Bitcoin, Cryptocurrency, and the Impact on the Financial Services Industry

BILL LABOON (LABOON@CS.PITT.EDU)

LECTURER, COMPUTER SCIENCE DEPARTMENT, UNIVERSITY OF PITTSBURGH

What is Bitcoin?

- A peer-to-peer, electronic cash system…
- which creates a cryptographically secure distributed ledger (*the blockchain*)…
- and secures it with *proof-of-work*…
- to enable *pseudonymous* transactions in a *decentralized* manner (with no controlling body or regulator).
- As of today, it is by far the most successful *cryptocurrency*.

The User's Perspective

- This presentation will explain HOW Bitcoin works…
- … but it is not necessary to know these details to use it.
- You can check your email without understanding (or knowing about!) TCP/IP, caching algorithms, or CPU process scheduling.
- At a high level, Bitcoin network consists of addresses and keys to those addresses

Wallet (Address and Key)

Bitcoin Address

SHARE

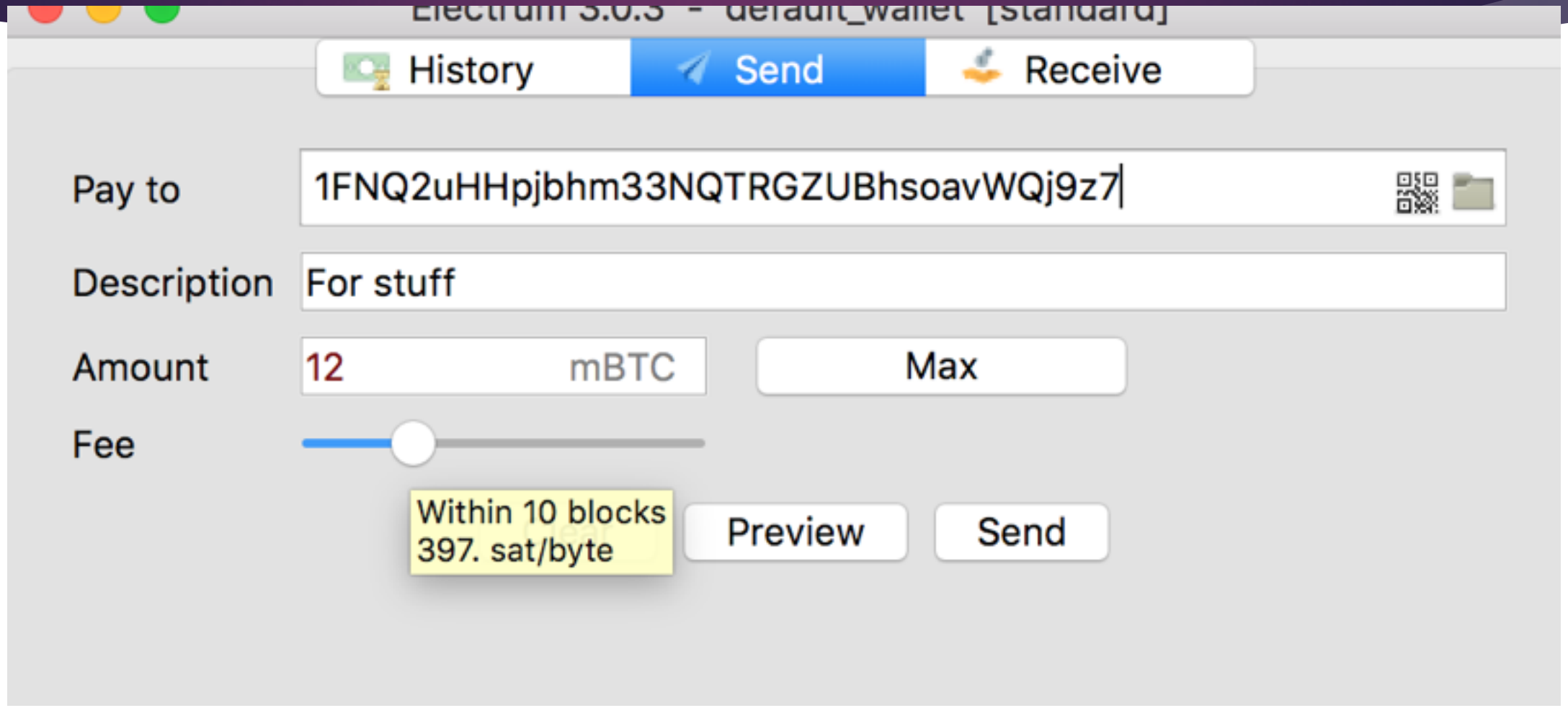
1FNQ2uHHpjbhm33NQTRGZUBhsoavWQj9z7

Private Key

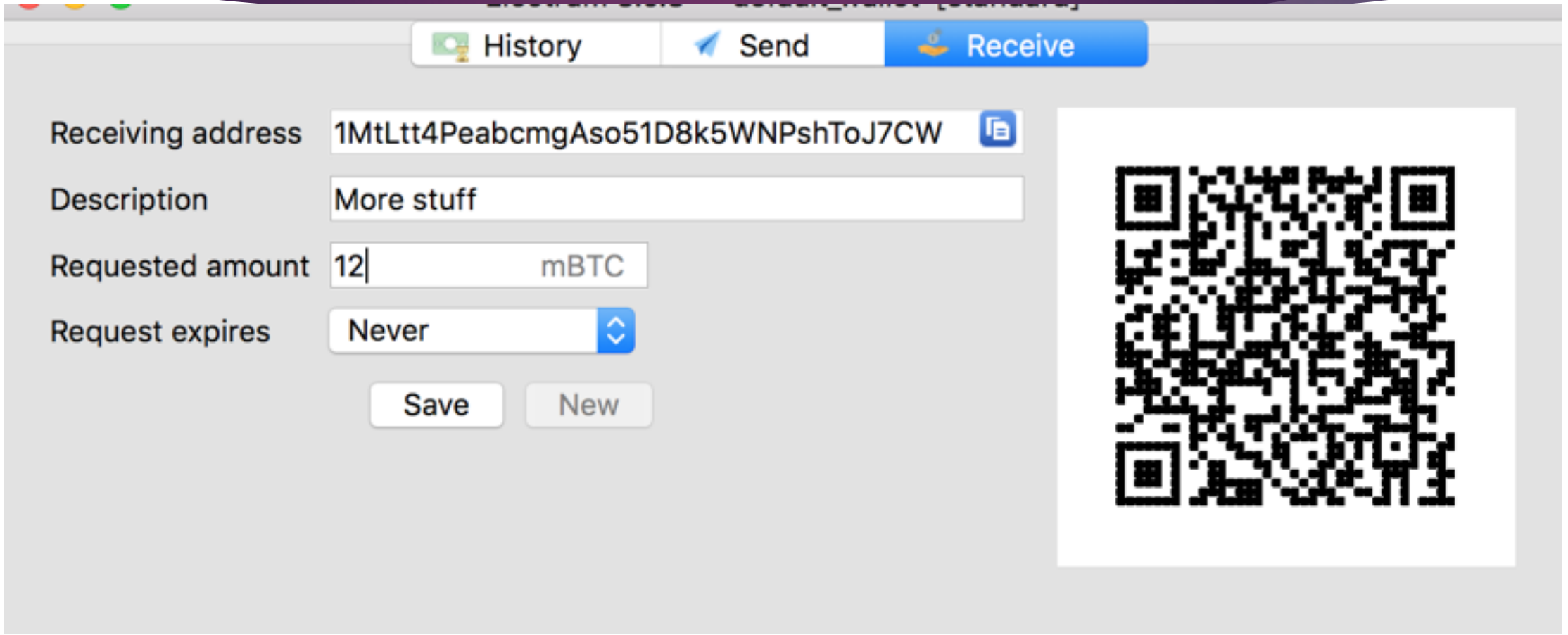
SECRET

L11EpZk2v1LJ6JCJTxxcSmm2WsAfbW51rPZdd1ebX4HimM97d1VZ

Sending Bitcoin



Receiving Bitcoin



How do you get bitcoin?

- **Mining:**
  - Creating Bitcoin by securing the network (discussed later - generally not done by individuals)
- **From another person -**
  - Convince someone who has bitcoin to give you some for something
- **From an exchange -**
  - By far the most common way
  - Just like trading currency (e.g. exchanging dollars for euros)
  - Numerous exchanges - Coinbase/GDAX, Poloniex, Kraken

So what is a bitcoin?

- Think if someone came into a bank and asked to see "their" dollar bills in their checking account
- Bitcoin is a further abstraction - there is no such thing as a "physical bitcoin" or "a bitcoin on the network"
- In fact, a bitcoin is just an arbitrary division - 1 / 21 millionth of all the value on the Bitcoin network
- Smallest value is a satoshi - there are 100 million satoshi in one bitcoin (= 2.1 quadrillion satoshi in Bitcoin network)

Bitcoin: A VERY Large Mail Room

1890112 3987254 2219071 7653421	99325231 80031287 81652837 98117262	97272727 98172652 88291542 22873651	65245567 90233746 00018276 91356483	83822733 89192635 11273525 33345981
7652352 8272636 9013463 8827345	77615343 66253411 98165473 00110872	43447691 00928371 01827777 82337257	88272633 91023932 99847574 99283644	86374561 10928373 77253526 99283731
8190292 9827362 3354677 8892837	72636451 91802927 29384761 83873647	01893820 29387271 99827326 44563289	10293833 29299384 00938272 99283762	67182001 22283736 99287362 99022837

Bitcoin: A VERY Large Mail Room

As long as I know the *Bitcoin address*, I can always insert money into the slot.

But I can't get it out without my *private key*.

A Bitcoin address plus a private key is a *wallet*.

86374561
10928373
77253526
99283731

You share your address but never your private key!

Accessing Your Wallet

- We need to take a short detour into one-way functions here…
- A one-way function is simple to do in one direction, but much more difficult going "backwards"
- By-hand example:
  - What is 3.5 to the 4th power?
  - What is the 4th root of 231.3441?

Accessing Your Wallet

- What is 3.5 to the 4th power?
  - Very simple to do!
- What is the 4th root of 231.3441?
  - Much more difficult - but what if I told you the answer was 3.9?
  - Very hard to calculate, but very easy to verify!
- The math problems in Bitcoin follow the same idea but MUCH more complex

Accessing Your Wallet

- Think of your wallet address as “231.3441” and your private key as “3.9”
- Anyone can send to “231.3441” but only you have the power to send from that address, since you know the answer to the math problem (key)

Much more complex

Bitcoin Address

SHARE

1FNQ2uHHpjbhm33NQTRGZUBhsoavWQj9z7

Private Key

SECRET

L11EpZk2v1LJ6JCJTxxcSmm2WsAfbW51rPZdd1ebX4HimM97d1VZ

- **SHARE (Address):**
  3,864,735,657,839,164,620,170,223,983,342,970,231,793,944,167,574,307,629,040
- **SECRET (Key):**
  16,352,452,327,361,720,873,228,280,772,068,220,842,709,704,046,398,069,492,223,434,257,762,933,086,993,622,020,815,355,768

Couldn’t someone just guess your secret key?

- Assume you know the address, you need the secret key
- Gather up billions of dollars of equipment, so you can try 100,000,000,000,000 (100 quadrillion) numbers per second
- Do this for 13.7 billion years (time since the Big Bang)
- That’s 43,209,800,000,000,000,000,000,000,000,000 possible secret keys

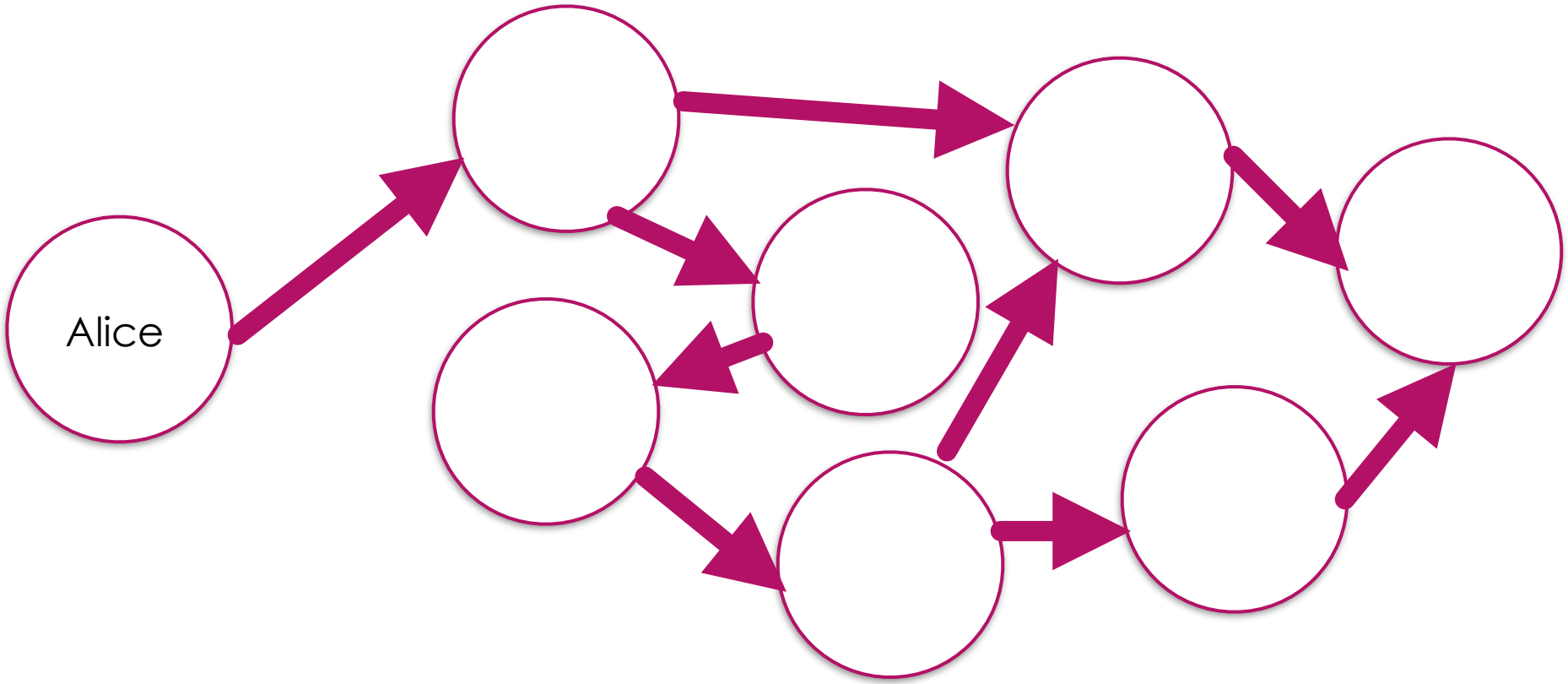
Couldn’t someone just guess your secret key?

- Congratulations, you have a:

  0.00000000000000000000000000000000000000373%

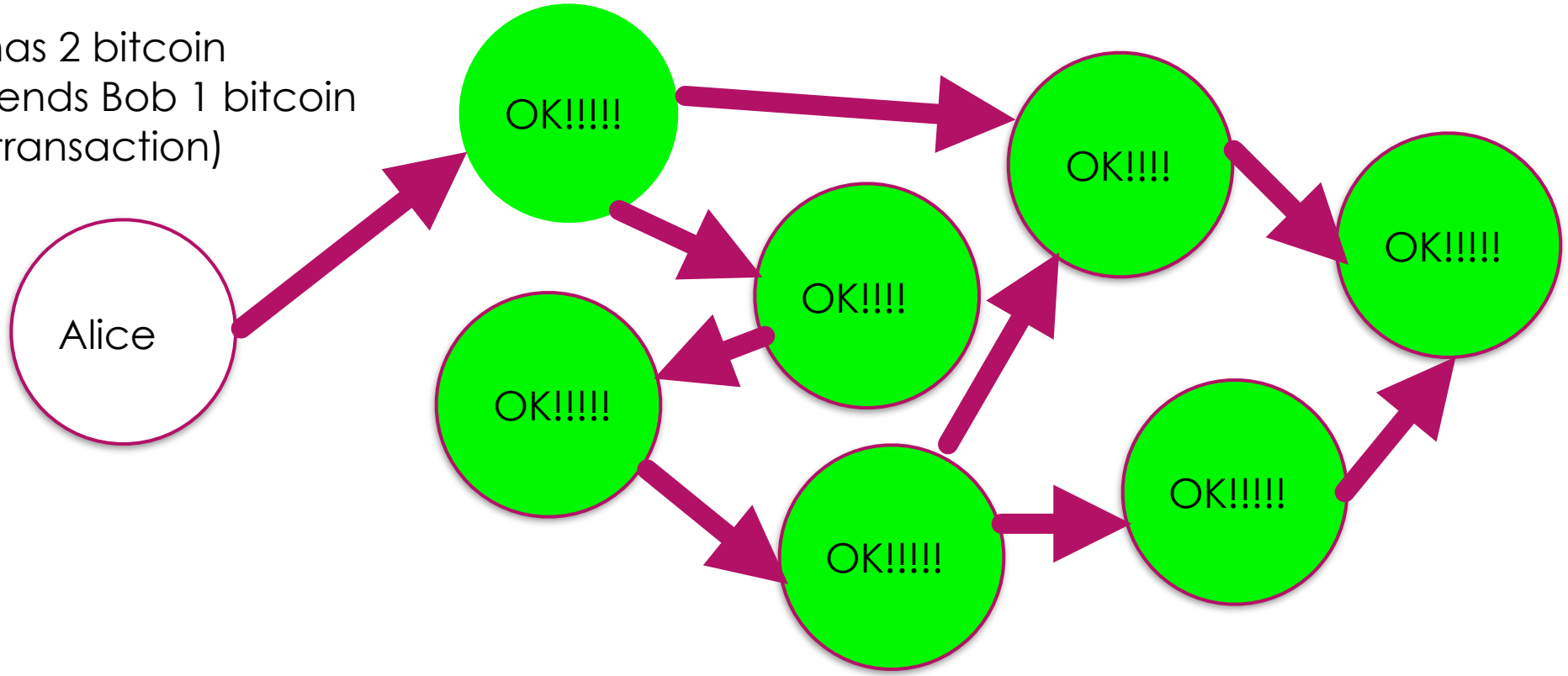
  chance of getting the key!

Distributed Consensus



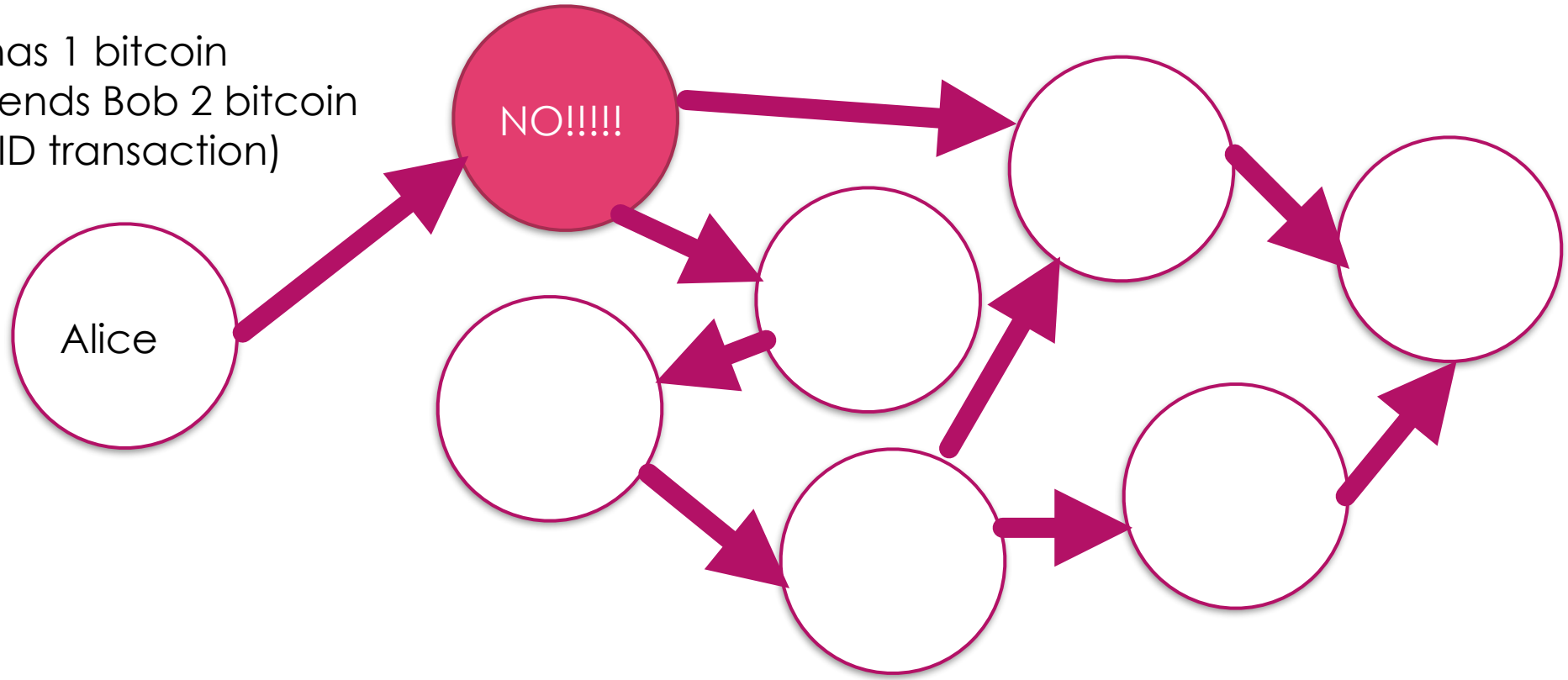
Distributed Consensus

Alice has 2 bitcoin
Alice sends Bob 1 bitcoin
(valid transaction)



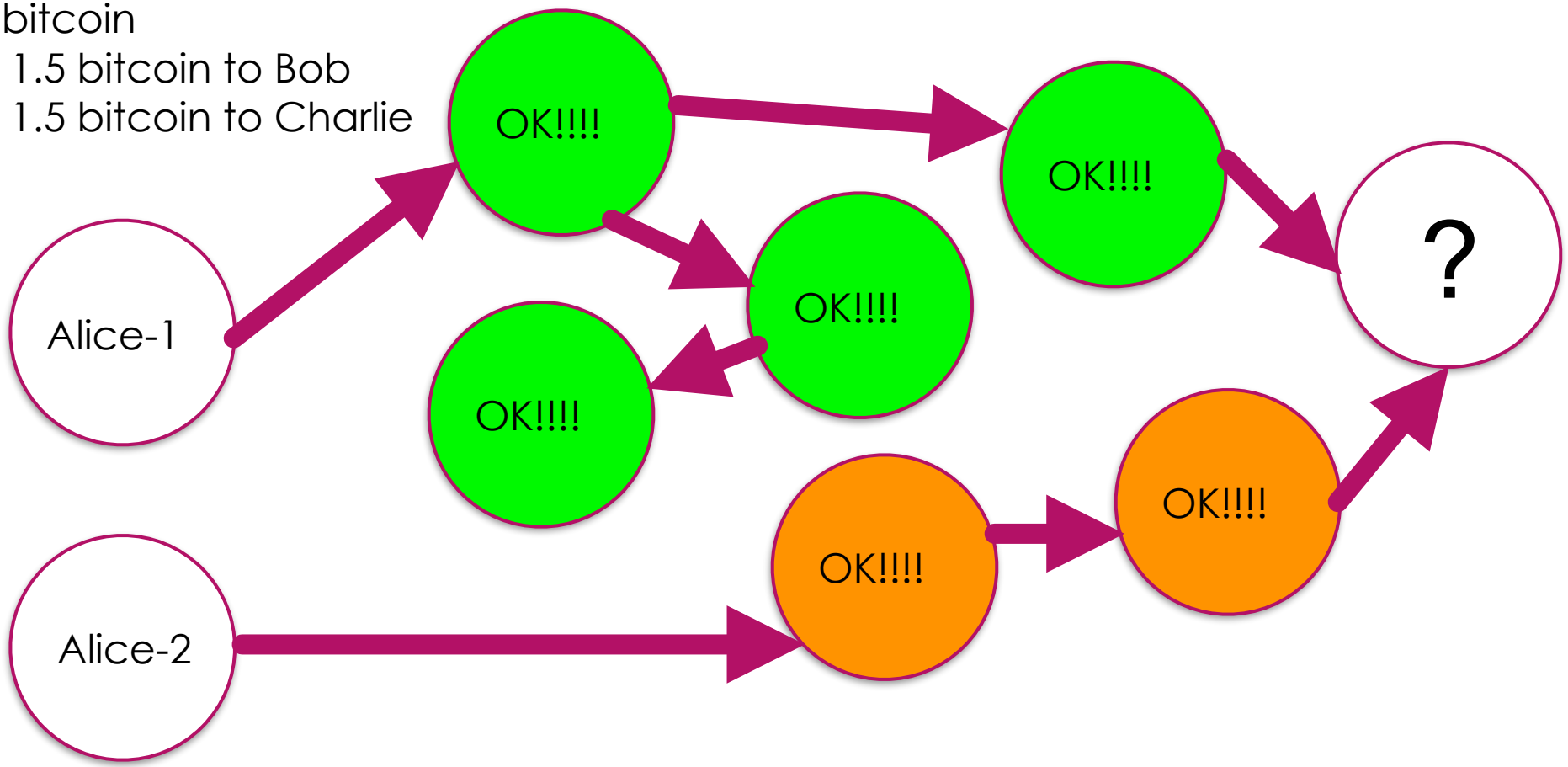
Distributed Consensus

Alice has 1 bitcoin
Alice sends Bob 2 bitcoin
(INVALID transaction)



Double-Spend Attack

Alice has 2 bitcoin
Alice sends 1.5 bitcoin to Bob
Alice sends 1.5 bitcoin to Charlie



Mining

- There are certain computers on the network which act as "miners"
- Miners bundle up transactions into blocks
- They are rewarded every time they create a block (thus, "mining") with a "block reward" and the transaction fees in all of the transactions

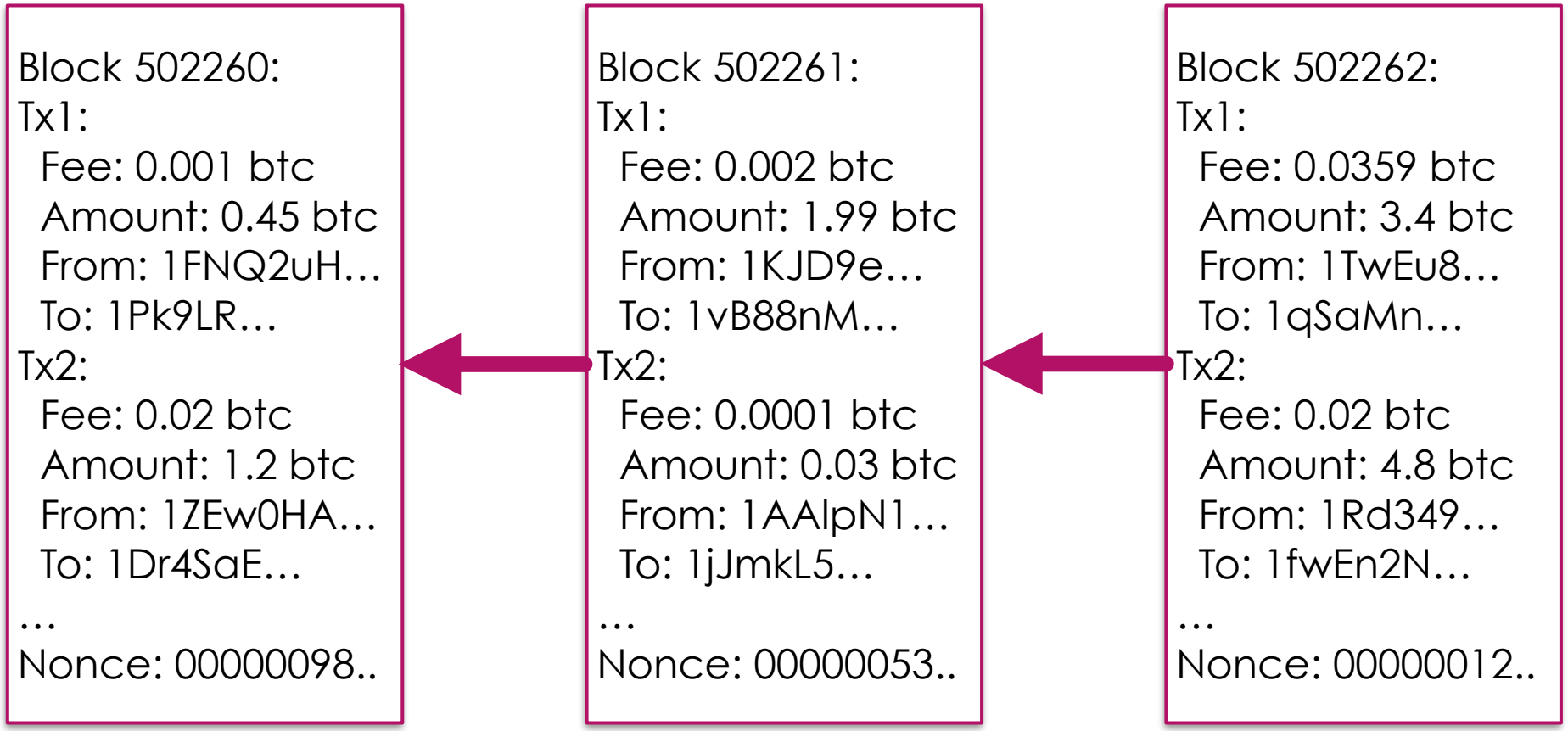
The Blockchain

- The blockchain is the "ground truth"
  - Miners bundle up valid transactions in order
  - They do lots of difficult calculations to make it a valid block (this is called *proof-of-work* - it proves that the miners are spending time and energy on securing the network)
  - First miner to figure out the solution and make a block, broadcasts it out to all nodes and other nodes check - hard to calculate but easy to verify
  - That miner gets all transaction fees (~ 5 bitcoin recently) in the block plus a "coinbase" (currently 12.5 bitcoin)
  - The coinbase is where all bitcoin originate

The Blockchain

- Adding a block to the blockchain takes massive amounts of computing power
  - Specialized computers - ASICs - are used for this purpose - ordinary computers are orders of magnitude too slow
  - Current Bitcoin network “hashrate”: 15 quintillion hashes per second
  - Takes ~ 10 minutes to make a block
  - Note that ~ 10 minutes is self-correcting

The Blockchain



The Blockchain

- **For small transactions:** seeing the transaction is valid in the transaction pool is probably enough security
- **For medium-sized transactions:** wait until it has been confirmed and in a block
- **For large-scale transactions:** wait until confirmed by six blocks

Decentralized, Trustless, Deflationary

- If you are running a full node, there is never a need to trust any other nodes
- It is easy for your computer to verify that everybody is following the rules
- This means that there is no central authority on the network
- Inherently deflationary - only 21 million bitcoin will ever be mined
- If you lose your key or send to a bad address - those bitcoin are gone!

Other Popular Cryptocurrencies

- Ethereum
- Ripple
- Dogecoin
- Monero
- Vertcoin

Ethereum - Trusted Computing

- "Programmable money" - allows you to do relatively complicated programs
  - Bitcoin has some advanced features (e.g. multi-sig) but not like this
  - Pros and cons! More chance for attacks/errors/etc.
- Examples:
  - Smart (self-executing) contracts
  - Dapps (distributed applications)
  - ICOs (running another cryptocurrency on the Ethereum network)
  - DAOs (distributed autonomous organizations)

Ripple - Fast and Scalable Transfers

- System for fast monetary transfers between registered gateways
- Allows for very cheap (< 1 cent) transactions
- Has need for financial intermediaries, unlike Bitcoin
- Uses a consensus protocol instead of proof-of-work

Dogecoin - An Inflationary Coin

- Similar to Bitcoin, but inflationary
  - 5.256 billion new coins minted every year, forever
- Started as a “joke currency”, but has a “market cap” of over one billion dollars

Monero - An Anonymous Coin

- Truly anonymous, instead of pseudonymous
- Bitcoin has an entirely transparent ledger, and every computer on the network can see the entire history of the blockchain
  - if you can associate, say, address 31kDa9o7h7UVn13Xegvky3Bq9omSYH6T1d with “Joe Schmoe”, then I know Joe Schmoe has 16,126 bitcoin in his account
  - Advertising a high net worth can be dangerous!
- Monero forces anonymous, and not just pseudonymous, transactions
- Downside: relatively slow transactions, heavy nodes, major KYC issues

Vertcoin - An ASIC-Resistant Coin

- Bitcoin mining must be done on ASICS - specialized computers that are good for nothing else
  - Oyster fork (ASIC) versus Swiss Army knife (general purpose computers)
- Result: centralized mining operations (most in China - ~81% or Iceland - ~5%)
- Vertcoin miners can run on regular computers and still be viable
- The aim is to be as decentralized as possible
- Downside: less “stickiness” since people can repurpose miners!

So what does it all mean?

- Cryptocurrency provides an alternative financial system
- Not necessarily better or worse, but different

Strengths

- Trusted, transparent transactions
- Censorship resistance (easy to bypass regulatory controls)
- Simple, fast long-distance and cross-border transactions
- In-system inflation is minimal, controlled, and set by the algorithm

Weaknesses

- Very unforgiving
- Sometimes-high transaction fees
- Censorship resistance (easy to bypass regulatory controls)
- Volatile pricing
- Possible weaknesses in algorithm or code
- No telling which cryptocurrency/-ies may become dominant
- Inflation cannot be controlled by external sources

“Everyone their own Swiss bank”

- One person can carry millions, or even billions, of dollars on a piece of paper in their pocket
- But if anyone else copies this paper, that money is **gone**
- Make a typo and you could burn your bitcoin forever
- External companies (e.g. Coinbase) can provide safe storage, acting as a secondary layer on top of the Bitcoin network

Compliance Risk

- Forensic analysis of the blockchain is possible, but difficult
- What happens when a customer tries to deposit bitcoin that were recently stolen?
- What about bitcoin that were stolen 100 transactions ago?
- How about bitcoin that went through a “mixer”?
- Should exchanges that store bitcoin censor outgoing transactions?

Accounting/Regulatory Issues

- Many unresolved regulatory questions about cryptocurrency
- If I swap Litecoin for Bitcoin, is that a taxable event? Or a like-kind exchange?
- Bitcoin is currently considered a “property” - thus, every time it is used to buy something, you need to figure out your capital gains on it
- There is a need for tools/companies to automate this bookkeeping

Questions?

BILL LABOON (LABOON@CS.PITT.EDU)

LECTURER, COMPUTER SCIENCE DEPARTMENT, UNIVERSITY OF PITTSBURGH