Lecture 4

How to Store and Use Bitcoins

Lecture 4.1:

Simple Local Storage

To spend a Bitcoin, you need to know:

* some info from the public blockchain, and

* the owner's secret signing key

So it's all about key management.

Lecture 4

How to Store and Use ~~Bitcoins~~
Secret Keys

Goals

availability: You can spend your coins.

security: Nobody else can spend your coins.

convenience

Simplest approach: store key in a file,
on your computer or phone

Very convenient.

As available as your device.

device lost/wiped ⇒ key lost ⇒ coins lost

As secure as your device.

device compromised ⇒ key leaked ⇒ coins stolen

Wallet software

Keeps track of your coins, provides nice user interface.

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

Encoding addresses

Encode as text string: base58 notation

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

or use QR code

Lecture 4.2:

Hot and Cold Storage

Hot storage

online

convenient but risky

Cold storage

offline

archival but safer

separate keys

Hot storage

online

Cold storage

offline

hot secret key(s)	payments	cold secret key(s)
cold address(es)		hot address(es)

Hot storage

online

hot secret key(s)

cold address(es)

Cold storage

payments

offline

Problem:

Want to use a new address (and key) for each coin sent to cold

But how can hot wallet learn new addresses if cold wallet is offline?
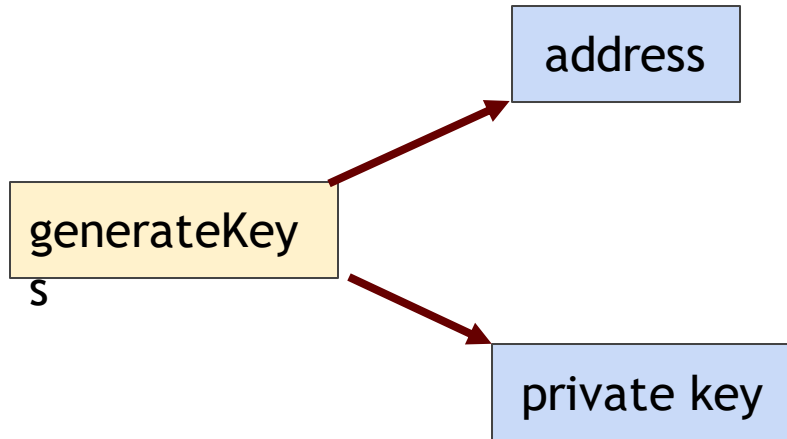
Awkward solution:

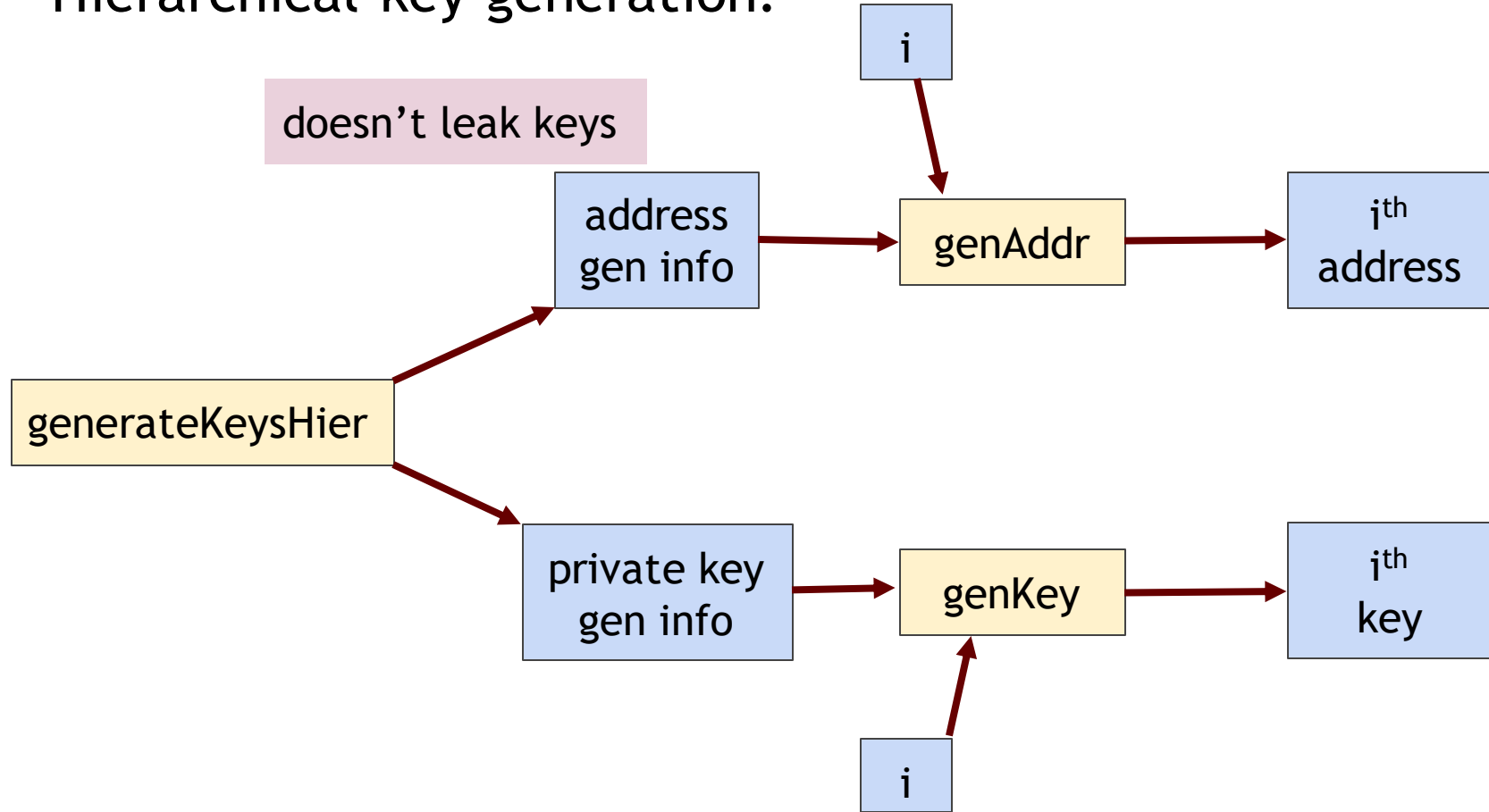Generate a big batch of addresses/keys, transfer to hot beforehand
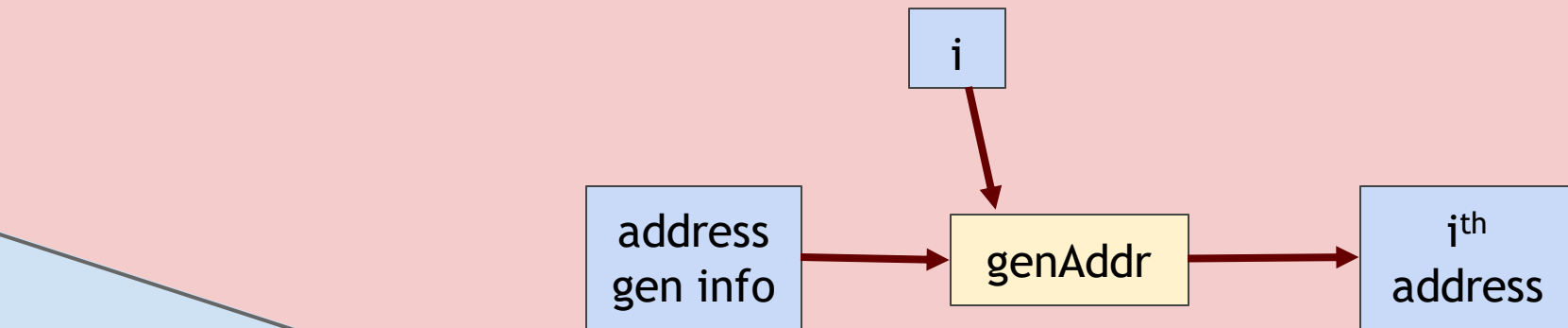
Better solution:

Hierarchical wallet

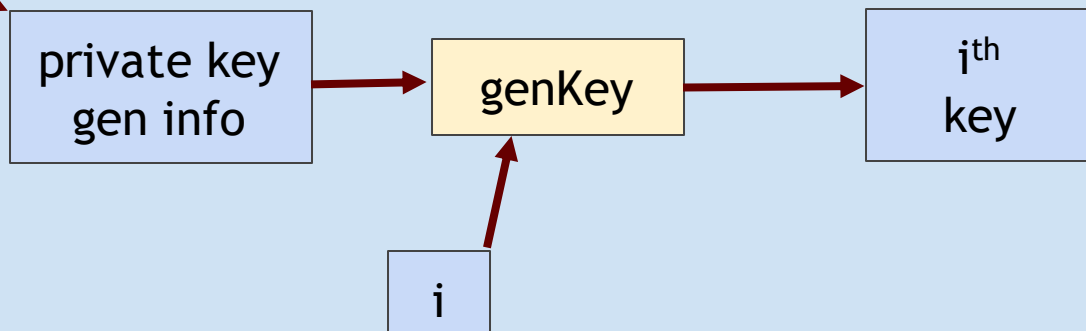# Regular key generation:

Hierarchical key generation:

hot side

i

address
gen info → genAddr → i^{th} address

generateKeysHier

cold side

private key
gen info → genKey → i^{th} key

i

How to store cold info

(1) Info stored in device, device locked in a safe

(2) "Brain wallet"

encrypt info under passphrase that user remembers

(3) Paper wallet

print info on paper,

lock up the paper

(4) In "tamperproof" device

device will sign things for you, but won't divulge keys

Lecture 4.3:

Splitting and Sharing Keys

Secret sharing

Idea: split secret into N pieces, such that
    given any K pieces, can reconstruct the secret
    given fewer than K pieces, don't learn anything
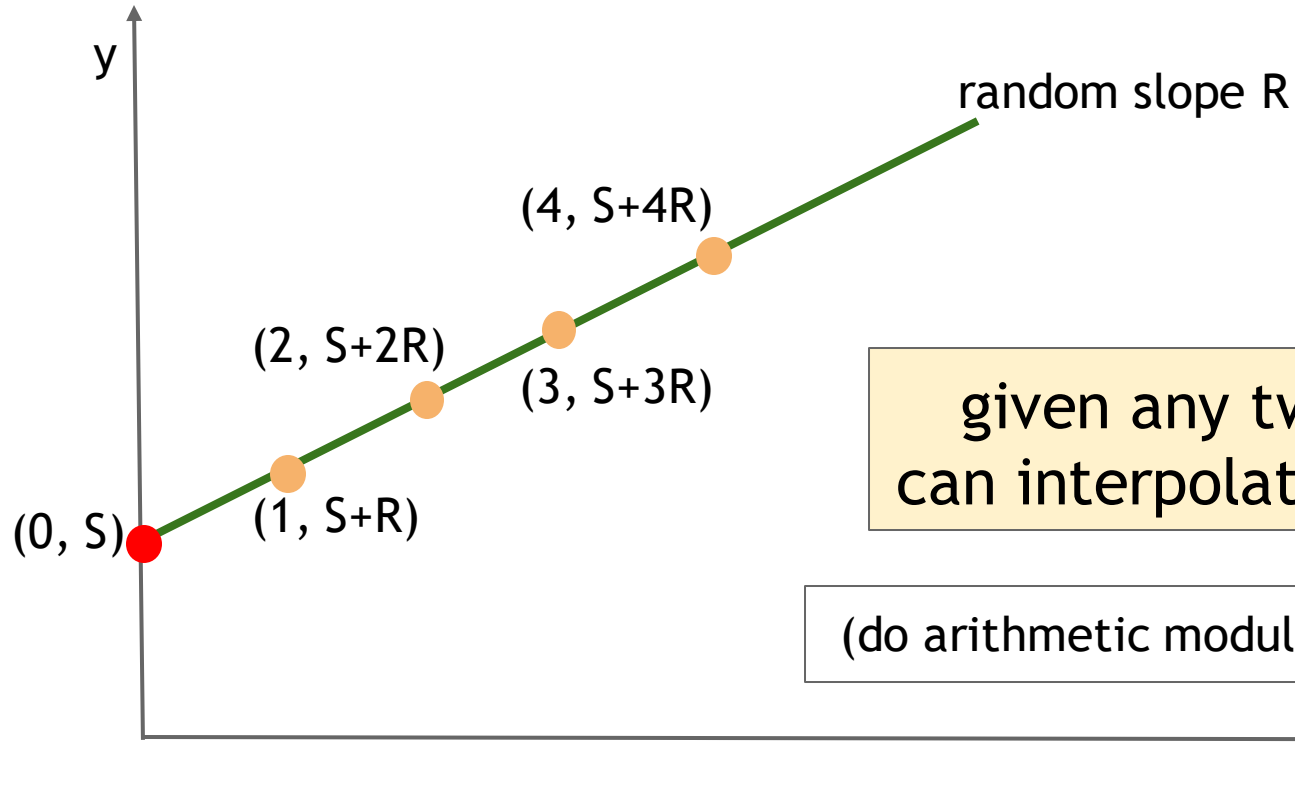
Example: N=2, K=2
    P = a large prime
    S = secret in [0, P)
    R = random in [0, P)

split:
    $X_1 = (S+R) \bmod P$ $X_2 = (S+2R) \bmod P$

reconstruct:
    $(2X_1 - X_2) \bmod P = S$

y

random slope R

(4, S+4R)

(2, S+2R)

(3, S+3R)

(1, S+R)

(0, S)

given any two points,
can interpolate and find S

(do arithmetic modulo large prime P)

x

Secret sharing

Equation	Random parameters	Points needed to recover S
$(S + RX) \bmod P$	R	2
$(S + R_1X + R_2X^2) \bmod P$	R_1, R_2	3
$(S + R_1X + R_2X^2 + R_3X^3) \bmod P$	R_1, R_2, R_3	4

etc.

support K-out-of-N splitting,
for any K, N

Secret sharing

Good: Store shares separately, adversary must
        compromise several shares to get the key.

Bad: To sign, need to bring shares together,
        reconstruct the key. $\Leftarrow$ vulnerable

Multi-sig

Recall multi-sig from Lecture 3.

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

Example

Andrew, Arvind, Ed, and Joseph are co-workers.
Their company has lots of Bitcoins.

Each of the four generates a key-pair,
        puts secret key in a safe, private, offline place.

The company's cold-stored coins use multi-sig, so that three of the four keys must sign to release a coin.
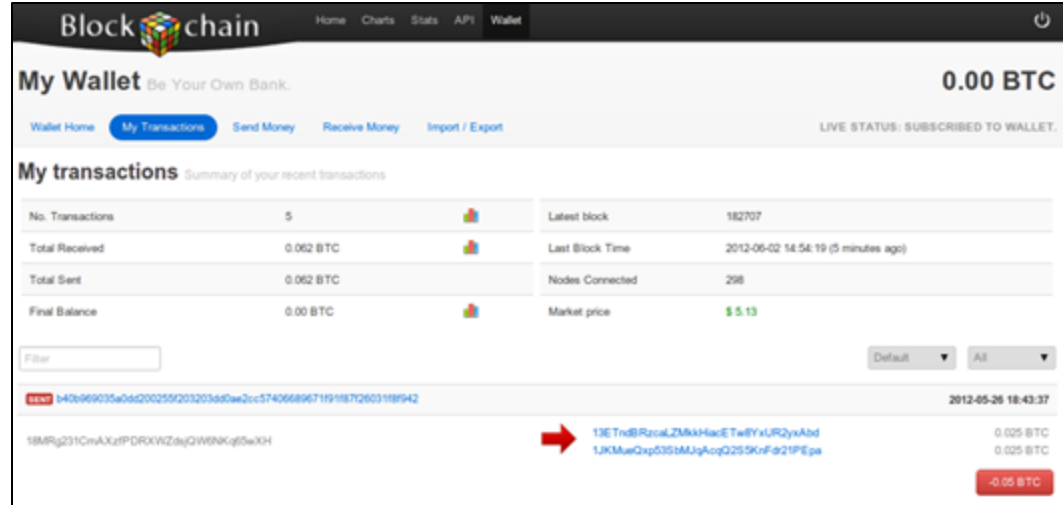
Lecture 4.4:

Online Wallets and Exchanges

Online wallet

like a local wallet
    but "in the cloud"

runs in your browser
    site sends code
    site stores keys
    you log in to access wallet

Online wallet tradeoffs

convenient: nothing to install, works on multiple devices

but security worries
            vulnerable if site is malicious or compromised

ideally, site is run by security professionals

Bank-like services

you give the bank money (a "deposit")
bank promises to pay you back later, on demand

bank doesn't actually keep your money in the back room

typically, bank invests the money
keeps some around to meet withdrawals ("fractional reserve")

Bitcoin Exchanges

accept deposits of Bitcoins and fiat currency ($, €, …)

      promise to pay back on demand

lets customers:

      make and receive Bitcoin payments

      buy/sell Bitcoins for fiat currency

         typically, match up BTC buyer with BTC seller

What happens when you buy BTC

suppose my account at Exchange holds $5000 + 3 BTC
I use Exchange to buy 2 BTC for $580 each

result: my account holds $3840 + 5 BTC

note: no BTC transaction appears on the blockchain
only effect: Exchange is making a different promise now

Exchanges: Pros and Cons

pro: connects BTC economy to fiat currency economy

easy to transfer value back and forth

con: risk

same kinds of risks as banks

Charles Ponzi

Study: 45 percent of Bitcoin exchanges end up closing

TECHNOLOGY / 26 APRIL 13 / by IAN STEADMAN

Tweet   Like   14   8 +1

A study of the Bitcoin exchange industry has found that 45 percent of exchanges fail, taking their users' money with them. Those that survive are the ones that handle the most traffic -- but they are also the exchanges that suffer the greatest number of cyber attacks.

Computer scientists Tyler Moore (from the Southern Methodist University, Dallas) and Nicolas Christin (of Carnegie Mellon University) found 40 exchanges on the web which offered a service of changing bitcoins into other fiat currencies or back again. Of those 40, 18 have gone out of business -- 13 closing without warning, and five closing after suffering security breaches that forced them to close. Four other exchanges have

Almost half of all exchanges close *Shutterstock*

Bank Regulation

for traditional banks, government typically:

imposes minimum reserve requirements

must hold some fraction of deposits in reserve

regulates behavior, investments

insures depositors against losses

acts as lender of last resort

Proof of Reserve

Bitcoin exchange can prove it has fractional reserve.
fraction can be 100%

Prove how much reserve you're holding:
publish valid payment-to-self of that amount
sign a challenge string with the same private key

Prove how many demand deposits you hold: ...

Merkle tree with subtree totals

each hashpointer includes total value in its subtree

H( ) H( )

H( ) H( )   H( ) H( )

H( ) H( )   H( ) H( )   H( ) H( )   H( ) H( )

user1 acct   user2 acct   user3 acct   user4 acct   user5 acct   user6 acct   user7 acct   user8 acct
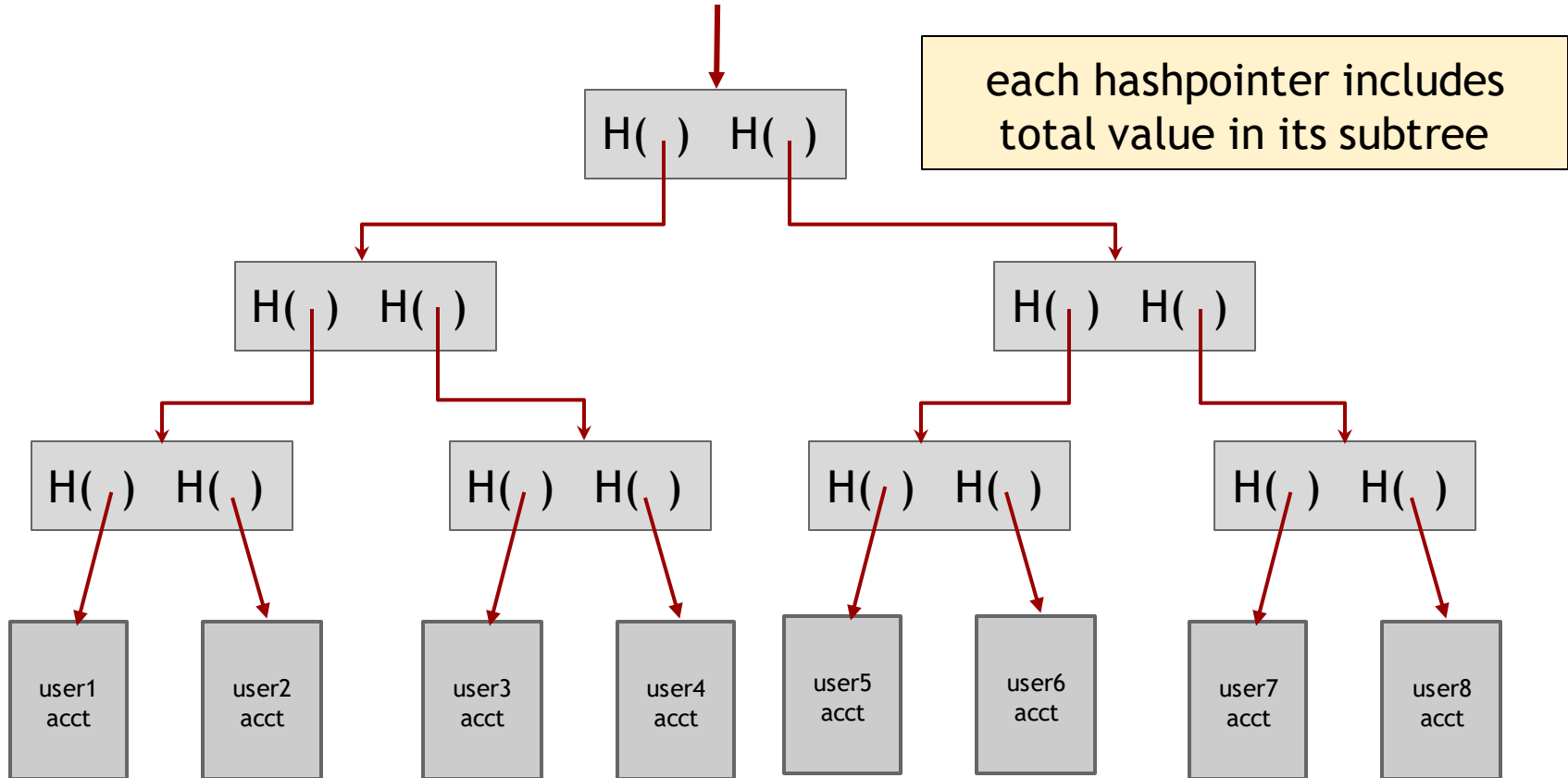
Checking that you're represented in the tree

show O(log n) items

H( ) H( )

H( ) H( )

H( ) H( )

your
acct
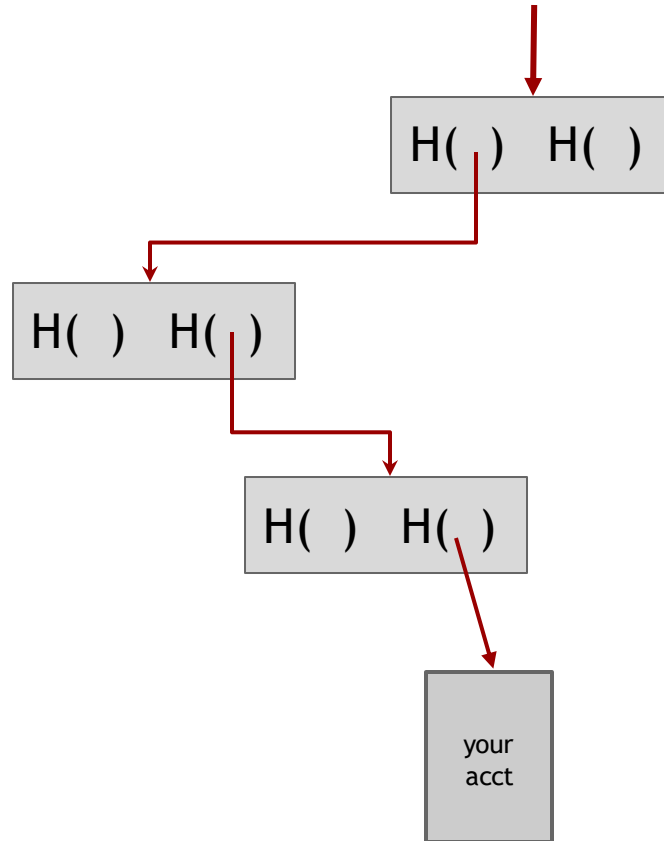
Proof of Reserve

Prove that you have at least X amount of reserve currency

Prove that customers have at most Y amount deposited

So reserve fraction ≥ X / Y

Lecture 4.5:

Payment Services

Scenario: merchant accepts BTC

customer wants: to pay with Bitcoin

merchant wants:

   * to receive dollars

   * simple deployment

   * low risk (tech risk, security risk, exchange rate risk)

HTML for
payment button

merchant

payment service

(5) confirm <transID, amount>

(4b) ok so far

(4) redirect

(3) payment interaction

(1) Pay with BTC button <transID, amount>

(2) clicked <transID, amount>

user
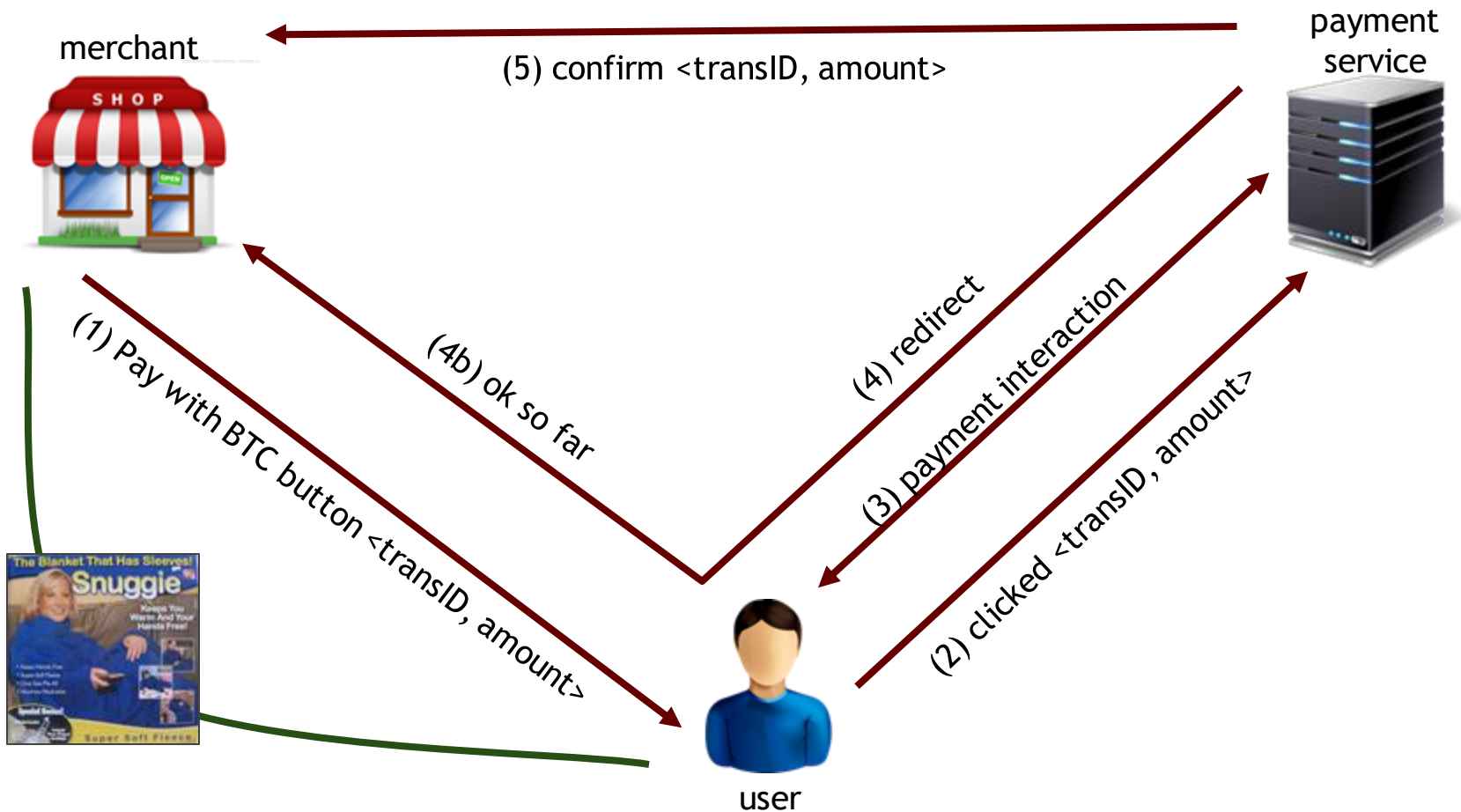
End result

customer: pays Bitcoins

merchant: gets dollars, minus a small percentage

payment service:

      gets Bitcoins

      pays 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

Interesting economics, discussed in later lecture

How are transaction fees set today?

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 0.01 BTC or larger, and

priority is large enough

Priority = (sum of inputAge*inputValue) / (trans size)

Otherwise fee is 0.0001 BTC per 1000 bytes

Approx transaction size: $148 \, N_{inputs} + 34 \, N_{outputs} + 10$

Most miners enforce the consensus fee structure.

If you don't pay the consensus fee, your transaction will take longer to be recorded.

Miners prioritize transactions based on fees and the priority formula.

Lecture 4.7:

Currency Exchange Markets

http://bitcoincharts.com/markets

	Symbol	Latest Price	30 days	Average	Volume	Low/High	Bid	Ask	24h Avg.	Volume	Low/High
▼	BitStamp USD bitstampUSD	582.54 2 min ago		620.52 -37.98 -6.12%	155,811.67 96,683,593.16 USD	570.5 658.88	581.13	582.54	585.63 -3.09 -0.53%	6,189.14 3,624,569.60 USD	574.15 596
	Bitfinex USD bitfinexUSD	619.78 6 days, 5 hrs ago		632.10 -12.32 -1.95%	126,042.21 79,671,138.43 USD	593.37 665	579.31	580.49	—	0.00 0.00 USD	— —
▼	btc-e USD btceUSD	572.78 0 min ago		615.51 -42.73 -6.94%	106,578.66 65,599,931.43 USD	562 654.381	572.541	572.779	576.33 -3.55 -0.62%	3,396.32 1,957,406.31 USD	566.001 585.85
▼	itBit USD itbitUSD	581.69 just now		618.36 -36.67 -5.93%	34,726.55 21,473,457.56 USD	571 662	580.27	581.11	582.64 -0.95 -0.16%	1,607.07 936,342.67 USD	577 587.99
▲	ANX USD anxhkUSD	593.43896 29 min ago		624.73 -31.29 -5.01%	30,902.66 19,305,871.63 USD	565.166 687.21424	577.2	593.34886	587.47 5.97 1.02%	1,476.78 867,565.29 USD	565.3373 602.06006
▲	LocalBitcoins USD localbtcUSD	977.52 9 min ago		665.75 311.77 46.83%	17,221.75 11,465,390.41 USD	492.94 2529.6	1163.78	558.61	636.33 341.19 53.62%	840.60 534,896.62 USD	531.87 2500
	1coin USD 1coinUSD	605.3 4 days, 6 hrs ago		625.85 -20.55 -3.28%	14,973.92 9,371,488.64 USD	601.5 664.5	605.1	605.3	—	0.00 0.00 USD	— —
▼	hitbtc USD hitbtcUSD	583.41 0 min ago		622.80 -38.39 -6.32%	14,778.51 9,205,987.87 USD	573.23 657.47	581.54	583.33	587.71 -4.30 -0.73%	459.21 269,883.25 USD	576.72 594.67
▲	CoinTrader USD cotrUSD	589.76 31 min ago		619.79 -30.03 -4.85%	1,460.39 905,136.91 USD	0.1 700	580	588.37	585.16 4.60 0.79%	76.52 44,773.46 USD	580.66 599.68
▼	Camp BX USD cbxUSD	593 1 hr, 36 min ago		633.51 -40.51 -6.40%	1,062.60 673,170.82 USD	585.14 670	595	604	606.28 -13.28 -2.19%	36.03 21,844.39 USD	585.14 626.8
▼	Ripple USD rippleUSD	583.71244672 6 min ago		621.33 -37.62 -6.05%	567.36 352,513.96 USD	574.98 655.99	582.03	585.71244671	584.69 -0.97 -0.17%	18.40 10,757.11 USD	575.6908721 590.9794998
▲	Kraken USD krakenUSD	586.5 18 min ago		625.75 -39.25 -6.27%	169.82 106,263.87 USD	574.57864 658.87046	586.5	597.75871	583.67 2.83 0.49%	1.37 800.09 USD	574.57864 591.90124
▼	bitKonan USD bitkonanUSD	581 2 hrs, 48 min ago		624.21 -43.21 -6.92%	99.32 61,997.57 USD	551 668	581.08	615	605.10 -24.10 -3.98%	2.43 1,467.97 USD	581 610
▲	The Rock Trading Company USD rockUSD	581 0 min ago		613.09 -32.09 -5.23%	77.86 47,734.81 USD	575 699.99	587.24	604.91	578.77 2.23 0.39%	2.15 1,244.36 USD	575 581
▼	Justcoin USD justUSD	579.92 16 hrs ago		624.54 -44.62 -7.14%	59.56 37,197.01 USD	578.113 700	614.93	631.21	589.41 -9.49 -1.61%	0.30 175.70 USD	578.197 599.999
▲	BitBay USD bitbayUSD	586.57 4 hrs, 57 min ago		609.30 -22.73 -3.73%	58.04 35,361.52 USD	547 631.12	586.44	588.17	586.45 0.12 0.02%	1.17 688.35 USD	583.98 586.57
▲	Vircurex USD vcxUSD	620.00124 8 hrs, 57 min ago		620.23 -0.23 -0.04%	3.76 2,329.85 USD	590 710	621	648	601.61 18.39 3.06%	0.05 30.40 USD	590 620.00124

Buying or selling	⦿ I want to buy bitcoins	**City:**	Princeton, United States
	○ I want to sell bitcoins		
Amount:	1000 USD ⇕	**Payment method:**	Cash ⇕ 🔍 Find offers

Results for buy bitcoins with cash near Princeton, United States

Trader	Distance	Location	Price/BTC	Limits	
joey777 (16; 100%) ⦿	19.0 miles	Trenton, NJ, USA	**635.01 USD**	50 - 1100 USD	Buy
Eotnak (0) ⦿	19.8 miles	Titusville, Hopewell Township, NJ 08560, USA	**616.80 USD**	25 - 1500 USD	Buy
billcashout (30+; 100%) ⦿	22.9 miles	New Jersey 18, New Brunswick, NJ, USA	**694.34 USD**	500 - 800 USD	Buy
James_Howlett (70+; 100%) ⦿	26.3 miles	Edison, NJ, USA	**651.72 USD**	500 - 1000 USD	Buy
BTCypher (100+; 100%) ⦿	28.4 miles	Levittown, PA, USA	**640.00 USD**	250 - 2900 USD	Buy

📍 Show more on map for buy bitcoins with cash

Basic market dynamics

market matches buyer and seller

large, liquid market reaches a consensus price

price set by supply (of BTC) and demand (for BTC)

Supply of Bitcoins

supply = coins in circulation (+ demand deposits?)

coins in circulation: fixed number, currently ~13.1 million

When to include demand deposits?
    When they can actually be sold in the market.

Demand for Bitcoins

BTC demanded to mediate fiat-currency transactions

Alice buys BTC for $

Alice sends BTC to Bob — BTC "out of circulation" during this time

Bob sells BTC for $

BTC demanded as an investment

if the market thinks demand will go up in future

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)

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

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

Equilibrium:

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