today
wallet operation
coin selection
SPV walkthrough
node types and problems
last time: sync
get software, connect
get headers
get blocks
replay history
arrive at utxo set
what about my money
how to pay people?
how to get paid?
software that manages this is called a "wallet"
wallet function
send and receive money
simple right?
need to receive money before you can send, so start with that
Receive address

Most output scripts are pay to pubkey hash (P2PKH)

The opcodes are all the same, with only the hash changing.

Address standard for hashes in ascii, e.g:
1F8f12E4uJDiTRLdPy1oze6aoh2o8yJCSJ
Receive address

Most output scripts are pay to pubkey hash (P2PKH)

The opcodes are all the same, with only the hash changing.

Address standard for hashes in ascii, e.g:

1F8f12E4uJDiTRLdPy1oze6aoh2o8yJCSJ
addresses on servers
keep a bunch of addresses on server
keep private keys offline
list of addresses can run out
pubkey generation without privkey?
BIP32 simplified

pubkey P, randomizer r

privkey p

A = P + hash(r,1)*G

a = p + hash(r,1)
BIP32 simplified

Can put pubkey and random data on server

server can make addresses as needed

observers can't link the addresses

revealing P and r would allow linking addresses but not stealing funds
Request payment

Hey, want this jacket? Send a coin to 1F8f12E...

(Note that Bitcoin does not attempt to solve the fair exchange problem; payments are not contingent on delivery of goods)
have I gotten paid?

Add your pubkey hashes to a list

For every transaction, look at every output script

If the script matches your PKH script, you got money!
wallet utxo list
Keep track of received payments
Save all the utxos to disk
txid:index, amount, which key, height
next, spend them
You want to send 6 coins somewhere; find utxos totalling over 6, use them as inputs, then add outputs.

<table>
<thead>
<tr>
<th>Wallet Address</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>884d:0</td>
<td>5 coins</td>
</tr>
<tr>
<td>b427:1</td>
<td>3 coins</td>
</tr>
<tr>
<td>1BobAddr2zKLw</td>
<td>6 coins</td>
</tr>
<tr>
<td>1AliceChange392</td>
<td>2 coins</td>
</tr>
<tr>
<td>Address</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>884d:0</td>
<td>1BobAddr2zKLw</td>
</tr>
<tr>
<td>b427:1</td>
<td>1AliceChange392</td>
</tr>
</tbody>
</table>
# coin selection

1 input, 1 output

Half the size, half the fee

<table>
<thead>
<tr>
<th>a273:3</th>
<th>1BobAddr2zKLw</th>
</tr>
</thead>
<tbody>
<tr>
<td>(6 coins)</td>
<td>amount: 6 coins</td>
</tr>
</tbody>
</table>
coin selection
A tricky problem (NP-hard) but heuristics work OK in practice
What are we optimizing for?
coin selection
optimize for:
minimize number of inputs used...
easy! Just pick biggest utxos
coin selection
optimize for:
minimize number of inputs used...
easy! Just pick biggest utxos
Want to minimize inputs next time as well; Ideally eliminate change output
coin selection

privacy concerns: Using 2 utxos in the same tx 'links' them; people can see that it's probably the same entity

maximum anonymity:
coin selection

privacy concerns:
Using 2 utxos in the same tx 'links' them; people can see that it's probably the same entity

maximum anonymity:
Always 1 input txs! (tons of txs)
losing money just because you signed a tx doesn't mean your money's gone broadcast? got into a block? Listen for your own utxos getting spent in every block
losing money
just because you signed a tx doesn't mean your money's gone
broadcast? got into a block?
Listen for your own utxos getting spent in every block
losing money
just because you signed a tx doesn't mean your money's gone
broadcast? got into a block?
Listen for your own utxos getting spent in every block
(same wallet on multiple computers)
intermission

0xff seconds to walk around, check on pset miner, etc

note that current pset high scores can be obtained by

$ nc hubris.media.mit.edu 6299

(seems not to work on MIT wifi)
wallets without bitcoin
We've talked about running bitcoin: syncing headers, checking signatures, building utxo set
But can you use bitcoin without doing this?
wallets without bitcoin

We've talked about running bitcoin: syncing headers, checking signatures, building utxo set

But can you use bitcoin without doing this?

Get someone else to do it!
full node
what was just called bitcoin many call a "full node"
Also possible are "lite nodes" or "SPV nodes"
SPV
simplified payment verification
mentioned in whitepaper
can verify work without much data
SPV howto
connect, get headers, verify
tell node all your addresses
for each header, ask if you gained or
lost utxos
verify merkle proof of response txs
SPV howto
connect, get headers, verify
tell node all your addresses
for each header, ask if you gained or lost utxos
verify merkle proof of response txs
SPV howto

connect, get headers, verify
tell node all your addresses
for each header, ask if you gained or lost utxos
verify merkle proof of response txs
SPV howto
connect, get headers, verify
tell node all your addresses
for each header, ask if you gained or
lost utxos
verify merkle proof of response txs
Merkle verification
Provide siblings up to top;
my tx must be in there
SPV problems
connect, get headers, verify
this is the same as for full nodes, so that's OK
SPV problems

tell node all your addresses

wait what?! Tell all your addresses?

Node needs to know what txs to send you. If they send all, no savings

Bloom filters; poor privacy

Block based filters are better
SPV problems
for each header, ask if you gained or lost utxos
any possible problems here?
SPV problems
for each header, ask if you gained or lost utxos
easy to lie by omission
mitigate by connecting to more nodes
... but then share your addresses with even more people!
SPV howto
verify merkle proof of response txs
merkle proofs are quick
but prove inclusion, not exclusion
SPV and beyond
So SPV sounds pretty bad and I think I'll stick to my full node. But I gotta ask, is there something worse than SPV? ... asking for a friend.
Not even SPV (NEP5V)
Websites, phone wallets
Send all your addresses, ask if you have utxos
Server responds that you do. Cool.
Build txs, sign, send to server.
NESPV issues
Any potential problems?
NESPV issues
Any potential problems?

Server can:

say you got paid when you didn't
say you lost money when you didn't

If in browser, even more fun
Further

API based wallets sound real bad.

But we can do worse, right?
Someone else's coins
Don't even have keys. Just have a website where they run a node* / wallet and owe you money/
Tends to end badly.
Always misses the point.

*guess which kind. OK maybe don't.
<table>
<thead>
<tr>
<th></th>
<th>Full node</th>
<th>SPV</th>
<th>API query</th>
<th>Hold my key</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>170GB</td>
<td>50MB</td>
<td>1MB</td>
<td>1MB ?</td>
</tr>
<tr>
<td>storage</td>
<td>4GB</td>
<td>50MB</td>
<td>0B</td>
<td>0</td>
</tr>
<tr>
<td>speed</td>
<td>hours</td>
<td>seconds</td>
<td>1 sec</td>
<td>0</td>
</tr>
<tr>
<td>privacy</td>
<td>OK</td>
<td>poor</td>
<td>poor</td>
<td>none</td>
</tr>
<tr>
<td>security</td>
<td>OK</td>
<td>medium</td>
<td>poor</td>
<td>none</td>
</tr>
</tbody>
</table>
wallets are fun
still big usability issues
interesting problems all around

Have fun with Ethan on Wednesday,
good luck w/ pset!