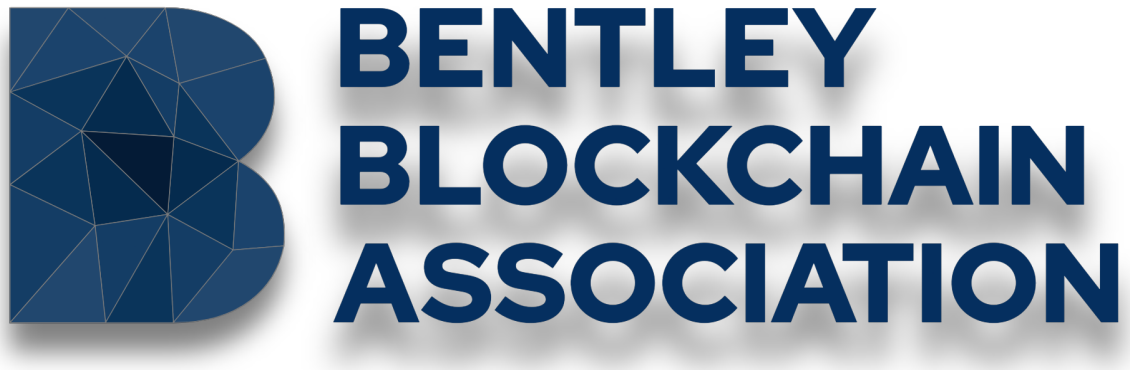


The Future of Blockchain Accounting & Auditing

Bentley Blockchain Association

May 17 2023

Acknowledgments

Rebecca Curry
President

Christopher Guyette
VP of Research & Development

Lucas Vanroboys
Research Analyst

Samuel Capobianco
Research Analyst

Nicolas Saliou
Research Analyst

BENTLEY BLOCKCHAIN ASSOCIATION

Content

Introduction

Cryptocurrency, coupled with blockchain technology, have firmly established their permanence in the digital landscape. Despite the necessary regulatory interventions to counteract bad actors within the ecosystem, the potential to harness the inherent trustless characteristic of this nascent technology is palpably clear in 2023. At the Bentley Blockchain Association, we recognize the major hurdle for adopting crypto-based companies lies in the capability to accurately account for and audit cryptocurrency holdings and obligations. In the wake of the FTX collapse, American accounting organizations should set the tone for conversations around regulation.

Both private and public companies utilize accounting and audit principles outlined by the American Institute of CPAs (AICPA), and the Securities Exchange Commission (SEC). These principles are implemented by external firms, most notably the "Big 4" accounting and audit firms. However, there is still debate over the solvency of any firm related to cryptocurrency, as illuminated by FTX and its reserve insufficiency. To combat any debate over cryptocurrency exchanges and custodians, regulators must develop a standardized framework for Proof of Reserves, and require certifications for blockchain accountants to learn the Proof of Reserves methodology.

The crypto ecosystem's expansion and variety of products have highlighted potential issues surrounding the centralization of databases, off-chain transactions, omnibus wallets, and the challenge of interpreting these records. While audits should be conducted to maintain licenses, Proof of Reserves aims to enhance the audit process by broadening its depth and scope to account for the expansion of the ecosystem. In order to increase transparency and trust for stakeholders in the industry, the AICPA framework will have to address issues surrounding reporting accuracy, addressing various types of reserves and liabilities, and mitigating counterparty risk, while strictly enforcing these issues on a systematic scale.

This research paper will provide an overview of the AICPA's current digital asset framework, dive into the leaders in blockchain auditing, analyze Coinbase and Binance's auditing practices post-FTX, and a suggestion for the future of the Proof of Reserves system for Web3 companies in 2023 and beyond.

Part 1: Regulatory Landscape

AICPA's Current Framework

With no clear guidance on digital asset accounting and auditing practices, the AICPA released resources to help firms take the necessary steps to ensure proper asset verification. One of the most comprehensive AICPA resources is the "Accounting for and Auditing of Digital Assets Practice Aid". This practice aid offers nonauthoritative guidance on how to account for and audit digital assets under GAAP and FASB standards. This document is updated as needed to keep up with new asset development in the space, and the SEC has provided comments and revisions on several accounts.

Accounting Under AICPA[1]

In accounting practice, it is essential that firms and auditors understand the nature of the assets held on a company's balance sheet. Therefore, when evaluating digital assets, the AICPA has deemed them as intangible assets that, when purchased for cash, should be measured at cost. Therefore, when processing the receipt for a digital asset transaction, it should be measured as a noncash consideration at its estimated fair value. With cryptocurrency markets being very volatile, assets may trade at different prices. So, in determining the fair value of a digital asset, the AICPA suggests that firms should use the principal market. The principal market refers to a reliable market with the greatest volume for the asset or liability in consideration. Once the fair value is determined, the digital asset should be accounted for using methods that are company-specific:

Exchanges: If a firm is selling digital assets to a customer as part of normal business activities, the sale should be accounted for as revenue under FASB ASC 606. If the transaction is not part of normal business activities, it should be accounted separately from revenue under FASB ASC 610-20. Entities also need to keep track of the value of digital assets over time. For this, the AICPA recommends developing a method for identifying units bought and sold using the FIFO method.

[1] https://www.aicpa-cima.com/resources/download/accounting-for-and-auditing-of-digital-assets-practice-aid-pdf

Investment Managers: Investment companies holding digital assets must navigate accounting a little differently than exchanges. The AICPA recommends that if an investment company decides to interact with digital assets, it should consider whether the activities are consistent with those of an investment firm. If an investment company does decide to invest in digital assets, it must determine whether each asset represents a debt security, equity security, or other investment. Then, the firm must measure the fair value of the digital asset(s).

Broker-Dealers and Custodians: Broker-dealers and custodians need to follow special guidelines with regard to digital assets as well. For registered broker-dealers, the SEC has actually released a Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities. This statement gives some guidance on how broker-dealers should navigate accounting for digital assets. In terms of revenue recognition, the AICPA suggests that broker-dealers act similarly as if it was a stock transaction, and recognize commission income when the broker-dealer satisfies their performance obligations under contract (FASB ASC 606).

Stablecoins: There is also a large variety of digital assets including stablecoins, derivatives, NFTs, and more. The AICPA aims to help firms make the right accounting decisions but can not provide general rules because digital assets may have different circumstances. Therefore, they recommend that firms consider the purpose of the digital asset, the issuing entity, whether it's collateralized, and more. Then, apply GAAP and FASB standards to determine how the asset is classified and how to account for it.

Auditing Under AICPA[2]

On the audit side of the framework, the AICPA intends to help auditors ensure proper asset verification. They first suggest that auditors have a thorough understanding of the nature of an entity and its environment. However, there are a lot of other considerations that an auditor must keep in mind if a firm is involved with digital assets: types of digital assets held, how the entity maintains custody of

[2] https://www.aicpa-cima.com/resources/download/accounting-for-and-auditing-of-digital-assets-practice-aid-pdf

the assets, whether the entity holds digital assets on behalf of others, what types of wallets are used, the entity's transactions, and much more.

On top of understanding the entity's processes, it is important for auditors to understand risk management and controls. Auditors must investigate an entity's policies and procedures as well as how they assess risks in the Web3 space. The AICPA suggests that digital assets should be safeguarded through strong encryption, multi-signature wallet addresses, off-chain wallet keys, and a multitude of other control processes that auditors must verify to ensure a thorough audit.

In the AICPA's practice aid, they offer guidance on lending and borrowing, mining, client acceptance and continuance, and laws and regulations with related parties. As new developments occur within the Web3 space, the AICPA and other accounting organizations will update digital asset accounting and auditing guidelines. Though, with no clear regulatory guidance on digital assets, the "Big 4" and other firms involved with digital assets will have to refer to the AICPA's guidelines, and other published works to help them navigate digital asset accounting and audit.

Digital Asset Advisory

Traditional audit firms have been reluctant to work with cryptocurrency, blockchain, and Web3 companies due to a lack of knowledge, understanding, and regulatory guidance. Many of these firms, including all of the 'Big 4', have experimented with the space, but have since pulled back. The risks of taking on Web3 clients outweigh the potential benefits, as evidenced by Armanino's loss of credibility from auditing FTX.US before its collapse. This lack of professional audit resources leaves blockchain-based companies without the necessary stamps of approval to grow credibly. With this problem, some firms see an opportunity and are working to develop blockchain audit techniques, standards, and frameworks, despite the absence of regulation which may eventually lead to regulatory standards and frameworks for Web3 accounting.

Bentley Blockchain's "Big 4" Digital Asset Teams

With the "Big 4" (PWC, KPMG, EY, and Deloitte) being some of the most trusted entities in the world, it is exciting to see how they have developed their digital asset teams. Additionally, there are non-Big 4 firms that have stepped up to fill the market need. This section provides an overview of what we believe are the four most impactful accounting and audit firms in the blockchain space, including honorable mentions.

1) Deloitte

Deloitte was an early mover to the space during the previous bull market and is the only traditional Big 4 firm to still have a Web3-based, publicly traded client: Coinbase. This loyal relationship has given Deloitte the opportunity to grow and evolve in the Web3 space with an early-mover and industry leader at the forefront of blockchain regulations. No other audit firm has this experience. Also, many of their current clients are also innovating and building within the Web3 space like Microsoft, Blackrock, Charles Swab, Loews, and many more[3]. In the coming years, many of the traditional clientele of Big 4 firms may have Web3 auditing activity and with Deloitte's experience with Coinbase, they may be best positioned to capitalize on this evolution. Finally, there are reports that Circle, the parent company of the second largest stablecoin (USDC) will be switching over to Deloitte for their audits in 2023[4].

2) Grant Thornton

Grant Thornton has experience auditing Circle and Coinbase before they both moved to Deloitte in 2022 and 2020 respectively. For Coinbase, Grant Thornton got everything prepared for them to go public in 2021, one year after they moved to Deloitte[5]. Grant Thornton has audited Circle, the parent company of the second-largest stablecoin, USDC since 2019. "These audits have been filed publicly with the U.S. Securities and Exchange Commission (SEC)" as Circle made a push to become publicly traded "via blank check" SPAC in 2022 (fell through after FTX

---

[3] https://managementconsulted.com/big-4-audit-clients/

[4] https://www.bloomberglaw.com/product/tax/bloombergtaxnews/crypto/XFVFPJ5G000000?bna_news_filter=crypto#jcite

[5] https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm

collapse)[6]. Coinbase is a main fiat on/off ramp and Circle is connecting the digital asset economy to the world reserve currency (USD). Grant Thornton has dealt with some of the largest, and most influential players in the Web3 space. This proven track record and earned credibility place the audit firm at the top of Web3 auditing.

3) Marcum LLP

Marcum audits 3 of the 5 largest publicly traded mining companies–Marathon Digital Holdings Inc., Riot Blockchain Inc., and Cipher Mining Inc– with their "proprietary industry-specific audit tools.[7] They also claim to hold "several privately held crypto companies, including crypto exchanges" but withheld to list specific details[8]. In that same interview with Bloomberg, Marcum Chairman and CEO Jeffrey Weiner doubled down on the Web3 industry by saying "We are not getting out of [blockchain auditing]" when asked if the firms were going to drop their Web3 clientele like Armanino, Mazars, the Big 4 and other audit firms did. Marcum's commitment to the space plus their experience with 3 publicly traded mining companies and other Web 3 firms make them stick out as an elite blockchain accounting firm.

4) Ernst and Young (EY)

EY seems to be taking more of a research, partnership, and education-based approach to the blockchain space until more structured regulation is in place. While they do not have notable blockchain-based 'clients,' they do have many current clients– Google, Apple, Amazon, Meta, and State Street–who are actively pursuing blockchain innovations[9]. Knowing this, EY has begun learning, building infrastructure, and positioning itself properly for when the time is right. For example, their "alliance with TaxBit" which "provides [Web3] organizations with a suite of [tax and accounting-based] solutions."[10] Also, the EY Global Blockchain Summit hosts "innovators and industry leaders in the event that aims to reframe blockchain

---

6 https://www.bloomberglaw.com/product/tax/bloombergtaxnews/crypto/XFVFPJ5G000000?bna_news_filter=crypto#jcite

7 https://www.marcumllp.com/industries/digital-currency-blockchain

8 https://www.bloomberglaw.com/product/tax/bloombergtaxnews/financial-accounting/X6BJH1E4000000?

9 https://managementconsulted.com/big-4-audit-clients/

10 https://www.ey.com/en_gl/news/2022/12/ey-announces-alliance-with-taxbit-to-support-tax-reporting-requirements-for-digital-assets

through industrialized, sustainable and scalable solutions"[11]. Finally, the "EY Blockchain Analyzer: Reconciler" is a public tool for "reconciling off-chain enterprise records with on-chain transactions, tracking wallet balances" and offers a "digital signature verification feature."[12] EY's passive, behind-the-scenes activity positions them well to jump into blockchain auditing when the time is right, or their current clients force their hand.

Honorable Mentions:

KPMG: While KPMG's current web3 clientele and past experience are limited, they are making efforts to position themselves as a leader in the space when structured regulation is established. KPMG has established a blockchain-specific branch to their business and has named it "KPMG Chain Fusion®."[13] As per KPMG's website "Chain Fusion integrates with blockchain API services, enabling us to efficiently use data from multiple blockchains in a reliable and consistent format." With KPMG's Big 4 status and many of their notable clientele having strong Web3 initiatives–Fidelity, Costco, Citigroup, BNY Mellon, Home Depot, and more–they are well positioned to grow their blockchain audit presence.

Mazars: Before the dramatic collapse of FTX, Mazars accumulated an impressive Web3 clientele: Binance, KuCoin, and Crypto.com to name a few[14]. In an effort to avoid loss of credibility by association, they dropped their entire Web3 clientele until further notice. Their Web3 experience is arguably the strongest of anyone out there, and if they continue to stay up-to-date during their hiatus, they could crack the BBA Research Teams 'Blockchain Big 4' list.

Prager Metis: The first and only accounting firm to have their headquarters in the metaverse–Decentraland (19,144) to be exact[15]. Their intentions to separate themselves from others as a blockchain niche accounting and auditing firm is clear, but so is their affiliation with the FTX collapse[16]. If the firm can clear its name and

---

11 https://eyblockchainsummit.virtualeventsite.com/

12 https://www.ey.com/en_gl/news/2022/05/ey-announces-general-availability-of-ey-blockchain-analyzer-reconciler

13 https://audit.kpmg.us/kpmg-chain-fusion.html

14 https://www.cnbc.com/2022/12/16/mazars-suspends-all-work-with-crypto-clients-including-binance-cryptocom.html

15 https://pragermetis.com/metaverse/

16 https://www.wsj.com/articles/ftx-auditors-doubled-as-crypto-industry-cheerleaders-11668709049

re-instill credibility within its Web3 niche, the BBA Research Team will evaluate its standing.

The Role of Traditional Accounting & Auditing Firms

There simply needs to be an intersection between traditional accounting and auditing standards, and blockchain firms. In an interview with Cointelegraph[17], Henri Arslanian (PwC's global crypto leader) said,

> **"Although Bitcoin was designed with a trustless ideology, the reality is that the industry still requires trusted entities to catalyze the development of the ecosystem" - Henri Arslanian**

And it is not only Bitcoin that has been designed with a trustless ideology, the larger digital asset space embodies trustless, decentralized principles. When thinking about institutional adoption, it is crucial that more conservative firms see that Web3 and blockchain firms interact with traditional, trusted entities in a positive manner. Consumers and other stakeholders will also propel the adoption of blockchain firms if there is more transparency and trust. In another interview with Cointelegraph[18], BC Group CEO, Hugh Madden said that

> **"Auditing, like regulatory clarity, provides confidence to all stakeholders that companies are operating transparently and adhering to expected industry standards. As the business of digital assets continues to grow and mature, and compliance and regulatory standards become more robust, auditors will continue to play a pivotal role". - Hugh Madden**

With the "Big 4" being some of the most trusted entities in the world, it is promising to see how they have developed their digital asset teams over the years to better assist the blockchain space. The non-Big 4 firms stepping up to fill the gap are a deliberate indicator of this pressing need for blockchain accounting and audit.

---

[17] https://cointelegraph.com/news/the-big-four-are-gearing-up-to-become-crypto-and-blockchain-auditors
[18] https://cointelegraph.com/news/the-big-four-are-gearing-up-to-become-crypto-and-blockchain-auditors

Part 2: Proof of Reserves Post-FTX

Understanding and Preventing Fraud

As mentioned previously, the recent FTX scandal has raised concerns regarding the transparency and security of cryptocurrency exchanges. FTX, the cryptocurrency exchange, was buying Stadium Names and Super Bowl Ads, while its founder, Sam Bankman-Fried, was lobbying Congress to benefit FTX's role in American politics. At the same time, Bankman-Fried was manipulating FTX's Bitcoin, Ethereum, and Altcoin reserves to illegally utilize customer deposits. The scandal was uncovered by blockchain analytics firm Nansen, revealing that FTX had been falsely inflating its reserves and the company was taking out loans with its native cryptocurrency FTT as collateral. Headquartered in the Bahamas, the FTX team took advantage of the lack of a regulatory framework to get into the pockets of the most powerful politicians and business people in America.

FTX's inevitable bankruptcy allowed American regulatory institutions to evaluate auditing practices for crypto-native companies. Currently, understanding the solvency of exchanges that are handling millions of dollars every second is at the forefront of regulatory debate. According to the Cambridge Centre for Alternative Finance, 40% of crypto exchanges do not publish reserve balances, while 23% only partially disclose them[19] Additionally, crypto liabilities are even more difficult to track. FTX printing its own token and using it as collateral for loans is a prime example of lacking proof of liabilities as well. Without formal standards or requirements for exchanges to disclose their assets, users are unable to fully trust these counterparties. Bad actors can easily manipulate their balances. One proposition is requiring Proof of Reserves – an auditing mechanism that requires cryptocurrency exchanges to affirm their reserves using cryptographic proofs.

In the case of FTX, Proof of Reserves could have prevented the scandal by exposing the discrepancy between the exchange's reported balances and its actual balances. As an offshore entity in an already unregulated industry, there were no formal standards or requirements for FTX to disclose its reserves. Alongside the creation of

[19] https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf

the FTT token, FTX took advantage of the lack of a regulatory framework and was not expected to provide Proof of Reserves. In a tweet following the scandal, Sam Bankman-Fried tried to verify FTX.US's reserves using a spreadsheet he created. SBF published his own "Proof of Reserves" in a tweet:

Date	Creator	Customer balances	Tokens	FBO bank	Corp bank	LedgerX	Corp Nov 11	LedgerX Nov 11	Other Bank
November 10th	SBF	497,323,421	484,676,723	23,918,495	90,577,638	250,000,000	90,577,638	250,000,000	0
November 11th	S&C	More than $181m	181,000,000	29,400,000	235,900,000	128,400,000	114,300,000	250,000,000	34,400,000
	Creator	Total bank	Wallet		Total Assets		Max Customer	Est Customer	
November 10th	SBF	364,496,133	484,676,723		849,172,856		497,323,421	497,323,421	
November 11th	S&C	428,100,000	181,000,000		609,100,000		497,323,421	199,128,204	
	Creator	Min NAV	Est NAV		FBO+Token-Customer				
November 10th	SBF	351,849,434	351,849,434		11,271,796				
November 11th	S&C	111,776,579	409,971,796		11,271,796				

These are simply numbers on a spreadsheet inputted by SBF with no way of verifying that these assets even exist. There must be a way for exchanges to prove assets-liabilities on hand using cryptography or other blockchain-based security protocols. Currently, there is no way for SBF to legitimately publish a Proof of Reserves trusted by all parties involved. Proof of Reserves would allow for the location and history of transactions to be validated and tracked on a real-time basis. Instead of trusting numbers inputted by a human, this process can be automated and trusted with a Proof of Reserves auditing system.

To make Proof of Reserves a viable future, it is important to understand how current players in the industry are auditing their reserves and how Proof of Reserves could change current accounting and audit practices. In the next section, two of the largest cryptocurrency exchanges in the world –Coinbase and Binance – are evaluated to compare how they currently audit their reserves in the wake of the FTX situation.

Case Study: Coinbase (Public) vs. Binance (Private)

This section outlines the details, differences, and shortfalls in auditing practices and PoRs for two of the world's largest exchanges: Coinbase and Binance. The BBA Team selected Coinbase because of its publicly traded status (NASDAQ: COIN), SEC filing regulations, and custodian business model (where PoRs are especially relevant). Binance was selected because it is a direct competitor to Coinbase but without SEC affiliations and regulatory oversight.

Coinbase

Coinbase users must satisfy strict KYC and AML policies, like pictures of government-issued IDs, proof of home address, and social security information before accessing the platform. This ensures every Coinbase user can be identified and held responsible for their activities, transactions, and taxes.

Coinbase is audited externally by Deloitte, which enforces SEC regulations and frameworks[20]. The SEC then reviews these audits on an annual basis to confirm regulatory compliance. Coinbase is the only publicly traded Web3/crypto company to have an external audit performed by a 'Big 4' firm.

Per Deloitte, a specific process of PoR's audits and/or on-chain analysis for Coinbase is not made clear, but there is a clear emphasis and focus within certain areas. For example, establishing "Internal controls" for "implementing blockchain solutions and digital asset management" and "properly account[ing] for and disclos[ing] digital asset transactions."[21] As per Coinbase, Deloitte asked them to move assets in "randomly selected cold storage wallets" to prove ownership of the cryptographic keys[22]. Coinbase also states that Deloitte tries to "tell the story of how those numbers came to be" through Merkle Tree analysis (Coinbase). With that PoR data and results have never been made public by Deloitte or Coinbase, and only reassured by the two. One thing worth noting is that starting in Q2 2023 an amendment to Staff Accounting Bulletin (SAB) No. 121 called "Series FF" will make

[20] https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm
[21] https://www2.deloitte.com/us/en/pages/audit/solutions/blockchain-solutions-for-digital-asset-transactions.html
[22] https://www.coinbase.com/blog/how-crypto-companies-can-provide-proof-of-reserves

cryptocurrency custodians record customer deposits (liabilities) and assets as specific cryptocurrency names and amounts on financial statements[23]. This added clarity and transparency will make the audits and PoRs for publicly traded cryptocurrency custodians like Coinbase much easier going forward.

Binance

Binance also requires all of its users to satisfy KYC and AML policies before gaining access to the platform. This process includes government-issued photo ID, Proof of home address, and social security.

As a private company, Binance is not required to be externally audited but has hired auditors in the wake of FTX's collapse to re-instill trust and credibility. The last PoR audit was done by Mazars in early December and "At the time of assessment, Mazars observed Binance controlled [Bitcoin] assets in excess of 100% (101% to be exact) of their total platform liabilities[24] There is some skepticism about the legitimacy of these audits as they only contained Bitcoin and Wrapped Bitcoin assets/liabilities. Bitcoin makes up the majority of Binance's asset/liability value, but they support over 120 different cryptocurrencies. Another area of concern is that not all corporate documentation and financials were released to Mazars for the audit. Mazars has since dropped Binance as a client in an effort to ditch blockchain exposure until there is more clarity in the space.

In response to public hesitations and criticism, Binance made an effort to demonstrate confidence in their financials and PoR by asking Big 4 firms to audit them. These firms have all rejected the invite, in order to avoid private, cryptocurrency-related companies that do not follow SEC accounting practices and guidelines[25]. With no credible auditors to provide a stamp of approval like that of Coinbase, Binance has reported to their own monthly Merkle Tree audits with zkSnark (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) self-assessments: a cryptographic proof system used in Proof of Reserves protocols, providing a way to mathematically demonstrate the existence and

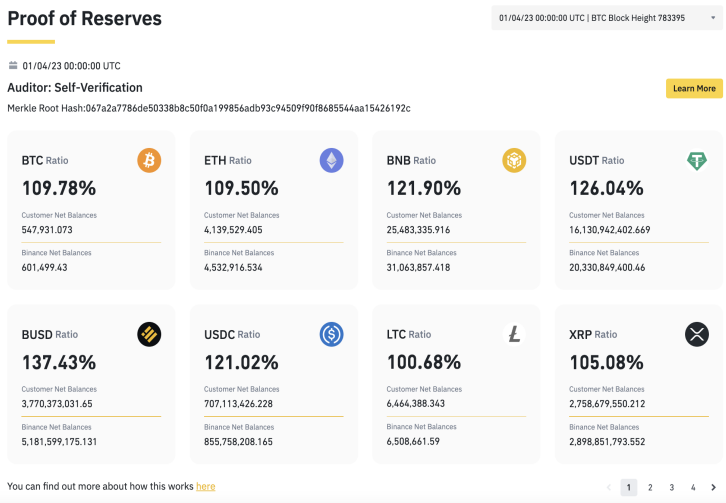
---

23 https://www.sec.gov/oca/staff-accounting-bulletin-121

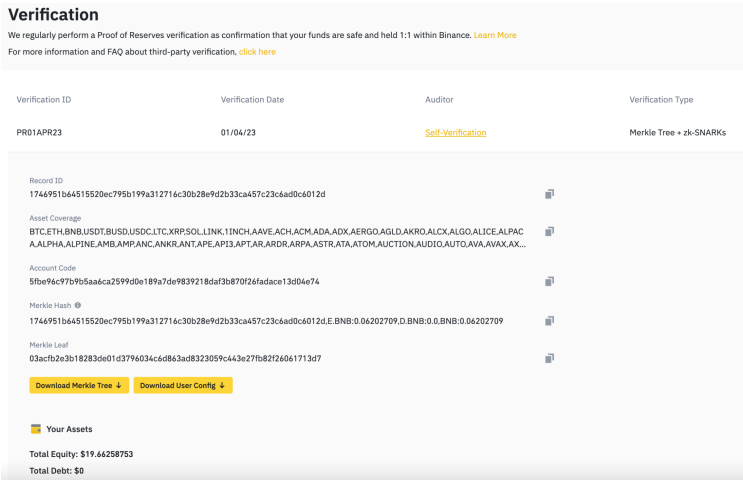
24 https://www.coindesk.com/business/2022/12/07/binances-bitcoin-reserves-are-overcollateralized-says-audit/

25 https://www.binance.com/en/feed/post/125201

accuracy of reserves held by an entity without revealing specific details about the reserves or requiring interaction with the entity holding them. Binance publishes the reserve ratios, Merkle Tree, Leaf, and Hashes for the top 25 liabilities/assets for public due diligence[26].



In addition to this, Binance provides monthly documents to the Merkle Tree data for each user's individual holdings to personally test and validate. While the documents are there, critics emphasize how large and complex the documents are (some hundreds of thousands of Excel sheet rows long) and how it only takes one placeholder leaf hash to negate the validity of the Merkle Tree.



26 https://www.binance.com/en/proof-of-reserves

Key Comparisons:

Coinbase does not need to be as public about PoR information. Users appreciate its affiliations with credible organizations and time-tested regulatory institutions, like the SEC. Some critics highlight concerns about how Deloitte and Coinbase do not make their PoR analysis public, but Deloitte appears to be a leader in the Blockchain auditing space and that satisfies public consensus. Binance has attempted to evoke the same sense of confidence in its users, but its private status limits this. To make up for the shortfall, Binance publishes zk-SNARK proof Merkle Trees to the public despite skeptics concerned about hidden misguiding/corrective activities. With over $900M of VC funding recently dropped into ZK solutions, there is high potential for using a ZK-backed approach. Ultimately it comes down to what resonates most with public sentiment; Deloitte's blockchain audit team and the SEC, or the general public. The BBA Research Team's conclusion is that Coinbase has more transparency and regulator attention making malicious or manipulative on-chain transactions less feasible than its private counterpart Binance.

Part 3: A Hypothetical PoR Framework

Proof of Reserves Framework: Our Suggestion

Proof of Reserves is a concept that refers to a cryptographic mechanism by which cryptocurrency exchanges or custodians prove to their users that they hold the funds they claim to hold. The aim of Proof of Reserves is to increase transparency and trust among users by reducing the risk of fraud or insolvency by the service provider.

There are various methods that can be used for Proof of Reserves, each with its own advantages and limitations. Some examples of Proof of Reserves methods:

On-chain verification: Providing users with the public addresses of the exchange's or custodian's wallets, allowing them to independently verify the balance of these wallets on the blockchain. By doing this, users can confirm that the exchange or custodian holds the funds they claim to hold. Examples of exchanges that use on-chain verification include Kraken and Bitfinex.

Multi-signature verification: Using a multi-signature wallet, where multiple keys are required to access the funds. The exchange or custodian provides one key, while the user provides another. This allows the user to independently verify the balance of the wallet without having access to the private key. An example of an exchange that uses multi-signature verification is BitGo.

Trusted third-party audit: Hiring an independent third-party auditor to fully audit the exchange or custodian's funds. The auditor provides a report that confirms the balance of the exchange or custodian's wallets. This method provides a high level of assurance but is often costly and time-consuming. An example of an exchange that has undergone a trusted third-party audit is Coinbase.

Overall, Proof of Reserves is an important mechanism for increasing transparency and trust in the cryptocurrency ecosystem. Exchanges and custodians should provide users with greater confidence in their services, which can ultimately help to drive adoption and growth in the industry. Our team has researched these methods

and has come to our own conclusion on how Proof of Reserves audits can be done in the future. This section outlines our Hypothetical Proof of Reserves Framework:

Certification for Blockchain Accounting and Audit

Our suggestion to the AICPA is to establish a certification to audit blockchain companies using a standardized Proof of Reserves methodology. Just as the CPA is the gold standard for traditional accounting and audit practitioners, establishing a CPA for blockchain-facing accountants could validate the cryptocurrency industry. A potential 'CBA'–Certified Blockchain Accountant–would have the same status CPAs have in the traditional, public accounting space only within the blockchain space. This would then allow internal audit teams and external audit firms to hire credible and reliable resources. Having certified individuals performing internal and external audits on blockchain protocols, companies, and organizations, the public would have a newfound confidence in them, finally bringing the PoR stamp of approval to the blockchain space.

The framework and criteria to achieve this certification are hard to predict, but the BBA Research Team believes a prospective 'CBA' will have extensive knowledge of the cryptocurrency ecosystem – understanding the protocols behind lending, borrowing, staking, and other custodial practices. A CBA will also have to be a partner to the SEC and other global regulators. A CBA must have sound ethical principles, with an emphasis on their fiduciary responsibility of providing impartial Proof of Reserves audits. Most importantly, a CBA will have to study the technical, mathematically-derived concepts behind actually performing a Proof of Reserves audit for a crypto-based company. On top of the technical aspects, there must be standardized attestation periods to ensure CBAs can account for all recent transactions within a crypto-based company. These concepts, both technical and objective are outlined below:

PoR Attestation Periods

One of the most debated issues when developing a strong PoR framework is how often to perform attestations. Conducting thorough PoR attestations takes time and it may be impractical for custodians to conduct daily or weekly attestations. Hence, we suggest that on a quarterly basis, custodians should perform complete PoR attestations with the involvement of an external auditor. Quarterly filings that are verified by external auditors will provide transparency and trust for all stakeholders assuming there is no fraud committed in between attestation periods. A large concern for PoRs is that it is only a snapshot of a firm's accounts. This means that custodians could borrow a lot of assets to appear solvent for the attestation period. To prevent this kind of fraud, we intend to implement a Multi-Party Computation (MPC) control mechanism which will be discussed in more detail in "Risk Management and Controls".

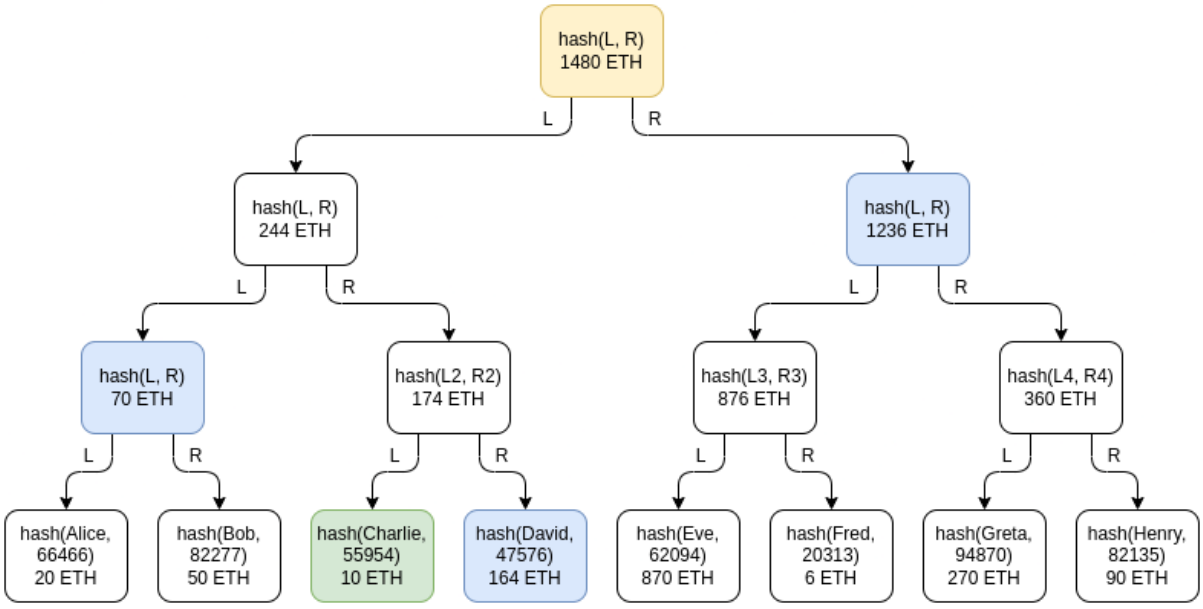
Additionally, we also want to provide custodian clients with the opportunity to ensure their assets are solvent. So, we want to add a user-facing PoR that allows users to collectively verify their individual balances. Binance currently does this on a monthly basis which we believe is a strong time frame. The more often these attestations are conducted, the better. Hence, we suggest that custodians should perform user-facing PoRs at least once a month. Though one aspect we would like to change about Binance's current user-facing PoR is its readability. Earlier, we discussed how Binance's reports to its users consist of Excel files with hundreds of thousands of rows of Merkle tree data. We suggest that custodians create a better UI/UX that presents the users with a readable report of the solvency of their assets. The Merkle tree data can be added as a supplementary document as well, but creating a user-friendly interface goes a long way in establishing transparency.

Technical Specifications

Our technical recommendation is to send each user a Merkle sum proof of their holdings and publicly publish a ZK attestation to verify that all balances in the Merkle tree are non-negative.

Merkle Proofs

The implementation of Merkle trees has been the standard in PoRs and similar exchange proofs since 2015. Allowing users to verify that their assets are covered, Merkle trees consist of user balances, hash pairs, and a root hash. Exchanges would send each user the necessary and randomized balances in the tree, enabling them to verify that their balance is accounted for in the root hash.



Merkle tree sent to Charlie(green). The blue nodes are what Charlie can see to verify his balances. The yellow is the root hash, which is publicly published to all users. [27]

Although better than other user-facing implementations, Merkle Trees are not without limitations. In the previous example, for Charlie(green) to verify his balances, he finds out that two people have 70 Eth and four people have 1236 Eth. Regardless,

[27] https://vitalik.ca/general/2022/11/19/proof_of_solvency.html

Merkle trees remain the leading method of conducting PoRs and are the most attainable method of user-facing PoR for most exchanges with exchanges such as Kraken, Kucoin, Derebit, and BitMex using them.

ZK Methods

In the near future, ZK methods of verifying user balances are likely to become the dominant method of conducting PoR attestations. ZK Snarks & Starks (ZK Succinct Non-interactive Argument of Knowledge and ZK Test with Transparent and Scalable Arguments respectively) are two common methods of implementing ZKs in PoRs with Binance and OKX, among others, taking advantage of the wealth of security and accuracy benefits that ZK methods provide. Gaining traction over the past few years, ZK methods of attestation have been rarely implemented due to the relatively complicated and unstandardized mathematics required to use them. Called "Moon Math" prior to 2017, the scope of researchers capable of understanding and improving upon them has been limited resulting in slower progress, but as the field of mathematics advances, the outlook is promising[28].

Snarks

Zk-Snarks are a way of verifying user balances without revealing any sensitive information about other users. Proving that computation has a particular output very quickly regardless of the underlying computation length, ZK-Snarks are ideal for verifying user balances in exchanges such as Binance with 100M+ accounts. Using Elliptic Curve pairings and polynomial commitments, ZK Snarks can verify large amounts of information with ease and speed. Major limitations include a lack of a completely trustless setup and the potential for minimal data leakage at large scale (Buterin, Intro to ZK-Snarks)[29].

Starks

ZK-Starks are similar to ZK Snarks in that they can compute large volumes of information without revealing the inputs. Relying on far simpler mathematical principles, ZK-Snarks can prove and account for positive balances without needing

[28] https://vitalik.ca/general/2021/01/26/snarks.html
[29] https://vitalik.ca/general/2021/01/26/snarks.html

trusted set up or ECC pairings, with only one major fallback: the size of the proof. ZK-Snarks can be hundreds, or even thousands of times larger than ZK-Snarks, increasing computation duration and cost (Buterin, Starks, P1)[30].

Considerations and Comparison

ZK Snarks and ZK Starks each have their benefits and limitations and as a result exchanges should choose which method to use, depending on their standings. Other potential methods of implementing ZK attestations are being researched, and a clear industry standard may appear in the coming months or years. The Mathematics involved with ZK Methods of attestation are beyond our scope of expertise; a cryptographer would be required to set the standards for mathematical methods of verifying ZK snarks and Merkle trees.

Risk Management and Controls

In our framework, we believe that it is imperative to implement strong controls to reduce the risk of fraud. The FTX case is a prime example of how firms can manipulate funds to take advantage of their users. Therefore, we highly recommend that when auditors (or CBAs in our case) are conducting control matrices, they look for the below controls. These controls are just a few examples of what custodians can implement to ensure privacy and security when conducting PoRs.

Secure Multi-Party Computation (MPC)[31]

MPC is a powerful control mechanism for PoRs that will help minimize the risk of fraud or manipulation by a single party. This cryptographic tool is designed to help secure digital assets by ensuring the integrity and confidentiality of the relevant data. It allows for multiple parties, such as the custodian and independent auditors, to collectively compute a function without revealing their individual inputs. This technology in conjunction with zk-proofs provides the utmost level of privacy and security. It also is a strong method of fraud detection as auditors can perform cross-checks and comparisons of data from different sources involved in the PoR

[30] https://vitalik.ca/general/2017/11/09/starks_part_1.html
[31] https://www.fireblocks.com/what-is-mpc/

attestation. This will help to prevent custodians from borrowing large amounts of assets to appear solvent for their attestation.

Comprehensive Address Tracking

On-chain wallet address tracking for cryptocurrency exchanges and custodians allows auditors to follow the transactions of a crypto-based company. Companies like CoinMarketCap and Glassnode have released products that are tracking the on-chain wallet addresses of the largest cryptocurrency exchanges, including Binance, BitFinex, and Bybit. Address tracking will allow auditors to confirm the integrity of reserves and detect any discrepancies or potential irregularities.

Segregation of Duties:

Segregation of duties is crucial in a Proof of Reserves audit to ensure the integrity and reliability of the process. Different individuals or teams should be responsible for custody and control of reserves, data management and analysis, and approval and verification of audit findings. This separation helps to minimize the risk of errors, fraud, and unauthorized activities, promoting transparency and accountability in the audit process.

References

AICPA. (2022, December 9). *Accounting for and auditing of Digital Assets Practice Aid* . AICPA & CIMA. https://www.aicpa-cima.com/resources/download/accounting-for-and-auditing-of-digital-assets-practice-aid-pdf

Betz, B., & Braun, H. (2023, May 9). *Binance's Bitcoin Reserves are Overcollateralized, New Report Says*. CoinDesk . https://www.coindesk.com/business/2022/12/07/binances-bitcoin-reserves-are-overcollateralized-says-audit/

Binance. (2023, January 5). *Proof of Reserves*. Binance. https://www.binance.com/en/proof-of-reserves

Blandine, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., Zhang, B., & Cloud, K. (2019, April). *Global Cryptoasset Regulatory Landscape*. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf

Coinbase Global, Inc. (2021, February 25). *Form S-1*. https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm

COINCU. (2022). *Coincu on Binance Feed: Binance: 4 Major Auditing Firms Refuse to Audit Reserves for Private Crypto Companies*. Binance Feed. https://www.binance.com/en/feed/post/125201

Curtis, M. (2022, May 11). *EY announces general availability of EY Blockchain Analyzer: Reconciler*. https://www.ey.com/en_gl/news/2022/05/ey-announces-general-availability-of-ey-blockchain-analyzer-reconciler

Deloitte. (2023). *Audit and advisory services for blockchain and digital assets*. https://www2.deloitte.com/us/en/pages/audit/solutions/blockchain-solutions-for-digital-asset-transactions.html

Dimajo, B. (2022, December 16). *EY announces alliance with TaxBit to support tax reporting requirements for digital assets*. https://www.ey.com/en_gl/news/2022/12/ey-announces-alliance-with-taxbit-to-support-tax-reporting-requirements-for-digital-assets

Eaglesham, J., & Kowsmann, P. (2022, November 17). *FTX Auditors Doubled as Crypto Industry Cheerleaders*. https://www.wsj.com/articles/ftx-auditors-doubled-as-crypto-industry-cheerleaders-11668709049

EY. (2023). *2023 EY Global Blockchain Summit | 9-12 May 2023*. https://eyblockchainsummit.virtualeventsite.com/

Fireblocks. (2023). *What is MPC (Multi-Party Computation)?*. Fireblocks. https://www.fireblocks.com/what-is-mpc/

Jolly, D. (2023, January 17). *Stablecoin Issuer Circle Adds Big Four Firm Deloitte for Audits*. https://www.bloomberglaw.com/product/tax/bloombergtaxnews/crypto/XFVFPJ5G000000?bna_news_filter=crypto#jcite

KPMG. (2023). *KPMG Chain Fusion*. https://audit.kpmg.us/kpmg-chain-fusion.html

Management Consulted. (2023, January 12). *Big 4 Audit Clients*. https://managementconsulted.com/big-4-audit-clients/

Marcum LLP. (2023). *Digital Assets & Blockchain: Finding Clarity In The High-Speed Digital Assets Landscape*. https://www.marcumllp.com/industries/digital-currency-blockchain

Martin, P. (2022, November 25). *How crypto companies can provide proof of reserves*. https://www.coinbase.com/blog/how-crypto-companies-can-provide-proof-of-reserves

PragerMetis. (2023). *Metaverse*. https://pragermetis.com/metaverse/

Rooney, K., & Sigalos, M. (2022, December 16). *TECH Mazars Group suspends all work with crypto clients including Binance, Crypto.com, citing concerns over public perception of proof of reserves*. https://www.cnbc.com/2022/12/16/mazars-suspends-all-work-with-crypto-clients-including-binance-cryptocom.html

U.S. Securities and Exchange Commission. (2022). *Staff Accounting Bulletin No. 121*. U.S. Securities and Exchange Commission. https://www.sec.gov/oca/staff-accounting-bulletin-121

Vitalik. (2021, January 26). *An approximate introduction to how zk-snarks are possible*. Vitalik. https://vitalik.ca/general/2021/01/26/snarks.html

Vitalik. (2022, November 19). *Having a safe CEX: Proof of solvency and beyond*. Vitalik. https://vitalik.ca/general/2022/11/19/proof_of_solvency.html

Vitalik. (2017, November 9). *Starks, part I: Proofs with polynomials*. Vitalik. https://vitalik.ca/general/2017/11/09/starks_part_1.html

Wagner, C., & Strack, B. (2022, December 16). *As Crypto Auditors Call It Quits, What Will Take Their Place?* https://blockworks.co/news/crypto-auditors-call-it-quits

White, N. (2022, December 19). *Marcum Raises Risk Assessments for Crypto Audit Clients*. https://www.bloomberglaw.com/product/tax/bloombergtaxnews/financial-accounting/X6BJH1E4000000?

Wolfson, R. (2022, May 29). *The Big Four Are Gearing Up to Become Crypto and Blockchain Auditors*. https://cointelegraph.com/news/the-big-four-are-gearing-up-to-become-crypto-and-blockchain-auditors