Figure Markets

# Truth over Trust:

# Delivering on the Potential of MPC

By Alex Chen & Arnab Mitra

# Executive Summary

Figure Markets addresses challenges with asset custody on centralized exchanges through an unique implementation of multi-party custody (MPC) technology. Through our MPC methodology, investors remain in control of their assets through self-custody with the added reassurance that keys are not easily misplaced[1], all while taking advantage of trading efficiencies traditionally limited to custodial-only exchanges.

The emergence of decentralized finance brought a new wave of innovation in financial technology, offering individuals unprecedented control over their assets. However, this shift comes with a number of challenges. Central to these challenges is the management of private keys used to create the digital signatures required to access, control, and manage digital assets in the investor's blockchain accounts.

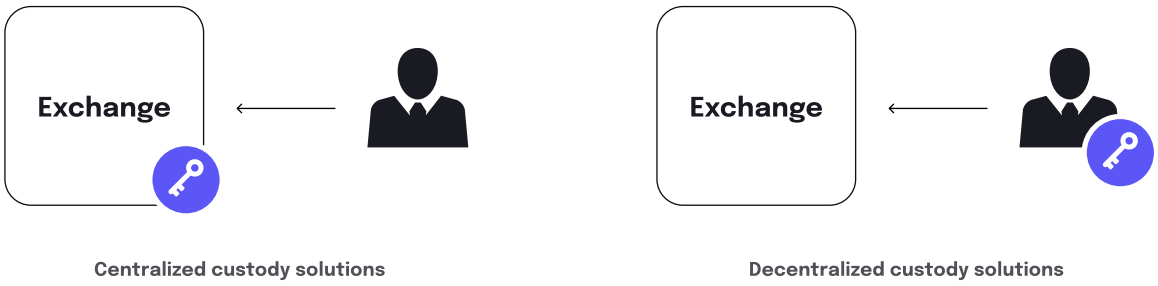
Prevalent approaches to key management offer a binary choice–centralized or decentralized solutions–each with its own set of limitations. **Centralized solutions,** including **custodial wallets** offered by many cryptocurrency exchanges, provide convenient key management to investors. However, these solutions entrust key management to exchanges or custodians who sign blockchain transactions on the investors' behalf.

While this model simplifies user experience, it contradicts the foundational principle of decentralization and the promise of blockchain technology by creating a single point of failure. Investors release control of their assets to their custodians or exchanges, exposing them to significant risks. These entities, who use centralized processes to decide whether a user can complete transactions, can also unilaterally abscond with funds without investor consent. This vulnerability is evidenced by recent incidents where organizations misused or stole client assets.

**Decentralized solutions,** including **self-custody wallets,** give investors complete ownership of their private keys, promoting a self-directed and autonomous experience. While this approach eliminates reliance on custodians by allowing only the owners of self-custody wallets to sign blockchain transactions, it places a security burden on investors and increases the risk of permanent loss of digital assets.

*[1] Utilizing guided mnemonic phrase backups*

For instance, an investor may misplace private keys (or equivalent mnemonic seed phrases) by losing access to their mobile device or computer.

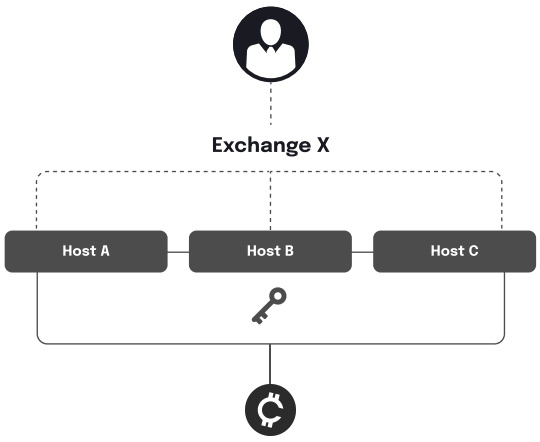



Centralized custody solutions

Decentralized custody solutions

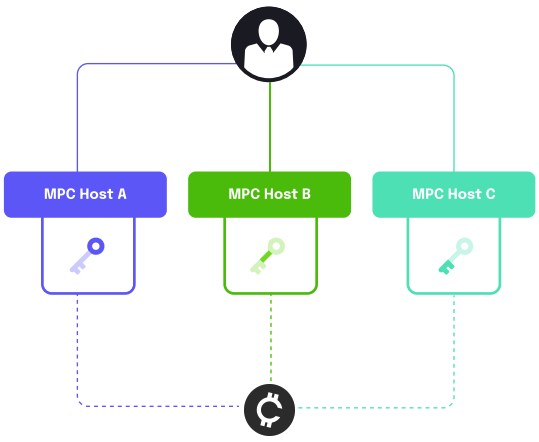
While the use of MPC technology in blockchain wallets has recently been popularized as a decentralized solution, the servers in the MPC construct that collaborate to sign transactions are typically under the control of one entity, defeating the purpose of a true MPC construct. Further, master backup keys, which exist for convenience completely bypass the MPC signing process, are also common. These practices result in a single entity having the ability to misuse or steal customer assets while running an MPC set up, resulting in the same challenge MPC was expected to address. In contrast, in a decentralized MPC custody construct, independent trusted MPC hosts must come together to move customer assets.

Centralized MPC Custody




Exchange controls all hosts

Decentralized MPC Custody




Hosts are independent

Blockchain wallet management challenges are particularly pronounced for institutional investors, since the choice between security and usability poses a significant barrier to entry to the digital asset space. Institutional investors need secure solutions that protect their substantial investments while increasing operational efficiency and meeting compliance requirements.


MPC
Technology

# Brief Overview

MPC enables multiple parties to participate together in a computation while protecting individual parties' private data. When private information is combined under an MPC protocol, a computation is performed in a way where no information can be inferred and no dishonest individual party can force honest parties to produce incorrect results.

In the context of digital asset trading and security, MPC technology is often used to create MPC custodial accounts and protect cryptographic keys. This differs from a traditional cryptocurrency wallet, where the complete private key required to authorize a transaction is either stored with a trusted custodian/exchange or held by the investor.

## Key MPC Definitions

| | |
|---|---|
| **Multi-party computation (MPC)** | A cryptographic protocol that enables multiple participants to collectively compute a specific result without disclosing their private data. |
| **Wallet** | A software application that holds private key information for one or more blockchain accounts.<br><br>The term "wallet" is often used as shorthand for the public and private keys required to receive and sign blockchain transactions.<br><br>Transactions include transfers of assets and transmission of blockchain messages. |

| | |
|---|---|
| **MPC custodial account** | An account that holds digital assets where the private key is protected using cryptography and requires the collaboration of multiple parties to sign blockchain transactions. |
| **Private key share** | A partial representation of a complete private key. An individual private key share cannot sign for blockchain transactions independently. However, when combined with other private key shares through an MPC protocol, they can collectively sign a blockchain transaction.<br><br>The MPC protocol prevents any MPC hosts from revealing their private key shares or information that could lead to the reconstruction of the full private key. |
| **MPC hosts** | Well-established, independent entities in the blockchain space who host servers to support the MPC network.<br><br>Each MPC host holds a private key share. MPC hosts follow software-defined rules and policies before they participate in the signing of blockchain transactions. |
| **Decentralized MPC custodial accounts** | MPC custodial accounts where private key shares are distributed to a number of distinct MPC hosts.<br><br>Thresholds ensure that the number of key shares presented must be greater than the number held by the MPC host with the most shares, ensuring no single MPC host can unilaterally move investors' assets. |

# Self-Custody Through MPC Technology

Figure Markets is creating a marketplace for digital and traditional assets that leverages the best of traditional and decentralized finance. From a single platform, investors will be able to trade a variety of assets, including crypto, stocks, and alternative investments, without the traditional myriad of intermediaries, delays, or unnecessary costs.

The core of Figure Markets is an exchange that supports high-frequency trading via matching off-chain and transparency of ownership through on-chain settlement. It allows retail and institutional investors to trade assets from Layer 1 (L1) blockchains like Bitcoin, Ethereum, and Provenance.

Trades on the Figure Markets exchange can be settled in both USD (fiat) and USDC. By leveraging MPC custodial accounts on any other L1 blockchain network, we can quickly support trading of additional cryptocurrencies trading on these networks. We avoid the use of smart contracts for cross-chain support, as they have been susceptible to hacks and headline-worthy crypto thefts[2].

One of our core tenets is that our customers have the right to maintain complete control over their assets until the moment they trade. Figure Markets firmly believes in truth over trust– the ownership and existence of an asset and claims to those assets should be without a doubt, true.

To support these beliefs and our investors, Figure Markets leverages MPC technology to enable self-custody. We provide all investors with MPC custodial accounts, which allow for the deposit and withdrawal of L1 assets. Additionally, we employ decentralization in the MPC custodial accounts to ensure that no single entity can move assets without investor consent.

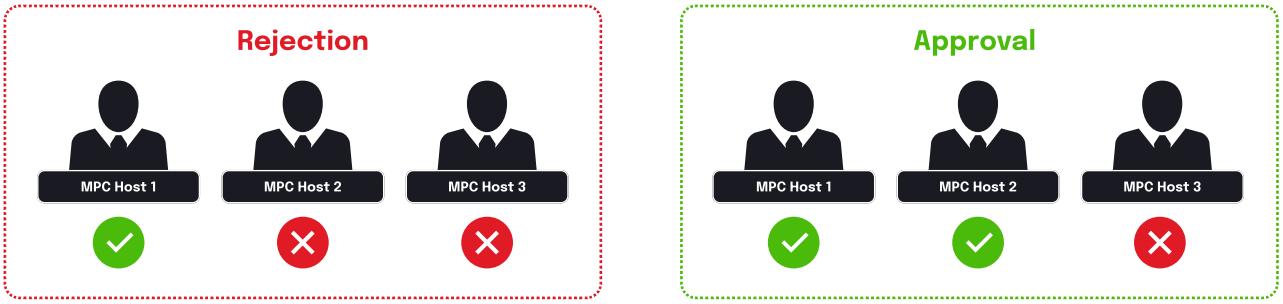
*[2] According to Crypto Hacks 2023: Full List Of Scams And Exploits As Millions Go Missing, successful attempts by scammers hacking smart contracts resulted in losses of $138 million in 2023.*

## Decentralized Custody

For each supported L1 network, Figure Markets creates dedicated MPC custodial accounts. We have established a network with trusted third-parties to host MPC nodes[3] protecting the MPC custodial accounts. MPC hosts are carefully vetted through a selection process, ensuring only institutions with solid track records and ongoing business in the blockchain space are allowed to participate. We have the ability to grow the MPC network and include more MPC hosts for further decentralization.

Decentralized custody is enabled by ensuring the private key shares are distributed amongst MPC hosts. Multiple MPC hosts each hold a necessary, but insufficient private key share to sign off on blockchain transactions. Because private keys direct the movement of assets, the custody of L1 assets is decentralized, requiring two or more MPC hosts to independently agree before depositing and transferring assets to an investor wallet.

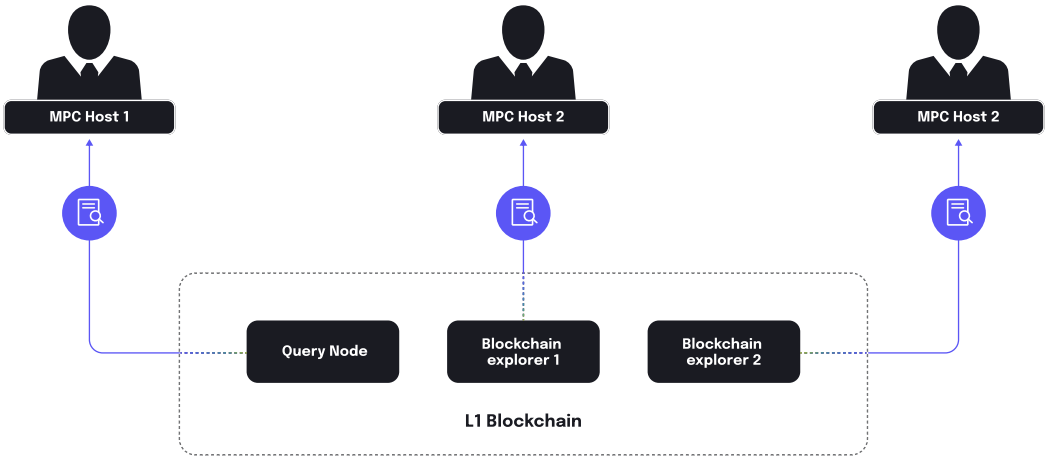
**Thresholds** are established and enforced through software to require n private key shares to be present for a blockchain signature where n > m. Figure Markets has defined the threshold, m, as the maximum number of key shares each MPC host is allowed to hold, preventing any single MPC host from signing blockchain transactions unilaterally.




**Policies** are used to specify the authorized individuals or software programs that must authorize a transaction before the MPC hosts will sign the blockchain transaction. Policies can be created by Figure Markets to protect investors assets. For instance, a policy can require the MPC system to ensure no network anomalies exist before processing a transaction. For institutional investors, policies can be defined by their admins to specify approval processes for withdrawal, such as requiring the digital signature of a finance executive for withdrawals over $10 million in value. These policies are part of Figure Market's MPC solution, are captured in code, and enforced decentrally through software.

*[3] A node is a single computer that can interact with and is part of, a blockchain network. On most blockchains, each node is a single and separate computer which stores all of the information on the blockchain, also known as a distributed ledger.*

**Decentralized decision making** ensures each MPC host independently reviews relevant blockchain data from different sources and follows software-enforced policies before signing a blockchain transaction. For example, the complete verification of a deposit into an MPC custodial wallet can be verified by each MPC host through different data sources.




Decentralized custody, decision making, thresholds, and policies all culminate in a shared outcome of a decentralized custodial account that protects against misuse of deposited digital assets and increases the control that investors have over their assets. Representations of the deposits held by investors are always redeemable for the original digital asset and are thereby suitable for trading on the exchange.

## Security and Backups for Decentralized Key Share Management

To protect against asset key loss, when a new MPC custodial account is created, private key shares are generated by each MPC host and encrypted with unique keys held only by the MPC host. The encrypted key shares are distributed among all other participating MPC hosts for backup purposes. Because MPC hosts only have their own decryption key, they are unable to decrypt the other MPC hosts' encrypted key shares.

This practice provides another layer of key share backup alongside local backups each MPC host runs on a regular basis. In the unlikely event that a local backup is unavailable, MPC host A can ask any other MPC host for a copy of their encrypted key shares, and use their own decryption key to make a full recovery of their private key shares.

If an MPC host ever loses an MPC node,[4] they still have access to their assets as the system natively backs up all policy engine state and MPC key shares in encrypted form.

*[4] The more nodes that a system has, the more difficult it becomes to cheat the entire system. That's because tampering with a blockchain will, more often than not, require a bad actor to control over 51% of the nodes.*

## Security Entitlements

The concept of a Security Entitlement (SE) is not new in finance. In traditional finance, when an investor deposits financial assets into a “securities account” held by an intermediary and meets the conditions outlined in the Article 8 of the Uniform Commercial Code (UCC), they acquire an SE.[5] This SE is, then, tracked in a traditional centralized database maintained by the intermediary. This construct has also been implemented by centralized cryptocurrencies exchanges, in anticipation of this concept extending the application of SEs into the digital asset space.

Unlike centralized exchange operators, Figure Markets offers digital representation of SEs in tokenized form, which are held by investors through self-custody. When investors deposit or acquire cryptocurrencies on the Figure Markets exchange, they receive tokenized SEs that represent a beneficial ownership interest in the assets maintained in the exchange’s decentralized MPC custodial accounts.

An investor using Figure Markets will be able to track their legal rights with respect to deposited assets. Since these tokenized SEs are held in self-custody and represented on Provenance Blockchain, a public layer 1 blockchain optimized for financial transactions, the risk of Figure Markets being able to remove, change, or misrepresent the quantity of an investor’s SEs is significantly mitigated, whereas that risk largely persists in centralized exchanges.

The sum of all outstanding SEs for a given L1 asset is always equal to or less than the quantity of L1 assets held in the decentralized MPC custodial account. This ratio is guaranteed because MPC hosts continually audit the L1 blockchain to ensure receipt of the L1 asset and monitor the total amount of SEs in circulation. Any investor can also perform this audit, as information about the decentralized MPC custodial accounts, the L1 assets within those accounts, and the SEs are ledgered on public L1 blockchains. This transparency ensures that any holder of an SE can look at the aggregate amount of outstanding SEs and verify that the amount of L1 assets held in the MPC custodial accounts is sufficient to cover future withdrawals.

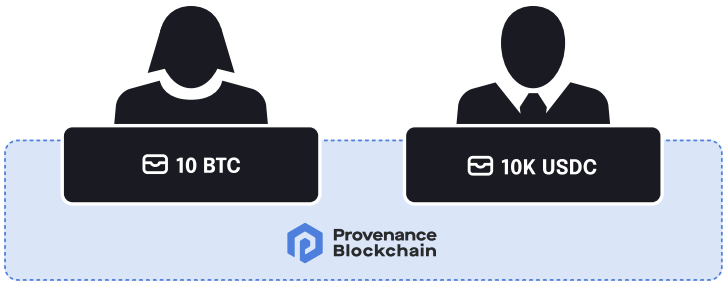
SEs can be traded on the Figure Markets exchange, redeemed for L1 assets held in the decentralized MPC custodial accounts, or sent to other investors via peer-to-peer (P2P) transfers. To ensure transparency, the ownership and aggregate quantity of SEs is visible to any interested party. Consequently, SE transfers and ownership information is recorded on the Provenance Blockchain, ensuring all parties can easily view this information.

*[5] As of August 2023, 13 states have approved the 2022 Amendments to Section 8 of UCC which extended the concept of security entitlements to digital assets. The legislation is currently in other states with an expectation to eventually be approved.*

Figure Markets ensures that SEs can be redeemed for the original L1 asset through a safeguard mechanism that involves two key elements: UCC Article 8 and agreements with MPC hosts. These mechanisms combine to minimize the risk of adverse claims to the investor's interests in their deposited assets. Agreements with each MPC host stipulate that they will sign blockchain transactions to release deposited assets after the corresponding SEs are surrendered, and, since investors hold SEs in self-custody, they can also directly surrender them to withdraw their assets from MPC custody. And, in the unlikely event of Figure Markets's insolvency, investors retain beneficial ownership of the underlying assets.

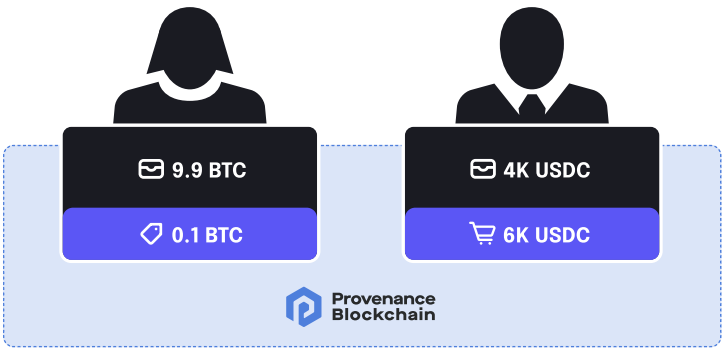
## Trading

To support our core tenet of truth over trust, SEs are publicly ledgered and settled on the Provenance Blockchain. The public ledger serves as a continuously auditable source of truth of ownership, allowing anyone to verify that the amount of outstanding SEs always has a corresponding amount of L1 assets available for withdrawal in the decentralized MPC custodial accounts.




Alice and Bob hold 10BTC and $10K in USDC, respectively through self-custody

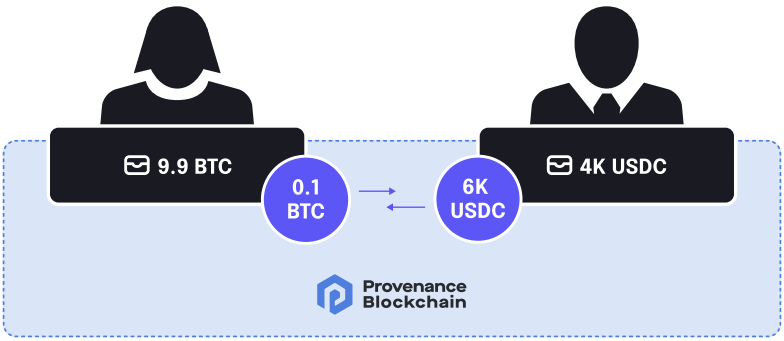
Investors hold their SEs in self-custody wallets, not custodial wallets, having complete control over their assets. When placing a trade, investors are prompted to commit their assets to the exchange, which serves two purposes: 1) it allows investors to offer the SEs for sale, and 2) it prevents the withdrawal of any SEs that are committed to an order. Until trades are executed and settled, investors retain full visibility of the SEs in their self-custody wallet. Investors may always regain control over their assets by canceling unfilled orders and withdrawing unsold SEs at any time.




Alice places a sell order for 0.1 BTC at $60K/BTC. Bob places a buy order for 0.1BTC at $60K/BTC

### Settlement of Trades on a Layer 1 Blockchain

Upon a trade match, Provenance Blockchain will honor the investors' orders and settle transactions bilaterally, transferring SEs and fiat equivalents between the investors. Settling SEs on the Provenance Blockchain also allows investors to benefit from faster transaction speeds and significantly lower trading fees compared to other common L1 blockchains because trade settlement is completed via Provenance not through custodial accounts on the ETH/BTC network. Therefore, investors do not incur network fees on the Bitcoin or Ethereum networks during trading, and fees on those networks are only incurred upon deposit or withdrawal of those assets.




Alice places a sell order for 0.1 BTC at $60K/BTC. Bob places a buy order for 0.1BTC at $60K/BTC

This streamlined settlement structure offers significant cost efficiency, particularly for active traders who frequently execute multiple trades daily, as no Bitcoin or Ethereum fees are required to settle each trade, unlike on many decentralized exchanges. This approach is particularly beneficial for institutional investors, who can be significantly impacted by volatile network fees. Fluctuation in these fees can reduce or eliminate potential profits, disrupting their trading strategies.

### Cross-Collateralization of Any Blockchain Assets

A core offering of Figure Markets is collateralization, the use of a virtual asset as collateral to secure a loan. Additionally, Figure Markets enables investors to cross-collateralize, or borrow against any assets in their self-custody wallet. These could include SEs from their deposits or purchases of Bitcoin, Ethereum, USDC, or other assets like HASH.

To obtain a loan, investors simply need to specify the assets and amounts they would like to offer as collateral. Once they digitally agree to the terms, the collateral remains visible in the investor's self-custody account, with a control hold placed on the assets, and the loan proceeds are deposited into their account. Once the loan is repaid, the assets will be unlocked for withdrawal, sale, or collateralization again.

Unlike other centralized crypto exchanges, Figure Markets leverage MPC technology to support cross-collateralization while ensuring that investor assets are held in self-custody. Any tokenized asset represented on a public blockchain can be represented as an SE in a self-custody wallet. Consequently, various SEs representing different assets can be used to secure a loan, simplifying the cross-collateralization process.

# Summary

Figure Markets's implementation of MPC technology is an innovative solution that bridges the gap between traditional and decentralized finance. Through decentralized MPC custodial accounts, we enable investors to retain complete control over their assets, while benefiting from the efficiency of a centralized exchange.

Unlike traditional exchanges, no single entity holds the keys to investor assets. Instead, the private keys are fragmented and shared among MPC hosts. By combining decentralized MPC custodial accounts with SEs tracking on Provenance Blockchain, investors can manage their assets through self-custody and their digital assets are protected from misuse or theft. This approach eliminates the risk of a single point of failure, which is inherent in centralized custody solutions.

To foster transparency and verifiability, we utilize SEs that represent 1:1 the assets held in the decentralized MPC custodial account. These SEs are publicly ledgered on the Provenance Blockchain, allowing anyone to verify the existence and quantity of underlying assets. By leveraging the Provenance Blockchain for settlement, we are able to offer faster transaction speeds and lower costs.

Our unique approach to custody and settlement is particularly beneficial for institutional investors. Our platform goes beyond offering increased transparency and asset control; it also reduces trading costs, making it more cost-effective to manage larder portfolios.

Additionally, Figure Markets offers robust security measures tailored to institutional needs. Institutional investors have the ability to require approvals from multiple institutional admins for asset withdrawals through multisig self-custody wallets.

They can also configure the platform to require additional approval from qualified custodians or other trusted partners to authorize movement of assets.

Through the combination of decentralized MPC custody with a high-performance matching engine, Figure Markets provides individual and retail investors a secure, compliant, and efficient platform to navigate the digital asset space.

## About Figure Markets

Figure Markets combines the liquidity of traditional finance with decentralized asset control. Individual and institutional investors can trade digital assets, access secure crypto-backed loans, and explore investment opportunities in a single, convenient platform. Learn more at **www.figuremarkets.com.**