Proof of Assets

A Summary Analysis

Bitcoin Policy Institute

Authors: Matthew Pines, David Zell, Grant McCarty, Jason Brett

About the Bitcoin Policy Institute

The Bitcoin Policy Institute[1] is a nonpartisan, nonprofit organization researching the policy and societal implications of Bitcoin and emerging monetary networks. BPI believes that the internet is changing society's relationship with money as profoundly as it has with information. To ensure sound policy, the U.S. needs rigorous research that moves past hype and cynicism alike. BPI fellows represent economists, technologists, climate scientists, lawyers, and philosophers who work to provide relevant insights to policymakers, journalists, and the public at large.

Matthew Pines
Fellow - National Security and Geoeconomics

Matthew Pines is a Managing Consultant at the Krebs Stamos Group, a cybersecurity and geostrategic intelligence consultancy. He has over ten years of experience helping the government and private sector firms address pressing security and resilience challenges. He has conducted dozens of assessments of national preparedness, emerging technology, and strategic security programs for the U.S. government. As a National Security Fellow at the Bitcoin Policy Institute, he conducts research and analysis to help policy-makers understand the implications of Bitcoin as an emerging technology. He holds a master's degree in Philosophy and Public Policy (with Distinction) from the London School of Economics and Political Science and a bachelor's degree in Physics and Philosophy (with Honors) from Johns Hopkins University.

David Zell
Co-Executive Director

David Zell is the Co-Executive Director of the Bitcoin Policy Institute and a Visiting Fellow at the Foundation for Research on Equal Opportunity. Prior to co-founding BPI, David was the Director of Policy at BTC Inc. Before that, he was a Fellow at the University of Alabama where he studied political science.

Grant McCarty
Co-Executive Director

Before founding the Bitcoin Policy Institute, Grant served as the Executive Director of the Bitcoin Advocacy Project and the Co-Director of Policy and Public Affairs at Bitcoin Magazine. Prior to those roles, Grant was running his own marketing consulting firm and digital marketing agency. He also founded an education startup dedicated to reducing inequity in college admissions, he worked as the CMO for a fintech startup in Silicon Valley, and he was the COO and co-founder of a nonprofit focused on developing an online learning platform for young students. He received his undergraduate degree from the University of Alabama and his MBA from Johns Hopkins University.

Jason Brett
Policy Director

Jason formerly served as a regulator at the FDIC during the last financial crisis. Additionally, he has extensive experience in developing and implementing successful governmental affairs programs for various companies, including clients of Key Bridge Advisors. While serving as Policy Director for ConsenSys, he was responsible for their domestic and international policy during a key period of their growth. Jason has also worked as a consultant at Booz Allen Hamilton, the Operations Director for the Digital Chamber of Commerce, and the Founder of the Value Technology Foundation, a non-profit technology think tank. He is also a forbes.com contributor who writes on policy issues related to bitcoin, other cryptocurrencies, and blockchain. Jason holds an MBA from American University and a bachelor's degree from Cornell University.

---

[1] https://www.btcpolicy.org/


BITCOIN · DIGITAL · DECENTRALIZED · PEER TO PEER
1 TROY OZ .999 FINE COPPER .999 MONEY OF THE FUTURE METAL

Table of Contents

Introduction

Recent events in the digital assets market have cast issues of counterparty risk into sharp relief. High profile failures and acute stresses experienced by major custodians, algorithmic stablecoins, and other institutional intermediaries have revealed a number of structural issues in the market. These events have drawn the scrutiny of regulators and policymakers concerned about consumer protection, financial stability spill-overs, and malicious behavior. On November 8, Rep. Patrick McHenry, the Republican leader of the House Financial Service Committee, released a statement on the events involving trading platforms FTX and Binance: "The recent events show the necessity of Congressional action. It's imperative that Congress establish a framework that ensures Americans have adequate protections while also allowing innovation to thrive here in the U.S." More stringent regulation may be on the horizon. More importantly, FTX's liquidity crisis underscores the industry's existential need to mature on its own. Now is the time for market participants to identify private, voluntary solutions to improve transparency and instantiate related best practices.

Proof of Reserves, Assets, and Solvency

One such solution emerging in the market goes by the moniker "**Proof of Reserves**" (PoR), which is a method that uses techniques of cryptographic verification to publicly demonstrate possession of digital assets sufficient to cover outstanding liabilities. Hours after Binance signed a nonbinding letter of engagement to buy competitor FTX, CEO Changpeng Zhao publicly pledged[1] to adopt proof of reserves in order to achieve "full transparency." There are various approaches across different types of user liability (e.g., asset-backed tokens, crypto platform account liabilities, crypto security instruments) and different terms used in different use-cases. Readers are encouraged to review the Chamber of Digital Commerce's thorough report on Proof of Reserves[2] for a thorough presentation of these issues and related policy recommendations.

1 https://twitter.com/cz_binance/status/1590055819416330240?s=42&t=xwF9FofvWLRpYSGpqOHLbw

2 https://d3h0qzni6h08fz.cloudfront.net/reports/Proof-of-Reserves-.pdf

Importantly, PoR (as commonly used) only accounts for the digital asset liabilities of a entity–other liabilities must be accounted for by traditional audit processes and attestations to actually prove that a given entity has the *assets* it claims and that these assets fully cover extant liabilities. A complete, public attestation of "**Proof of Solvency**" thus involves showing that one's liabilities (both digital and fiat assets) are covered by one's assets.

Even in this case, the term "proof" is somewhat of a misnomer, as there are other conditions (e.g., key duplication, hidden encumbrances, window-dressing, post-audit loses, auditor incompetence/duplicity, auditor-auditee collusion, etc.) where the "proven" liabilities or assets may not reliable. Also, importantly, such attestations are point-in-time and must be regularly and frequently updated to be continuously valid.

This paper uses the term "**Proof of Assets**" (PoA) to refer only to those methods of public cryptographic verification of digital assets. We do not assess attestation standards or accounting methods for liabilities that exist outside of a digital ledger. Here, we **review recent market dysfunction** (Section 1), broadly **assess relevant industry policies and practices** (Section 2), and **examine potential benefits of expanded Proof of Asset assurances** (Section 3).

Our key findings:

- Recent market dysfunction has been exacerbated by lack of transparency and associated counterparty mistrust across digital asset custodians and market participants.

- These crises will likely spur greater industry convergence to a consistent set of standards and practices, more entities are adopting Proof of Assets, and firms are developing market-based approaches that increase transparency and support more effective self-regulatory solutions.

- Increased transparency using proof-of-asset techniques will provide more information on counterparty risk, reducing the chance of systemic default contagion and improving user trust in their custodial relationships.

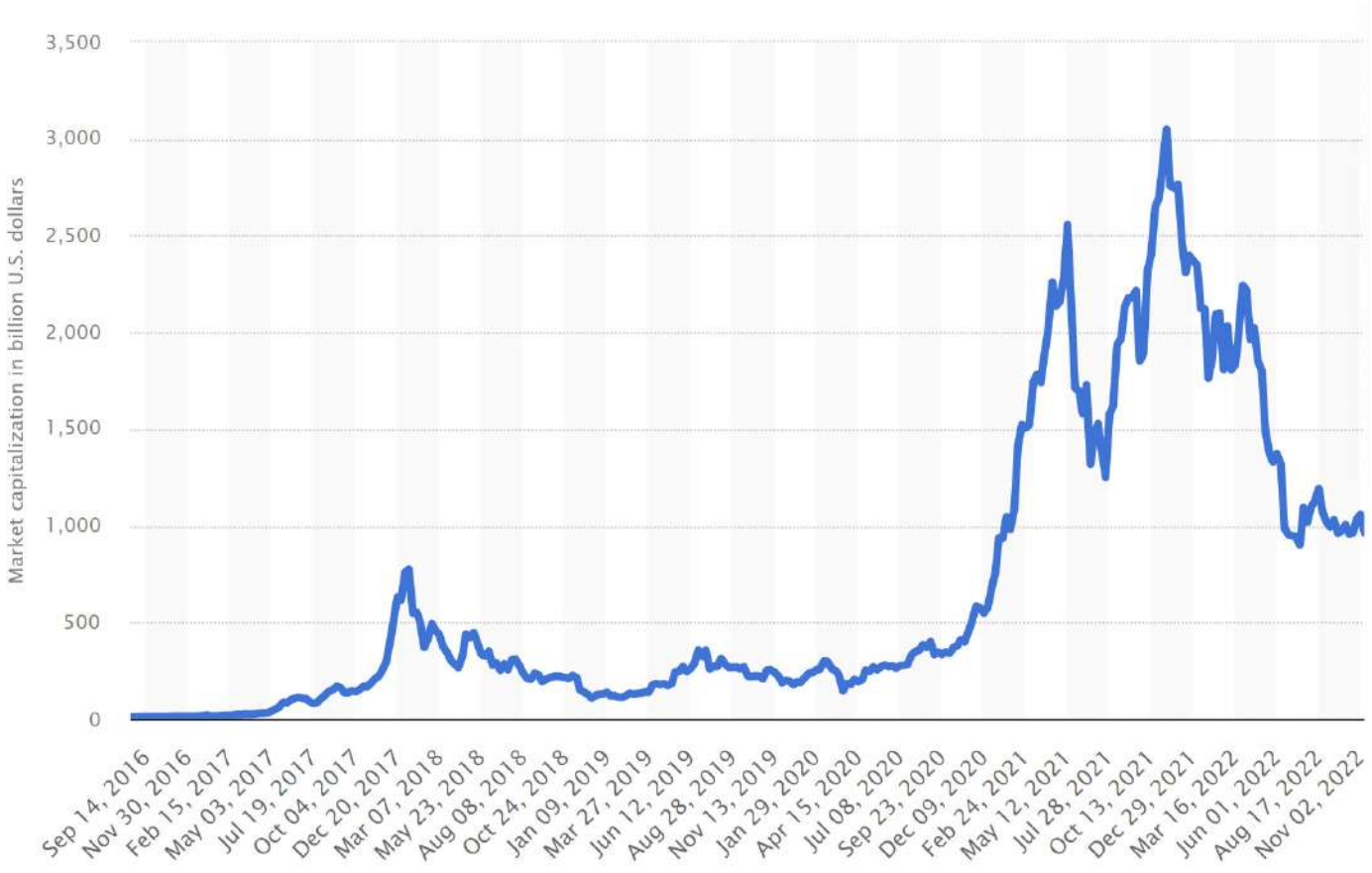
1 Review of Recent Market Dysfunction

After a bull market that saw total cryptocurrency market capitalization peak at just over $3T in November 2021, macroeconomic and global liquidity conditions deteriorated and digital assets dramatically declined, shedding almost $2T in total market value in about seven months. At the time of writing, the overall market is hovering around $1T in total market value, roughly four-five times the range of valuation the market saw in the last bear market recovery 2018-19.

Exhibit 1

Overall cryptocurrency market capitalization per week (in billion U.S. dollars)

Worldwide: July 2010 to September 2022



Additional Information: Note that due to changing exchange rates, the USD values as reported can change. This also applies in retrospect.

Sources: CoinGecko; BitInfoCharts © Statista 2022

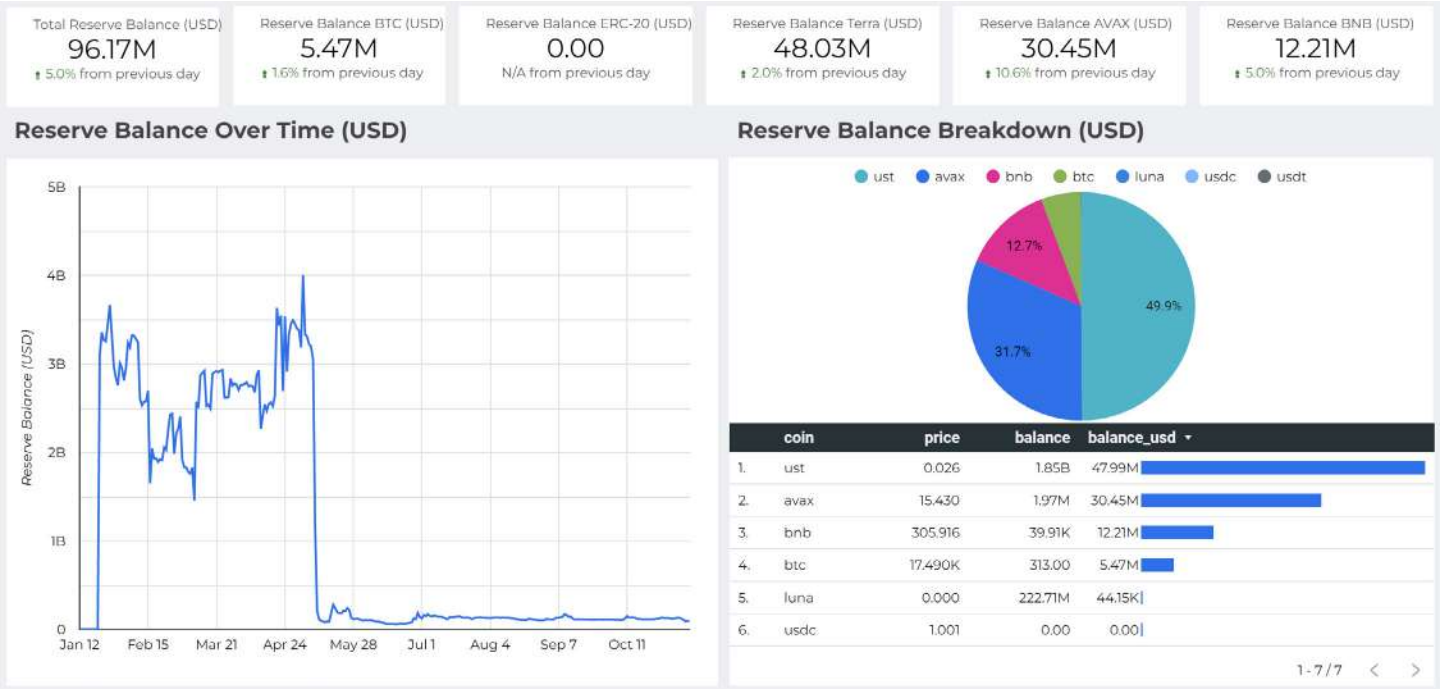
Falling asset values placed particular strain on tokenomic and business models that relied on leverage and the rehypothecation of digital asset collateral. Just as traditional shadow banking systems are prone to run risk without a lender-of-last-resort backstop, the relatively nascent crypto-asset ecosystem found itself facing a classic contagion-dynamic. The bull market led to the explosion of leverage (liability expansion) and rehypothecation (re-pledging) of collateral that multiplied and extended chains of counterparty risk across the market.

Importantly, in such conditions it isn't merely the degree of counterparty exposure, but the *uncertainty* around such exposure that exacerbates market instability. As exemplified by the past several day's whirlwind of rumors and speculation about FTX and Alameda Research, fear and doubt quickly erode informal webs of trust. No one can be exactly sure how exposed their direct counterparties are to third-party risks. Falling asset fallings lead to margin calls, selling begets more selling, and classic doom-loop of market panic sets in.

This is exactly what occurred in digital asset markets from March to June in 2022. While overall market conditions were fragile as a result of the leverage conditions described above, the proximate trigger for the crash is commonly thought to be in the failure of the Terraform Labs-backed algorithmic stablecoin Terra (UST). The inherent instability in the construction of the stablecoin peg mechanism revealed itself as its reserve collateral–LUNA and BTC assets held by the Luna Foundation Guard (LFG)–fell in value, precipitating a vicious feedback loop and market run dynamic.

Exhibit 2

Luna Foundation Guard (LFG) Reserves



- Please note the BTC reserve balances have been loaned out as voted by the LFG Council: LFG Council has voted to execute: Loan $750M worth of BTC to OTC trading firms to help protect the UST peg; Loan 750M UST to accumulate BTC as market conditions normalize.
- The traders will trade the capital on both sides of the market to help accomplish both #1 and #2, eventually maintaining parity of the LFG Reserve pool (denominated in BTC) as market conditions progressively stabilize.
- For more details, please reference: https://twitter.com/LFG_org/status/1523512196965167104?s=20&t=J37oL3QuvuBJIS_jBoVSgA.

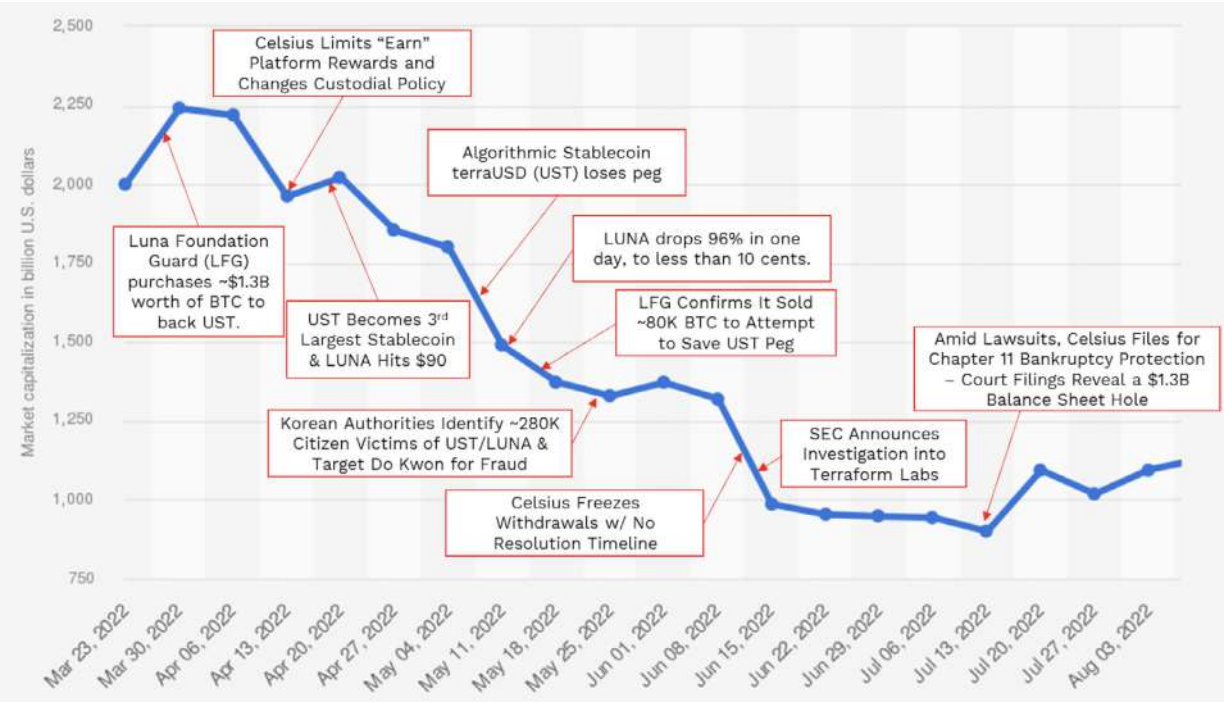
Over a matter of days, the UST-USD peg completely failed, LUNA lost more than 96% of its value, and the LFG foundation revealed that it had been forced to liquidate more than 80,000 BTC in the process. While this was a substantial failure—at its peak UST was the 3rd largest stablecoin and Korean authorities identified approximately 280,000 apparent victims in South Korea alone–it was the resulting contagion that made it a systemic event across the crypto market.

The prominent crypto hedge fund 3AC had deep exposures to these failing assets and suffered crippling losses.[1] As a result, 3AC defaulted on substantial obligations to a broad range of other major institutions. One can see UST and LUNA as akin to the mortgaged-backed securities and credit default swaps that became toxic assets bringing down Lehman Brothers in 2008. In this case, it was 3AC that turned out to be a source of systemic risk to the digital asset market, as a raft of other firms quickly found themselves on the brink of insolvency.

Exhibit 3

Timeline of Events: LUNA/Celsius

Worldwide: July 2010 to September 2022



Additional Information: Note that due to changing exchange rates, the USD values as reported can change. This also applies in retrospect.

Sources: CoinGecko; BitInfoCharts © Statista 2022

[1] https://www.cnbc.com/2022/07/11/how-the-fall-of-three-arrows-or-3ac-dragged-down-crypto-investors.html#:~:text=3AC%20told%20the%20Wall%20Street,when%20the%20stablecoin%20project%20failed.

A major crypto-asset platform, Voyager Digital, acknowledged a major hit to its books from 3AC's defaults and suspended withdrawals.[1] BlockFi, a leading crypto lending platform, was also hit by 3AC-related losses and relied on a $400 million revolving credit line from FTX US to avoid insolvency.[2]

A more significant failure, however, was Celsius Network, which suspended all trading, swaps, and customer withdrawals on June 13.[3] Celsius sought Chapter 11 bankruptcy protection a month later and revealed in court filings that it owed $4.7 billion to thousands of users.[4] Many of these users were lured to the platform on the promise of high returns from "staking" their assets, only to find that, unlike FDIC-insured banking deposits, their funds were no more than unsecured loans to a now bankrupt entity. Lawsuits quickly followed, as well as the belated scrutiny of various state and federal regulators and law enforcement.[5,6]

The dominoes continued to fall throughout the summer as a large number of crypto exchanges and lending platforms had to "temporarily" reduce withdrawal limits or suspend them altogether. The following displays just some of the entities that were affected, representing explicit defaults on obligations to hundreds of thousands (if not millions) of users around the world.

1 https://www.cnbc.com/2022/07/01/voyager-digital-suspends-all-trading-deposits-and-withdrawals-.html

2 https://www.theblock.co/post/155516/blockfi-strikes-680-million-credit-deal-with-ftx-us-outlines-acquisition-path?utm_source=twitter&amp%3Butm_medium=social

3 https://web.archive.org/web/20220709030130/https://gizmodo.com/celsius-bitcoin-price-crypto-withdrawals-scam-money-tan-1849051951

4 https://www.pymnts.com/cryptocurrency/2022/celsius-founder-reportedly-withdrew-10m-in-weeks-before-bankruptcy/

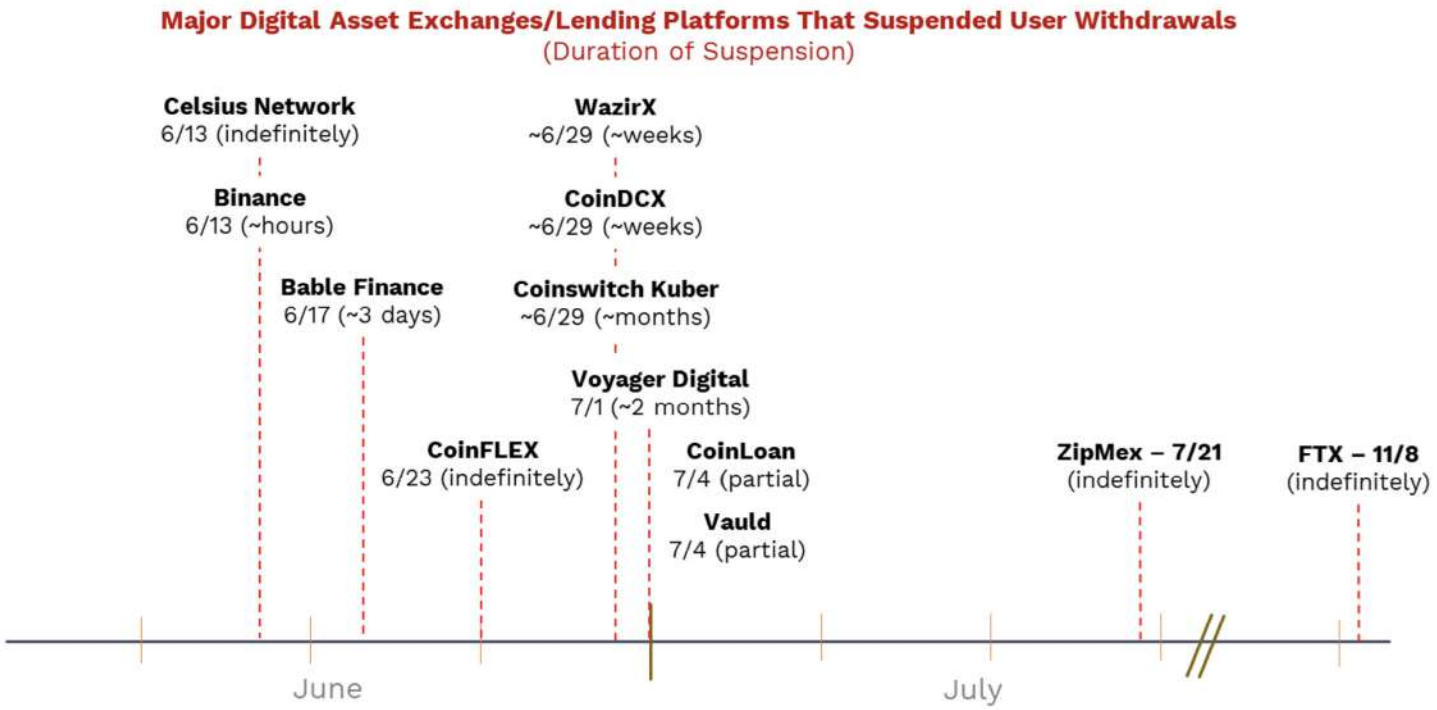
5 https://www.reuters.com/legal/government/bankrupt-crypto-lender-celsius-agrees-examiner-review-2022-09-09/

6 https://www.cnbc.com/2022/06/16/state-securities-regulators-investigating-celsius-accounts-freeze.html

Exhibit 4

Major Digital Asset Exchanges/Lending Platforms That Suspended User Withdrawals

Duration of Suspension



Sources for graphic: Celsius Network[1], Binance[2], CoinFLEX[3], Babel Finance[4], WazirX[5], CoinDCX[6], Coinswitch Kuber[7], Voyager Digital[8], CoinLoan[9], Vauld[10], ZipMex[11], FTX[12])

1 https://www.cnbc.com/2022/06/20/celsius-asks-users-for-more-time-to-fix-issues-after-withdrawal-freeze.html#:~:text=Celsius%20halted%20withdrawals%20for%20customers,hitting%20a%20number%20of%20companies.

2 https://web.archive.org/web/20220709030130/https://www.theguardian.com/technology/2022/jun/13/crypto-lender-celsius-network-halts-withdrawals-extreme-market-conditions#:~:text=Binance%20said%20in%20a%20statement,bitcoin%20network%20withdrawals%2C%20Binance%20said.

3 https://fortune.com/crypto/2022/08/10/crypto-exchange-coinflex-files-for-restructuring-after-halting-withdrawals-in-june/

4 https://web.archive.org/web/20220705234033/https://babel.finance/article-views.html?id=50

5 https://news.bitcoin.com/india-freezes-crypto-exchange-wazirxs-bank-assets-binance-claims-acquisition-of-wazirx-was-never-completed/

6 https://coingeek.com/coindcx-restricted-withdrawals-will-strengthen-compliance-and-risk-framework/

7 https://inc42.com/features/coinswitch-coindcx-struggle-to-address-user-issues-as-crypto-tds-comes-into-effect/

8 https://bitcoinist.com/crypto-broker-voyager-to-resume-cash-withdrawals/

9 https://www.coindesk.com/business/2022/07/05/crypto-lender-coinloan-latest-to-limit-user-withdrawals/

10 https://www.bloomberg.com/news/articles/2022-07-04/crypto-lender-vauld-freezes-withdrawals-weighs-restructuring

11 https://techcrunch.com/2022/07/20/zipmex-pauses-withdrawals-until-further-notice/

12 https://www.coindesk.com/business/2022/11/08/ftx-exchange-halts-all-crypto-withdrawals/

As noted above, leverage and rehypothecation are expected features of most financial systems, especially the type of shadow banking market structures that proliferated in the latest crypto bull run.

The reinforcing dynamics of human psychology, market optimism, and speculation that lead to asset bubbles inevitably tip the other way, driving contraction of balance sheets, falling collateral values, margin calls, forced selling and rippling waves of defaults that can undermine the solvency of (what only days prior) were seen as solid institutions.

Lack of transparency significantly aggravates these dynamics, as was seen in the cascade of default risk driven by the opacity of counterparty exposure to the UST/LUNA collapse and 3AC. Customers of exchanges and retail oriented lending platforms suddenly found their custodied assets converted into pari-passu credit claims now at the mercy of bankruptcy courts (potentially in a foregin jurisdiction).

Though increased transparency may not have prevented all the failures noted above, proof of assets/reserves would have likely mitigated the acute contagion, driven as it was in moments by *uncertainty* over one's counterparty risk–whether they were "good for it" or not. In conditions of such uncertainty, fear predominates, market participants assume the worst, and attempt to be the "first out the door".

These conditions are ones where the collateral damage can spread far beyond the initial failure, making it critical to explore and implement market-driven solutions that can reduce counterparty risk, bolster consumer trust, and improve accountability across the industry.

All this leads to our first key finding:

Recent market dysfunction has been exacerbated by a lack of transparency and associated counterparty mistrust across digital asset custodians and market participants.

2 Assessment of Current Transparency-related Industry Policies and Practices

As the collapse of Celsius and BlockFi's travails showed, lack of transparency can lead to dramatically different (and obscured) risk profiles for different platforms. Consumers should be able to easily find reserve policies, exchange leverage ratios, and understand rehypothecation and investment practices. Emerging solutions in this area promise to help users assess how platforms may be using leverage and fractional reserves to generate the source of offered yield. The market is a good discriminator of bad behavior and those platforms that lose customer trust will see loss of business. Recent positive trends in the market may make it possible to produce more broadly available, accurate, and persistent reputation and reporting systems for retail customers.

Many industry participants have recently voluntarily adopted some form of Proof of Reserves or Proof of Assets[1]. In particular, Kraken[2], Nexo[3], Coinfloor[4], Gate.io[5], HBTC[6], BitMex[7], and Ledn[8] have conducted a Proof of Reserve attestation within the last two years. Many of these custodians and lending platforms either self-assess or use auditor assistance to make attestations and allow users to validate the proof from a Merkle root. Most are point-in-time, account-specific processes, while others are ongoing with various frequencies (e.g., semi-annual).

1 https://niccarter.info/proof-of-reserves/

2 https://www.kraken.com/proof-of-reserves

3 https://real-time-attest.trustexplorer.io/nexo

4 https://coinfloor.co.uk/hodl/proof/

5 https://www.gate.io/article/17489?from=banner_proof

6 https://hbtc.zendesk.com/hc/en-us/articles/360046287754-HBTC-100-Proof-of-Reserve

7 https://blog.bitmex.com/proof-of-reserves-liabilities-bitmex-demonstration/#:~:text=BitMEX%20has%20always%20been%20an,the%20top%20of%20the%20file.&text=Therefore%20this%20file%20can%20be,that%20the%20funds%20are%20spendable

8 https://ledn.io/en/proof-of-reserve

Firms have approached the task of increased transparency in different ways. From 2014 to 2021, bitcoin exchange Coinfloor produced monthly "Provable Solvency Audits."[1] While the exchange did not publish third-party verification of the state of its liabilities, the effort was laudable and prescient. Firms like Gate.io and HBTC launched Proof of Reserves initiatives with third party attestation of liabilities, but both efforts were point in time analyses rather than proof on an ongoing basis. This model comes with obvious limitations – namely that a malicious firm could borrow capital on a short term basis to inspire undue confidence in the size of its holdings. In February of this year, Kraken partnered with accounting firm Armanino LLP to publish a Proof of Reserves feature that allows users to verify the existence of their funds.[2] Kraken has pledged to conduct a similar audit on a semi-annual basis. While firms have experimented with different market-based transparency solutions, the rate of Proof of Reserves adoption is skyrocketing following FTX's liquidity crisis. As of November 9th, eight prominent exchanges followed Binance in pledging to increase transparency through Proof of Reserves: Gate.io, KuCoin, Poloniex, Bitget, Huobi, OKX, Deribit and Bybit.[2]

We expect recent market events to drive further adoption of proof of assets. Progress with major entities adopting these practices is clear cause for optimism. In the wake of the recent crises, firms will increasingly seek out ways to gain the trust of potential customers. The obvious strategy for such entities is to integrate proof of assets and proof of reserves into their platforms, allowing them to starkly differentiate their product from competitors. It is reasonable to assume that given recent events, consumers will increasingly prefer responsible, transparent platforms over their opaque counterparts. As more entities adopt these practices, users will have access to more information to compare different products and make more risk-informed choices across platforms and services.

For example, firms like Hoseki[3] are developing much-needed, innovative solutions that provide a range of tools to help both platforms and their users gain better visibility, control, and use over their digital assets. These types of tools enable digital asset holders to accurately attest to their ownership and enable more transparent forms of fractional reserve lending that mitigate uncertainty-driven counterparty risks.

1 https://d3h0qzni6h08fz.cloudfront.net/reports/Proof-of-Reserves-.pdf

2 https://blog.kraken.com/post/12774/verify-your-bitcoin-and-ether-balances-on-kraken-with-proof-of-reserves/

3 https://www.coindesk.com/business/2022/11/09/crypto-exchanges-scramble-to-compile-proof-of-reserves-as-ftx-contagion-grips-markets/

4 www.hoseki.app

These types of tools and an emerging industry-consensus around their benefits can support the formation of self-regulatory organizations (SROs) that use attestations, cryptographic verification, and transparency policies to reduce overall market risk and improve customer protections. These developments are nascent but already established and they need time to mature to show their fruits. Given the nascency of these technologies and the incentives spurring their adoption, we encourage policymakers to give the industry time to continue its trend of self-regulation before employing a balanced and prudent regulatory framework.

This leads to our second key finding:

The recent series of crises will likely spur greater industry convergence to a consistent set of standards and practices, more entities are adopting Proof of Assets, and firms are developing market-based approaches that increase transparency and support more effective self-regulatory solutions.

3 Assessment of Potential Benefits of Expanded Proof-of-Asset Assurances

It is technically straightforward to implement proof-of-assets at any centralized custodian, who merely needs to regularly disclose the complete set of digital assets addresses they claim to control. Anyone can then sum the amounts visible in these addresses at a particular block height. Doing this on a regular and consistent basis, and signing messages or transactions with the same set of public keys, can engender confidence that such disclosures are accurate.

As noted at the start, Proof of Solvency requires Proof of Assets + Proof of Liabilities. This latter portion of the formula is much more challenging to implement, especially in ways that preserve user privacy.[1] While technical schemes may make this more feasible (e.g., randomly shuffling and splitting individual account balances between multiple leaves of the Merkle tree), these are somewhat complex to implement, and create risks if done incorrectly (exposing user data). Further, these cryptographic techniques will likely have to be joined by the audit services of a trusted accounting firm.

1 https://blog.bitmex.com/addressing-the-privacy-gap-in-proof-of-liability-protocols/

That being said, there is ample low-hanging fruit to be had by having most custodial platforms move to implement Proof of Asset solutions. The key benefits accrue to the following:

- **Trust:** Users that see regular, reliable PoA attestations are likely to increase their confidence in the transparency of a platform, which if done across the industry, will increase aggregate levels of trust between users and custodians, an desirable outcome as long as users still seek to have a third-party hold their digital assets.

- **Auditability:** While PoA by itself doesn't amount to Proof of Solvency, it is a necessary condition for it, one which takes advantage of the cryptographic features of digital assets to enable more sophisticated, efficient, and privacy-preserving financial audits.

- **Fraud:** Dishonesty can't and won't be eliminated from the market, but if good actors adopt Proof of Asset best practices, there is less room for bad actors to freely exploit customer confidence.

- **Customer Protection:** Users of digital asset custodians deserve to see their service providers take due care in the protection of their assets and deploy available solutions that demonstrate an institutional commitment to transparency and accountability.

- **Counterparty Risk:** Proof of Asset solutions won't eliminate leverage, but implementations by systemically important market entities can help mitigate the sorts of fear-driven run dynamics that often stem (in part) from uncertainty over one's counterparty's asset holdings.

This leads to our third key finding:

Increased transparency using proof-of-asset techniques will provide more information on counterparty risk, potentially mitigating the chance of systemic default contagion and improving user trust in their custodial relationships.

Conclusion

High profile failures and acute stresses experienced by major custodians, algorithmic stablecoins, and other institutional intermediaries have revealed a number of structural issues in the digital asset market. While regulators have their prerogatives, it is important for market participants to identify private, voluntary solutions to improve transparency and instantiate related best practices.

One such solution exists that takes advantage of the publicly validatable nature of digital assets like Bitcoin. The cryptographic features of these assets makes it straightforward for a custodian to public an independently verifiable proof of the assets in its possession.

To recap, in this summary report we **review recent market dysfunction** (Section 1), broadly **assessed relevant industry policies and practices** (Section 2), and **examined potential benefits of expanded Proof of Asset assurances** (Section 3).

Our key findings were:

- Recent market dysfunction has been exacerbated by lack of transparency and associated counterparty mistrust across digital asset custodians and market participants.
- These crises will likely spur greater industry convergence to a consistent set of standards and practices, more entities are adopting Proof of Assets, and firms are developing market-based approaches that increase transparency and support more effective self-regulatory solutions.
- Increased transparency using proof-of-asset techniques will provide more information on counterparty risk, reducing the chance of systemic default contagion and improving user trust in their custodial relationships.

Proof of Assets and related transparency policies are not a panacea for malfeasance or other market risks, but they are eminently feasible (as demonstrated by the limited but growing number of institutional implementations). They clearly represent net positive low-hanging fruit for the digital assets industry to deploy and improve transparency with market-based approaches.

www.btcpolicy.org

Bitcoin Policy Institute