CHAMBER OF DIGITAL COMMERCE

Proof of Reserves

The Practitioner's Guide to an Emerging Standard for Increasing Trust and Transparency in Digital Asset Platform Services

Chamber of Digital Commerce

The Chamber of Digital Commerce is the world`s largest trade association representing nearly 200 members in the digital asset and blockchain industry. Our mission is to promote the acceptance and use of digital assets and blockchain technologies. We are supported by a diverse membership that represents the industry globally, including the world`s leading innovators, operators, and investors in the digital asset and blockchain technology ecosystem. These businesses include leading edge start-ups, software companies, global IT consultancies, financial institutions, insurance companies, law firms, and investment firms Consequently, the Chamber and its members have a significant interest in the development of responsible laws to support blockchain technologies.

Proof of Reserves Initiative

The Proof of Reserves Initiative is an industry-led initiative of the Chamber of Digital Commerce, created to be a key resource for digital asset exchanges and custodians in enabling consumers to have reasonable expectations of their service providers and to have comfort that their digital assets are held in a manner consistent with industry norms. Comprised of more than 100 industry participants, the Initiative includes accounting, audit, and legal experts, technologists, capital markets professionals, former regulators, and practitioners from around the globe. The Proof of Reserves Initiative develops best practices for digital asset platforms to demonstrate adequate reserves of assets to another party through a form of proof.

Acknowledgments:

The Chamber of Digital Commerce would like to thank the following individuals and organizations for their valuable contributions to the production of this report.

Leadership:

NOAH BUXTON

Managing Director
Blockchain & Digital Assets
Practice Leader
Armanino LLP

NIC CARTER

Partner, **Castle Island Ventures** &
Co-Founder**, Coin Metrics**

AMY DAVINE KIM

Chief Policy Officer
Chamber of Digital Commerce

PATRICK SOUTH

Business Development
TRM Labs

SALVATORE TERNULLO

Co-lead, Cryptoasset Services
KPMG

Authors

SAM ABBASSI
Fidelity

MICHELLE CHOPPER
Cohen & Company

WILLIAM COLEMAN
Cohen & Company

OKIKI FAMUTIMI
KPMG

BRUCE TUPPER
CoinRegTech

SAM WYNER
KPMG

Contributers

MIKE CARTER
Bittrex

MICHAEL MARZELLI
Deloitte

JOSEPH MCGLAWN
ErisX

JEREMY NAU
Armanino

DONNA REDEL
Fordham Law School

JENNIFER SANDEFUR
Friedman LLP

JAY SCHULMAN
RSM

PETER TAYLOR
Deloitte

PETE TEIGEN
IBM

TYLER WALTON
Cohen & Company

Contents

I. Introduction

A. EXECUTIVE SUMMARY

As the use and acceptance of digital assets grows through statements and actions by publicly traded companies such as MicroStrategy Incorporated, Citi, Tesla, and others, the services provided for digital assets must evolve to meet them. Expectations of these service providers become more sophisticated as the ecosystem evolves and grows. While this evolution creates challenges in several sectors, the best practices outlined in this paper propose to solve the problem of proving that an entity holds digital assets sufficient to cover its outstanding liabilities, or Proof of Reserves.

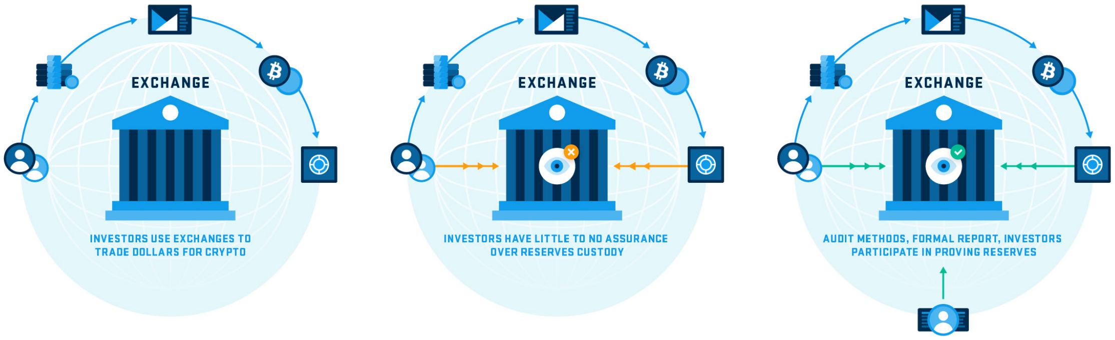
While several types of Proofs of Reserves exist, this paper focuses on Proof of Platform Reserves - a proposed solution for entities serving as digital asset exchanges or custodians. Some platforms currently offer forms of Proof of Reserves for their customers and regulators. To create a more harmonized approach, we believe a set of best practices is necessary to enable consumers to have reasonable expectations of their service providers and to have comfort that their digital assets are held in a manner consistent with industry norms. These best practices also provide trust, privacy, and transparency through good digital hygiene.

Broadly speaking, we propose that a Proof of Platform Reserves utilize blockchains' native cryptographic techniques in a way that can be confirmed individually and confidentially by each customer.

B. WHAT IS PROOF OF RESERVES

Proof of Reserves is a term of art for the digital asset[1] and blockchain industry; it is not a wholly new concept. It is merely a method used by an organization to demonstrate that it possesses adequate reserves of assets to another party through a form of proof. Proof of Reserves was originally conceived as a method for centralized digital asset exchanges and custodians (hereinafter, "digital asset platforms") to show users that they held enough bitcoin to meet all customer liabilities. Broadly speaking, proving reserves is a process whereby an organization provides information to engender trust regarding custodial digital asset holdings, whether for specific customers, the wider market, current or future partners, regulators, the digital asset platform's management, or some combination thereof. Said differently, the Proof of Reserves is a means of using cryptography to promote transparency and trust signals where a user, customer, or counterparty would rely on another party to hold digital assets on their behalf. In this technical guidance, the authors seek to lay the foundation for reaching consensus regarding "Proof of Reserves" as a term of art within the digital asset industry.

[1] "Digital asset" as it is used in this paper is defined as "an asset that resides on a distributed ledger."


EXCHANGE
INVESTORS USE EXCHANGES TO TRADE DOLLARS FOR CRYPTO
EXCHANGE
INVESTORS HAVE LITTLE TO NO ASSURANCE OVER RESERVES CUSTODY
EXCHANGE
AUDIT METHODS, FORMAL REPORT, INVESTORS PARTICIPATE IN PROVING RESERVES

For a number of reasons, not excluding the nascence of the industry, there appears to be a lack of clarity of the definition and best practices of Proof of Reserves for digital asset market participants. The demand by customers for more assurance over digital asset reserves is no longer an undercurrent, it is overt. Customer demand is driving digital asset platforms to ask professional service firms to address the demand.

While there are parallels to existing finance industry standards, practices, and norms, in today's multi-faceted marketplace for digital assets, we notice a number of key differences that result in the need for differing terminologies and best practices:

i. **Digital asset infrastructure is evolving:** Users, investors, and holders of digital assets are not currently afforded the same level of regulatory clarity, competitive choice, transparency, and audit standards for specialized industries available in traditional fiat banking and financial markets.

ii. **Customers have differing expectations regarding reserves:** Users of digital asset platforms generally expect their assets to be fully reserved (an asset for each corresponding liability), meanwhile service agreements may not address these reserve commitment expectations.

iii. **The potentially bearer-like nature of digital assets is unique:** Lost or misappropriated private keys/assets are not as easily replaced to make victims of loss or fraud whole.

iv. **The lack of widely available insurance for on-platform digital asset balances amplifies counterparty risks:** Customers, in limited cases, benefit from insurance for on-platform digital asset balances, but this is not currently widely available.

v. **The global nature of the industry means the use and trade of digital assets is borderless:** Customers often rely on counterparties (*i.e.,* exchanges and custodians, stablecoin issuers, and decentralized protocols) that are outside their local geography and may be subject to differing regulatory obligations.

C. A FRAMEWORK FOR UNDERSTANDING VALIDATION OF RESERVE ASSETS IN DIGITAL ASSET USE CASES

While it is undoubtedly true that there are no bright-line rules defining "Proof of Reserves" in the digital asset space today, we can enumerate the myriad of current and future scenarios in which some level of assurance over digital asset reserves would be useful. Market participants' expectations of transparency will carry over into digital assets and, as a result, interest in applications of Proof of Reserves will grow over time. Therefore, the authors propose a framework outlining Proof of Reserves scenarios, as well as a taxonomy of relevant terms applicable to each scenario, to provide enduring value to market participants, regulators, and professional service providers.

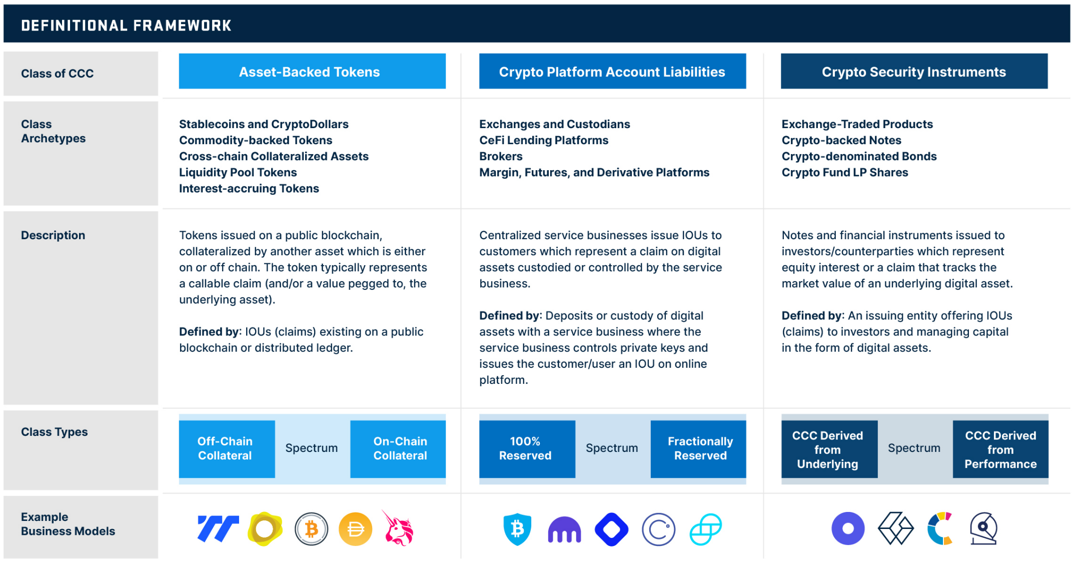
The framework presented below is intended to be broad and flexible enough to capture the "universe" of Proof of Reserves scenarios. While the taxonomy presented will inevitably be both open to interpretation and, ultimately, market-determined, an initial taxonomy is needed now. Currently, market participants and platforms are using the terminology "Proof of Reserves" too loosely for the ecosystem to determine what weight and meaning they should assign to such an offer of proof. Therefore, the conclusions that customers are able to reasonably draw from reviewing a service provider's Proof of Reserves should be based on the nature of the business activity and in the context of broader disclosures for financial statements.

The framework below is primarily anchored by the consideration of the type of user liability created when a custodial relationship is entered into by two (or more) parties. The type, or "class," of liability, herein called **"Crypto Collateralized Claim'' ("CCC")** allows one a meaningful starting point to determine (1) the character of the asset reserves/collateral that users would require assurance over *(i.e.,* a digital asset, commodity, fiat, or some mix thereof); (2) what specific Proof of Reserves procedures would be useful and reasonably reliable for consumers; and (3) suggested terminology/taxonomy that can be utilized to distinguish between different approaches to proving reserves.

1. Three-Pronged Model

The three-pronged model depicted below draws upon current Crypto Collateralized Claims offered by both centralized and decentralized organizations in the market today. For use cases that one believes fall outside of this framework and the resulting taxonomy, the spirit of the framework should guide the reader to consider the procedures and forms of proof that would be adequate given the learnings herein for asset-backed tokens, crypto platform account liabilities, and cryptocurrency security instruments.

COLLATERALIZED CRYPTO CLAIM (CCC) FRAMEWORK & TAXONOMY



DEFINITIONAL FRAMEWORK

Class of CCC	Asset-Backed Tokens	Crypto Platform Account Liabilities	Crypto Security Instruments
Class Archetypes	Stablecoins and CryptoDollars Commodity-backed Tokens Cross-chain Collateralized Assets Liquidity Pool Tokens Interest-accruing Tokens	Exchanges and Custodians CeFi Lending Platforms Brokers Margin, Futures, and Derivative Platforms	Exchange-Traded Products Crypto-backed Notes Crypto-denominated Bonds Crypto Fund LP Shares
Description	Tokens issued on a public blockchain, collateralized by another asset which is either on or off chain. The token typically represents a callable claim (and/or a value pegged to, the underlying asset). **Defined by:** IOUs (claims) existing on a public blockchain or distributed ledger.	Centralized service businesses issue IOUs to customers which represent a claim on digital assets custodied or controlled by the service business. **Defined by:** Deposits or custody of digital assets with a service business where the service business controls private keys and issues the customer/user an IOU on online platform.	Notes and financial instruments issued to investors/counterparties which represent equity interest or a claim that tracks the market value of an underlying digital asset. **Defined by:** An issuing entity offering IOUs (claims) to investors and managing capital in the form of digital assets.
Class Types	Off-Chain Collateral Spectrum On-Chain Collateral	100% Reserved Spectrum Fractionally Reserved	CCC Derived from Underlying Spectrum CCC Derived from Performance
Example Business Models			

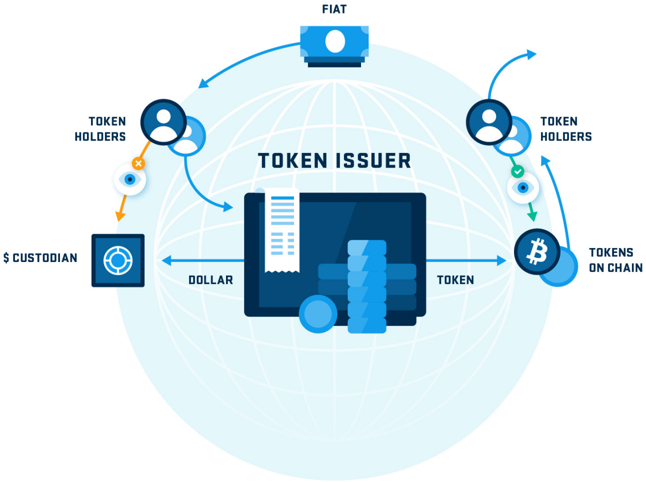
PROPOSED TAXONOMY FOR PROOF OF RESERVES USE CASES

Class of CCC	Asset-Backed Tokens	Crypto Platform Account Liabilities	Crypto Security Instruments
Specific Proof of Reserves Terminology	"Proof of Collateral Reserves" (PoCR)	"Proof of Platform Reserves" (PoPR) Focus of this Guidance Document	"Proof of Instrument Reserves" (PoIR)
Generic Terminology	"Proof of Reserves"		

2. Illustrative Use Cases for the Three-Pronged Model

For illustration, a use case for each class of CCC is presented below. This list is not exhaustive.

- In the case of a **centralized, fiat-backed stablecoin** issuer, the class of liability created is an **asset-backed token**, pegged to the value of the underlying fiat, and with at least 1:1 reserve of fiat to maintain redeemability. Therefore, the character of the asset to be reserved is fiat dollars; the purpose of Proof of Reserve procedures is to prove fiat account balances are in excess of circulating tokens; and the suggested terminology for such an offer of proof is "Proof of Collateral Reserves."[2]



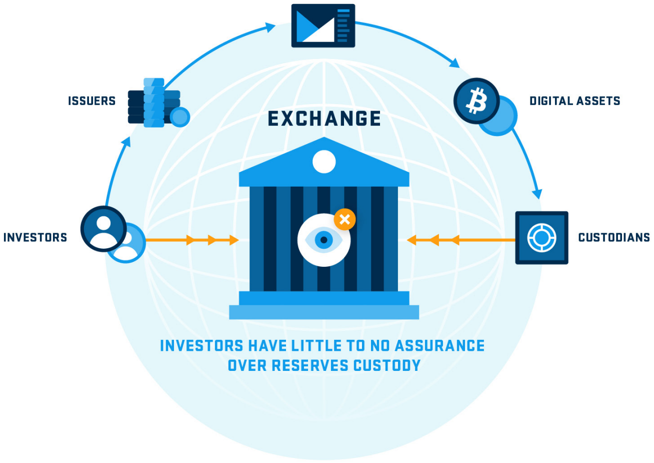
- In the case of a **decentralized, cryptocurrency-backed stablecoin**, the class of liability created is an **asset-backed token**, pegged by different means to the value of a chosen fiat, with an elastic and/or variable supply of cryptocurrency collateral/reserves. Therefore, the character of the asset to be reserved is a cryptocurrency or second token; the purpose of relevant procedures is to prove that on-chain collateral retains greater value than the

[2] Examples include USDC and USDT.

- liability, *i.e.*, the stablecoin, created; and the suggested terminology for such an offer of proof is “Proof of Collateral Reserves” (“PoCR”).[3]

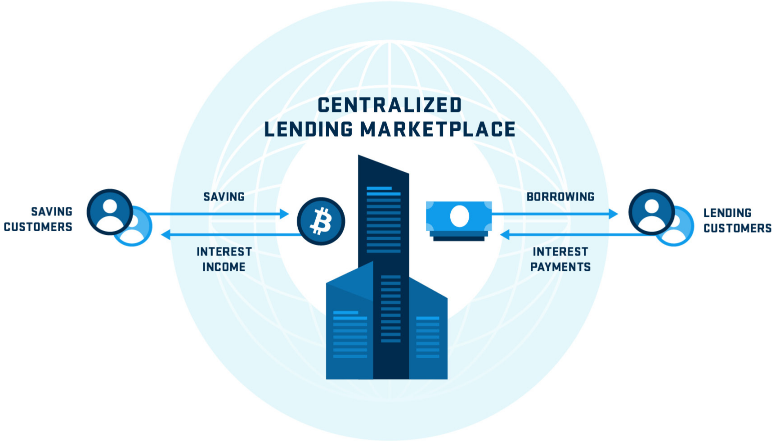
**Note: non-asset backed algorithmic stablecoins are not addressed in this model since there is no collateral position and, therefore, does not require Proof of Reserves.*

- In the case of a user’s **bitcoin holdings with a digital asset platform**, the class of liability created is a **Crypto Platform Account Liability**, where the digital asset platform or service provider holds digital assets on the customer’s behalf in an amount equal to the customer’s on-platform account balance. Therefore, the character of the asset to be reserved is a cryptocurrency or digital asset; the relevant procedures are, generally, to prove both the total platform liabilities and the reserved digital assets; and, the suggested terminology for such an offer of proof is “Proof of Platform Reserves” (“PoPR”).



- In the case of a user’s **bitcoin holdings with a centralized digital asset lending business**, the class of liability created is a **Crypto Platform Account Liability**, where the digital asset platforms or service provider holds digital assets and loan note receivables on the customer’s behalf in an amount equal to or greater than the customer’s on platform account balance. Therefore, the character of the assets to be reserved is both cryptocurrency/digital asset and loan note receivables; the relevant procedures are, generally, to prove both the total platform liabilities and the reserved digital assets, synthetics and notes; and, the suggested terminology for such an offer of proof is PoPR.

[3] For instance, on the Maker Protocol, users may lock up different cryptocurrencies like ETH or UNI in a Maker Vault and generate DAI, a stablecoin, against the value of those assets up to a given collateralization ratio. Users may always verify their reserves looking up by their Vault number on public user interfaces, such as Oasis.app/borrow or Defiexplore.



- In the case of an **exchange-traded product**, for example, the class of liability created is a **Cryptocurrency Security Instrument**, where the note issuer holds digital assets and/or other financial instruments to collateralize or hedge the total value of notes outstanding. Therefore, the character of the asset to be reserved is a cryptocurrency or digital asset (and potential other financial instruments allowed by the issuer's prospectus); the relevant procedures are, generally, to prove both the total number and value of notes outstanding and the reserved digital assets; and, the suggested terminology for such an offer of proof is "Proof of Instrument Reserves" ("PoIR").

D. WHY PROOF OF RESERVES IS IMPORTANT FOR THE INDUSTRY

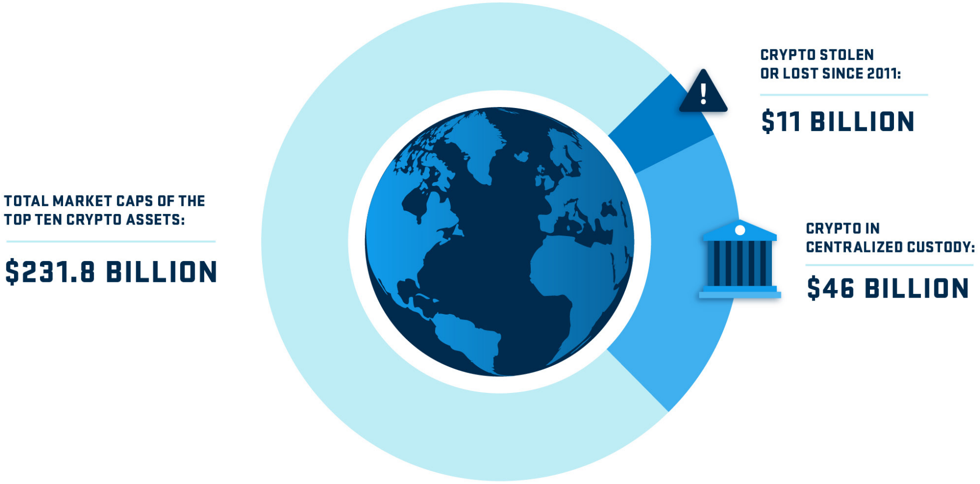
Proof of Reserves is important for all constituents and participants in the digital asset ecosystem. Distilled down, perhaps the most important reason is the creation of norms, guidelines, and standards where such maturity is needed. Norms and standards for proving digital asset reserves across global markets will offer users much-needed transparency, allow users to better assess risk, weed out bad actors, demonstrate the ability to self-regulate, and also address the systemic risks that would threaten further adoption of, and innovation using, digital assets.

Over the past five years we have seen consistent themes from global regulators aiming to develop policies that foster innovation while protecting market integrity and investors. The scale and scope of change that public blockchains present offers many complexities in the interpretation and advancement of regulatory structures, but also presents opportunities to utilize the value attributes of the technology to transform current norms of risk management, audit execution, and regulatory oversight. PoPR is an exciting embodiment of this opportunity where organizations leverage the immutability of a public blockchain and native cryptographic mechanisms to provide proof of existence and control of digital assets held by centralized organizations on behalf of their customers.

PoPR is an exciting embodiment of this opportunity where organizations leverage the immutability of a public blockchain and native cryptographic mechanisms to provide proof of existence and control of digital assets held by centralized organizations on behalf of their customers.

As the overall size of the digital assets space grows, both in market capitalization and number of organized participants and consumers, potential cascading risks have emerged.

Reinforced by persistent cyber-attacks and thefts from digital asset platforms resulting in the loss of customer funds, a narrative of self-regulation to address this risk is gaining attention. At current asset valuations, more than $10B[4] digital assets and tokens have been compromised by malicious actors,[5] with limited success in attempts to recover them.[6] The frequency and gravity of these events have placed a global regulatory spotlight on the unique risks that digital assets present given their nature as digital bearer-style instruments native to decentralized networks. This spotlight has manifested into evolving regulations across the world with custody and safekeeping of assets garnering ubiquitous enhanced consideration.



Retail investor sentiment has heightened in intensity alongside increased engagement from institutions, best reflected by major treasury investments from private[7] and public corporations.[8] The nature of institutional compliance and risk management requirements and expectations are a force for positive change. As one example, sophisticated investors and institutional customers have driven digital asset platforms to pursue formal attestations – an independent CPA auditor's reporting on an examination of controls at a service organization relevant to user entities' internal control of financial reporting (SOC 1[9]) or relevant to Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy[10] (SOC 2[11]) – performed under the AICPA's attestation standards (may

[4] Based on valuations calculated in November of 2020. Matthew Leising, *Halting $9.8 Billion in Theft Is Key to Crypto Growth, KPMG Says,* Bloomberg (Mar. 2, 2020), https://www.bloomberg.com/news/articles/2020-03-02/halting-9-8-billion-in-crypto-theft-key-to-growth-kpmg-says.

[5] KPMG US, Cracking Crypto Custody (Mar. 2, 2020), https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/kpmg-cracking-crypto-currency.pdf.

[6] Brian Barrett, *Hack Brief: Hackers Stole $40 Million from Binance Cryptocurrency Exchange,* Wired (May 8, 2019), https://www.wired.com/story/hack-binance-cryptocurrency-exchange/.

[7] Microstrategy, *MicroStrategy Adopts Bitcoin as Primary Treasury Reserve Asset,* Businesswire (Aug. 11, 2020), https://www.businesswire.com/news/home/20200811005331/en/MicroStrategy-Adopts-Bitcoin-as-Primary-Treasury-Reserve-Asset.

[8] Square, *Square, Inc. Invests $50 Million in Bitcoin* (Oct. 8, 2020), https://squareup.com/us/en/press/2020-bitcoin-investment.

[9] Ass'n of Int'l Certified Prof'l Accountants, *SOC 1® - SOC for Service Organizations: ICFR,* https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report.htm (last visited Mar. 23, 2021).

[10] Ass'n of Int'l Certified Prof'l Accountants, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (TSP Section 100)(Includes March 2020 updates)), https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf.

[11] Ass'n of Int'l Certified Prof'l Accountants, *SOC 2® - SOC for Service Organizations: Trust Services Criteria,* https://www.aicpa.org/

include International Standards on Assurance Engagements). Third-party assurance reporting over the internal control environments for financial reporting and IT systems at digital asset platforms provide a high level of assurance for users; however, depending on the scope of these reports, they may or may not prove reserves of the digital asset platform against customer liabilities at a given point in time. Users of a SOC report will need to determine if the report addresses the concerns of the user based on their assessment of the risks associated with the activity for which they have engaged the third party. And, while the filing of audited financial statements with regulators has also become more commonplace in the United States and abroad, those annual reports are (1) not available to customers, even large institutional customers; and (2) so infrequent as to be of limited value in assessing the narrow question of whether a digital asset platform is properly reserving digital assets against customer's on-platform liabilities.

With this backdrop, PoPR has been elevated as an exciting opportunity to utilize blockchain's tamper-resistant and native cryptographic functions to provide enhanced transparency to customers. What's more, with this paper as a starting point for further awareness and standardization, we can see an important connective tissue of trust emerge. Indeed, the methods, processes, and tools used to perform PoPR present foundations and learnings that can be leveraged by regulators, investors and partners in mainstream payments and finance to foster safe adoption.

II. Key Drivers for the Need of Proof of Reserves Guidelines

A. TRUST & TRANSPARENCY FOR CONSUMERS, MARKETS, AND REGULATORS

Digital assets have grown significantly by all measures since the release of Satoshi Nakamoto's landmark Bitcoin white paper, both in the total number of tokens/instruments in circulation as well as total market capitalization.[12] While regulators in different jurisdictions have taken different approaches to policy concerns, it is generally true that there remains skepticism or lack of trust which hinders further investment and innovation. The innovative power of public blockchain projects to date is staggering: the ability to establish monetary supply by code (*i.e.,* bitcoin); stablecoins' impact on cross-border payments, and the prospect of issuing legal tender currency on a blockchain. However, in almost all cases, current financial products residing on public blockchains lack the trust extended to legacy financial products. Digital assets are touted for their transparency and auditability, and public blockchains offer paradigm-shifting levels of transparency, but centralized parties' databases obfuscate customer balances and transfers. As a result, one can see transactions from a given bitcoin wallet, but one cannot see the databases of the centralized digital asset platforms to verify that all customer balances maintained by those platforms are represented in the wallet addresses presented.

The need to prove that a centralized party in fact maintains control over an asset held in reserves is becoming more mainstream. For example, the Office of the Comptroller of the Currency ("OCC")

interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html (last visited Mar. 23, 2021).

[12] Satoshi Nakamoto, *A Peer-to-Peer Electronic Cash System*, bitcoin.org (Oct. 31, 2008), https://bitcoin.org/bitcoin.pdf.

recently issued interpretive guidance for national banks providing cryptocurrency custody services[13] and payment activities.[14] The European Central Bank ("ECB") issued a white paper addressing the appropriate regulation and oversight of stablecoins, seeking to assess stablecoins and the underlying reserves based on three scenarios: (i) as a digital asset function; (ii) as a new payment method; and (iii) as an alternative store of value.[15] The Financial Stability Board ("FSB") and the Bank for International Settlements ("BIS") issued recommendations and potential regulatory frameworks for stablecoins.[16] Lastly, the Commodity Futures Trading Commission ("CFTC") issued guidelines to futures commission merchants ("FCMs") regarding the holding of virtual currency in segregated accounts of customers.[17] This guidance was necessitated by the growing open interest in the bitcoin futures and options contracts. These regulators expect the reserves of digital assets to meet applicable regulatory standards and address financial stability measures.

In sum, standards, methods, and awareness regarding the proving of reserves would be additive across a number of uses. PoPR, if more widely adopted, could be the most important component of trust transparency and investor protection in digital assets seen to date.

B. AUDITABILITY

Blockchains offer tamper resistance, decentralized trust, and auditability. However, blind spots may form around digital asset platforms because, as centralized intermediaries, many transactions and account balances are not committed to a public blockchain. Instead, the record of these transactions is only held in proprietary databases of these central service providers ("off-chain transactions"). It is common practice for digital asset platforms to hold customer assets in co-mingled wallets (*i.e.,* omnibus accounts/wallets) which are not publicly auditable by customers. Therefore, the promise of publicly available transactional data and auditable ledgers can be hampered due to the digital asset platforms' use of off-chain transactions and co-mingled wallets.

Digital asset platforms in the United States are required to submit audited financial statements to state regulators in order to maintain their state money transmission licenses. These audits are performed by independent CPA auditors to provide reasonable assurance in the form of an opinion that the financial statements present fairly, in all material respects, the financial position of the company and the results of its operations and its cash flows in accordance with generally accepted accounting principles. The independent CPA auditor's written opinion provides a layer of trust and independent oversight. However, the financial statements may not be publicly available or sufficient for customer protection

[13] OCC, Interpretive Letter 1170, *Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers* (July 22, 2020), https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf.

[14] OCC, Interpretive Letter 1174, *OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities* (Jan. 4, 2021), https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf.

[15] European Central Bank, Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision (Sept. 2020), https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247-fe3df92991.en.pdf.

[16] Fin. Stability Board, Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements (Oct. 2020), https://www.fsb.org/wp-content/uploads/P131020-3.pdf; and Douglas Arner, Raphael Auer, and Jon Frost, Stablecoins: risks, potential and regulation, Bank for Int'l Settlements (Nov. 2020), https://www.bis.org/publ/work905.pdf.

[17] Commodity Futures Trading Comm'n, *CFTC Staff Issues Advisory on Virtual Currency for Futures Commission Merchants* (Oct. 21, 2020), https://www.cftc.gov/PressRoom/PressReleases/8291-20.

purposes when considering reserve of digital assets against customer funds liabilities.

The principles contained in this paper seek to address this deficiency by prescribing methods and procedures which can inform standards – PoPR.

C. FRAUD DETERRENCE

A Proof of Reserves standard, viewable publicly, can prevent untrustworthy activities like holding partial reserves or not disclosing a loss of reserves. Furthermore, digital asset platforms and custodians, just like all centralized platforms, are "honey pots" for hackers. A standard audit practice would help to deter and may reveal with a reasonable assurance any such loss of reserves.

D. CUSTOMER PROTECTIONS

In the United States, the money transmitter licensing regime across the states and territories presents a wide array of compliance requirements designed in major part to provide protections for consumers in that state. State regulators generally require money services businesses ("MSBs") to adhere to certain customer protections (*i.e.,* maintain certain capital reserves and attain audited financials on an annual basis). In addition, New York has both a money transmitter licensing statute as well as a virtual currency business activity license, or "BitLicense," that adapts the money transmitter requirements to service providers that support virtual currency business activity.[18] Wyoming has gone further and developed a Special Purpose Depository Institution, state chartered banks that receive deposits and conduct other incidental activities, including fiduciary asset management, custody, and related activities, for digital assets. While these regimes have been helpful in building a regulatory framework for digital asset service providers, the industry could leverage technological solutions to effectively enhance their consumer protections, such as work towards a self-regulatory norm of proving reserves using PoPR, strengthening consumer trust in virtual assets.

E. COUNTERPARTY RISK

Counterparty risk is the likelihood a party to a transaction may not fulfill all of its obligations or default on the tradable instrument. To address counterparty risks, there is a bustling industry of risk assessment services and vendor management providers that is mostly unseen by retail investors. Publicly traded companies, investment funds, family offices, and private companies all engage in some level of counterparty risk assessment and management. These assessments include trading compliance reports, security questionnaires, independent inspections, and consulting reports. As one example, standard trading agreements (*i.e.,* ISDA Master Trading Agreement) contain legal provisions that address various counterparty risks and have been upheld by the courts.

Counterparty risk management is beginning to make its way into digital assets and the management

[18] Note that the Bitlicense requirements contemplate a 100% reserve requirement for digital assets, *"(b) To the extent a licensee stores, holds, or maintains custody or control of virtual currency on behalf of another person, such licensee shall hold virtual currency of the same type and amount as that which is owed or obligated to such other person. See* N.Y. Comp. Codes R. & Regs. tit. 23 §200.9(b) (2020).

of reserve funds. An impediment to established funds and fiduciaries allocating capital into digital assets or related businesses has been the lack of reporting standards – namely, reliable information that a large fund would need from a digital asset platform. PoPR provides a starting point for shared methods that can be relied on by all types of counterparties as they assess counterparty risk in exchange and custody of digital assets.

F. NON-STANDARDIZED APPROACHES

As of May 2021, only a handful of examples of digital asset platforms complete a proof-of-reserves-like exercise. Among these, there is a vast disparity in the methods and approaches utilized, the level of transparency provided, and the independence of the party performing the testing. One of the first publicly available proof of reserves assessments performed by an independent public accounting firm with a formal report on findings (based on standards for attest engagements issued by the AICPA) took place in 2020, over a decade after the creation of Bitcoin.

Other market participants have attempted to address users' requests for transparency, including transparency dashboards and periodic reporting. Additionally, Chainlink, a leading oracle network provider, recently announced a "proof of reserves reference contract" which could be utilized to bring proof of reserves data on chain for use by smart contracts. Early examples include the Wrapped Bitcoin project providing the total supply of bitcoin held by BitGo and reserving the wBTC Ethereum tokens, and Trust Token's offering a data feed for the total supply of U.S. Dollars held to collateralize the circulating supply of their TrueUSD stablecoin tokens across multiple public blockchains. All in all, the terminology – proof of reserves – is starting to see interest and application to multiple custody scenarios. Without a framework of understanding, and a market-recognized taxonomy to describe proof of reserves, consumers will continue to experience non-standard approaches.

III. Background

A. UNDER THE HOOD: CUSTODY, AND EXCHANGE OF DIGITAL ASSETS

Different varieties of service providers exist in the digital assets ecosystem. Their differences are worth briefly bearing out.

The first class of entities is referred to as centralized exchanges. These are institutions that facilitate the indirect trading of digital assets, provide access directly to digital assets with a single orderbook, or offer custody solutions. Some exchanges even manage p2p lending markets or provide prime services and other concierge services like OTC trading. Many of these exchanges are vertically integrated and conjoin the functions that would be disaggregated in traditional capital markets. Many users choose to store their digital assets with exchanges. Thus, the term "exchange" can be a misnomer – these firms not only manage trading but also handle retail-facing client services and custody. Proof of Reserves is extremely salient for these institutions in particular, as many are regulated as money transmitters in the U.S. and these regulatory agendas do not treat them as the equivalent of crypto banks.

The second class of entities in this category is dedicated custodians. Some exchanges have begun to outsource this function, kicking off an unbundling and a specialization that accompanies the maturation of the market. These custodians focus solely on safeguarding customer assets. Unlike commercial banks, this is not a depository engagement, as the custodians are not lending out the assets and earning a spread. Instead, they pursue a fee-based model, or treat custody as a loss-leader.

Third, a number of digital asset service providers have begun to obtain limited-purpose bank charters at both the state level and the federal level, blurring the lines between crypto-native institutions and the world of regulated deposit-taking. Crypto firms Avanti and Kraken Financial have both received Special Purpose Depository Institution charters from the State of Wyoming, permitting them to hold cryptoassets and fiat currency on a full-reserve basis on behalf of clients, while the Office of the Comptroller of the Currency granted the crypto custodian Anchorage Digital Bank a national trust bank charter. In both cases, these charters are more narrow than standard bank charters.

Dedicated centralized lenders make up the fourth class. Both retail and institutional-facing lenders exist. The business model involves taking custody of digital assets and lending them out to firms that need crypto-native liquidity, like arbitrage firms, market makers, or proprietary trading firms. These lenders also may seek a yield on various internal trading strategies like popular futures basis trade, or by putting capital to work in decentralized finance strategies. The lenders earn the difference between the interest rate that they charge borrowers, and the interest rate paid out to customers. These lenders will typically hold a fraction of funds in reserve for liquidity purposes.

Lastly, a variety of protocols exist in the fifth class, decentralized finance, which are sometimes referred to as 'lending' protocols. These systems facilitate the pooling of liquidity such that users can engage in overcollateralized borrowing. Automated risk management prevents the pools from taking a loss when the value of the collateral falls. Users can earn a return by providing liquidity to these pools, but they aren't engaging in lending in the traditional sense. Unlike the centralized lenders listed above, users can withdraw their liquidity at any time without causing a liquidity crisis.

It's worth noting that these categories are not mutually exclusive. Certain service providers facilitate custody, exchange, and brokerage, and interoperate with decentralized finance protocols, while others occupy a single vertical. Increasingly, the trend is towards specialization as the service provider landscape matures.

B. A SHORT CHRONOLOGY OF COMPROMISES EXPERIENCED BY DIGITAL ASSET PLATFORMS

The rise of digital assets has presented new challenges to security and safekeeping of digital assets, as well as opportunities. The finality of transactions on public blockchains presents new and unique risks that must be managed through defense-in-depth approaches to cybersecurity. The reality of these risks has been highlighted by a series of asset compromises from digital asset platforms. This is a core driver behind the need for enhanced transparency in a "trust, but verify" model presented in Proof of Reserves. Below is a table containing a list of a number of digital asset platform compromises within the last 10 years:[19]

Date	Platform	Value (Crypto)[20]	At-time Value (USD)[21]	Current Value (USD, as of Dec. 31, 2020)
2011-2014	Mt. Gox	850,000 BTC	$680,000,000+	$15,450,858,000
2012	Bitfloor	24,000 BTC	$250,000	$436,259,520
2014	Poloniex	97 BTC	$116,000	$1,763,216
2014	Cryptsy	13,000 BTC 300,000 LTC	$9,500,000	$260,079,240
2014	Bitstamp	19,000 BTC	$5,200,000	$345,372,120
2016	Bitfinex	120,000 BTC	$66,000,000	$2,181,297,600
2016	DAO	3,600,000 Ether	$70,000,000	$2,072,736,000
2018	BitGrail	17,000,000 Nano	$195,000,000	$19,890,000
2018	Coincheck	523,000,000 NEM	$500,000,000	$93,078,310
2018	Bithumb	Not Disclosed	$31,000,000	N/A
2019	Binance	7,000 BTC	$40,000,000	$127,242,360
2020	Lendf.me/ dForce	57,992 ETH 581 BTC (via imBTC, WBTC, HBTC) 425 MKR 5,178 LINK 39,968 KNC 110,383 BAT 1,817 HT 38,180 LEND $9.46 Million USD in Stablecoins	$25,000,000	$37,069,356
2020	KuCoin	1,008 BTC 11,543 ETH 19,834,042 USDT-ETH 18,495,795 XRP 26,733 LTC 999,160 USDT $147 Million USD in ERC20 tokens $87 Million USD in Stellar Tokens	$275 Million+	$210 Million+

As displayed above, billions of U.S. dollars in value were extracted from exchanges, with the most notable being Mt. Gox seven years ago. Because there was no consistent procedure at that early stage in the industry where Mt. Gox checked their on-chain holdings against customer balances to ensure that they held full reserves, the public did not know that the exchange had been compromised. Additionally, monitoring, alerting, and auditing tools can perform these checks consistently and inform management of the unauthorized access or unauthorized withdrawal. This would result in either preventing or mitigating the reputational and operational damage of having large amounts of funds

[19] The Chamber of Digital Commerce and Microsoft found that these breaches are human driven, *i.e.,* errors in the code or malicious actors using phishing scams, etc. Chamber of Digital Commerce, Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry (Mar. 2018), https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2018/03/Blockchain-Cyber-Security_WhitePaper_Single-Page_Linked.pdf.

[20] Coinmarketcap, Historical Snapshot - 29 November 2020 (Nov, 29, 2020), https://coinmarketcap.com/historical/20201129/.

[21] *Id.*

withdrawn maliciously. Proof of Reserves helps mitigate potential risk and loss of consumer funds.

C. SIMILAR BUT DIFFERENT: PROOF OF SOLVENCY AND PROOF OF RESERVES

Proof of Solvency involves company liabilities that would exist outside of a distributed ledger and ultimately its ability to operate as a going concern in the future. By contrast, Proof of Reserves refers to the existence of digital assets at a given point in time and does not include all assets or liabilities to which a business may be subject.

Moreover, this paper contemplates that a PoPR can be performed by a third-party consultant, or an independent certified public accountant. Attestation standards promulgated by AICPA specifically prohibit attestations related to matters of solvency.[22]

Therefore, PoPR should be offered to provide users assurance regarding the reserve of customer digital assets, not the overall financial health of the digital asset platform provider.

D. THEORY AND PUBLICATIONS ON PROOF OF RESERVES

Within the Bitcoin sector, an admission of the inevitability of re-intermediation has existed since the earliest days of the protocol. Famously, Bitcoin pioneer Hal Finney, recipient of the first Bitcoin transaction, laid out his vision in December 2010 for a system in which Bitcoin would serve as a reserve asset in a neo-free banking context.[23] Hal justified such a system by pointing out that it would enable the scaling of the Bitcoin protocol – with Bitcoin being analogous to a utility settlement system like Fedwire or ACH – while creating secondary systems for payments using bitcoin IOUs.

Under such a system, the trustlessness of these bitcoin IOU transactions could not be guaranteed, as they would be occurring on bank ledgers rather than on the chain directly. However, certain guarantees as to the integrity of bitcoin held at custodial institutions can still be attained, thanks to bitcoin's native auditability. This distinguishes bitcoin from other monetary commodities like gold, which is costly to validate, and hence circulates in walled gardens like the LMBA in standardized format.[24]

In June 2011, Mt. Gox CEO Mark Karpeles sought to assuage customers by conducting a self-send of 424,242 BTC.[25] As early as 2013, Bitcoin developer Greg Maxwell discussed systems for establishing proofs of reserve, describing the 'merkleized approach' to the problem:[26]

> *The idea is simple enough. Two halves. First you show how much funds you have via signmessage for actual coins on the chain. That[']s [sic] easy enough. Then you need to prove how much you should*

[22] Concepts Common to All Attestation Engagements: Attestation Interpretations of Section 105 (AT-C Section 9105) (Oct. 22, 2019), https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/at-c-00105-9.pdf.

[23] Hal, Comment to Bitcoin Bank, BitcoinTalk.org (Dec. 30, 2018, 1:38 AM), https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211.

[24] *See* LBMA, Good Delivery Rules and Governance, http://www.lbma.org.uk/good-delivery-rules (last visited Mar. 23, 2021).

[25] Sophie Knight, At Mt. Gox Bitcoin Hub, 'Geek' CEO Sought Both Control and Escape, Reuters (Apr. 20, 2014), https://www.reuters.com/article/us-bitcoin-mtgox-karpeles-insight/at-mt-gox-bitcoin-hub-geek-ceo-sought-both-control-and-escape-idUSBREA3K01D20140421.

[26] IRC Transcript of Gmaxwell Describing His Prove-How-(Non)-Fractional-Your-Bitcoin-Reserves-Are Scheme (May 8, 2013), https://web.archive.org/web/20170822073453/https://iwilcox.me.uk/2014/nofrac-orig.

> *have. This is a little trick[i]er [sic]. You could just publish EVERYONE's balances i.e. by account ID but that['']s [sic] undesirable for privacy and commercial reasons.*

In that same thread, Maxwell goes on to describe how aggregating hashed user information in a Merkle Tree could enable customers at a digital asset platform to efficiently verify their membership in the set without being exposed to the entire contents of the liability set. Maxwell adds that such a procedure would not inhibit fractional reserve, nor would it prevent theft, but it would prevent the hiding of thefts and would "inhibit long cons" – *i.e.,* situations where a digital asset platform was insolvent for a long period of time. And while the digital asset industry witnessed some abrupt hacks, like that of Bitfinex in 2016, it also suffered some long-term insolvencies that would have been exposed by an active PoR procedure. Both Mt. Gox and Quadriga, two of the most infamous digital asset platform failures, were examples of long-term insolvencies.

According to Maxwell, the 'asset' side of the equation was trivial to prove, for instance with the signmessage procedure. The liabilities side was trickier, and required listing user balances, albeit with some possibility of obfuscation.

The ultimate motivation behind Proof of Reserves as envisioned by Maxwell was to give customers of custodial institutions the ability to verify for themselves that these entities were solvent and fully reserved. The subsequent history of PoR involves trying to render this procedure more practical, more privacy-preserving for the digital asset platform and its users, and consistent with established accounting procedures. The core motivation remains the same, and each additional digital asset platform insolvency or failure increases the urgency of this mission.

In February 2014, Zak Wilcox published a formalization of Bitcoin developer Greg Maxwell's and Peter Todd's ideas and discussions of the Proof of Reserve concept, focusing on the Merkle Approach.[27] It was in that same month that the largest digital asset platform in Bitcoin, Mt. Gox, ceased trading and announced its insolvency. While the Mt. Gox situation was not immediately clear, its apparent failure increased industry attention around the problem of proving reserves held within custodial institutions. Also in February 2014, executives from Coinbase, Kraken, Bitstamp, BTC China, Blockchain.info, and Circle – effectively the largest custodial institutions in the Bitcoin industry at the time – published a joint statement reaffirming their commitment to secure custodial practices:[28]

> In order to re-establish the trust squandered by the failings of Mt. Gox, responsible bitcoin exchanges are working together and are committed to the future of bitcoin and the security of all customer funds. As part of the effort to re-assure customers, the following exchanges will be coordinating efforts over the coming days to publicly reassure customers and the general public that all funds continue to be held in a safe and secure manner: Coinbase, Kraken, BitStamp, Circle, and BTC China.

[27] Zak WIlcox, Proving Your Bitcoin Reserves, iwilcox.me.uk (Feb. 27, 2014), https://web.archive.org/web/20170114112433/https://iwilcox.me.uk/2014/proving-bitcoin-reserves.

[28] Circle, Joint Statement Regarding MtGox (Feb. 25, 2014), https://www.circle.com/blog/joint-statement-regarding-mtgox.

In March 2014, user Olalonde created a Javascript implementation of the Wilcox/Maxwell ideas on Github.[29] With investors rightly spooked by the Mt. Gox insolvency, a number of institutions published informal PoR attestations, with varying levels of verifiability. In short order, Coinkite, Coinbase, Bitstamp, Kraken, Coinfloor, Huobi, OkCoin, and Bitpay published attestations as to their reserves. Of these, only Kraken and Coinfloor provided customers with the ability to independently verify their inclusion in the liability set. Only Coinfloor continued its PoR attestations to the present day.

After the flurry of activity in 2014 and 2015, digital asset platforms lost their public enthusiasm for PoR. Despite this, development of the core ideas continued. In October 2015, Bonneau et al., published "Provisions: Privacy-preserving Proofs of Solvency for Bitcoin Exchanges,"[30] introducing a Zk-Proof approach to the liability side of the equation, potentially abating privacy concerns around the data sharing requirements. Decker et al published "Making Bitcoin Exchanges Transparent,"[31] in November 2015, also aiming to increase privacy in PoR implementations. In February 2019, Steven Roose of Blockstream published a Bitcoin Improvement Proposal,[32] a blog post,[33] and a software library aimed at formalizing Proofs of Reserve. Other recent papers focus on potential attacks on the Merkle Approach[34] or extending PoR to digital asset platforms custodying more privacy-enhanced digital assets.[35]

E. CURRENT STATE OF PROOF OF RESERVES

Today, there is no defining standard for conducting a Proof of Reserves. The industry standout is bitcoin exchange Coinfloor, which has produced 79 consecutive monthly "Provable Solvency Audits" since April 2014.[36] It does not use a third-party firm to verify that the accounting of liabilities is complete. However, Coinfloor deserves plaudits for keeping the PoR flame burning during the long period subsequent to 2015, and for remaining consistent with the ongoing reports during a lengthy period. Detailed information around Coinfloor's implementation can be found in Part IV, Section C, Subsection 5.

Perhaps as a reaction to the Quadriga insolvency (which would have been evident far earlier if customers had insisted on a PoR process), certain Canadian digital asset platforms have become attuned to the necessity of demonstrating sound custodial practices. In 2019 and 2020, respectively, digital asset platforms Bitbuy[37] and ShakePay[38] released third-party memorandums summarizing their custody

[29] Olalonde, Proof of Solvency, GitHub (Mar. 21, 2014), https://github.com/olalonde/proof-of-solvency.

[30] Gaby G. Dagher et al., Provisions: Privacy-preserving Proofs of Solvency for Bitcoin Exchanges, ACM Digital Library (Oct. 2015), https://dl.acm.org/doi/abs/10.1145/2810103.2813674.

[31] Christian Decker, et al., Making Bitcoin Changes Transparent, https://link.springer.com/chapter/10.1007/978-3-319-24177-7_28

[32] Steven Roose, [bitcoin-dev] [BIP Proposal] Simple Proof-of-Reserves Transactions, Linux Foundation (Jan. 29, 2019), https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2019-January/016633.html.

[33] Steven Roose, Standardizing Bitcoin Proof of Reserves, Blockstream (Feb. 4, 2019), https://blockstream.com/2019/02/04/en-standardizing-bitcoin-proof-of-reserves/.

[34] Kexin Hu, Zhenfeng Zhang, and Kaiwen Guo, Breaking the Binding: Attacks on the Merkle Approach to Prove Liabilities and its Applications, 87 Computers and Security 101878 (Nov. 2019), https://www.sciencedirect.com/science/article/pii/S0167404818314093

[35] Arijit Dutta and Saravanan Vijayakumaran, MPRove: A Proof of Reserves Protocol for Monero Exchanges, 2019 IEEE European Symposium on Security and Privacy Workshops (June 2019), https://ieeexplore.ieee.org/abstract/document/8802437. Arjit Dutta and Saravanan Vijayakumaran, Revelio: A MimbleWimble Proof of Reserves Protocol, 2019 Crypto Valley Conference on Blockchain Technology (June 2019), https://ieeexplore.ieee.org/abstract/document/8787552.

[36] Coinfloor UK, *Bitcoin Audits*, https://coinfloor.co.uk/hodl/proof/#reports (last visited Mar. 23, 2021).

[37] CipherBlade, Bitbuy Proof of Reserve and Security Audit Report, Bitbuy, https://bitbuy.ca/assets/documents/Bitbuy%20Proof%20of%20Reserve%20and%20Security%20Audit%20Report.pdf (last visited Mar. 23, 2021).

[38] CipherBlade, Shakepay Proof of Reserves and Security Report, Shakepay (Aug. 24, 2020), https://shakepay.com/docs/Shakepay_Proof_

processes. These reports, consisting of CipherBlade's summary of their on-premises analysis, merely contain the opinion of a third party and do not offer a listing of liabilities for customers to verify. Additionally, the digital asset platforms in question do not provide cryptographic evidence of their ownership of client assets to the general public. In January 2020, the Canadian Securities Administrators ("CSA") suggested that digital asset platforms might be compelled to grant end-users immediate delivery of digital assets purchased on those platforms, a move likely motivated by the high-profile failures of the Quadriga and Einstein digital asset platforms. The CSA focused on the fact that digital asset platforms offer end users IOUs for digital assets, implying that these may constitute derivatives contracts:

> Staff is aware that some Platform operators are of the view that the Platforms they operate are not subject to securities legislation because they only allow for transactions involving crypto assets that are not, in and of themselves, derivatives or securities. However, based on our analysis of how trading occurs on Platforms, we note that some Platforms are merely providing their users with a contractual right or claim to an underlying crypto asset, rather than immediately delivering the crypto asset to its users. In such cases, after considering all of the facts and circumstances, we have concluded that these Platforms are generally subject to securities legislation.[39]

While this guidance has not yet been implemented, the CSA has sent a clear warning to digital asset platforms regarding their custody practices. If digital asset platforms proactively institute a PoR process and give customers confidence that their assets are fully reserved, such onerous measures could be abated.

Outside of Canada, several digital asset platforms have lately begun to undertake PoR processes. Notably, in 2020, HBTC published a guide to proving full reserves for their BTC, ETH, and USDT (Omni and ERC20) balances, employing the Merkleized liability approach.[40] In May 2020, Gate.io partnered with Armanino LLP to produce a Proof of Reserves assessment,[41] including a user-friendly verification dashboard.[42] While both the Gate and HBTC PoR initiatives allowed customers to verify that their balances were included in the liability set, neither was conducted on an ongoing basis. Point in time assessments are weaker, as under-reserved digital asset platforms could temporarily borrow funds from a third party to pass a PoR assessment. This flow would likely become clear to a third party analyzing the flow of funds from the digital asset platform undertaking a periodic PoR process.

Notably, the language these digital asset platforms use to describe their processes designed to give customers confidence that their assets are under their active control differs considerably. The industry has not yet settled on a stable definition for a Proof of Reserves nor has it standardized nomenclature. Gate describes a "Proof of 100% collateral;" Coinfloor touts their "Provable Solvency Report" and

of_Reserves_and_Security_Report.pdf.

[39] Canadian Securities Administrators, CSA Staff Notice 21-327 Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets (Jan. 16, 2020), https://www.osc.gov.on.ca/documents/en/Securities-Category2/csa_20200116_21-327_trading-crypto-assets.pdf

[40] HBTC, *HBTC 100% Proof of Reserve*, https://support.hbtc.co/hc/en-us/articles/360046287754-HBTC-100-Proof-of-Reserve (last updated Nov. 9, 2020).

[41] Gate.io, *Gate.io Provides Proof of 100% Collateral* (First-Ever Among Mainstream Exchanges) (May 16, 2020), https://www.gate.io/article/17489?from=banner_proof.

[42] Armanino LLP, *Trust Explorer Proof of Reserves*, https://proof-of-reserves.trustexplorer.io/ (last visited Mar. 23, 2021).

"Bitcoin Audits;" HBTC, Shakepay, and Bitbuy refer to a "Proof of Reserve."

IV. Proof of Platform Reserves, Solutions, and Guidelines

A. OBJECTIVES, DESCRIPTIONS, & APPROACH TO COMPLETING A PROOF OF PLATFORM RESERVES ENGAGEMENT

1. Objective of a "Proof of Reserves" Engagement

The ultimate purpose of a PoPR is to prove to customers of a digital asset platform that the service provider owns and controls digital assets equal to, or in excess of, its liabilities to customers. In short, a Proof of Platform Reserves aims to prove **customer liabilities are less than or equal to the assets it holds on behalf of customers.**

> **In short, a Proof of Platform Reserves aims to prove customer liabilities are less than or equal to the assets it holds on behalf of customers.**

As discussed, a PoPR also grants customers of a digital asset platform the ability to confirm that their account balances (*i.e.,* their liabilities on the platform) were included within the PoPR. To accomplish this, a data structure known as a Merkle Tree hash acts as a "seal" of all the accounts included within the assessment into a single alphanumeric string, known as a Merkle Root. In one possible approach, customers can then search to ensure their account (*i.e.,* Merkle Leaf) appropriately links to the Merkle Root, demonstrating inclusion within the PoPR. There are advantages and limitations to relying on this approach discussed below.

2. Scope of Proof of Platform Reserves

The scope of a PoPR engagement can vary depending on the specific business model and operations of the platform provider. The most simple case is a bitcoin only exchange; the more complex case is a multi-asset exchange offering a variety of financial products and services.

In certain business models, digital asset platforms may utilize the underlying assets held on behalf of customers to earn yield, use as collateral, or otherwise encumber the underlying assets. In these instances, the type of customer claim created is not fully collateralized by the underlying digital asset for which the claim is redeemable.

The simple PoPR use case whereby a platform maintains 100% of like-kind assets on behalf of customers is outlined below. However, management and practitioners should be aware that for more complex financial products and services, a signed agreement between the auditor and the digital asset platform – and additional audit procedures – may be needed in order to address off-chain instruments and liabilities.

Therefore, digital asset platforms that create more complex CCCs, and wish to complete a PoPR, may require additional procedures or offers of proof not detailed in this paper. However, this does not preclude these types of customer claims (and custodial liabilities) from being scrutinized using a broader definition of the term, Proof of Reserves. For the purposes of this paper, the term “Proof of Platform Reserves” is used to precisely denote the specific type of Proof of Reserves whereby a digital asset platform holds funds on behalf of customers (i.e., 100% reserved, or some lesser fraction agreed to by customers); the reserve assets are in-kind (*i.e.,* bitcoin account balances are reserved by bitcoin); and, the customer’s claim is redeemable for the digital asset (*i.e.,* bitcoin account balance can be withdrawn on chain to another wallet).

A digital asset platform may “pool” digital assets held on behalf of customers into a single address and track a customer’s account balance using a separate ledger (off-chain) software; alternatively, the platform may segregate user funds using specific addresses mapped to each individual user account. Management and professional service providers should be aware that company funds commingled with customers funds in pooled wallets can complicate the presentation of customer reserves.

To illustrate the nature of customer assets in the context of a PoPR, two situational examples denote applicability to perform a PoPR:

1. A customer sends bitcoin to a receiving address controlled by a digital asset platform. The digital asset platform sweeps the bitcoin into cold storage addresses whereby customer bitcoin is “pooled” and maintained until redemption activities are initiated by customers. The digital asset platform always maintains “physical” bitcoin equal to, or in excess of, customer liabilities. **A PoPR could be utilized to demonstrate the platform’s control over the appropriate reserve percentage of customer digital assets at a point in time.**

2. A customer sends bitcoin to a receiving address controlled by a digital asset platform. The digital asset platform aggregates the assets and sends it to a third party to generate yield, some of which may or may not be shared back with the platform’s customer. **A PoPR could satisfy some customers in providing additional assurance over the asset holdings at a point in time, but would necessarily require management, a consultant or CPA auditor to test and/or report on off-chain receivables (the agreement with the third party to return the principal amount lent).**

This paper contemplates reasonable flexibility for management, consultants, and CPA auditors in performing a PoPR; however, it is recommended that these parties pay careful consideration to the currency denomination of the claim vs. the underlying digital asset. For example, a customer balance of 0.5 BTC should be reserved by 0.5 of BTC-denominated assets, not an equivalent dollar value of ETH or stablecoins. While some management, consultants, or CPA auditors may find an alternative reserve model to be appropriate, what is most important is clear and accurate presentation and disclosure to the user in a PoPR.

3. Customer Assets in a Proof of Platform Reserve

In the context of a Proof of Reserves, customer assets refer to blockchain-based (or DLT-based) assets held and controlled by a digital asset platform on behalf of the customer. In the context of a PoPR, the assets held on behalf of the customer are redeemable for the underlying asset for which the customer has placed on or acquired on the platform.

Some blockchain-based assets custodied by a digital asset platform held on behalf of customers may, in itself, represent a claim on another underlying asset. An example of this scenario is when a digital asset platform holds stablecoins or other asset-backed tokens on behalf of a customer. The customer sends a stablecoin to a digital asset platform, which itself is a claim on the underlying asset held with a third party or token issuer. However, the digital asset platform typically makes no representations regarding the redeemability of the stablecoin for the underlying asset (most popularly, U.S. dollars), but only that the digital asset platform will deliver the blockchain-based asset (the stablecoin), whether it is convertible or not with the issuer. Therefore, these types of asset-backed digital assets can be included within a PoPR but make no obligations on the convertibility of the underlying asset by the original issuer.

Guide for Eligible Assets during a Proof of Platform Reserves

Assets Likely Suitable for All Proof of Platform Reserves Assessments	Assets Potentially Suitable for Proof of Platform Reserves Assessments, but Modified Assertions & Procedures
Bitcoin, ether, & other blockchain-based assets	Notes payable from counterparties, claims on exchange-traded products
Stablecoins and other asset-backed tokens whose ownership rights are represented as a token on a blockchain	Assets encumbered by liens or held as collateral for other purposes

4. Customer Liabilities in a Proof of Platform Reserves

When digital asset platforms allow customers to send bitcoin to their account maintained by the platform, or acquire bitcoin on the platform, the platform has created a liability to the customer. The customer has an account balance on the platform and the platform holds the underlying digital assets on behalf of the customer. Typically, the liability exists and is tracked on the digital asset platform's internal customer database.

From the digital asset platform's perspective, a customer's liability and the claim on assets can be fungible or non-fungible. For instance, most digital asset platforms "pool" assets held on behalf of customers. The customer owns a claim on assets held within the "pool" of assets. A claim on assets held within the pool does not grant the customer a specific private key, but rather any applicable asset from the pool. Other customers are also granted the same rights to their assets held within the pool. Therefore, the claims on assets are perceived as fungible. However, in certain instances, digital asset platforms hold customer assets within a specific digital asset address. Underlying assets in this approach are not pooled and the claims are not fungible.

5. Utilizing a Merkle Proof in a Proof of Reserves

A Merkle Proof can be utilized by management, consultants, and/or CPA auditors to invite customers to independently confirm that their account and on-platform balance were included in the platform's proof of reserves calculation. A Merkle Proof consolidates large amounts of data (in this case, customer liabilities) into a single alphanumeric hashed string *(i.e.,* 409609170) and enables users to confirm their input (customer liability balance) was included within the data aggregated into the Merkle Root Hash. This method of customer participation in proving reserves is also privacy-preserving for customers.

The blockchain-based digital assets held by the platform are, with some nuances, relatively easy to verify in terms of amount and control. A digital asset platform can publish hot and cold storage wallet addresses and consultants and/or CPA auditors can validate token balances using a reliable blockchain explorer. A digital asset platform can also prove ownership of addresses with strategies noted below.

However, confirming customer liability balances presents more risk of fraud or mistake by management, consultants, or CPA auditors. If, for instance, a digital asset platform has experienced a loss, or management is attempting to defraud customers, they may underreport liabilities to give the impression the digital asset platform is fully reserved. This key risk of underreporting customer account liabilities is precisely why the Proof of Platform Reserves uses a Merkle Proof strategy to give customers the ability to verify their individual claim on a digital asset platform (please see Section C for technical details).

The user verification experience typically entails noting a user's balance and an identifying characteristic (such as an anonymized Account ID) as of the time of the Proof of Reserve. This exercise of running all on-platform accounts and respective liabilities for a given digital asset can be performed by management, a consultant, or a CPA auditor by utilizing readily available hashing algorithms (to anonymize Account IDs) as well as open source Merkle Tree generators. Further technical specifications and understanding for Merkle Trees is provided in Section C below.

6. The Role of an Independent Third Party in a Proof of Platforms Reserves

To date, practical considerations have prevented PoPR assessments and/or reporting from being completed in a fully trustless peer-to-peer manner given the centralized nature of platforms. Even in the best examples, where management publishes send-to-self transactions to show total bitcoin holdings and proof of control over their private keys, results can be mis-represented or mis-reported. An independent and trustworthy third party can add tremendous value to a platform's Proof of Reserves strategy. A PoPR approach benefits from an independent third party to lend credibility to the reporting of both liabilities and the reserve assets.
An independent CPA auditor's assessment and reporting (in accordance with professional standards) on a PoPR may provide the highest level of assurance for concerned users as they

operate under professional codes of conduct, auditing standards, ethical duties, as well as subject to peer review and professional licensing and regulatory oversight regimes

An independent CPA auditor is particularly valuable when performing procedures to test the reserve of customer's digital assets (customer assets and liabilities). The independent CPA auditor's activities will include identifying and appropriately assessing the risks associated with reporting complete and accurate assets and liabilities based on obtaining reliable information from the digital asset platform and public blockchain. This information may pertain to the digital asset platform's business environment, customer and vendor arrangements, operating model, governance, fraud risk factors, use of technology, personnel competency, and environment of internal control that includes IT controls. A robust risk assessment is a continuous process and will provide indicators of risk for which procedures and further consideration can be focused. For example, a digital asset platform that offers multiple types of digital assets to a globally distributed retail customer base will likely have a high number of counterparties with varying account balances across multiple legal and tax jurisdictions. The risk assessment for that type of digital asset platform would look very different from a digital asset platform that only offers institutional investors custodial services for bitcoin.

7. Completeness & Accuracy

A robust risk assessment helps identify the specific risks that need to be addressed through appropriate procedures to determine the completeness and accuracy of reserves of customer's digital assets.

Completeness of Customer Liabilities is challenging to address because of the wide possibility of scenarios that may create a claim on digital assets.

Claims on customers' assets: An assessment of the various jurisdictions where transactions are performed and customers reside may uncover risks associated with a particular type of transaction. Compliance with local laws and regulations in how the platform provides services and managing customers will reduce the risk of creating legal liability for the platform or customer. Conversely, there may be specific jurisdictions for which the local laws and regulations should be scrutinized regarding the digital asset platform's activities to identify any unrecorded legal liabilities. Similarly, a specific jurisdiction's tax rules and enforcement methods may trigger a tax liability (*i.e.,* indirect taxes).

Customer Account Balances (*i.e.,* **digital asset platform liabilities):** The most important data points required to determine the completeness of Customer Liabilities are the digital asset platform's internal books and records **(generated from the digital asset platform system) that includes the** customer database; and records of customer transactions (*i.e.,* sending and receiving of digital assets). These components together allow the digital asset platform to reconcile its books and records to the on-chain balance for the omnibus account (in cases where reserve assets are pooled). This function is impossible for any party outside of the digital asset platform organization to complete unless granted special access privileges. In practice, this typically entails understanding the digital asset platform's customer database, observing an output of customer accounts and their associated balances, and testing the report extract for reasonableness. An assessment of the process and procedures for updating and maintaining this information may uncover risks associated with data collection, automated processing, or areas where manual intervention is performed. For example, the process for closing and removing customer accounts may allow for manual adjustments for special circumstances. This may create a risk that a customer account may be inappropriately removed - while their digital assets have not been transacted - from the digital asset platform's records and thus excluded from the customer listing. Loose database administrative access controls would present the same risk to completeness and accuracy of the digital asset platform's records. To address this risk, a CPA auditor may choose to: (1) perform procedures to identify a population of deleted or removed customer profiles during the period; (2) perform testing to determine if those records were properly excluded from the customer listing; (3) test database access or other related controls; and, (4) develop other procedures which, in the auditor's professional judgement would address the identified risks.

A Reliable Merkle Tree Generator & Verifier Tool function as intended: While digital asset platforms often publish the Merkle Tree Generator and Verifier Code used on public forums, an independent CPA auditor can provide assurances to the lay user of the verifier application. This user may not have the expertise to understand the intricacies of the software being used.

The Merkle Root Hash that "seals" the Complete Customer Account Balance Listing: To "seal" the customer Account Balances (noted above), the independent CPA auditor could publish a hash or "fingerprint" of the customer account balance export that was observed. This Merkle Root Hash links to all customer account balances included with the PoPR, and the path is observable using a reliable Merkle Verifier tool.

Overstatement of Customer Liabilities is traditionally an area of lower risk due to the nature of the digital asset platform's business.

Typically, there is little incentive for a digital asset platform to overstate Customer Liabilities. However, this area should not be ignored as there may be risks that arise from fictitious customer accounts or customer transactions that represent related-party transactions.

Reconciliation of Customer Liabilities to Customer Assets: Procedures should be performed to reconcile the customer account and transaction listing (if determined to be complete), and the on-chain activity and balances of the omnibus account.

Due Diligence Checks on Potential Encumbrances to Customer Assets: An independent third party is also in a unique position to perform reasonableness checks on other aspects of the digital asset platform. These checks provide reasonable assurances that customer assets are free from liens or other encumbrances.

Completeness of Customer Assets

Reporting Total Asset Balances when Address Privacy is Maintained: While a digital asset platform can publish owned addresses and enable users to verify their balances, many digital asset platform providers wish to maintain address privacy. In these scenarios, an independent CPA auditor has an important role in testing the digital asset transactions transactions are properly included within the customer's asset balance as a component of the total assets reported as controlled by the digital asset platform.

Accuracy of Customer Assets

Testing Exclusive Ownership of Private Keys of Owned Addresses: A digital asset platform can prove access to a private key by methods discussed below. However, the results of an independent CPA auditor's procedures can provide confidence that the digital asset platform is not colluding with a third party to gain temporary access, that the private keys maintained by the digital asset platform are maintained securely and the digital asset exists on-chain.

8. Digital Asset Platform's Environment of Internal Control

It is important to note that a PoPR should be accompanied by an assessment of the effectiveness of the digital asset platform's environment of internal control with a focus on how it intersects with blockchain technology.[43]

As discussed, a robust risk assessment will uncover specific risks for procedures used to conduct a PoPR. This assessment will also uncover specific risks for which the digital asset platform should have internal controls (automated or manual activities) that are operating in a manner that reduces or minimizes the impact of risk. Procedures can then be planned and performed to determine the appropriate design and operation of internal controls over a PoPR. Due to the complex and technical nature of digital assets and blockchain technology, it may not be possible to conduct a Proof of Reserves without an assessment of the design and operating effectiveness of the digital asset platform's environment of internal control (depending on the CPA auditor's judgment and/or the specific standards under which any summary reporting (attest reporting) is offered).

The internal control activities may include activities that are being performed by a third party (*i.e.,* custodial services). These activities should be considered a component of the digital asset

[43] Jennifer Burns, Amy Steele, Eric E. Cohen, and Sri Ramamoorti, Blockchain and Internal Control: The COSO Perspective, Committee of Sponsoring Organizations of the Treadway Commission (July 2020), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-blockchain-and-internal-control-the-coso-perspective.pdf.

platform's environment of internal control. The digital asset platform should expect to receive from the third-party provider an independent report on its internal controls. The independent report of the third-party provider may include design descriptions, confirmation of sound operating procedures, and a description of the services to be performed by this provider.

B. FURTHER TECHNICAL CONSIDERATIONS

As alluded to in previous sections, a PoPR can be performed by management, third-party consultants, or independent CPA auditors. Where there is flexibility in the approach, there is necessarily variance in the persuasiveness of each. While the independent CPA auditor's involvement in the assessment and reporting of a PoPR provides the highest level of assurance and the most persuasive and valuable result, the sections below contemplate techniques, procedures, and methods to expand on how a PoPR can be executed.

C. VALIDATING LIABILITIES, TECHNICAL SPECIFICATION FOR USE OF MERKLE TREE PROOFS

1. Overview

The most challenging technical aspect of conducting a Proof of Platform Reserve is validating liabilities owed to customers of the digital asset platform. As mentioned above, proving liabilities is the riskier formulae in this equation (confirming Customer Assets & Customer Liabilities) because a digital asset platform may be incentivized to underreport liabilities to a third party (*e.g.,* customer, regulator) if the digital asset platform is undercollateralized. The industry has coalesced around a technique referred to as the "Merkle Approach" to provide additional persuasiveness and customer participation around PoPR.

2. Main properties

The Merkle Tree is not a novel concept, nor is it foreign to the world of cryptography, digital assets, and blockchain, let alone database design. The Bitcoin blockchain uses Merkle Trees for data organization and validation. In fact, Git, Bittorrent, ZFS, Dynamo, and the Certificate Transparency framework all benefit from the merits of integrity and authentication afforded to their systems by Merkle Trees. In the same vein as zip or tarball files (protocols for data compression), a Merkle Tree compresses data into a single string of characters, which can be used to prove the verity of the compressed data without disclosing anything about the underlying data itself.[44]

For example, in the Bitcoin protocol, transactions comprise the content of a block in the blockchain. These transactions are coupled together in pairs and hashed.[45] The hashes are subsequently paired and hashed, those results are also paired and hashed down the tree until a single hash value remains, known as the Merkle Root. The Merkle Root is then added as one of

[44] Ralph C. Merkle, A Certified Digital Signature (Nov. 1979), http://www.merkle.com/papers/Certified1979.pdf.

[45] Hashing is the process whereby an input of arbitrary length is given and a fixed output is returned. Importantly, the output is unique to the input and will change with the slightest variance of the input. See Jake Frankenfield, Cryptographic Hash Functions, Investopedia (Feb. 4, 2020), https://www.investopedia.com/news/cryptographic-hash-functions/.

several parameters within the block header of a Bitcoin block, making the verification process (checking to see if a transaction exists in a given block) fast and efficient. A user would only need to know the hashes along the path of the tree to verify a transaction.[46]

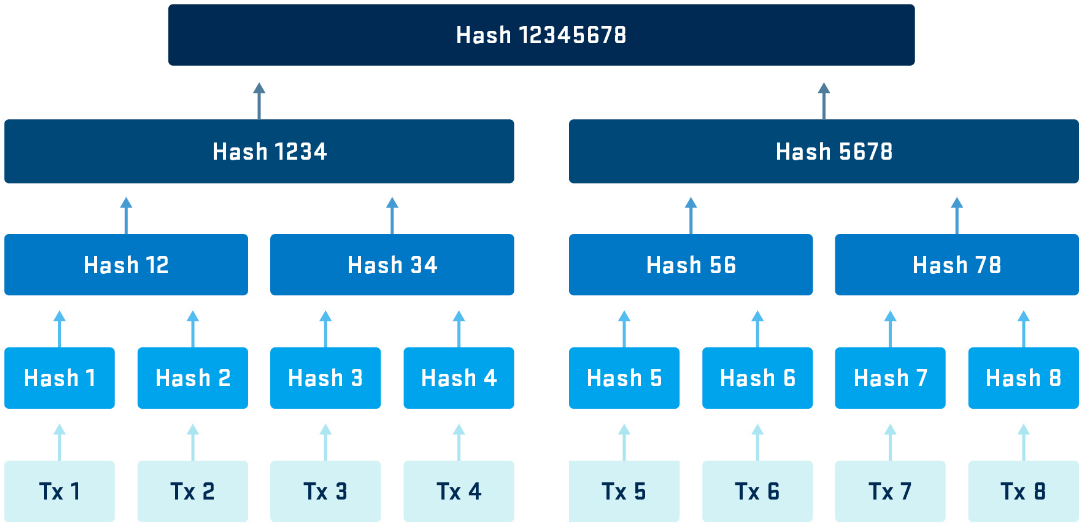


Figure 1. This is a representation of a Merkle Tree with eight corresponding transactions ("Tx"), the data block bordered in green at the top is the Merkle Root.

Figure 1 represents a single Bitcoin block and its corresponding Merkle Tree. The bottom row squares represent individual transactions in a given Bitcoin block. Each transaction is hashed (Hash 1, Hash 2, etc.). These resulting digests (outputs of the hashing function) are referred to as "leaf nodes" in the Merkle Tree, with the objective of getting all the way down to the root via intermediary "branches." The result of hashing data is called a "digest." Each digest is then paired with another digest and concatenated (linked) together (Hash 12, Hash 34). These internal nodes are referred to as branches in the Merkle Tree as they fill the routes in between the leaves and the root of the tree. The hash of the concatenated digest is taken (Hash 1234) and repeated until there are no more intermediary nodes and the root node is found (Hash 12345678).

3. Detailed Description

Merkle Trees serve as the base foundation for several different systems, and also grant utility for non-distributed compute and data validation. When applied to proving on-platform account liabilities, the Merkle Approach can be utilized in much the same way that is shown above. Instead of Merkleizing Bitcoin transactions, the Merkle Approach injects a user balance and a user Account ID (as an already hashed value) as the primary data blocks. This hash value is the SHA256 (a common cryptographic hashing algorithm) digest of the concatenated "user

[46] Andreas M. Antonopoulos, Mastering Bitcoin, Chapter 7: Blockchain, https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html#:-:text=Merkle%20trees%20are%20used%20in,is%20included%20in%20a%20block.

identifier," user "balance," and a random "nonce." The nonce is a one-time random number and is used as a privacy preserving technique, similar to salt for password encryption.[47] The nonce ensures that customers cannot infer anything about other nodes on their path to the Merkle Root and should only be known to the digital asset platform and the customer.

The balance is also a critical variable when verifying liabilities. A malicious digital asset platform can pair two different customers with identical account balances together when concatenating leaf nodes and provide different versions of the tree to each. For this reason, the user balances should be included in either leaf hashes or unsummed child balances in the internal hashes.

User ID	Balance	Nonce(hex)
Alice	15	j188t
Bob	137	e972r
Carol	.912	7662n
Dave	41.88271	p834k

Table 1. This is the table of customer records. These are example nonces, much longer ones should be used in production.

```
hexstr (
        sha256 (
         concat( str(userID), str(balance), hexstr(nonce) )
        )
)
```

Snippet 1. This code snippet demonstrates how these values of "userID," "balance," and "nonce" would be concatenated using the "concat()" function, hashed using the sha256() function and converted to hexadecimal using the hexstr() function. The str() function converts a given value to a string.

Alice's account would result with the following output:

```
hexstr (
        sha256 (
         concat( str(Alice), str(15), hexstr(j188t) )
        )
)
 = 9091adcfef70259e7f7aeedb41bfa30a57341725eb295bf3af435e425d098d4a
```

[47] Wilcox supra note 27.

Snippet 2. The function has been updated with Alice's values. When this function is run, the resulting output is the message digest: 9091adcfef70259e7f7aeedb41bfa30a57341725eb295bf3af435e425d098d4a

User ID	Balance	Nonce(hex)	Hash
Alice	15	j188t	9091a...
Bob	137	e972r	c31b0...
Carol	.912	7662n	a38f7...
Dave	41.88271	p834k	c87e0...

Table 2. The hash values are added in the table. These values result from the function in Snippet 1, the hash full values have been cut off for simplicity in this example.

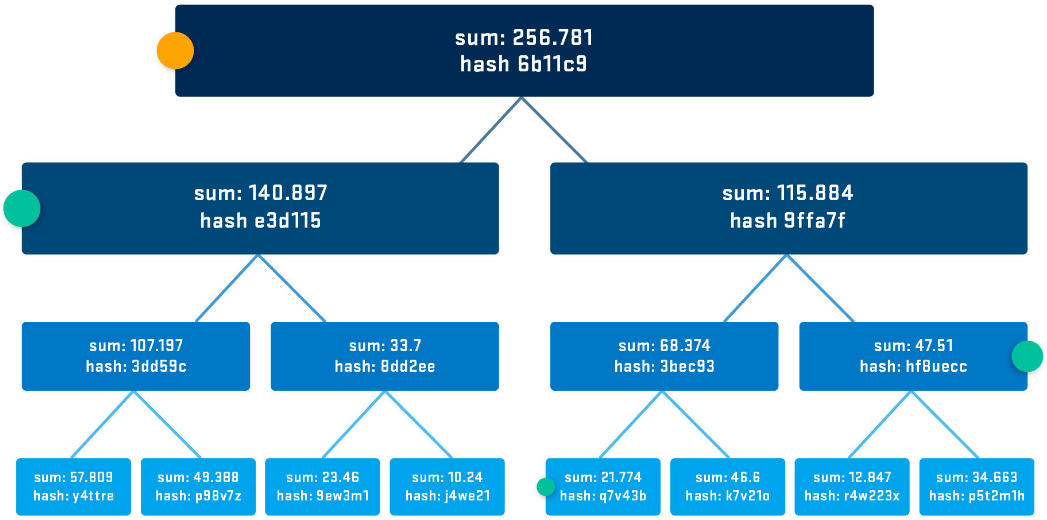


Figure 2 represents a Merkle Tree with the nodes along a customer's verification path in green, inside of each internal node are the sum of their child nodes along with the corresponding hash. The root node can be found at the beginning of the tree in orange.

This section has contemplated that the PoPR (and the Merkleizing of liabilities) is performed for a platform provider that reserves 100% or more of the customer liabilities. In the future, there might exist a scenario where the Customer Liabilities issued by a digital asset platform are a fraction of the Customer Assets through a fractional reserve scheme. In theory, the customer would enter into this agreement knowingly and would expect to only see a predefined fraction of their custodied assets. This is done by introducing a multiplicative fraction factor to the liabilities of the digital asset platform where the result would output true if the Customer Assets are greater than the fraction of the Customer Liabilities.

4. How to Ensure Accurate Results

Though clean and simple to implement, execute, and use, the Merkle Approach is not without limitations. It specifically does not protect against an undercollateralized digital asset platform that can convince its customers that their custodied assets have been summed in the total published liabilities, where in fact only a subset of custodied assets have been summed and included. By selectively tweaking and altering the nodes along the verification path to a customer's leaf node, the customer can be falsely assured that their custodied assets were included in the sum total. Effectively, no two internal nodes would be the same and each customer verification would authenticate against a path specifically constructed so that the internal nodes along that authentication path would have a value no less than the maximum of the child balances. A relatively straightforward way to ameliorate this vulnerability is to include the unsummed child balances of both child nodes in the internal parent nodes. That way, every intersecting node in two successfully verified paths remains the same. This retains the caveat that, in practice, all customers would need to verify their account balances to ensure absolute integrity. However, limiting the possibility of fraudulent Merkle authentication paths gives a certain level of assurances that are likely sufficient for a Proof of Liabilities.

Lastly, involvement of an independent and qualified third party can further provide a check against such a scheme. Specifically, where the third party is involved in collecting a complete and accurate snapshot of the platform's customer database (anonymized user ID + user account balance) prior to creating the Merkle Tree and root hash, the third party can check the raw data for negative account balances and duplicate records.

5. Implementations

An external CPA auditor-assisted Merkleized liability proof is a three-step process, in practice. First, an auditor generates the Merkle Tree with user balances provided by the digital asset platform. Second, the auditor verifies the total user balance and publishes the Merkle Tree and root hash. And third, the user independently verifies their account balances using a Merkle verifier tool.

As an example, Gate.io builds the leaf nodes in their Merkle Trees with two values: user id ("UID") and balance. Each value is first hashed and then concatenated to form the leaf nodes. The same process of hashing, concatenating, and hashing is then applied to construct the Merkle Root. It is important to note that Gate.io does not introduce a nonce value when defining the leaf nodes of a Merkle Tree.

More specifically, when engaging in an actual attestation (as was done on May 4th, 2020 observed by Armanino LLP), Gate.io frames a three-step process:

1. Gate provides the auditor with the user balances that are then imported by the auditor into an HTML file to generate the Merkle Tree.

2. The auditor then verifies the Merkle Root, along with the user count, and summed user balances and publishes the Merkle Tree (saved in plaintext) for customers to verify.

3. The platform then invites customers to participate in verifying that the customer's account and balance were included in the Merkle Approach by importing the retrievable Merkle Tree plaintext file into a verify HTML file (verifier.html) that is provided by Gate.io. The customer must also provide their hashed UID (this is retrieved from Gate.io) and their balance at the time of the Proof of Reserves assessment. The success message displays the Merkle root hash as well as the position of the node in the tree. It is important to note that in the final customer-verification step, the Merkle Tree's root is re-calculated using the imported file so that the customer can verify that the hash is correct.

Digital asset platforms conduct their PoPR in varying ways. For instance, **Coinfloor** publishes a transparency report on a monthly basis that includes a bitcoin transaction sending all funds in the current attestation from one address in custody to another, proving ownership (known as a send-to-self transaction). The digital asset platform also publishes an obfuscated list of customer liabilities with corresponding accounts that can be identified with a secret authentication token and the timestamp at which the report was created. Customers compute the SHA1 digest of the message from their dashboard and find the resulting output in the publicly published liabilities list to verify their balance.[48] They also include the SHA256 hash of the report inside of the bitcoin transaction.

Kraken conducted a PoPR in a three-step process similar to that of Gate.io; however, Kraken used a signmessage procedure to demonstrate to the auditor that they were in control of funds at that time. Kraken then produced a Merkle Tree with all customer accounts and balances with the auditor publishing the Merkle Root. In the final step, the customer could verify that the funds were secure by logging into the Kraken account and viewing the report with corresponding information specific to their account. Kraken also provided the customer with the hashes from the leaf node to the root hash so that customers could independently verify their balance.

Note that **HBTC** conducted a process similar to Kraken's except that a third-party auditor was not explicitly involved. Customers retrieve their user ID, balance, and nonce to verify liabilities.[49]

Name	Unsummed child balances	Nonce	FOSS (Free and Open Source Software)
Gate	n	n	y
Coinfloor	unknown	y	n
Kraken	n	y	y/n
HBTC	n	y	y

[48] Coinfloor, *Coinfloor's First Provable Solvency Report* (Apr. 17, 2014), https://blog.coinfloor.co.uk/post/82980052547/security-transparency-and-reliability-coinfloor.
[49] HBTC *supra* note 40.

Table 3: Non-exhaustive list of digital asset platforms that practice Proof of Platform Reserves and corresponding implementation parameters.[50]

D. VALIDATING LIABILITIES, ZERO KNOWLEDGE PROOFS

1. Overview

The Merkle Approach provides several benefits to both the digital asset platform and customers with respect to cryptographic verification of liabilities but leaves much to be desired within the scope of privacy. A zero-knowledge proof is a cryptographic method that proves knowledge of some secret without revealing the secret itself.[51] Using this technique, a digital asset platform is able to hide from public view information such as the customer holdings and total liabilities of the digital asset platform, as well as maintaining unlinkability between a digital asset platform's Bitcoin addresses. This is important for the financial privacy of customers. The Provisions approach is explored within the context of zero-knowledge proofs.[52]

2. Main Properties

Provisions formalizes a proof of liabilities scheme that offers privacy as it relates to the total liabilities of a digital asset platform, as well as any other account balances. The Maxwell approach lacks privacy guarantees in two areas. It (a) reveals the total liabilities of a digital asset platform in the root node; and (b) using a balanced binary Merkle Tree, it reveals the balance of the sibling node in a child-parent node relationship along a customer's authentication path (refer to Section C2 – Main Properties of the Merkle Tree section).

Provisions proposes a scheme with two properties as it relates to Proof of Liabilities:

1. No information is revealed about customer holdings

2. The total liabilities of the digital asset platform are not revealed and remains secret

3. Detailed Description

The Provisions method uses a list procedure as well as a Merkleized version of the protocol, with the Merkleized version acting as an extension to the base list protocol. A digital asset platform publishes a list of liabilities with a distinct entry for every customer. Customers are provided a unique ID which commits to their account-specific information, *i.e.,* username, email address, account number.

[50] Kraken, *Proof of Reserves Audit Process*, https://www.kraken.com/en-us/proof-of-reserves-audit (last visited Mar. 24, 2020).

[51] Manuel Blum, Alfredo De Santis, Silvio Micali, Giuseppe Persiano, Non-Interactive Zero Knowledge (May 1990). https://apps.dtic.mil/dtic/tr/fulltext/u2/a222698.pdf.

[52] Gaby G Dagher, Benedikt Bunz, Joseph Bonneau, Jeremy Clark, and Dan Boneh, Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges iacr.org (Oct. 26, 2015), https://eprint.iacr.org/2015/1008.pdf.

$CID = H(ID||n)$

where CID is cryptographic commitment,
where H is a hash function,
where ID is the unique ID of the customer,
where n is a nonce.

$<CID, z, \Pi>$

where z is a Pedersen commitment[50] to the customer account balance,
where Π is a knowledge proof showing that z is well formed.

Similar to the Maxwell Approach outlined in the previous section, a customer checks their account information against the publicly available list of accounts. In this case, the customer verification process is done in three steps:

1. The customer logs in and is privately given n and r. The r value is a string used to open(reveal) a commitment to the customer balance. It is important to note that both of these values (n and r) are provided by the digital asset platform.

2. The customer uses n to open their commitment CID and verify that it commits to the account information (username, email, or account number)

3. The customer uses r to open the commitment z and verify their account balance

There are two additional steps that would likely be carried out by an independent CPA auditor, but can be performed by the customer:

4. The integrity of the remaining entries in the liabilities list are validated by checking the proof, π, for each entry.

5. The total liabilities are computed, which is a Pedersen commitment to the sum of all balances (the digital asset platform's liabilities).

Given the significant computational overhead in the list method of the Provisions Approach, an extension is proposed where each leaf node contains the commitment CID and the commitment z and each internal node contains the hash of its children and the summation of their balances. This makes the approach more efficient as the Merkle tree extension allows the verification to scale logarithmically instead of linearly.

Fractional Reserves

The Provisions approach can be modified to commit to a fractional balance instead of a customer's true balance. Similar to the Merkle Approach, a fraction factor would be

[53] Torben Pryds Pedersen, Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing, Springer (1998), https://link.springer.com/content/pdf/10.1007%2F3-540-46766-1_9.pdf#page=3.

implemented to the customers liabilities to reflect the fractional holdings of the digital asset platform.

4. Keep in Mind

Similar to the Merkle Approach, the Provisions method may not protect against a malicious digital asset platform that can manipulate the nodes along the verification path to a customer's leaf nodes resulting in a false attestation to customer liabilities. A malicious digital asset platform would simply need to identify the leaf nodes associated with a customer's account, extract the verification path and modify the commitments of the nodes along the path. As stated in Section IV(C)(3) How to Ensure Accurate Results, a method to mitigate this vulnerability is to include the unsummed balances in the internal nodes along the verification path to prevent the obfuscation of balance integrity. Using this patch, it is more likely that customers can be reasonably assured that their balance is included in the liabilities attestation of the digital asset platform.

E. ACCOUNT BALANCE ASSERTIONS FOR DIGITAL ASSET RESERVES

Returning now to the potential for management to engage an independent CPA Auditor to perform a PoPR, an auditor may, depending on the type of reporting involved, require "management assertions." Management assertions are claims made by the digital asset platform as to certain aspects of their business. The following four items are classified as assertions (traditionally in the context of a financial statement audit) related to the balances in accounts and ultimately within the PoPR calculation:

- *Completeness.* The assertion is that all assets that should have been recorded are fully reported.
- *Existence.* The assertion is that all assets recorded within the asset account balance actually exist. This assertion means that there has been no overstatement of assets.
- *Rights and obligations.* The assertion is that all assets presented by the entity actually belong to the entity.
- *Valuation and Allocation.* The assertion is that all assets have been recorded at their proper valuation.

A CPA auditor would need to perform different types of procedures in order to obtain sufficient appropriate evidence to test the assertions and form an independent opinion on management's assertions. There are eight types of standard audit procedures, including: inquiry, confirmation, inspection of records or documents, inspection of tangible assets, observation, recalculation, re-performance, and analytical procedures.

As proof of ownership and control of digital asset reserves is wholly reliant on the knowledge of control of the cryptographic keys, the CPA auditor should document their understanding of the control environment around key generation, storage, access, and recovery of those keys. Cryptographic key management includes:

- Key life cycle controls, including controls over: design and development, implementation, key generation, storage, access management, and retirement of the keys.

- The employees, contractors, or consultants that: designed and developed the cryptographic key architecture, implemented the cryptographic keys architecture, and generated the keys.

- Where and how the keys are stored and whether access to the keys is restricted to only authorized individuals and systems that need such access to perform their job duties and functions.

- The inventory of cryptographic keys maintained by the service organization, including the individuals with access to the keys and controls over the inventory's completeness and accuracy.

- Audit logging and review of access to cryptographic keys and whether the logs are stored in a manner that restricts access to users who do not have access to the keys.

- Whether the cryptographic keys have been split into multiple parts (shards), where a subset of those parts is used to recover the original cryptographic key and, if so, the individuals to which the shards have been distributed.

- If multi-signature cryptographic keys are used, the parties who must agree before a transaction can occur.

Understanding the control environment is critical in determining the appropriate testing approach for the digital asset reserve account balance.

1. Completeness of Digital Asset Reserves Listing

A PoPR would require a complete and authentic list of all assets – or of all the keys that belong to the entity (or at least a list sufficient to prove an adequate reserve percentage). It is always possible that not all digital assets in an entity's possession would be reported within their reserves listing and thus would not be included within the PoPR calculation; however, omitting assets under their control would negatively affect their ability to demonstrate that they still have control of all assets that have been entrusted to them. If internal control policies and procedures are adequate, there is reasonable assurance that all transactions and balances are being captured and recorded.

The independent CPA auditor should perform inquiries of management in order to gain an understanding of the process for receiving customer digital assets, safely storing those digital assets, and sending customer assets outside the organization when withdrawn by customers. These inquiries would also include an understanding of the technical components used in the custodial process, including, but not limited to, the types of wallets used, and the hardware and software involved in hosting, maintaining, and integrating with those wallets, as well as the signature schemes utilized.

In addition to inquiry, the independent CPA auditor may deem it necessary to obtain and review internal controls and process documentation from the entity, including the entity's Service and Organization Controls (SOC) reports, if applicable, as they would have a responsibility to understand how the entity conducts digital asset transactions and safeguards digital assets.

After gaining an understanding of the custody process and infrastructure, the CPA auditor would obtain the complete listing of digital asset wallet addresses.

2. Overview of Evidential Requirements for Validating Existence

Distributed ledger technologies are fundamentally multi-author data streams with a mechanism to allow identification of the acceptable (or official) branch known as the consensus mechanism. To validate, or authenticate, the existence of digital asset reserves on a DLT is to identify that the claimed data record is consistent with the blockchain (or rule set) that has been selected and placing reliance upon such blockchain where they reside.

Although many blockchain applications share some fundamental principles of trust and security through cryptography and decentralization, in order to determine whether the information obtained in the course of validating existence of digital asset reserves, one must consider the ***reliability of the blockchain*** and whether it meets certain requirements to qualify as a sufficient and appropriate source of "evidence". The following factors may be important when taking into account the relevance and reliability of information obtained from the blockchain, including its accuracy and completeness:

1. the stability of the consensus mechanism and whether alternative information is available which may be contradictory,
2. the depth of the community supporting the blockchain and whether there is evidence of general market acceptance by users of the relevance and reliability of information from the blockchain, and
3. soundness of the cryptography involved.

A reliable blockchain should have an effective design for its intended purpose and continue to operate as designed. The following elements of a blockchain can be considered as part of a risk assessment to conclude on its reliability and the existence of the associated digital asset.

1. **Deployment services** through which transactions are initiated and digital assets are observed
2. The **consensus protocol** that governs the agreement by the network for recording a digital asset's creation or transfer
3. **Network enablers** that maintain the distributed ledger
4. **Security** of the blockchain through cryptography
5. **Community of developers** that support the blockchain network

A digital asset may not exist if one or more of these elements indicates a risk to the reliability of the blockchain.

Deployment services - Individuals and businesses cannot directly interface with digital assets (*i.e.,* blockchain data) without the use of technology or service providers such as digital wallets, blockchain explorer software, and digital asset platforms. Deployment services can take many forms and bring various cyber and 3rd party risks, however those that offer data services (*i.e.,* data analytics, blockchain reader tools) present unique challenges to the existence of digital assets. Sophisticated users look to understand the deployment service's information technology and operational controls environment surrounding extraction and processing of data from the blockchain. A service auditor's report (*e.g.,* SOC report) is often requested from the service provider that would support reliability of its environment of internal control.

Consensus protocol - The consensus protocol is a blockchain network's governance mechanism that incentivizes node operators to reach the same conclusion about the validity and order of transactions. A blockchain's open-source software for running the consensus protocol may contain errors or bugs and if exploited could trigger an unintentional hard fork (*i.e.,* split of the blockchain). Blockchain records may be unreliable if critical vulnerabilities within the source code are not addressed in a timely manner. Unfortunately, service auditor reports (*e.g.,* SOC reports) are not available for public blockchains and it may not be feasible or effective for users to perform their own source code reviews. Users may consider methods to assess new developments and reports of vulnerabilities in code versions.

Network enablers - The activities for validating a blockchain (*e.g.,* staking a validator for a proof-of-stake blockchain, mining for a proof-of-work blockchain) are performed by the network enablers that run various types of nodes specific to each blockchain network. Most node operators are honest and work to support the reliability of blockchain records in pursuit of the consensus protocol's incentive model. The reliability of the blockchain records become more reliable as the blockchain network's node operators increase in number and diversity. Users may consider employing their own monitoring activities to understand and respond to risks in the network.

Security - The security of blockchain technology is inherent in its designed immutability (data that is cryptographically linked through the chain of blocks). This key feature of blockchain technology also poses challenges to reversing bad transactions or fixing unreliable smart contracts caused by user error or poor design. Users may need to rely on the internal control activities performed by smart contract owners and consider implementing their own internal controls around initiating transactions and recovering unintended transactions with smart contracts.

Community of developers - Each blockchain is designed to be distinct from other blockchains. The individuals, groups of individuals, and formal organizations that support a blockchain throughout its lifecycle constitute the community of developers. Their contribution and effectiveness are key for ongoing blockchain reliability. The community promotes adoption, provides academic and technical documentation, responds to feedback from users and node operators, performs research and development for the source code, organizes version updates, and performs source code testing and monitoring. The community is often organized around a non-profit foundation that provides leadership and governance over the blockchain. While commonly known public blockchains may have one or more active foundations, there are many abandoned blockchains where the foundation dissolved or failed to form. Users may consider employing their own monitoring activities to assess a community or foundation's effectiveness, integrity, talent, and version releases.

3. Proof of Control of (or Rights to) Digital Asset Reserves

Proof of Platform Reserves requires both proof of the existence of the digital asset reserves as well as proof of control (*i.e.,* a proxy for ownership) - or the entity's claims to possess those reserves.

Cryptographic Signatures

Certain DLTs support the use of the cryptographic signature technology giving digital asset platforms the ability to sign and verify messages that may serve as a test of their control of (or rights to) the digital asset reserves.

While there are a wide variety of cryptographic signature methodologies, in general, a cryptographic signature demonstrates knowledge of the private key, which is the data required to execute a transaction with such digital assets. Many reference wallets as well as many aftermarket wallets contain the tools needed to perform this process. Additionally, there are frequently publicly available code bases to facilitate creating and validating cryptographic signatures.

The validator will provide the signer (the platform) the message to be signed and then input the returned signature, the original message, and the associated asset address (or derivative thereof) into the compatible wallet software or other tool. The applicable tool will then show that the message was either verified or unverified. Verified means that the message was signed with the private key associated with the address of the asset held by the digital asset platform. The ability to generate the signature using the private key proves the private key holder's ability to transfer digital assets from the wallet, and thus demonstrates their control of the wallet.

A validation process can request that the wallet owner generate a signed message for those wallets that support the digital signature feature (ex: Bitcoin / Ethereum). The validator can then verify the message using the digital asset wallet or other tool available. Considerations for tool usage include public accessibility and usage.

Send to Self Transactions

Not all digital asset protocols have the ability to sign a message as described above. Therefore, an alternative procedure would be applied in order to verify control, or the rights, to such digital assets. In order to gain comfort that the digital asset platform has possession of the private key associated with the asset address, and thus verify the control, the validation process would request that the entity transfer a specific amount of the digital asset from the public address in question to another public address or digital asset platform account for which the validator can view the incoming transfer. The validator should incorporate certain elements of specificity for the transaction request – including time frame for execution and transaction amount - so as to ensure the transaction evidence noted by the validator is appropriately linked to their transaction request.

This is not the preferred method for verifying control of the private keys as it introduces risk and an unnecessary administrative burden on the entity as they may have to subsequently perform a reversal of the requested transaction. The request and subsequent reversal of a "send to self transaction" may be in conflict with or bypass the established internal controls over transaction processing.

Hierarchical Deterministic Wallets

In some cases, a protocol for deriving sub-addresses from a root address is used. This allows related sub-addresses to be derived in a predictable way from the root address thereby linking multiple sub-addresses. Frequently in these cases a new sub address is generated for each incoming transfer of a digital asset. This can allow for the control of the sub-addresses to be verified from verification of the single root address.

Because of implementation details, however, it is not always practical to verify the root address. This is further complicated because some implementations do not easily permit the selection of specific sub-addresses to be used as inputs to a transaction. In the event that digital assets are held in a hierarchical wallet where control is limited, the validation process may request all sub addresses are directly validated or all addresses swept into one address and then subsequently request the transfer of a specific de-minimis amount from that sole address as described above.

Multi-Signature Wallets

Single signature wallets need only one signature to sign a transaction and prove control of the digital asset reserves. A multi-signature wallet (or multisig, for short) requires one or more signatures to sign (and therefore authorized) a transaction. A multisig wallet is generally shared by two or more private keys.

The number of signatures required to sign a transaction will be lower or equal to the number of private keys. For example, a 2-3 transaction will require 2 of the 3 private key holders to sign the transaction. Thus, in order to perform the validation test outlined above, coordination is required by a minimum number of private key holders.

Secure Multi-Party Computation "MPC"

Secure multi-party computation relates to methodologies by which a group of parties can jointly compute a function dependent on inputs from each of the parties without revealing those inputs to the other parties participating in the computation. MPC protocols involve varying amounts of tolerance for bad actors.

MPC generally functions as an add-on layer of security that effectively allows distributed / fault tolerant representation of private keys.

F. REPORTING: THE FORM AND LEVEL OF PROOF

1. Comparison of Types of Attestation Engagements and Reporting

Third-party party assurance can be provided in various forms depending on the subject matter, level of assurance and intended audience. For example, a CPA auditor can perform an Agreed-Upon Procedures attestation engagement and issue a written report that provides a specified party with their findings about the reliability of the report's subject matter. This type of attestation may provide a high level of assurance to specific users of a digital asset platform, but the auditor's procedures and the subject matter are each defined by the platform and the report can only be shared with those parties specified for the engagement (*i.e.,* restricted use report, not available for the general public). Also, a third-party party assurance report is not the only means to communicate relevant information to customers regarding PoPR. There are current implementations of a PoPR where the digital asset platform makes available the relevant information about their custodied digital assets (*i.e.*, type, on-chain address, smart contract code, etc.), data feeds and information portals maintained by the digital asset platform along with detailed instructions for the steps that an entity (*i.e.,* customer, regulator) to perform their own due diligence to get a certain level of "comfort" around claims, holdings, availability, etc. However, customers and regulators often need a higher level of assurance in the form of a report issued by an independent third party.

The highest level of assurance is provided in the form of an attestation report issued by an independent CPA auditor in accordance with standards issued by a professional standards setting body (*i.e.,* the American Institute of Certified Public Accountants, or AICPA). The independent CPA auditor issues their report in which they express an opinion or a conclusion on a defined subject matter (*i.e.,* financial statements, internal controls) so that a user can make informed decisions. In the context of this paper, the subject matter in the auditor's report could relate to a PoPR.

In September 2020, the AICPA's Auditing Standards Board issued Statement on Standards for Attestation "SSAE" No. 21, Direct Examination Engagements. This supersedes and amends the professional standards to allow for two types of examinations that can form the basis for reports (strongest level of assurance) to be issued by independent CPA auditors: assertion-based examination (amended) and direct examination (new). The independent CPA auditor's SOC 1 and SOC 2 reports (discussed above) are issued to report on assertion-based examinations performed in accordance with standards under SSAE 18 (amended under SSAE 21). In situations where a digital asset platform determines to report its PoPR, the SOC 1 and SOC

2 reports may not provide assurance over the PoPR data (*i.e.,* Merkle Tree) but rather provide users with assurance over the environment of internal control of financial reporting and IT systems from which the PoPR data is generated. A Direct Examination Engagement (new under SSAE 21) might allow for an independent CPA auditor to measure PoPR data (*i.e.,* Merkle Tree) and report on the results. More analysis and research will be needed in order to determine if a Direct Examination Engagement would be suitable for PoPR. For example, it may be challenging for an independent CPA auditor to provide a report that is near real-time or more frequent than monthly or quarterly - which may or may not be sufficient for all users.

The examinations are outlined below to help consider their suitability for an independent CPA auditor to conduct an engagement and reporting for a PoPR. It is important to note these are written reports that cover data as of a point in time and a historical period of time. It may not be possible to automate all the procedures needed to support the issuance of these reports for real-time reporting, however further research and innovation may help overcome this challenge.

	Direct Examination	**Assertion-based Examination**
AICPA Attestation Standards (SSAE 21)[54]	AT-C Section 206	AT-C Section 205
Objective	To **obtain reasonable assurance** by measuring or evaluating the underlying subject matter against the criteria and performing other procedures to obtain sufficient appropriate evidence.	To **obtain reasonable assurance** about whether the subject matter is in accordance with (or based on) the criteria or the responsible party's assertion is fairly stated, in all material respects.
Purpose of Engagement	To provide users of information with an **opinion** that conveys the results of that measurement or evaluation. *the responsible party does not provide an assertion	To provide users of information with an **opinion** regarding the underlying subject matter, as measured or evaluated against suitable and available criteria.
Reporting	Express an opinion in a written report that **conveys the results** of that measurement or evaluation	A written opinion about whether (a) the subject matter is **in accordance with (or based on) the criteria in all material respects**, or (b) the responsible party's assertion is **fairly stated in all material respects**.

G. ADDITIONAL RISKS & CONSIDERATIONS

Not all Proof of Platform Reserve assessments are the same. The wallet and database infrastructure of a digital asset platform, the preferred balance between privacy and transparency of the digital asset platform, and other unique circumstances inherent to each specific Proof of Reserves creates an environment whereby trade-offs and their associated risks must be considered and disclosed to report users or mitigated by the auditor and digital asset platform. Below, we identify, describe, and analyze several of these considerations.

[54] Auditing Standards Board of the AICPA, Statement on Standards for Attestation Engagements No. 21, Direct Examination Engagements, AICPA (Sept. 21, 2020), https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-21.pdf.

1. Publication of Wallet Addresses

A. **Description:** In the context of a Proof of Platform Reserve, a digital asset platform will have to decide whether or not to publicly disclose the asset addresses for which the assets are controlled during the reporting phase of the Proof of Platform Reserve.

B. **Trade-Offs:** Publishing addresses included within the Proof of Platform Reserve enables third parties to self-verify asset balances published as part of the assessment. Disclosing addresses also enables 3rd-parties to re-perform the work of an auditor and hold them accountable to a certain extent. However, the privacy of the digital asset platform and its customers must be considered. Disclosing addresses creates potential risks for the digital asset platform, such as monitoring of digital asset platform addresses by malicious actors or competitors, and heightened risk of compromised key material related to xPubs and child keys.

C. **Potential Future Developments:** In the future, Zero Knowledge proof schemes may be developed to prove ownership of a specific address and the asset balance as of a point in time without disclosing the address itself. However, these potential methodologies are not yet widespread in the context of a Proof of Reserve.

2. The Inclusion of Addresses Holding Asset Balances in the Proof of Reserves

A. **Description:** digital asset platform providers can control millions of addresses. Oftentimes, many of these addresses are known as “Receiving Addresses,” which are addresses provided to customers to receive digital assets upon sending them into a platform. These receiving addresses are used as temporarily vessels to receive customers and map asset balances to a customer’s account. Upon reception, a digital asset platform sweeps these funds into longer-term, cold-storage wallets, which are used to maintain the bulk of the custodial funds. Many times, a digital asset platform will hold assets in excess of liabilities when excluding all receiving addresses.

B. **Trade-offs:** Excluding receiving addresses may not be desirable for a digital asset platform for many reasons. If any balances exist and receiving addresses are excluded, the overall collateralization percentage presented to 3rd-parties could be lower than if they were included. Additionally, excluding receiving addresses could cause the collateralization percentage to be reduced to under 100%. Additionally, users may want to see the “full picture,” which receiving addresses are certainly a part of. In the context of a Proof of Reserves, the digital asset platform and auditor may agree to exclude these receiving addresses within the scope of the Proof of Reserves to make the Proof of Reserves easier to execute. The Proof of

Reserves may be easier to execute from the auditor's and digital asset platform's perspective because they may have less addresses to confirm balances and ownership of.

C. **Potential Future Developments:** Currently, a limited set of reliable auditor tools exist optimized for a Proof of Reserves. Tools like block explorers, node-hosting services, and digital signature verifiers are accessible to an auditor, but they still require a heightened level of technical expertise. Additionally, these tools are typically not optimized to aggregated address asset balances and sign/verify digital signatures on a mass scale. However, in the future these tools may exist, making it easier for both the auditor and digital asset platform during a Proof of Reserves.

3. Confirming Exclusive Ownership of Keys

A. **Description:** It is very difficult for an auditor to verify private keys are only owned and controlled by the digital asset platform. Ideally, an auditor would have to be present during the creation of the private keys and associated backups and thereafter for all addresses in-scope during the Proof of Reserves. Even then, an auditor could never be 100% assured that the keys have not been compromised undetected by a malicious or colluding actor. Therefore, confirming absolute exclusive ownership of private keys is impossible by an auditor. However, steps can be taken, each providing different levels of assurance of exclusive ownership of private keys.

B. **Trade-offs:** The digital asset platform and auditor have to agree on a set of procedures related to ownership of private keys that are appropriate for the circumstances. If a digital asset platform wanted to provide a very high level of assurance to a specified party, they may invite the auditor and the specified party to a key creation ceremony, create the keys under the observation of these parties in a highly secure environment and transfer all funds to those newly created keys to prove exclusive ownership. However, these measures are typically not feasible. Therefore, the auditor and digital asset platform may agree to perform procedures that are commensurate with the need. Procedures may include gaining an understanding of the control environment that protect private keys, measures taken during the initial key ceremony, and more. Ultimately, the appropriate trade-off between feasibility and assurance must be determined by the executors of the Proof of Reserves. These trade-offs and assurances provided by the procedures performed should also be considered by users of the report.

C. **Potential Future Developments:** Developments and approaches related to Trusted Execution Environments ("TEEs") may become more relevant and useful to auditors in the context of a Proof of Reserves going forward. Additionally, the use and maturation of control frameworks related to private keys may evolve and become more useful in the context of a Proof of Reserves going forward.

D. **Risks Remain:** However, the inherent risk of being unable to confirm exclusive ownership of key material will be omnipresent because it is impossible to conclusively prove exclusive ownership of key material with 100% certainty.

4. Reliance on User Verification for Assurances

A. **Description:** An integral aspect of a Proof of Reserves is a feature that enables a user to confirm their account (liability) balance was included within the procedures performed. Under the hood, a user's balance manifests as a database entry within a database maintained by a digital asset platform. During a Proof of Reserves, an auditor is responsible for ensuring the list of user account balances provided by the digital asset platform is complete. There is always an inherent possibility of purposeful or accidental inclusions or exclusions of user accounts that could affect that integrity of the user account data. Users can contribute to bolster the reliability of the dataset, by verifying their account data was included. The more users that verify their account balance were appropriately included, the more assurance all other users gain. As more users verify they were included within the dataset, the more reliable the dataset becomes. In this way, each additional user verification during a Proof of Reserves contributes to the overall "herd-immunity" of assurance over the reliability of digital asset platform liability data.

B. **Risks Remain:** If a critical mass of users does not verify their account balances were appropriately included within the customer data extracted from the digital asset platform's database, the additional assurances provided by the Merkle Approach are devalued.

C. **Potential Future Developments:** The PoPR/Proof of Asset Reserves ("PoAR") scheme outlined above is less than 10 years old. In the future, a new and expanded Proof of Reserves scheme could be developed that could reduce the reliance on other users self-verifying.

5. Potential for Unaccounted-for Liabilities

A Proof of Reserves does not provide assurances regarding the solvency of the business entity. A Proof of Reserve may not include the assessment of any liens, encumbrances, or other Company liabilities that may affect the solvency or the redemption of customer funds

A. **Description:** As alluded to in previous sections, a Proof of Reserves does not provide assurances regarding the solvency of the business entity. A Proof of Reserves may not include the assessment of any liens, encumbrances, or other Company liabilities that may affect the solvency or the redemption of customer funds. These types of assurances over the entity as a whole are more likely to be provided in other types of assurance vehicles, like a

Financial Statement Audit.

B. **Potential Future Developments:** As Proof of Reserves assessments evolve and become more commonplace, standard Proof of Reserves procedure could include an examination of liabilities on the Company balance sheet, overall Company solvency, and a search for unrecorded liabilities.

6. Point-in-Time vs. Periodic Reporting

A. **Description:** The willingness of a digital asset platform to perform procedures to provide transparency to users is beneficial for digital asset platform users, the digital asset platform itself, and the digital asset ecosystem. However, a single Proof of Reserves, as of a specific point-in-time provides limited assurances. The collateralization health of a digital asset platform at one time confirmed during a Prove of Reserves does not provide assurances over future periods. A single Proof of Reserves could be compromised via digital asset platform collusion with other parties to “borrow” funds or an auditor is more likely to be “tricked” into performing procedures once and one time only. However, while risks would still remain, performing a Proof of Reserves on a periodic basis (*i.e.,* monthly, quarterly, or even annually) would provide much more assurance than a single point-in-time Proof of Reserve.

B. **Trade-offs:** Frequent Proof of Reserves assessment creates additional time and cost workloads on the digital asset platform. However, economies of scale can be reached that would drive down the efforts for each incremental assessment.

C. **Potential Future Developments:** As technology advances and audit methodologies evolve, real-time assurance for proving reserves may be possible.

The list of considerations and risks outlined herein is not exhaustive and is subject to expand and change as the digital asset industry evolved and Proof of Reserves methodologies mature. For instance, if PoPR/PoAR methodologies outlined herein are applied to fractionally reserved digital asset platforms, collateral make-up and counterparty agreement terms would be key considerations.

V. Conclusion

In February 2021, the market capitalization of digital assets broke the $1 trillion mark. This milestone signaled the arrival of new market entrants, such as institutions looking to diversify their portfolios and fortify their corporate treasuries, and large companies, such as PayPal, Visa, and others, who sought to offer digital assets to their customers and clients. Retail investors have also looked to digital asset markets to capitalize on new, innovative financial products and business models. This renewed focus on digital asset markets has not been limited to investors only; policy makers and regulators have also been paying close attention, keeping a watchful eye on market participants to guard against investor harm.

Proof of Platform Reserves will help maintain trust in digital asset service providers from both investors and government officials by giving them the ability to verify that digital asset platforms and custodians are maintaining their stated reserves, allowing customers to transact with confidence. As the digital asset ecosystem matures and digital asset service providers see an increase in the number of users around the world, they may need to adopt new methods such as PoPR to grow their businesses and continue to serve more customers. The industry best practices in this paper will guide them well as they evaluate how best to meet customer demand for Proof of Reserves.

CHAMBER OF
DIGITAL
COMMERCE