# Tether Vault

with

Vesper Technology

Safe Deposit Box for Tether Tokens

Carrying all your money…?

- Crypto Wallets are convenient, but…
  - Displays all your digital property to anyone
  - Security risks due to the nature of a digital wallet
    - Weak against hacking and phishing
    - Lost phone or USB may compromise the total control of your account.
    - Almost impossible to find and recover stolen property
- Is there any vault service as simple and safe as the bank safety deposit box?
  - Coinbase Vault, Bitcoin Vault, etc.
    - Company keeps and manages user's crypto key – Company still can see the data (https://www.investopedia.com/tech/coinbase-what-it-and-how-do-you-use-it/)
    - Security bleach happened: Hacking and account compromised
    - Slow transfer between vaults and wallets (may take few days)

Tether Token Vault
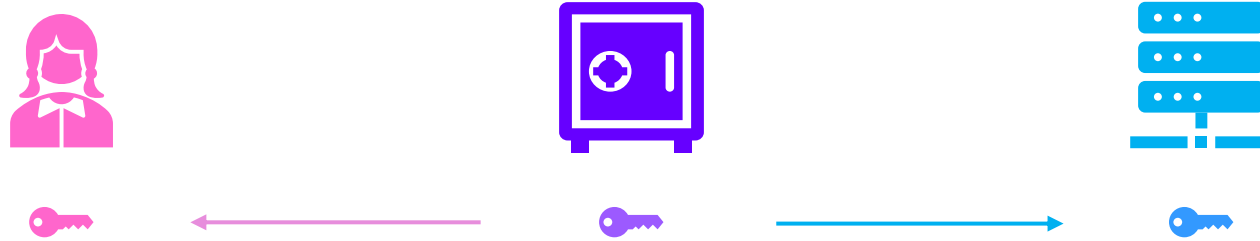
- Keeps the Tether tokens just like a bank safety deposit box
  - Account records are kept encrypted.
  - The encryption key will be separated into two (or more) separate partial keys
    - Separate keys are kept by separate and different entities (server, user, and etc.)
    - All keys must be used to decrypt the account record.
      - It is impossible to decrypt the token record only with the key from the server.

Instant Invalidation of Lost Keys
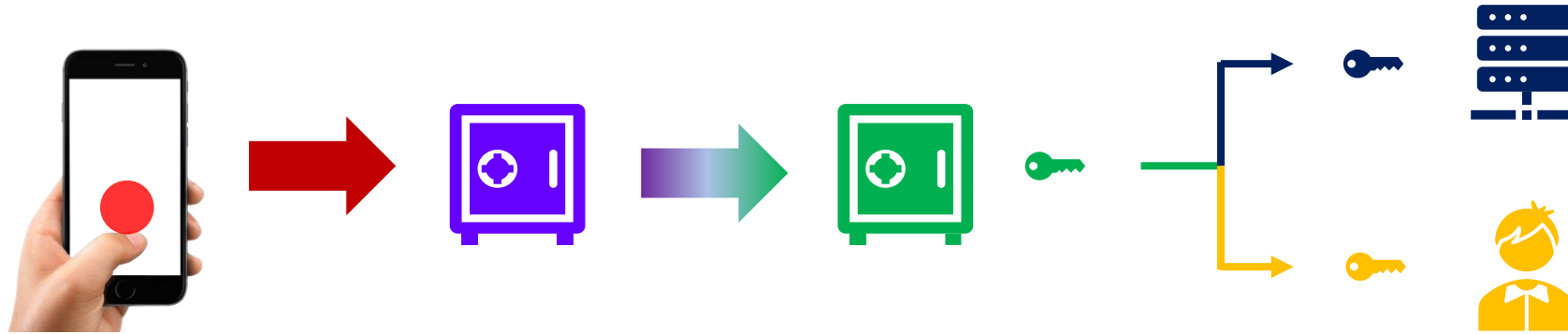
- Key-morphing feature of Vesper
  - Upon the request for 'key change' from the user, all encrypted account records will be 'morphed' into the new crypto records with the 'new' key without decryption.
    - Since it does not decrypt, there is no decrypted records on the server – Even company cannot see the data.
    - Existing keys will be invalidated instantly.
  - New key will also be separated into two (or more) partial keys.
    - New key(s) will be sent to the accounts/devices (phone, emails, etc.) that user has setup.

Server-side Security

- Server only keeps the encrypted account records and server-side keys.
  - Server-side keys alone cannot decrypt the account records.
  - Upon the detection of security breach, key-morphing will be automatically executed.
    - Instant invalidation of all existing keys
    - Account records will remain encrypted all the time.
    - All data on the server will work using the new key, of course.