Lecture #4: How to store and Use Bitcoins/Secret Keys

Lecture 4.1 Simple Local Storage

To spend a Bitcoin, you need to know: <u>So it’s all about key management</u>

- Some info from the public blockchain, and
- The owner’s secret signing key

Goals

Availability: You can spend your coins.
Security: Nobody else can spend your coins.
Convenience

Wallet software

Keeps track of your coins, provides nice user interface

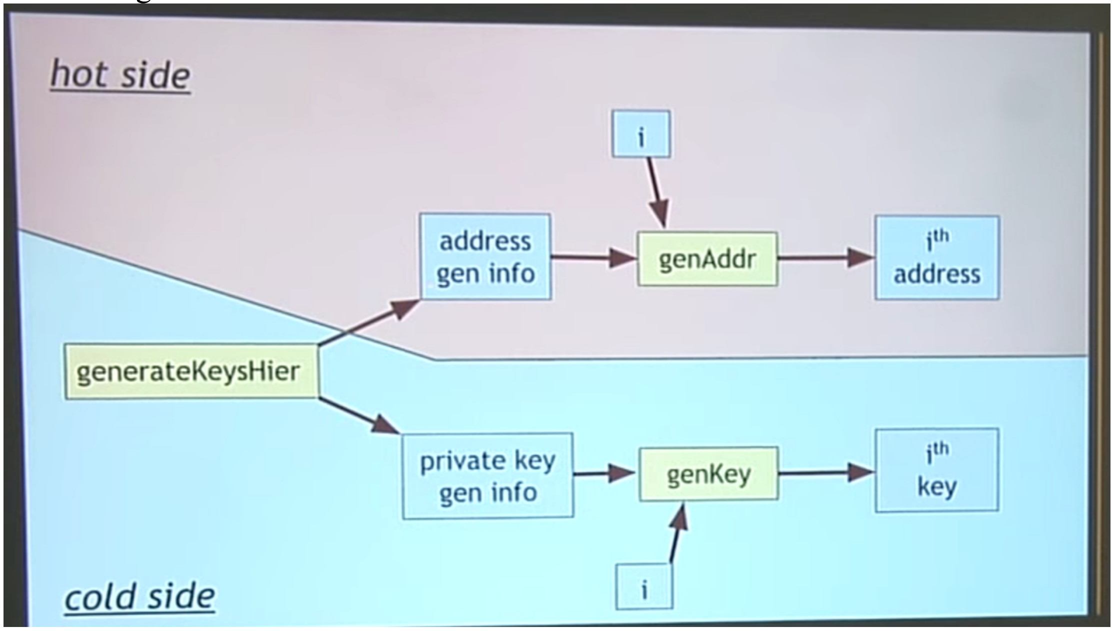
Nice trick: use a separate address/key for each coin.
  Benefit privacy (looks like separate owners)
  Wallet can do the bookkeeping, user needn’t know

Encoding addresses

<u>Encode as text string: base58 notation</u>
<u>QR code</u>

Lecture 4.2 Hot storage and Cold storage

Hot storage: online - convenient but risky
Cold storage:offline - archival but safer



Lecture 4.3 Splitting and Sharing Keys

Secret sharing

I*dea:* split secret into N pieces, such that
  Given any K pieces, can reconstruct the secret
  Given fewer than K pieces, don't learn anything

Good: Store shares separately, adversary must compromise several shares to get the key.
Bad: To sign, need to bring shares together, reconstruct the key. <= vulnerable

Multi-sig

Lets you keep shares apart, approve transaction without reconstructing key at any point.

Lecture 4.4 Online Wallets and Exchanges

Online wallet

Like a local wallet, but "in the cloud"

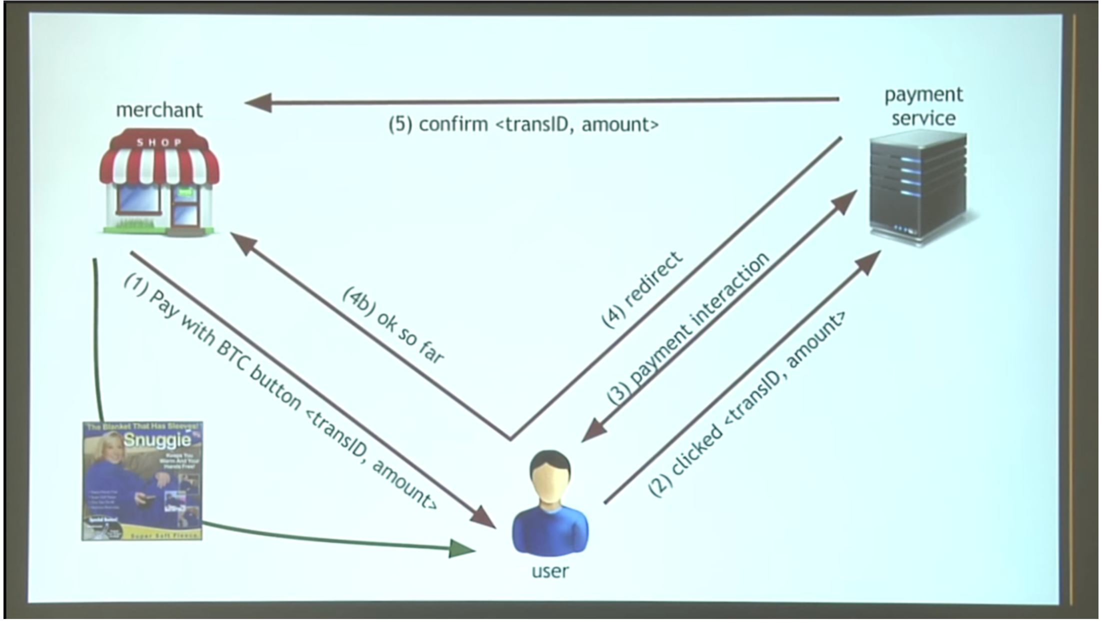
Tradeoffs

Convenient: nothing to install, works on multiple devices
But security worries:
  Vulnerable if site is malicious or compromised

Bank-like services

Bitcoin Exchanges

Lecture 4.5 Payment Services


merchant
payment service
(5) confirm <transID, amount>
(1) Pay with BTC button <transID, amount>
(4b) ok so far
(4) redirect
(3) payment interaction
(2) clicked <transID, amount>
user
Snuggie

End result:
Customer: pay Bitcoins
Merchant: get dollars, minus a small percentage
Payment service:
  Get Bitcoin

Pay dollars (keeps small percentage)
Absorbs risk: security, exchange rate
Needs to exchange Bitcoins for dollars, in volume

Lecture 4.6 Transaction Fees

Recall:
Transaction fee = value of inputs - value of outputs
Fee goes to miner who records the transaction

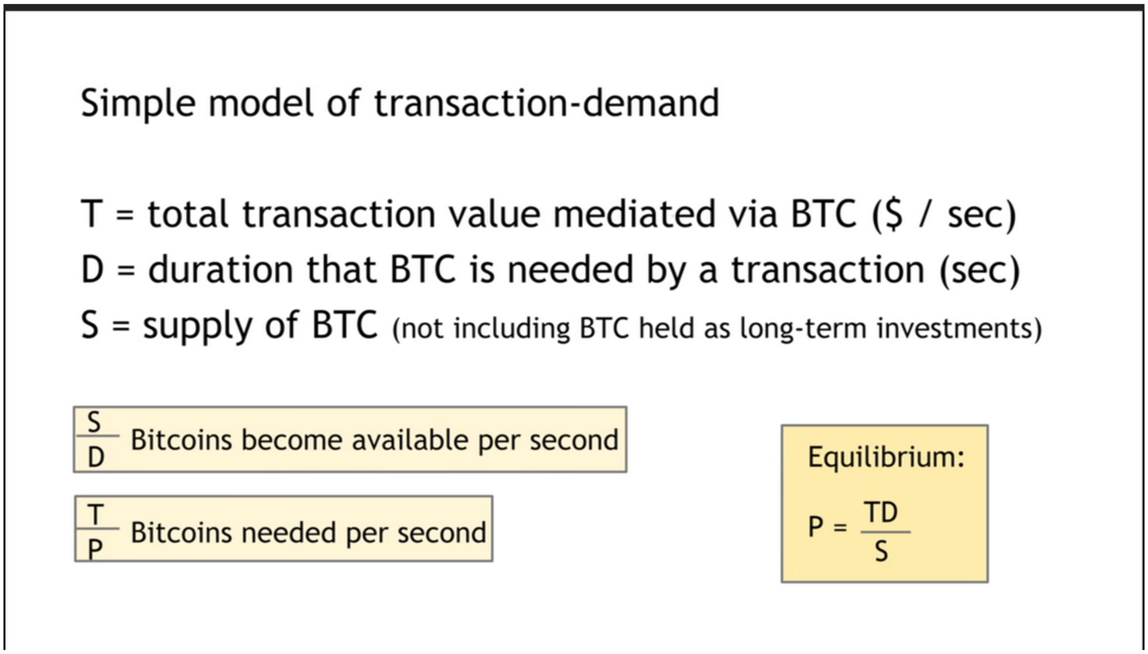
Costs resources for
Peers to relay your transaction
Miner to record your transaction
Transaction fee compensates for (some of) these costs
Generally, higher fee means transaction will be forwarded and recorded faster.

Current consensus fees:
No fee if
Tx less than 1000 bytes in size,
All outputs are 0.01BTC or larger, and
Priority is large enough
Priority = (sum of inputAge*inputValue)/(trans size)
Otherwise fee is 0.0001 BTC per 1000bytes.

Facts:
Most miners enforce the consensus fee structure.
Miners prioritize transactions based on fees and the priority formula.

Lecture 4.7 Currency exchange Markets

Demand for Bitcoins
BTC demanded to mediate fiat-currency transactions
BTC demanded as an investment



Simple model of transaction-demand

T = total transaction value mediated via BTC ($ / sec)

D = duration that BTC is needed by a transaction (sec)

S = supply of BTC (not including BTC held as long-term investments)

$\frac{S}{D}$ Bitcoins become available per second

$\frac{T}{P}$ Bitcoins needed per second

Equilibrium:

$$P = \frac{TD}{S}$$