Lecture 0 - History and Relevance of Cryptocurrency Technologies

Rylan Schaeffer and Vincent Yang

March 22, 2016

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

Cryptocurrency

- a digital currency in which cryptographic techniques are used to regulate the generation of units of currency and verify the transfer of funds
- cryptography : mathematical side of secure communication
- frequently operated independently of central authority, but not necessarily
- bank : term for central authority

Basic Modes of Trade

- Barter - Simple, requires coordination
- Credit - Transferable obligations, requires introduction of risk
- Cash - Universally exchangeable, requires bootstrapping, anonymous
- Digital desirable for convenience

Digital Credit

- Two Types:

  Direct e.g. Amazon

  Indirect e.g. PayPal
- Initially, sharing credit card details to unknown vendors over insecure channel seen as crazy
- FirstVirtual, 1994. Purely virtual office. Buyers enroll, provide credit card details. Buyer contacts seller. Seller contacts FirstVirtual, who contacts Buyer to confirm transaction.
- Secure Electronic Transaction, 1996. Communications protocol from VISA, MasterCard, private companies. Buyer and Seller agree on transaction. Buyer encrypts credit card info, transaction details, sends to Seller. Seller sends own view of transaction details, plus Buyer's encrypted information, to intermediary. Intermediary decrypts, confirms transaction.

Digital Cash

- Three types

  Commodity - value in themselves e.g. gold, silver, salt

  Representative - claim on commodity e.g. redeemable for gold, silver

  Fiat - declared by government to be redeemable for services and goods e.g. Dollar, Euro

- Advantages over Credit

  No risk

  Decentralized : central authorities frequently aren't transparent/democratic, manipulate monetary policy with economic effects

  Anonymous (somewhat)

- Two Key Problems

  Authentication i.e. no one other than person A can spend person A's money

  Double Spending i.e. person A cannot spend money multiple times

- David Chaum's Blind Signatures, 1983. Digital Signatures. Idea: Bank issues notes with serial numbers. Sellers check with bank to confirm that notes are not being double spent before confirming transactions.

  Chaum's contribution: when new note issued, recipient chooses serial number. Keeps number hidden from bank, and bank signs ("blind signature")

- Chaum, Fiat, Naor, 1988. Offline electronic cash. Allow double spending, focus on detecting. Every serial number is encoded. Each time coin is spent, recipient requires you to decode random subset and keeps a record. Still hides identity. When recipients go to bank to redeem notes, high probability that two random subsets will together decode your identity.

- Okamoto and Ohta allowed subdividing coins using Merkle trees

- Cypherpunks (community of activists advocating widespread use of strong cryptography as a route to social and political change) tried lots of versions