SUMMARY OVERVIEW OF ISSUES CONCERNING CRYPTO-ASSET CUSTODY

CFTC, TECHNOLOGY ADVISORY COMMITTEE

SUBCOMMITTEE ON VIRTUAL CURRENCIES

OCTOBER 3, 2019

PRESENTER

Chris Brummer
Georgetown University Law Center

THE CORE CHALLENGE OF CRYPTO-CUSTODY

- Custodying of crypto-assets is necessary in order to make a market.
- Cryptocurrencies are essentially digital bearer instruments.
- This creates unique challenges in terms of cybersecurity and governance
- It also generates a range of coping techniques, from procedural ('transactional' custody) to varying technological infrastructures

CUSTODIAL RELATIONSHIPS VARY

- Non-custodial Wallets (Self-Custodian)
- Exchange-Based Custodial Wallets
- Third Party Custodians (Non-exchange based)

SELF CUSTODY

- Customers become ‘weakest link’ in their own cybersecurity, of particular concern for retail investors and unsophisticated users of digital assets
- However, decentralized architecture creates lower paydays for cyber-criminals, and as such ‘harder’ targets
- Stymies liquidity insofar as systems are not interoperable.

EXCHANGE BASED WALLETS

Advantages

- Ease of use for customers; one stop shopping
- Greater cybersecurity and sophistication than customers

Challenges

- The "Honey Pot"
- Collapsed financial functions (market making, exchange and custody)
- Comingling of customer assets, front running, market manipulation particularly high risks in the absence of supervision and regulation

THIRD PARTY (NON-EXCHANGE) CUSTODIANS

Advantages

- Greater cybersecurity sophistication than retail holder
- May also alleviate (though not reduce) risks of exchange-based wallets where custodians are separately regulated affiliated entities

Disadvantages

- Liquidity challenges in the absence of inter-operable infrastructures
- Monitoring challenges given larger number of services providers

CUSTODIAL INFRASTRUCTURES

Hot Wallets

- Connected to the internet
- Trade liquidity (and eased liquidity management) for increased cybersecurity risks
- Scaleable

Cold Wallets

- Offline
- Trade nominal safety (though still human risk) for illiquidity
- Challenging Scaleability

THE WIDE VARIETY OF (POTENTIAL) CUSTODIAL PLAYERS

- Banks, Trust Companies
- Broker-Dealers
- Investment Advisers/Investment Vehicles
- Futures Commission Merchants
- Derivatives Clearing Organizations
- Foreign Depositories

FEW LARGE PLAYERS HAVE ENTERED DIGITAL ASSET CUSTODY

- In theory, large incumbent custodians might have advantages given their brand and credibility
- However, many institutional players appear to be skeptical. Potential explanations:
  - Inherent riskiness of asset
  - Lack of familiarity with digital assets
  - Questionable robustness of cybersecurity/technology
  - Regulatory compliance, litigation risk

CROSS-SECTORAL EXPECTATIONS (FOR REGISTERED ENTITIES)

- Maintain physical protection or control of customer assets;
- Prohibitions against comingling of assets
  - See, e.g., SEC Rule 15c3-3
  - See, e.g., CFTC Rules 1.20-1.29, 1.49, 22.1-22.17, 30.7
- (Deliver customer assets to customer in timely manner and/or when contractually agreed)

THE QUANDARY OF FORKING

- When custodians are in possession of cryptocurrencies when a fork arises, a number of questions arise.
- Is a custodian required to return to the account holder the forked cryptocurrencies along with the original cryptocurrency?
- What is the speed with which new, forked cryptocurrencies must be delivered to the account holder?
- What are the technical limitations, and costs of delivery of new tokens for custodians?
- What disclosures should be required for customers re: forking policy?

INTER-CUSTODIAL RELATIONSHIPS

- Due to cybersecurity (hacks), or volume, exchanges (registered and unregistered) can face liquidity crunches
- The inability to redeem customer redemption requests can harm the reputation of a custodian, and faith in the industry (like going to an ATM and unable to withdraw cash)
- Custodians may lend digital assets to one another without full disclosure of such activities to customers

DISCLOSURE, DISCLOSURE, DISCLOSURE

- "Full Spectrum" Counterparty risks
  - Cybersecurity practices and limitations
  - Operational
  - Conflicts
  - Balance Sheet/capitalization
- Forking Practices
- Insurance (Full vs. Partial) (Customer-based vs. Exchange-based)

CONTACT DETAILS AND NOTES

Chris Brummer
Professor of Law
Director, Institute of International Economic Law

Profile: chrisbrummer.com
Twitter: @chrisbrummerDR

All written materials are based on public information. Chris's views are just that, his own, and do not constitute legal advice and are subject to change.