elements, Accounts, or Items of a Financial Statement.

Risk Assessment: Crypto Shadow Banking


Cash
Crypto Assets
Securities
Venture Investments
Equity Investments
Debt Investments
Subsidiary Businesses
Primary Exchanges
Real Estate
Exchange Avoidance Actions
Other Avoidance Actions
Causes of Action

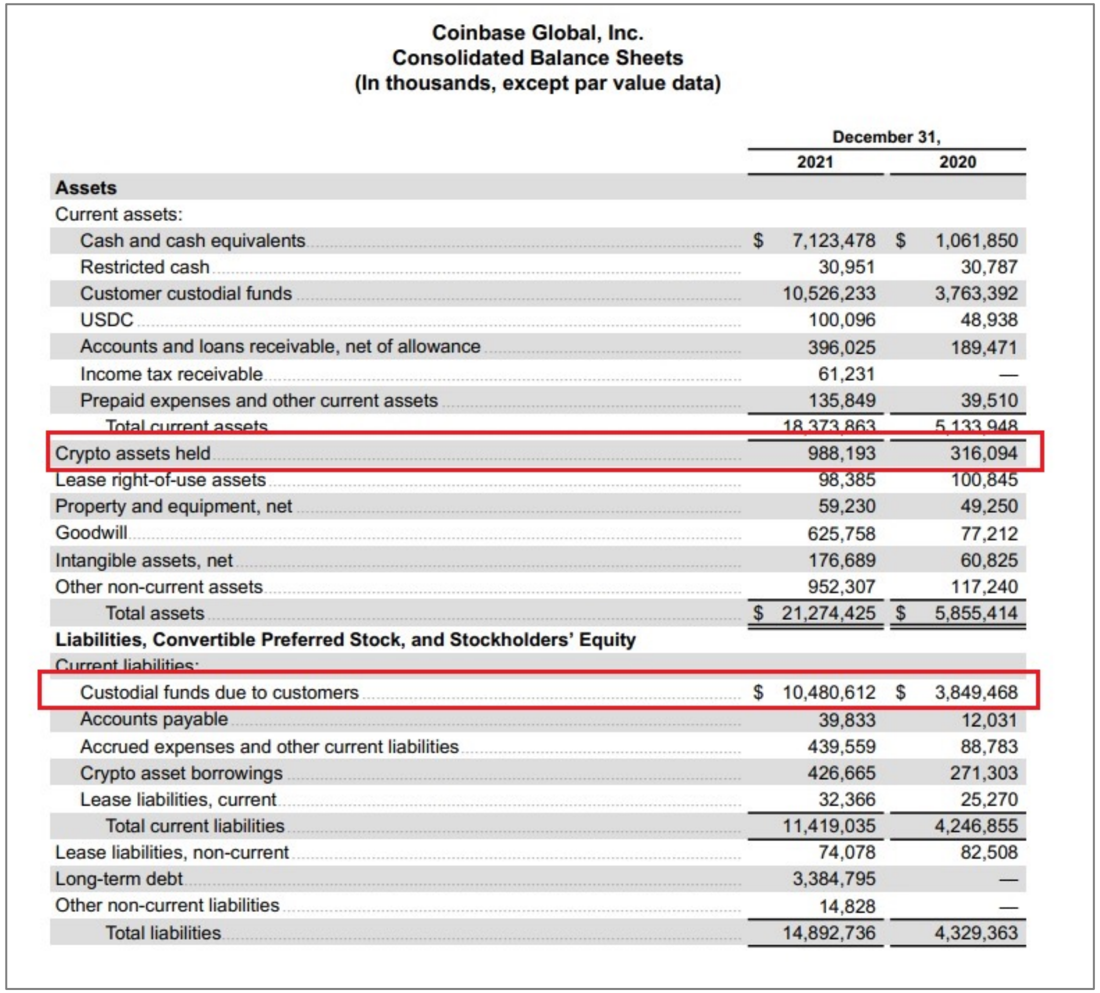
Alameda Research and small group of individuals had ability to remove assets from exchange

	Account Setting Code	Implications		Number of Accounts
Customers	`'borrow' = 0`	User **cannot** have a negative balance on the exchange. Once an account balance is negative up to an amount equal to posted collateral, net of fees, all positions are auto-liquidated.		7 Million
Market Makers	`'borrow' > 0`	User **can** have a negative balance up to a specified credit limit. Primarily used for market makers to receive lending from FTX.	Credit Limit	Greater than $0: 4,000 $1 Million to $150 Million: 41 $65 Billion: 1

Source: FTX Bankruptcy Case filings

- Crypto Industry's behind the curtain activity poses a huge challenge to the auditors.
- Bankruptcy documents of FTX provide an insight into the secretive activities of crypto world
- Among 7 million users of FTX, 41 were allowed to run into a negative balance up to 150 $ Mn and 1 was allowed a negative balance up to $65 Bn before the exchange would ask to settle the account.
- Such an exemption to some privileged users will put other customers funds at risk.

Audit of Financial Statement



Coinbase Global, Inc.
Consolidated Balance Sheets
(In thousands, except par value data)

	December 31,	
	2021	2020
Assets		
Current assets:		
Cash and cash equivalents	$ 7,123,478	$ 1,061,850
Restricted cash	30,951	30,787
Customer custodial funds	10,526,233	3,763,392
USDC	100,096	48,938
Accounts and loans receivable, net of allowance	396,025	189,471
Income tax receivable	61,231	—
Prepaid expenses and other current assets	135,849	39,510
Total current assets	18,373,863	5,133,948
Crypto assets held	988,193	316,094
Lease right-of-use assets	98,385	100,845
Property and equipment, net	59,230	49,250
Goodwill	625,758	77,212
Intangible assets, net	176,689	60,825
Other non-current assets	952,307	117,240
Total assets	$ 21,274,425	$ 5,855,414
Liabilities, Convertible Preferred Stock, and Stockholders' Equity		
Current liabilities:		
Custodial funds due to customers	$ 10,480,612	$ 3,849,468
Accounts payable	39,833	12,031
Accrued expenses and other current liabilities	439,559	88,783
Crypto asset borrowings	426,665	271,303
Lease liabilities, current	32,366	25,270
Total current liabilities	11,419,035	4,246,855
Lease liabilities, non-current	74,078	82,508
Long-term debt	3,384,795	—
Other non-current liabilities	14,828	—
Total liabilities	14,892,736	4,329,363

Proof of reserves is supposed to instill some added trust, but they aren't complete audits and don't necessarily provide a full picture of a company's financials, such as total liabilities (deposits) owed back to clients and other types of debt. Nor do they assess the quality of a crypto exchange's controls.

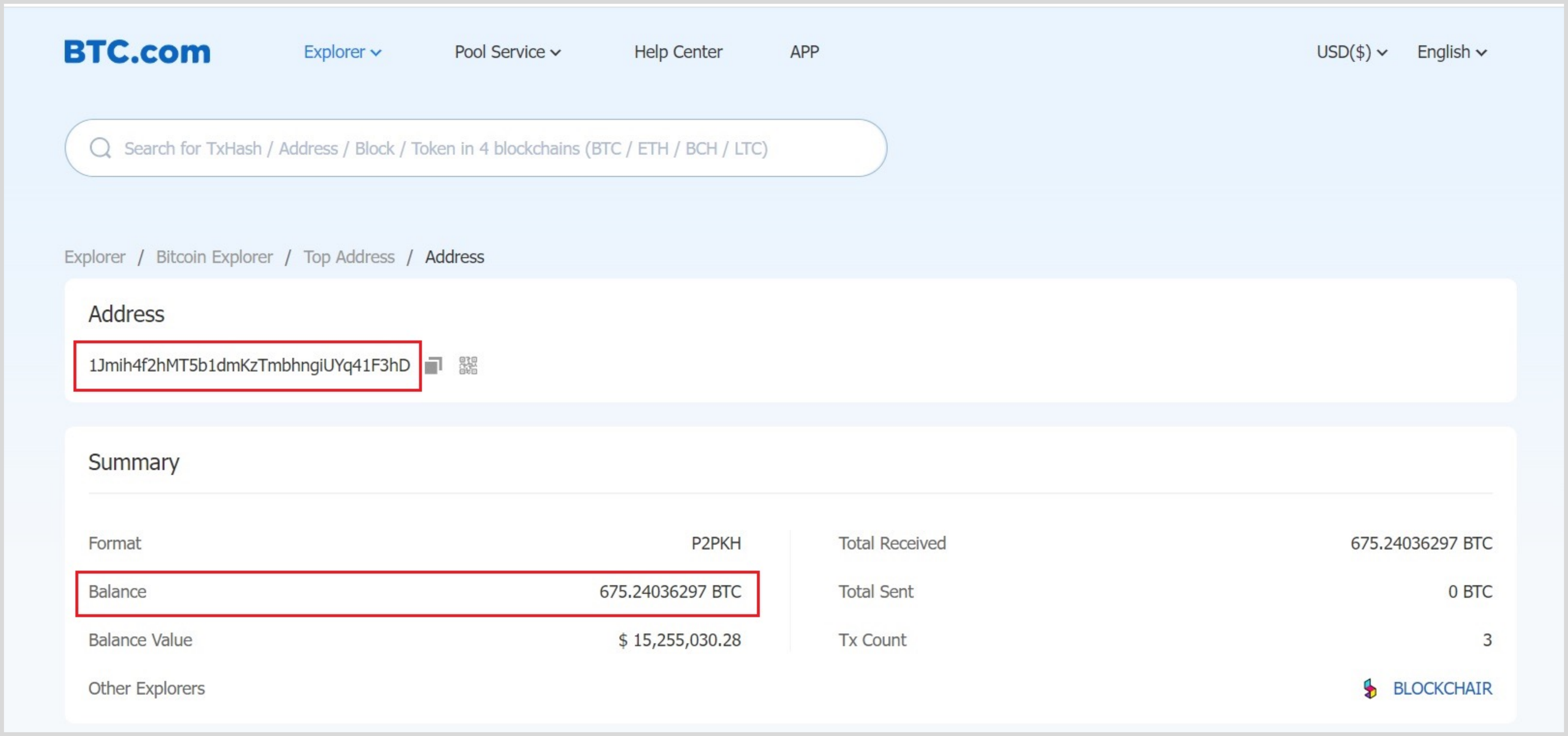
Preparing Financial Statement of Exchange would address many of the issues that were noticed in the recent reports on Proof of Reserves:-

- Financial position
- Liabilities other than customers liabilities
- Contingent liabilities
- Off-chain assets or real world assets
- Funds borrowed to boost Proof of Reserves

Verification of On-chain Assets

Coin	Public Address
1INCH	0x4cD3aa96836c133c9B9f27daFa7baF744D57404d
ATOM	0xceAE7673553c90d0a3cd1A494dA35eDe63910cBF
AVAX	0xD4997FF5b5DAA7638E9f20857c4D563BFBC97B18
AXS	0x758E2c2D1a362E2B3e613545e48285b03581EF43
BTC	1Jmih4f2hMT5b1dmKzTmbhngiUYq41F3hD

Wallet


BTC.com
Explorer
Pool Service
Help Center
APP
USD($)
English
Search for TxHash / Address / Block / Token in 4 blockchains (BTC / ETH / BCH / LTC)

Explorer / Bitcoin Explorer / Top Address / Address

Address

1Jmih4f2hMT5b1dmKzTmbhngiUYq41F3hD

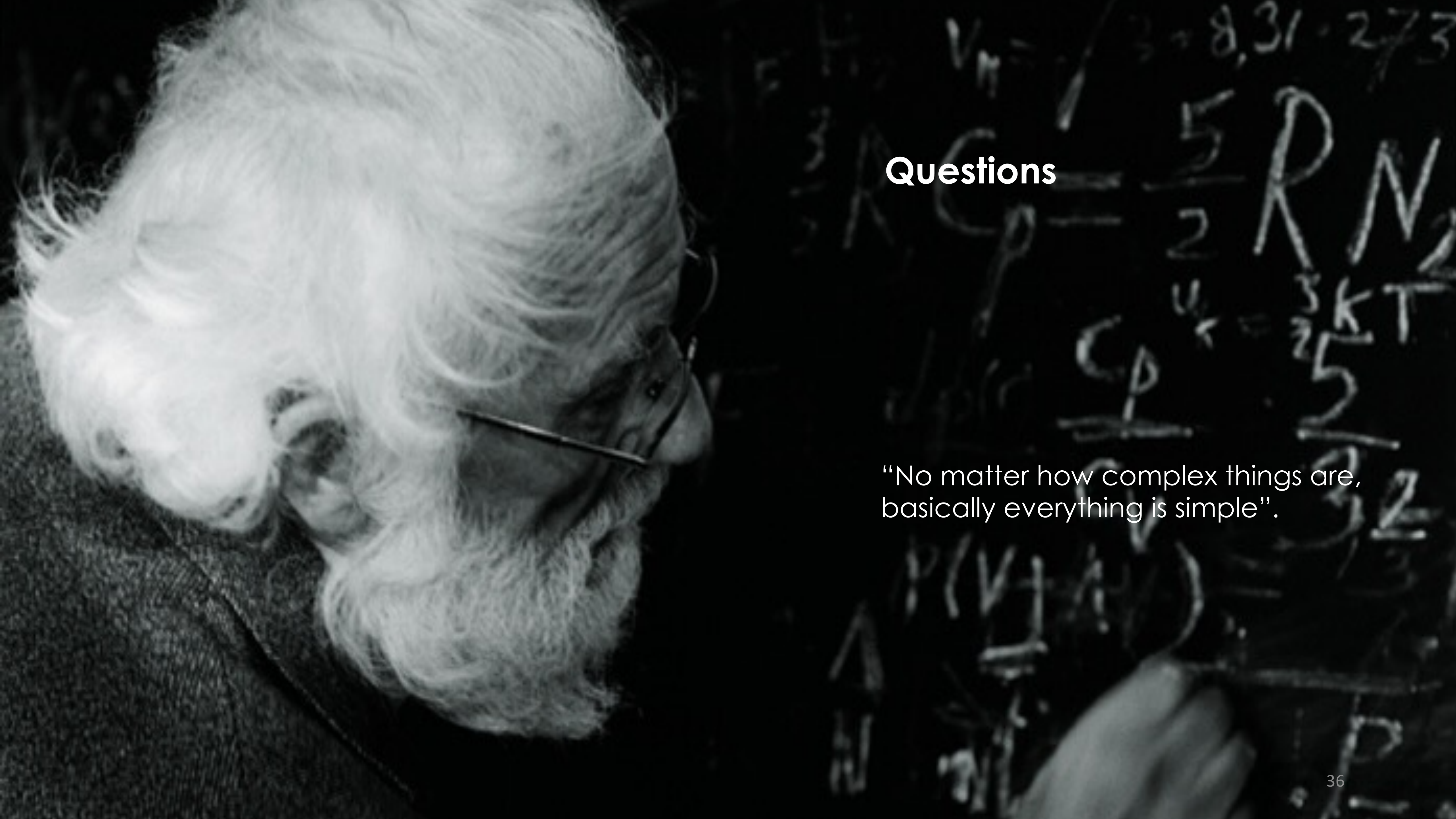
Summary

Format	P2PKH	Total Received	675.24036297 BTC
Balance	675.24036297 BTC	Total Sent	0 BTC
Balance Value	$ 15,255,030.28	Tx Count	3
Other Explorers			BLOCKCHAIR

Exclusive Control of Private Keys

One way to verify if the holder of crypto coins has exclusive control over Private Key is to ask the holder to sign a message using their Private Key. The holder can then provide the signed message, along with the public address associated with the Private Key, to a third party for verification. If the signature is valid and corresponds to the public address , it is likely that the holder has exclusive control over the Private Key.

It is important to note that a person can prove his control over the Private Key but it doesn’t mean that person is the true owner of the private key.



Questions

“No matter how complex things are,
basically everything is simple”.

THANK YOU

Vinod Kashyap

Email : vinod@ngdb.ai