Lecture 3 - Centralized Cryptocurrencies

Rylan Schaeffer and Vincent Yang

March 23, 2016

Note: This lecture is based on Princeton University's BTC-Tech: Bitcoin and Cryptocurrency Technologies Spring 2015 course.

Centralized Banking

- Centralize: to concentrate under a single authority
- Centralized banking means there is a single institution that manages supply, inflation, and interest.

Advantages to Centralization

- Automation:

  Easily manage a large number of keys e.g. Mastercard Europe

  Maintain secure infrastructure and improve operations/efficiency
- Centralized Monitoring:

  Record everything that happens easily; brings transparency
- Centralized Policy
- Easily update and track keys
- Easily update cryptographic schemes - swap out algorithms

CentralizedCoin

- I can generate coins, and give them unique ID's. I also sign these coins.
- I can pass them to anyone else - I sign the transaction; recipient can prove it's valid because it has my signature.
  Recipient can sign to pass to someone else.
- Chain of hash pointers can be used to follow it back. = verify
- Double Spending Problem
- Only I can write on the chain - everything has to pass through me
- This is centralized; how do you trust me?

Centralized Cryptocurrencies

- E-Gold (1996)

  Operated by Gold and Silver Reserve inc

  Let users open an account denominated in gold; could make instant transfers

  Grew to 5 million accounts; processing over 2 billion a year

  "e-Gold Special Purpose Trust" - actually held the gold; could see gold bars with serial numbers per acct.

  Hackers used flaws in Microsoft Windows OS's and phishing to compromise millions of e-gold accounts

  People thought it was *anonymous*, but really it was *pseudonymous*. Law enforcement identified many.

  Ponzi schemes via. eBay

  Patriot Act, after Sept 11, made operating a money transmitter business without a state money transmitter license a federal crime.

  Taken down 2007-2013; inability to provide reliable user identification and cut off illegal activity

  PayPal has done a better job, but still has to deal with the same problems.

  KYC - process of verifying clients' identity

- Liberty Reserve

  Shut down, also by Patriot Act, in May 2013.

- E-Gold and Liberty Reserve were popularly used for money laundering and shut down
- Can be shut down by the government at any time
- DigiCash by Chaum 1990

  Store money as data on your computer

  Transfer anonymously

  Lacked decentralization; the company's servers were used

  Went bankrupt in 1998

Source: `http://people.dsv.su.se/~matei/courses/IK2001_SJE/Chaum90.pdf`
Source: `http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF`