Course IV:

DeFi Risks and Opportunities

2. Governance, DNS, Oracle Risk, DEX and Custodial Risks

(v) Custodial Risk

Risks: Custodial risk

What is custodial risk?

- Cryptocurrency ownership is guaranteed by the possession of a **private key** – a **long random number** that cannot be guessed. For Bitcoin and Ethereum, the private keys are 256 bits or 64 hexadecimal characters.
- Private keys are used via a **digital signature algorithm** to sign transactions. Hence, you need your private key to **"spend"**.
- Custodial risk is **when you lose your private key**.
- Both **individual users and institutions** (corporations, endowments, etc.) are subject to custodial risk.

Risks: Custodial risk

Types of Custodianship

- Self-Custody: Build our own solution
  - In-house or commercial solutions that store crypto assets
  - Solely responsible for assets and not insured against unexpected events
- Partial Custody: Your own wallet + external solution
  - Includes 2-FA and multi-signature solutions (e.g., BitGo)
  - Aligns with needs of retail and high net-worth clients
- Third-party Custody: Hire a managed solution
  - Fully maintained by service provider(s)
  - Aligns with needs of institutions, needed by regulatory bodies

Risks: Custodial risk

Retail Users

- Retail users have a choice between custodial and non-custodial wallets
  - Non-Custodial Wallet (Self-Custody) : User has full control of keys
    - E.g., Hardware wallet, Web wallet (MetaMask – keys stored in browser), Desktop wallet (Electrum – stored on machine), Mobile Paper wallet
  - Custodial Wallet (Third Party Custody): 3rd party holds access to private keys
    - E.g., Coinbase, Binance
    - Users are subject to KYC/AML regulation

Risks: Custodial risk

The New York Times

Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

Stefan Thomas, a German-born programmer living in San Francisco, has two guesses left to figure out a password that is worth, as of this week, about $220 million.

https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html

Risks: Custodial risk

Exchange Hacks

- Several exchanges have been hacked, highlighting the security risk of cryptocurrencies
  - Mt. Gox (2011-2014) - 850k Bitcoin
  - Bitfloor (2012) - 24k Bitcoin
  - Bittfinex (2016) - 120k Bitcoin
  - Coincheck (2018) - 523 million NEM (Worth $500 million at the time)
  - Binance (2019) - 7k Bitcoin
- Stolen cryptocurrency is often not completely recovered

Risks: Custodial risk

Delegating custody

- If you delegate the ownership of your private keys, say to an exchange, there is risk the exchange will be hacked and the keys stolen.
- Exchanges keep most of the private keys in “cold storage” (either on a drive not connected to the Internet or hard copy in a physical vault)
- Some exchanges, like Coinbase, are insured. However, the insurance is only as good as the health of the insurer.

Risks: Custodial risk

Infrastructure by Custodians

- Wallet
  - Hot – Internet-connected solutions; fast and frictionless
  - Cold - Air-gapped or internet-isolated solutions; slower but very secure
- Storage Mechanism
  - Software – Digital platforms storing data on the internet or a network segment
  - Hardware – Specially built electronic devices storing data (e.g., Hardware Security Modules)
- Access Protocols
  - Multi Party Computation – Single signature computed by a distributed set of users
  - Multi-Sig – Uses multiple signatures from distinct private keys to secure a wallet

Risks: Custodial risk

Example of Infrastructure - Splitting keys

- Companies like BitGo offer multi-signature solutions
- Three keys:
  - Owner has two keys and BitGo holds one.
  - 2 of 3 keys can be used for a transaction
  - A hack of BitGo's key is useless because a single key cannot spend
- If a user loses one key, there is a backup

Risks: Custodial risk

Concerns around custodianship

- Latency vs Speed
  - Trading at low latency = having fast access to funds
  - But this raises questions around security and proper verification
- New Coins
  - Custodians don't support all newly invented coins for compliance
  - Some coins are offered in some countries and not in others
- Staking
  - Transaction validation on a PoS chain, can be done independently or through a custodian
  - Choose custodian wallet for staking based on proper care and due-diligence

Risks: Custodial risk

Top Custodians

- Coinbase Trust
- Bitgo
- Fidelity Digital Assets
- Bakkt Warehouse
- Kingdom Trust
- Several Banks looking into developing solutions – ING, BBVA, Northern Trust

Institutions looking into Crypto

- Facebook
- Visa
- PayPal
- Mastercard
- Goldman Sachs
- IBM

https://medium.com/blockchain4all/leading-us-based-crypto-custodian-providers-for-institutional-clients-3ba9b8683c6d#:~:text=Who%20are%20the%20leading%20crypto,the%20world's%20largest%20crypto%20custodian.
https://finance.yahoo.com/u/yahoo-finance/watchlists/top-crypto-bets/

Risks: Custodial risk

Regulatory Environment

- In the past, a lack of custody solutions has been a main reason why hedge and mutual funds could not invest in crypto
- Legal and regulatory environments for custodians and institutions have not been clearly defined
  - Custody Rule of Investment Adviser Act of 1940 – Institution with $150 million AUM needs a licensed custodian
- Federally charted banks are allowed to provide crypto custodial services

https://www.coindesk.com/sec-qualified-custodian-statement
https://www2.deloitte.com/us/en/pages/audit/articles/cryptocurrency-custody-regulations-from-occ-deloitte-us.html