CUSTONOMY

Custonomy Company Limited

Response to SFC's public consultation on its proposals to regulate virtual asset trading platforms

CUSTONOMY

Introduction

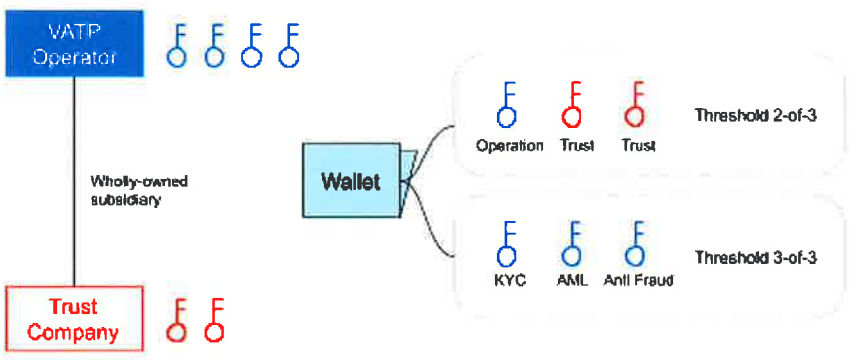
This response pertains to the Consultation Paper on Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed, published by the SFC on February 20, 2023. As a custody technology solution provider with years of experience in the market, this response aims to share insights on global virtual asset trends to enhance the sustainability of VATP operators from a technical standpoint. Our goal is to contribute knowledge that will enable authorities to refine their guidelines to bolster the integrity and efficiency of the virtual asset industry.

Suggestion 1) Adopt the MPC as the Common Practice of Crypto Key Management

In response to Question 6 of the consultation paper, we suggest implementing **Multi-Party Computation (MPC) custody solutions as a standard practice for VATP operators** to mitigate risks associated with virtual asset custody, both for hot storage and cold storage.

MPC is a cryptographic technique allowing multiple parties to compute a function without revealing their inputs. In virtual asset custody, it ensures no single party can independently access funds by dividing the private key among several parties. MPC wallets provide enhanced security compared to traditional wallets, particularly for high-value transactions.

MPC custody solutions can bolster exchange security, enhance proof of solvency monitoring, and foster customer trust. While Hardware Security Modules (HSMs) have been standard in traditional financial services, they pose accessibility and usability issues for virtual assets. Multi-signature (multi-sig) has limitations, such as custom development per ledger, limited support for large groups of approvers, and impracticality for most VASPs.



Some MPC solution providers offer self-custody options, complying with SFC guidelines that require virtual assets to be held in trust under a wholly-owned subsidiary. MPC wallets allow unlimited signers and enable composite threshold schemes, providing higher

security levels. By using two composite thresholds, MPC ensures proper internal policies and governance procedures are enforced.

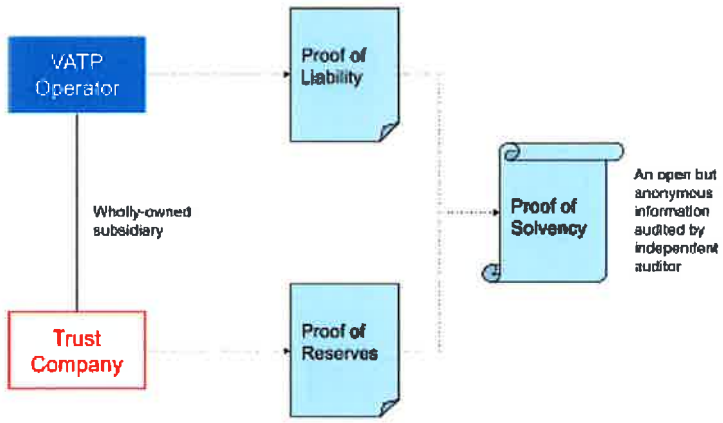
MPC significantly reduces fund misuse risk and ensures regulatory compliance. Its use enhances proof of reserve and provides a robust mechanism for fund security. Improved security applies to both hot and cold wallets, potentially allowing higher fund allocations in hot wallets in the future.

In conclusion, adopting MPC custody solutions can improve virtual asset trading platform security and resilience. Key benefits include real-time proof of reserves, enhanced transparency and accountability, and greater security, making MPC an increasingly popular choice for VATP operators.

Suggestion 2) Mandatory Timely Proof of Solvency for Licensing

We propose **mandating Proof of Solvency for VATP licensing** in response to Question 1 of the consultation paper. This requirement ensures customers' funds security and deters fraudulent activities by confirming that exchanges possess sufficient virtual assets and fiat currency to cover outstanding debts.

Regulation is crucial for authorities to mandate timely proof of solvency, enforce regular audits, and ensure public reporting. This fosters customer confidence in financial stability and mitigates fraud and insolvency risks. Implementing minimum capital requirements for operators can also prevent insolvency due to poor financial management.



Per Section III, Part 19a of the guidelines, the **VATP operator provides the "proof of liability" by maintaining detailed records of customer deposits**, while the **TCSP licensed trust company holds customer funds in trust and presents the "proof of reserves."** This structure delineates responsibilities for proof of solvency, preserving customer privacy and trust in fund security.

The frequency of proof of solvency audits varies depending on the jurisdiction and exchange. Some experts suggest daily or real-time audits using blockchain technology for increased transparency and accuracy. However, such frequent audits may be cost-prohibitive for smaller operators and disrupt exchange operations.

In conclusion, proof of solvency is vital for transparency and customer trust. The audit frequency depends on internal policies and regulatory requirements, with more frequent audits potentially offering greater confidence but at higher costs. Implementing appropriate wallet or crypto key management systems, such as adopting MPC, can improve proof of solvency cost and frequency while enhancing customer trust in fund security.

Suggestion 3) An Innovative MPC Governance Design for a Trustless Co-custody Model

In the proposed regulations, VATPs will be required to **hold customers' assets in segregated accounts** through a wholly owned subsidiary. While we acknowledge the SFC's proposal, we would like to highlight an alternative model based on cryptography for securely maintaining customer funds. This model utilizes MPC technology and a novel design in MPC governance, already in use for various applications.

With this model, **users generate a segregated wallet address through a simple Web2-like login** on the VATP's website or app. During sign-up, users create a password, which represents an encrypted part of the key used to authorize transactions. The wallet address generated consists of three key shards: one for the user, one for the VATP, and one for an independent third party, ensuring decentralization. A 2-out-of-3 threshold signature scheme is applied for valid blockchain signatures.

During regular operations, users can independently authorize transactions, with the third-party API key approving any user-initiated transaction. This provides users with direct control of their virtual assets and ensures transparency through blockchain-recorded transactions. The VATP alone cannot move user funds without consent.

Backup key shards can only be used for asset recovery if a user loses their key and requests assistance. With proper KYC and identification requirements, funds can be recovered using the VATP and third party's key shards. This

technology is flexible, allowing keys to be assigned differently based on risk-management policies and regulatory guidelines.

This solution offers native segregation of customer assets, as each client is assigned a unique wallet address during registration. Clients have direct key ownership while benefiting from fund recovery through MPC technology. The MPC design creates a trustless co-custodial solution, relying on MPC cryptography rather than the VATP's good faith.

We believe **this innovation effectively reduces counterparty risks** related to the mishandling of customer funds and could pave the way for novel approaches to centralized VATPs.

Conclusion

We strongly believe that the suggestion we have provided in this response will significantly **enhance the governing, monitoring, and transparency capabilities of the industry**. Our proposed measures will effectively **prevent the misuse of customer funds, minimize the risk of hacking and internal theft**, and provide **an effective mechanism for freezing fund transfers** in the event of a VATP operator filing for bankruptcy. Overall, the suggested measures will greatly improve the security and resilience of the industry, ensuring the protection of customers' assets and maintaining their trust.

About Custonomy

Custonomy, a dynamic Hong Kong-based startup, is an incubatee of the prestigious Hong Kong Science and Technology Parks Corporation (HKSTP). Our mission is to revolutionize the management, storage, and transaction of crypto assets with our innovative, institutional-grade Multi-Party Computation (MPC) key management solutions.

As a standard and compliance-driven organization, Custonomy proudly holds the ISO 27001 certification, reflecting our unwavering commitment to maintaining the highest level of security and reliability in the crypto asset management space.

Over the years, our groundbreaking work has garnered numerous accolades, solidifying our position as a leader in the fintech industry. Custonomy's award-winning achievements include the IFTA Fintech Achievement Award, Fintech Awards, TADs Awards, ICT Award, and Startup Express recognition.