HexTrust

The Custody 3.0 Era: Institutional Participation in the Decentralized Economy

Hex Trust Insights

Jun 2022

The Custody 3.0 Era: Institutional Participation in the Decentralized Economy

The digital asset market has been in a persistent downtrend since the sell-off began back in November 2021. It's too soon to tell if we are entering another sustained crypto winter but the Twitterati and crypto media seem to be increasingly forecasting frosty months ahead. Should this forecast become reality, it's worth remembering that the last crypto winter which started in 2018 lasted around 18 months, characterized by little to no levels of interest and engagement.

Most of the unsustainable money-grab ICOs held just before winter set in failed less than 6 months after launch. Reducing the hype helped wash out all the projects that never really provided value anyway, and left us with an ecosystem of projects built on solid foundations. Many of the top tier applications that brought the market back to life in early 2020 were built during this time. Whether history will repeat itself remains to be seen. However, we believe that the serious players will continue to build and refine their products. This will be our greatest competitive advantage and moat at the next bull market.

There are significant differences when comparing the factors that caused the winter in 2018 and the situation we are in now. Today's digital asset industry is no longer a number of standalone alternative financial applications, but rather a highly interconnected ecosystem with millions of daily active users and - despite recent outflows - many more millions in Total Value Locked. Large financial institutions and corporations have finally entered the space and are integrating digital assets into their business operations.

Any financial institution that seeks to invest in the digital asset industry and participate in the decentralized economy needs access to licensed digital asset custodians to ensure their operations comply with regulatory requirements, the digital assets they hold are secure, and that their business models are adapted to accommodate the changes.

Digital asset custodians have evolved significantly over the past decade to meet the needs of today's market and accelerate institutional adoption globally. Moving from a pure safekeeping play, the market is now equipped with institutional-grade custody and infrastructure providers that not only secure assets under custody but also provide further connectivity for those custodied assets across DeFi, NFTs, Web3, and the metaverse.

We're only at the beginning of the digital asset market's evolution, but we can already clearly define the distinct stages of digital asset custody.

The Evolution of Digital Asset Custody

Custody 1.0

Self-Custody

- Paper wallets or seed-phrases pressed onto metal sheets
- Security solutions rely on a combination of cold storage and hot wallets
- Delayed access to digital assets in cold storage, involving manual operations

Custody 2.0

Institutional-Grade Frameworks

- Fully licensed digital asset custodians create efficient market infrastructure
- Solutions designed to meet regulatory, operational, and compliance requirements
- Leveraging specialized technology and institutional-grade controls

Custody 3.0

Participating in the Decentralized Economy

- Access on-chain decentralized finance from the safety of custody accounts
- Universal connectivity across chains, protocols, and applications
- Enabling organizations to integrate digital assets into business operations

Custody 1.0: Self-Custody

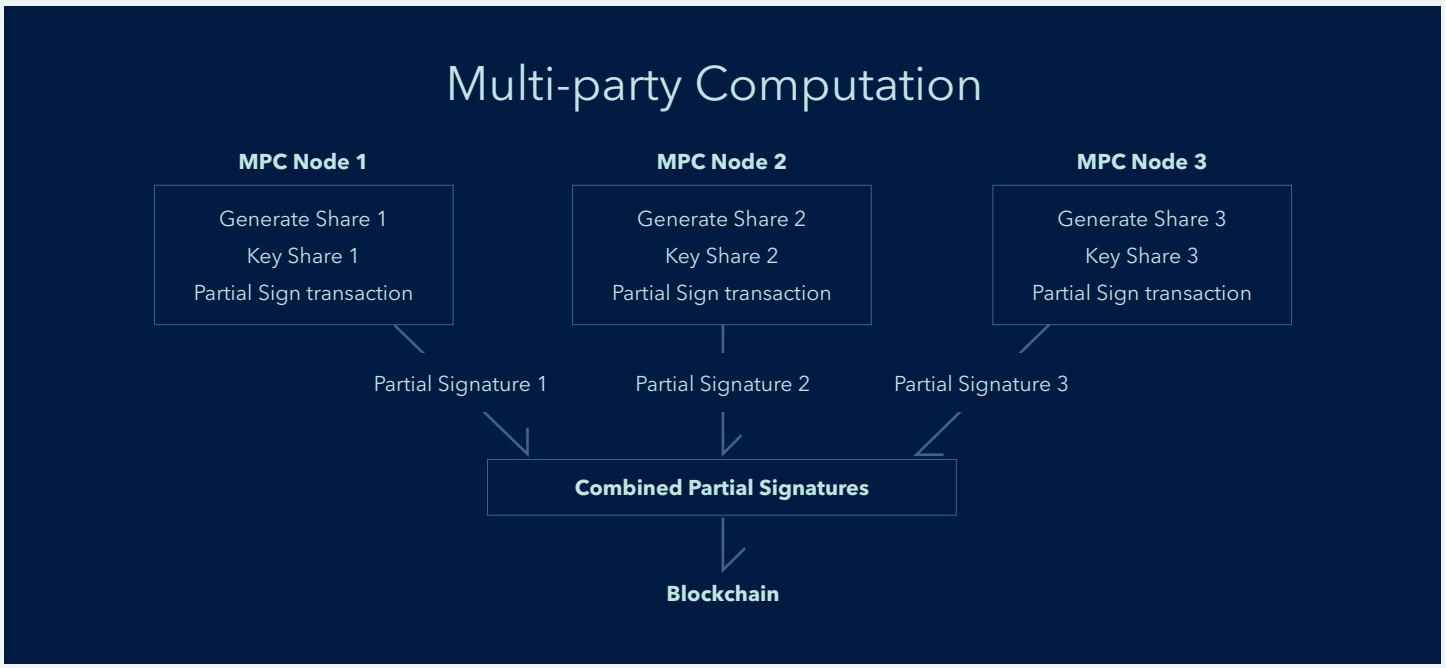
It seems like a lifetime ago, but back when Bitcoin mostly existed on the fringes of the internet, discussed on forums like bitcointalk.org and its network powered by the first retail adopters, the most secure method to store digital assets was in the form of self-custody. That typically meant paper wallets or seed-phrases pressed onto metal sheets kept in security boxes. At this point, Bitcoin mostly had retail value and any interest coming from institutional investors would have been negligible, so there was no need for institutional-grade digital asset custody solutions. That changed when Bitcoin adoption increased.

Around 2014, as retail activity surged more capital started to flow into bitcoin leading to increased security threats and sophisticated hacks - most notably the Mt. Gox exchange hack that resulted in the loss of 850,000 BTC, an amount valued at more than $450 million at the time and $18bn today. Following months of bearish conditions, the bull market kicked off in 2016 as the market expanded with a broader range of new digital assets such as Ethereum - providing a Turing-complete protocol which enabled the creation of smart-contracts and innovative use cases for digital assets.

Financial institutions finally started to grasp the full potential of blockchain technology, but entering the market in a meaningful way still presented complex challenges, in particular around the secure storage of digital assets under custody. During this time, most users including well-established exchanges still relied on self-custody, often hot wallets, which led to a persistent series of hacks.

Early custodial services provided by third-parties mostly offered cold storage solutions which meant private keys were stored using offline devices stored in secure vaults. But accessing digital assets in cold storage would often take days and involve a lot of human and manual operations - all elements prone to errors and exploits which did not meet institutional standards.

That led to the rise of numerous institutional-grade custody and infrastructure providers, including Hex Trust, which was established in 2018.



Custody 2.0: The Rise of Institutional-Grade Digital Asset Custodians

As larger firms started moving into the space, the challenges that custodians had to solve evolved into more complex issues. If Custody 1.0 required enterprise-grade security solutions, Custody 2.0 was about integrating those solutions into existing institutional frameworks to enable operational scalability and create efficient market infrastructure.

Regulated and fully licensed digital asset custodians were established with a focus on bridging the gap between the digital asset ecosystem and the traditional financial system, starting with custody solutions that meet stringent regulatory, operational, and compliance requirements.

At this stage, digital asset custodians began to offer institutions with secure and compliant services leveraging leading technology and institutional-grade controls including: multi-party computation (MPC), hardware security modules (HSM), multi-signature (multisig), customized transaction policies, comprehensive insurance coverage, regulatory compliance tools, and audited security and control frameworks. This opened up the pathway for accelerated institutional adoption, which was a phenomenon highly anticipated by early retail adopters.

Hardware Security Module (HSM) is a highly specialized hardware that can be customized to generate and store private keys, and to sign transactions at scale. These cryptographic modules can be certified under the Federal Information Process Standards (FIPS 140-2) standard to ensure specific security requirements. The IBM CryptoExpress HSM is rated FIPS 140-2 Level 4 for the highest level of certification achievable for commercial cryptographic devices.

Multi-party Computation (MPC) technology has existed for a while, but has only been applied to the field of digital assets in recent years. MPC allows for private key shards to be generated and used to produce signatures without the private key ever existing as a whole.

Digital asset custodians can be broadly categorized as licensed custodians, technology providers, or a hybrid of both. Licensed custodians are typically regulated financial institutions that assume the risk associated with the safekeeping of digital assets. Technology providers offer softer and/or hardware solutions that enable customers to safekeep their own assets. Hybrid providers like Hex Trust offer both types of solutions.

As jurisdictions across the globe start to provide a clearer regulatory framework, it's increasingly becoming a minimum requirement for third-party custodians to be licensed and regulated. Not only does this instill investor confidence and protection, it also paves the way for the creation of strategic digital asset hubs illustrated by the recent developments in locations such as Singapore and Dubai. Other typical obligations of a licensee include but are not limited to recordkeeping, detailed reporting, strict KYC/AML compliance, audited financials, and more. Reporting standards such as SOC I, II, ISO 27001, third-party audits, and regular penetration testing all provide further comfort to digital asset custody clients.

With the core custody challenges mostly solved for institutional investors from a technology and operations perspective, new needs and requirements have to be addressed. It is no longer sufficient for institutional investors to simply buy and hold assets in safe custody - they want the full breadth of services around custody to monetize digital assets.

Custody 3.0: Participating in the Decentralized Economy

The digital asset ecosystem has expanded significantly through decentralized finance (DeFi) over the past 2 years with dozens of blockchains, hundreds of interchain solutions, and thousands of decentralized applications. As the DeFi offering has become increasingly sophisticated, institutional investors are now focused on generating yield with digital assets and actively participating in the decentralized economy.

It's no surprise that investors are demanding access to protocols that could generate additional returns, and it will only increase as more tier 1 DeFi applications roll-out parallel services built specifically to meet regulatory requirements and compliance standards such as Aave Arc and Compound Treasury.

The Custody 3.0 era is about meeting those demands, which requires digital asset custody to evolve and include connectivity to on-chain

services and DeFi applications including staking, wrapping, delegating, DAO governance, trading, liquidity provision, token issuance, as well as financing and structured solutions. The key for regulated digital asset custodians is to build on the infrastructure put in place during the Custody 2.0 stage and offer the full breadth of on-chain services that enable all types of organizations to monetize digital assets - all within an operational framework set to the highest standards.

Our vision is that there will be universal custody where any assets and protocols will be supported, along with flexible signing, execution and deployment. As part of this fundamental infrastructure, we will be able to offer universal connectivity to the rest of the ecosystem, on-chain services such as staking, governance, and delegation that are interoperable across multiple-chains. All of these services would be highly scalable and accessible for institutional and consumer clients alike, designed against licensed and regulated frameworks.

Interestingly, with the emergence of the metaverse underpinned by a better understanding of how NFTs can be utilized, a greater number of new entrants to the digital asset industry are arriving whose journey starts at the Custody 3.0 stage. These are not necessarily financial companies, but rather organizations that seek to secure a competitive edge in their respective industries.

Examples include brokers of fine art such as Sotheby's diversifying into NFT collections, property developer Sun Hung Kai building up estates in the Sandbox, and tech giant Samsung running a virtual version of its NYC flagship store in Decentraland. For these new entrants, and the retail wave that will follow, the primary interest is in *utilizing* digital assets such as LAND NFTs, straight from the safety of institutional-grade custody.

During Custody 3.0, fully licensed digital asset custodians take on the role of trusted partners that enable financial institutions and organizations of all stripes to truly embed themselves in the industry and integrate digital assets into their business operations in a safe, scalable, and compliant manner.

Author:

Calvin Shen,
Managing Director at Hex Trust

Calvin has more than 10 years of financial services and investment experience across fintech start-ups and asset management. As the Managing Director at Hex Trust, Calvin works closely with clients to provide bespoke blockchain and custody solutions to help them bridge the worlds of digital assets and traditional finance. Prior to joining Hex Trust, Calvin was at Figure Technologies, a fintech and blockchain start-up based in San Francisco. Previously, he spent time at PIMCO, SSGA, Deloitte and BNY Mellon across portfolio management, business development and institutional sales based in the United States. He holds an MBA from Columbia Business School and a BA in economics from UC San Diego, and is a CFA and CAIA charterholder.

HexTrust

Digital Asset Custody Meets Innovation