Digital Currencies

Chris Head

Digital Monetary Trust

- Trusted central authority
- Tamper-resistant cryptographic coprocessor
- Anonymity of account holders' identities
- Deposits backed by investments into securities
- Closed 2005

e-gold

- Centralized account database
- Deposits measured in grams of gold
- Security responsibility placed on user
  - Some accounts emptied due to weak credentials
- Accounts frozen, shut down by US govt
- Deposits still unavailable to customers

Pecunix

- Similar to e-gold
- Still operational
- Stronger user authentication mechanisms

Game currencies

- Often initially obtained and used only in-game
- Often exchanged for “real” fiat currencies today
- World of Warcraft: gold and game accounts (dropped in-game, sold by players)
- FarmVille: “farm cash” (sold by Zygna)
- Second Life: “Linden dollar” (issued by Linden Lab, sold by players)

Liberty Dollar

- Gold/silver coins, certificates, digital accounts
- “Not a currency: a numismatic piece or medallion which may be used voluntarily as barter”
- Weird exchange rate mechanism
- FBI, secret service raid
- Guilty verdict
- Appeals ongoing

Ripple

- Peer-to-peer lending system
- Trust chains between users
- Example:
  - Carol gives Alice a good or service
  - Carol doesn't trust Alice
  - Alice agrees to owe Bob $10
  - Bob agrees to owe Carol $10

Bitcoin

- Distributed database
- Public transfers between anonymous accounts
- Secured by cryptographic primitives and probability
- Money supply automatically created without operator intervention (up to BTC 21M)
- Non-reversible transactions

Bitcoin: transaction verification

- Transactions grouped into blocks
- Blocks stored on all network nodes
- Rate-limiting by partial hash collision
- Incentives: mining, transaction fees
- Transaction must prove authority to use its inputs, delegate authority to use outputs
- Chain forking possibility → confirmation delay

Bitcoin: transaction authorization

- Bitcoin virtual machine architecture
- Outputs: “scriptPubkey”
- Inputs: “scriptSig”
- Concatenate and execute
- N of M officers
- Computation bounty
- Transaction sequence numbers, timestamps → escrow

Bitcoin: value

- Total money supply: ~BTC21M
- Current exchange rate (~4:15PM): $17.15USD
- Exchange rate ~1h earlier: $13.88USD
- Deflation?
  - Argument: everyone will save
  - Argument: everyone *must* spend sometime
  - Argument: equilibrium?
- Destruction of currency
- Lots of decimal places left! (eight)

Bitcoin: security (theory)

- Address check: SHA256 + RIPEMD160
- Address: ECDSA keypair
- Block chain: SHA256 (×2)

Bitcoin: security (practice)

- Allinvain incident:
  - Early adopter
  - Mined BTC25,000 (USD428,750)
  - Stored wallet on general-purpose Windows machine
  - Left it there even after virus scanners found viruses
  - BTC25,000 sent to LulzSec donation address
- Fallout: two camps
  - “OMGWTFBBQ Bitcoin should secure its wallet!”
  - “Idiot should've spent some of his half million on basic computer security”

Thank you!

If you liked this presentation, you know what to do:

16akfL2fcDDmy4JJ5pStfj5yrT8PAjWVXe