Response for Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission

Submitted by: PolyU and Cybaverse Academy Joint Lab on Law and Web3

- Professor Man Ho Allen Au, Director of PolyU and Cybaverse Academy Joint Lab on Law and Web3 and Professor of the Department of Computing at The Hong Kong Polytechnic University
- Dr. Xiapu Luo, Co-director of PolyU and Cybaverse Academy Joint Lab on Law and Web3 and Associate Professor of Department of Computing at The Hong Kong Polytechnic University
- Mr. Paul Li, Co-director of PolyU and Cybaverse Academy Joint Lab on Law and Web3 and Managing Director of Cybaverse Academy

Question 2:
Do you have any comments on the proposals regarding the general token admission criteria and specific token admission criteria?

Since a token is usually controlled by its smart contracts, the security of smart contracts is critical to the token and its holders. Therefore, the following security measures should be adopted before the token under the control of its smart contract is admitted for trading.

1. Code audit and security assessment of the smart contracts should be regularly performed, and the corresponding reports should be provided to the public.

2. It is preferred that the source code of the token's/virtual asset's smart contracts is publicly available for checking. If it is infeasible to release the source code, the detailed documentation/specification of the smart contracts should be released because they and the bytecode of the smart contracts can be checked for finding potential issues. For example, academic researchers have developed tools for finding various issues (e.g., inconsistency, defects, backdoor) in the bytecode of tokens' smart contracts or other kinds of smart contracts running on different blockchain platforms, e.g. [1-7].

3. There should be a system to monitor any changes made to the token's smart contracts because the unnoticed changes may cause unexpected consequences, such as financial loss, security vulnerability, etc. The system can be developed by the token's operators or the platform operators. Note that the smart contracts deployed on several blockchain platforms, including Ethereum can be changed.

4. It is preferred that the token's operators, especially those maintaining the token's smart contracts, adopt online protection techniques to detect potential attacks (e.g., [8-9]) or defend against attacks (e.g., [10]).

5. Since there are usually scams [11-12] and security incidents relevant to popular tokens, the list of such information should be kept updated and sent to the platform operators.

Question 3:
What other requirements do you think should be implemented from an investor protection perspective if the SFC is minded to allow retail access to licensed VA trading platforms?

More information about the virtual asset should be provided, especially the virtual asset controlled by smart contracts, for example,
1. The source code (if feasible) and the documentation/specification of the smart contracts controlling the virtual assets.
2. All known or detected security incidents and scams relevant to the virtual assets.
3. The price of the virtual assets may be manipulated via many channels [13,14], such as oracle, pump, and dump, flash loans, MEV, etc., a monitoring system is desired to detect and report such activities.

Question 6:
Do you have any suggestions for technical solutions which could effectively mitigate risks associated with the custody of client virtual assets, particularly in hot storage?

The following technical solutions may effectively mitigate some of the risks.

Custodial Theft Risk: Fraudulent exchange or employee stealing client's money. One possible way to mitigate this risk is to automate the monitoring process of the VATP's reserve versus the total liability. The technological solution called Proof of Reserve (PoR) may address this risk . PoR is a cryptographic mechanism that offers proof that an exchange or financial institution holds sufficient reserves to cover its liabilities. Currently, several cryptocurrency exchanges and custodians use PoR, such as Kraken, Bitfinex, Unchained Capital, and Coinbase. Despite this, there is still a lack of standardisation in PoR, and it may be vulnerable to manipulation or collusion. As a result, we recommend that VATPs adopt PoR mechanisms that are open-source and have algorithms published in peer-reviewed venues, allowing public scrutiny. Additionally, conducting PoR at regular intervals, such as daily, can serve as an alarm system when reserves are insufficient to cover liabilities.

Key Loss or Key Theft Risk:
Public and private keys are cryptographic keys used in virtual asset transactions to secure and verify the ownership and transfer of digital assets.
A public key is a unique alphanumeric code publicly shared on the blockchain and used to identify the virtual asset's owner. Sometimes it is referred to as an address. A private key is a secret code that is known only to the owner of the virtual asset. It is used to digitally sign transactions, thereby proving ownership of the asset and authorising its transfer.
If the private key of a virtual asset is lost (e.g., due to hardware failure), the asset under its control will be lost. If the private key is stolen, the thief will be able to conduct an unauthorised transfer of the asset.
To mitigate these risk, we suggest the use of threshold signatures (which belongs to the category of multi-party threshold schemes), a technical solution currently being considered for standardisation by the National Institute of Standards and Technology (https://csrc.nist.gov/Projects/threshold-cryptography).

In a threshold signature scheme, the secret key is divided into multiple parts (called shares), and each part can be stored in a separate server. The threshold specifies the minimum number of parts required to generate a valid signature. For example, in a 3-of-5 threshold signature scheme, at least three out of the five servers must participate and use their parts to sign a transaction. When a transaction needs to be signed, the servers collaborate and use their respective parts of the secret key to generate a signature collectively. The threshold signature is produced without the parties needing to share their parts of the secret key or reveal their private keys to each other. The resulting threshold signature is valid and can be verified by anyone with access to the single public key. Threshold signatures mitigate both the problem of key loss and key theft risks: in the above threshold setting (3 out of 5), transactions can still be signed even if 2 servers are damaged; and to steal a key, the hacker needs to control 3 servers. The thresholds can be adjusted to suit different risk levels. Most blockchains adopt ECDSA and efficient threshold ECDSA schemes, some of which are designed by local universities, are available (e.g., [17, 18]).

Additional Measures To Reduce Risk of Hot Wallet

A hot wallet is a wallet that is always connected to the internet. It is needed for the VATP to maintain a hot wallet so that it can be used to store, send and receive tokens. We suggest threshold signatures should be used for hot wallet with send function.

For hot wallet whose primary function is to receive virtual assets, we recommend using the role of public and private key so that only the public key is stored in the hot wallet. As an added layer of security, the VATP may consider using a multisig wallet for hot wallet to send money. A multi-signature (multisig) wallet is a type of cryptocurrency wallet that requires multiple signatures to authorise a transaction.

To mitigate the risks associated with custody of the virtual assets based on smart contracts (e.g., ERC-20 tokens, NFT), besides securing the clients' key, it is preferred for platform operators to have a system to monitor the smart contracts of the virtual assets, because the operators of these smart contracts can directly manipulate the virtual assets via smart contracts. The system needs to monitor the transactions relevant to these smart contracts in order to detect potential attacks and abnormal operations of the smart contracts [15,16].

References

[1] T. Chen, Y. Zhang, Z. Li, X. Luo, T. Wang, R. Cao, X. Xiao, and X. Zhang, "TokenScope: Automatically Detecting Inconsistent Behaviors of Cryptocurrency Tokens in Ethereum", Proc. of the 26th ACM Conference on Computer and Communications Security (CCS), London, UK, November 2019.

[2] Z. He, S. Song, Y. Bai, X. Luo, T. Chen, W. Zhang, P. He, H. Li, X. Lin, and X. Zhang, "TokenAware: Accurate and Efficient Bookkeeping Recognition for Token Smart Contracts", ACM Transactions on Software Engineering and Methodology (TOSEM), Volume 32, Issue 1, pp 1–35, February 2023.

[3] J. Chen, X. Xia, D. Lo, J. Grundy, X. Luo, and T. Chen, "DEFECTCHECKER: Automated Smart Contract Defect Detection by Analyzing EVM Bytecode", IEEE Transactions on Software Engineering (TSE), Volume: 48, Issue: 7, 01 July 2022

[4] W. Chen, Z. Sun, H. Wang, X. Luo, H. Cai, and L. Wu, "WASAI: Uncovering Vulnerabilities in Wasm Smart Contracts", Proc. of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA), Daejeon, South Korea, July 2022.

[5] N. He, R. Zhang, H. Wang, L. Wu, X. Luo, Y. Guo, T. Yu, and X. Jiang, "EOSAFE: Security Analysis of EOSIO Smart Contracts", Proc. of the 30th USENIX Security Symposium (USENIX SEC), Vancouver, Canada, August 2021.

[6] Z. Sun, X. Luo, Y. Zhang, "Panda: Security Analysis of Algorand Smart Contracts", Proc. of the 32nd USENIX Security Symposium (USENIX SEC), Anaheim, USA, August 2023.

[7] S. Cui, G. Zhao, Y. Gao, T. Tavu, J. Huang, “VRust: Automated Vulnerability Detection for Solana Smart Contracts”, Proc. of the 28th ACM SIGSAC Conference on Computer and Communications Security (CCS), Los Angeles, USA, Nov.2022.

[8] T. Chen, R. Cao, T. Li, X. Luo, G. Gu, Y. Zhang, Z. Liao, H. Zhu, G. Chen, Z. He, Y. Tang, X. Lin, and X. Zhang, "SODA: A Generic Online Detection Framework for Smart Contracts", Proc. of the 27th Network and Distributed System Security Symposium (NDSS), San Diego, California, February 2020.

[9] A. Li, J. Choi, and F. Long, “Securing Smart Contract with Runtime Validation”, Proc. of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation (PLDI), London, UK, June 2020.

[10] https://blocksecteam.medium.com/how-blocksec-rescued-stolen-funds-from-technical-perspectives-of-three-representative-cases-d9e9be682eaa

[11] P. Xia, H. Wang, B. Gao, W. Su, Z. Yu, X. Luo, C. Zhang, X. Xiao, and G. Xu, “Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange”, Proc. of ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS), Mumbai, India, June 2022.

[12] B. Gao, H. Wang, P. Xia, S. Wu, Y. Zhou, X. Luo, and G. Tyson, “Tracking Counterfeit Cryptocurrency End-to-end”, Proc. of ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS), Beijing, China, June 2021.

[13] J. Xu and B. Livshits, “The Anatomy of a Cryptocurrency Pump-and-Dump Scheme”, Proc. of the 28th USENIX Security Symposium (USENIX SEC), Santa Clara, USA, August 2019.

[14] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, A. Gervais, “SoK: Decentralized Finance (DeFi) Attacks”, Proc. of the 44th IEEE Symposium on Security and Privacy (S&P), San Francisco, USA, May 2023.

[15] T. Chen, Y. Zhu, Z. Li, J. Chen, X. Li, X. Luo, X. Lin, and X. Zhang, "Understanding Ethereum via Graph Analysis", Proc. of IEEE International Conference on Computer Communications (INFOCOM), Honolulu, USA, April 2018.

[16] M. Zhang, X. Zhang, Y. Zhang, Z. Lin, “TXSPECTOR: Uncovering Attacks in Ethereum from Transactions”, Proc. of the 29th USENIX Security Symposium (USENIX SEC), Boston, USA, August 2020

[17] Haiyang Xue, Man Ho Au, Mengling Liu, Kwan Yin Chan, Handong Cui, Xiang Xie, Tsz Hon Yuen, Chengru Zhang. Efficient Multiplicative-to-Additive Function from Joye-Libert Cryptosystem and Its Application to Threshold ECDSA, ACM CCS 2023

[18] Haiyang Xue, Man Ho Au, Xiang Xie, Tsz Hon Yuen, Handong Cui. Efficient Online-friendly Two-Party ECDSA Signature. ACM CCS 2021