

# An Introduction to Bitcoin

BILL LABOON ([LABOON@CS.PITT.EDU](mailto: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**

1CmMMUN6as6VKxjKZtFg9FPNbhQZDMbyX1

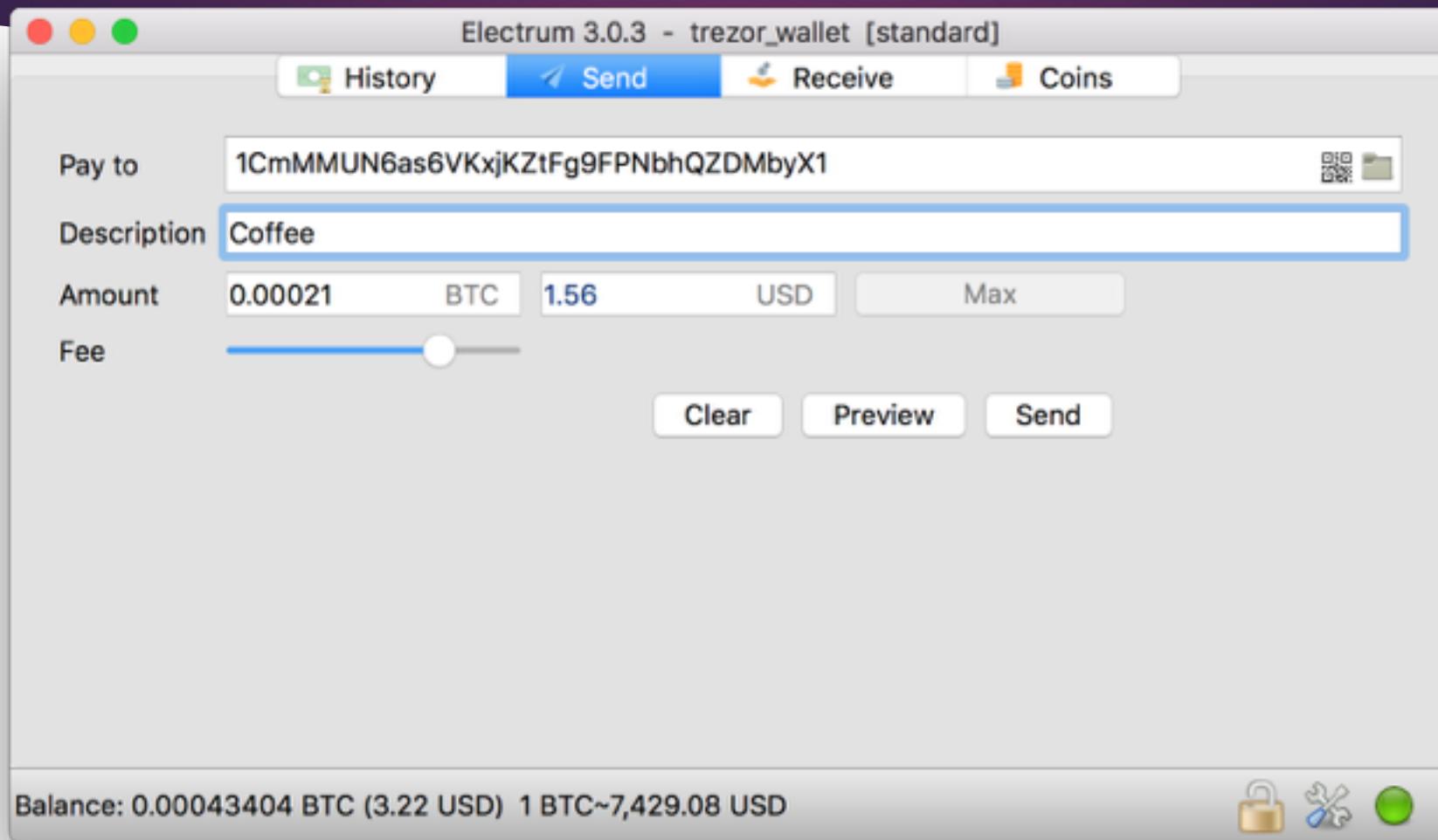
Private Key



**SECRET**

KyxgwmqzCiUQ1NvUZkQKet56rgwwuNZda8QChFV3DLEp9EVj54rB

# 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
- ▶ **From an exchange -**
  - ▶ By far the most common way
  - ▶ Just like trading currency (e.g. exchanging dollars for euros)
  - ▶ Numerous exchanges - Coinbase, 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!**

# Shared “mailroom”

- ▶ A copy of this “mailroom” is (in a manner of speaking) on every Bitcoin node in the network
- ▶ An alternative way to think about this is that every Bitcoin node has a spreadsheet which lists every transaction ever made on the Bitcoin network
- ▶ But this is a special spreadsheet where I can only move bitcoin from an address if I know the corresponding secret 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?
  - ▶ Relatively simple to do!
  - ▶  $3.5 * 3.5 * 3.5 * 3.5 = 150.0625$
- ▶ What is the 4th root of 231.3441?
  - ▶ Much more difficult - but what if I told you the answer was 3.9?
  - ▶ Extremely hard to calculate, but relatively easy to verify!
  - ▶  $3.9 * 3.9 * 3.9 * 3.9 = 231.3441$
- ▶ 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 want the secret key
- ▶ There is an attempt at something similar, the Large Bitcoin Collider, which checks ~ 4,000,000,000,000 keys per year - let's say that we have a system that can do that every second
- ▶ Do this for 13.7 billion years (432,342,079,200,000,000 seconds - time since the Big Bang)

Couldn't someone just guess your secret key?

Congratulations, you have a:

**0.00000005%**

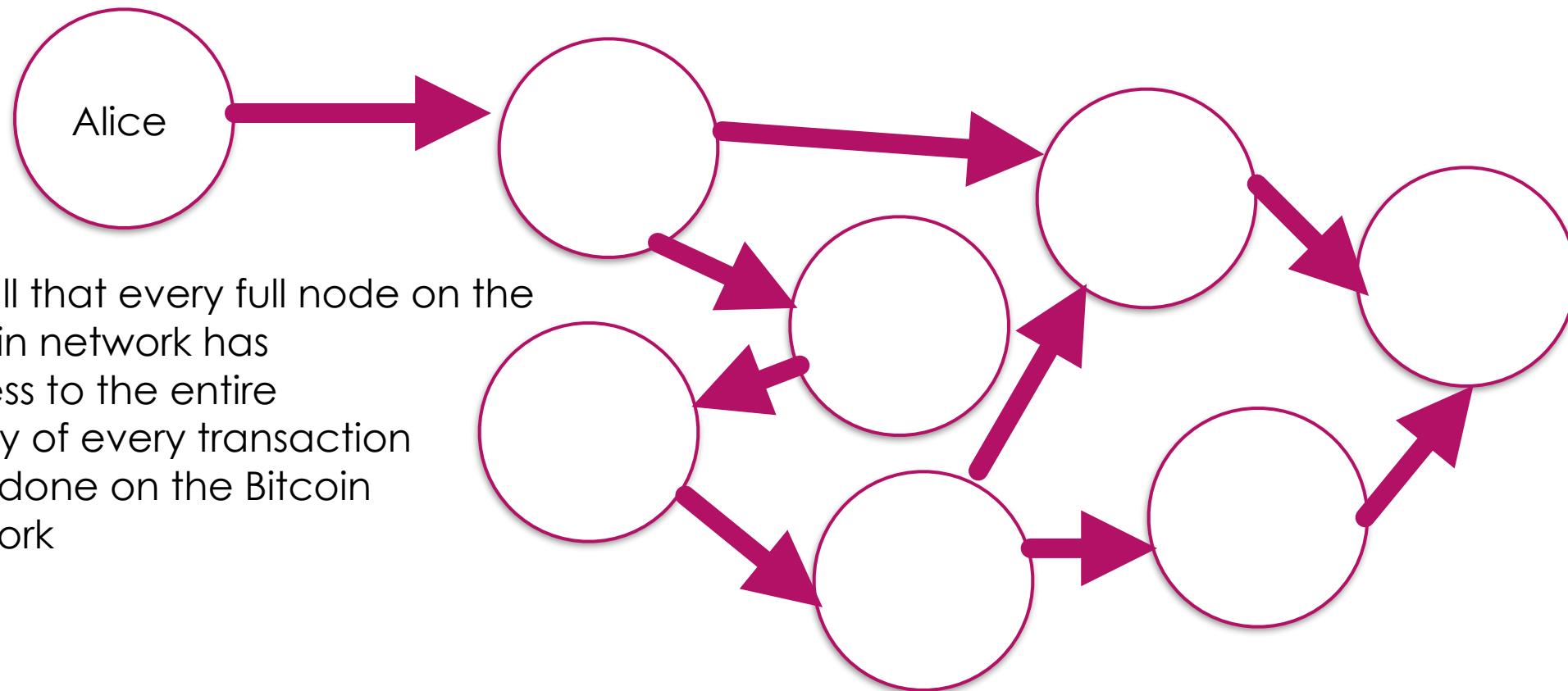
chance of getting the key!

That's about a 1 in 111 million shot...

# Game Theory

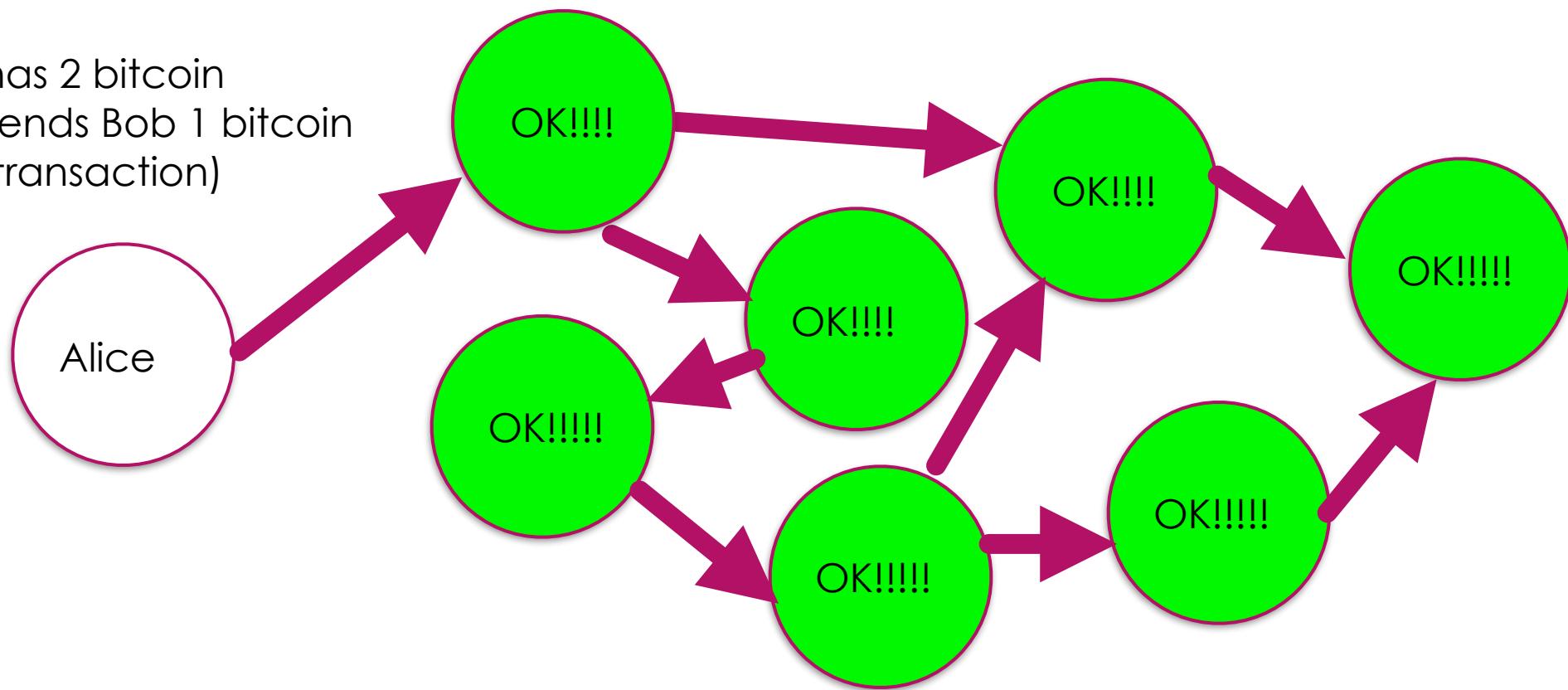
- ▶ With that much computing power, you'd make much more money just mining (or using it for something else)
- ▶ Bitcoin relies on the fact that for a given actor, it almost always makes sense to “play by the rules”
- ▶ Note that this does not preclude actors for whom money is not a primary concern!

# Distributed Consensus



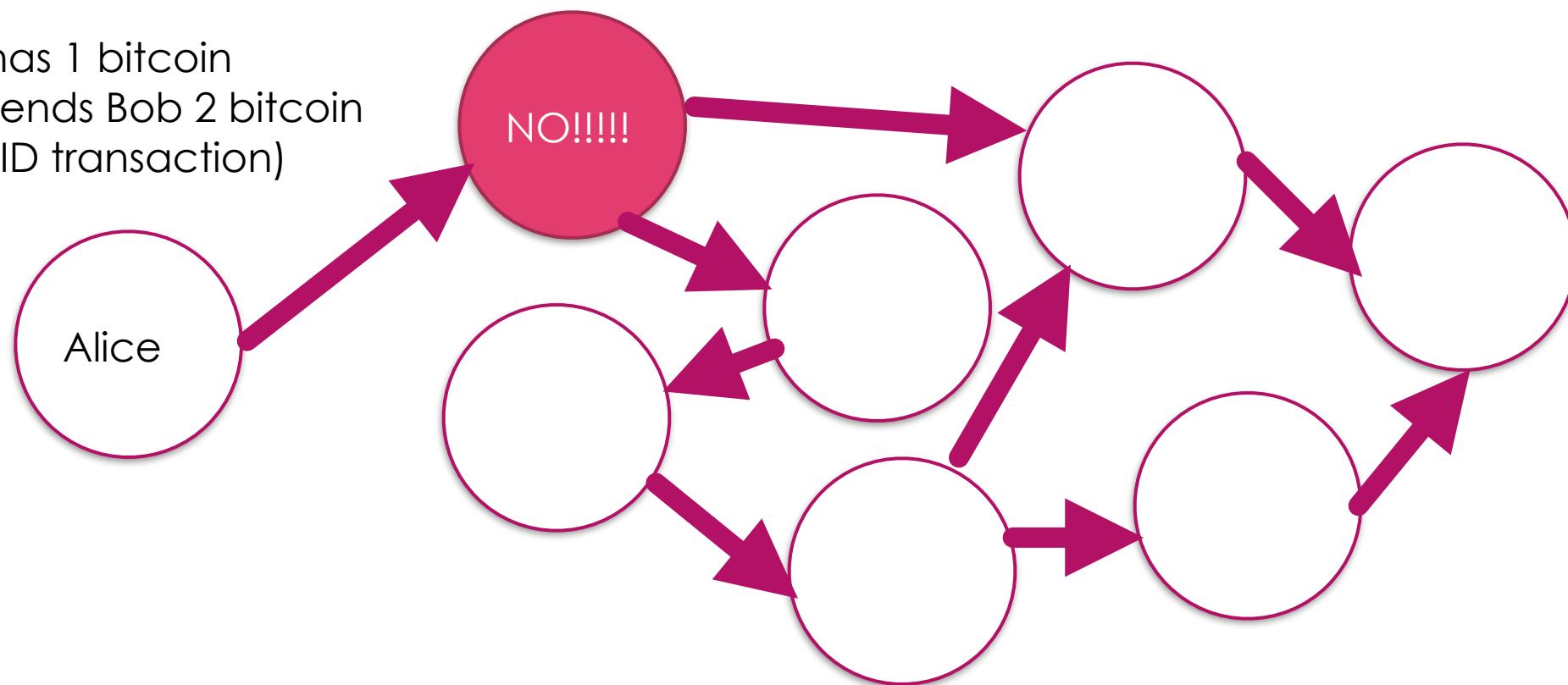
# Distributed Consensus

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



# Distributed Consensus

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

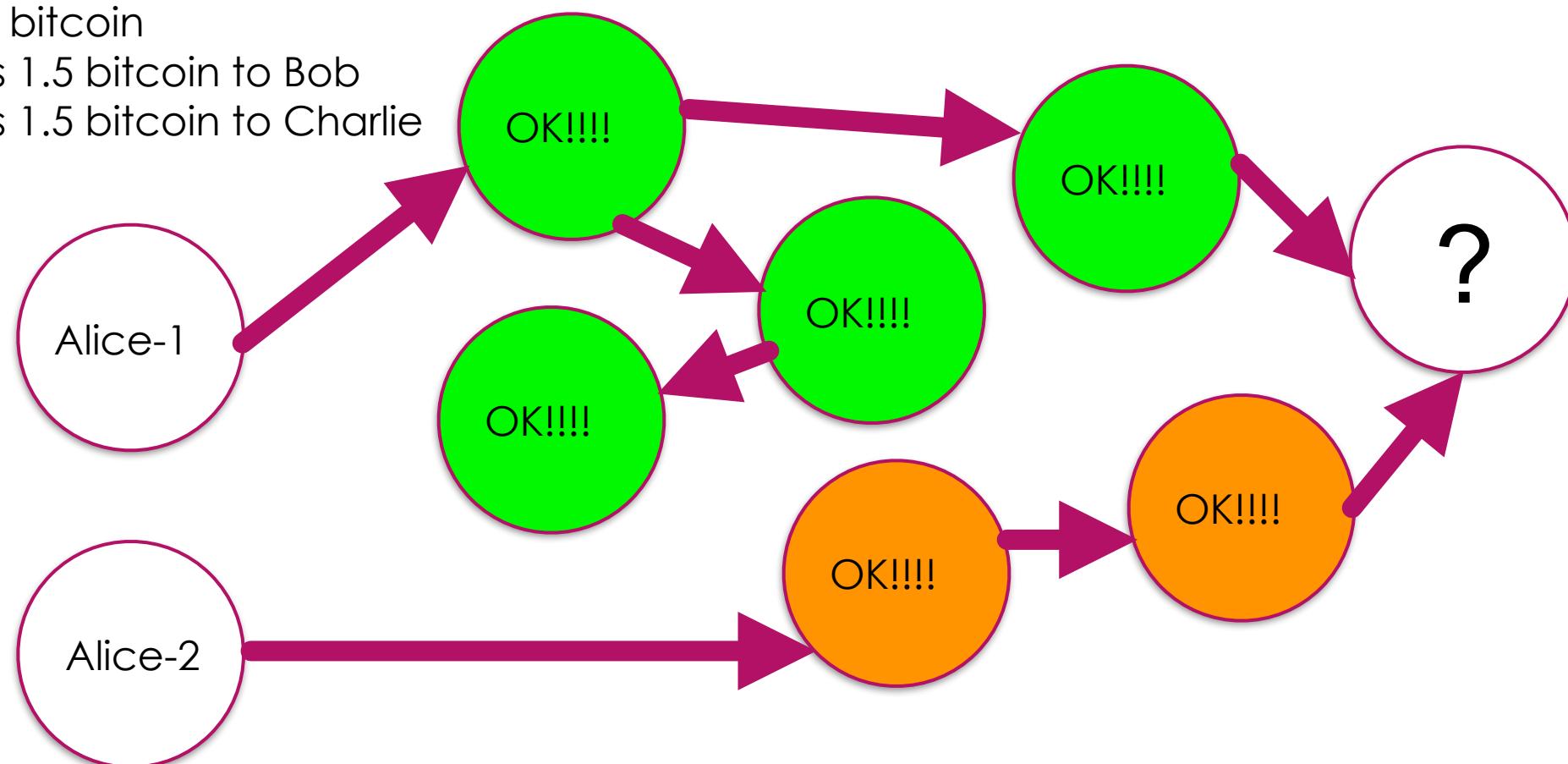


# Double-Spend Attack

Alice has 2 bitcoin

Alice sends 1.5 bitcoin to Bob

Alice sends 1.5 bitcoin to Charlie



# Two “Levels” of a Bitcoin Transaction

- ▶ Transaction pool (“mempool”) - A transaction that has been found to be valid based on previous information (but may be part of a double-spend)
  - ▶ These are subject to being dropped!
- ▶ Blockchain - A transaction that has been “mined” and now considered part of the “forever” history of the Bitcoin network
  - ▶ Also liable to be dropped, but MUCH less likely
  - ▶ After an hour or two, EXTREMELY unlikely

# 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 into “blocks”
  - ▶ 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 (~ 0.01 - 0.3 bitcoin recently, has been as high as ~ 13 bitcoin) in the block plus a “block reward” (currently 12.5 bitcoin)
  - ▶ The block reward 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”: 36 quintillion hashes per second
  - ▶ Takes ~ 10 minutes to make a block
  - ▶ Note that ~ 10 minutes is self-correcting

# The Blockchain

Block 502260:  
Tx1:  
Fee: 0.001 btc  
Amount: 0.45 btc  
From: 1FNQ2uH...  
To: 1Pk9LR...  
Tx2:  
Fee: 0.02 btc  
Amount: 1.2 btc  
From: 1ZEw0HA...  
To: 1Dr4SaE...  
...  
Nonce: 00000098..

Block 502261:  
Tx1:  
Fee: 0.002 btc  
Amount: 1.99 btc  
From: 1KJD9e...  
To: 1vB88nM...  
Tx2:  
Fee: 0.0001 btc  
Amount: 0.03 btc  
From: 1AAIpN1...  
To: 1jJmkL5...  
...  
Nonce: 00000053..

Block 502262:  
Tx1:  
Fee: 0.0359 btc  
Amount: 3.4 btc  
From: 1TwEu8...  
To: 1qSaMn...  
Tx2:  
Fee: 0.02 btc  
Amount: 4.8 btc  
From: 1Rd349...  
To: 1fwEn2N...  
...  
Nonce: 00000012..

# The Blockchain

- ▶ **For small transactions:** seeing the transaction is valid in the mempool is probably enough security (double-spends are difficult to do correctly)
- ▶ **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!

# Strengths

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

# Weaknesses

- ▶ Very unforgiving
- ▶ Censorship resistance (easy to bypass regulatory controls)
- ▶ Volatile pricing
- ▶ Possible weaknesses in algorithm or code
- ▶ Inflation cannot be controlled by external sources

# Other Popular Cryptocurrencies

- ▶ Ethereum
- ▶ Ripple
- ▶ Dogecoin
- ▶ Monero
- ▶ Vertcoin

# Questions?

PDF of slides available at:

[https://github.com/laboon/fei\\_bitcoin](https://github.com/laboon/fei_bitcoin)

BILL LABOON ([LABOON@CS.PITT.EDU](mailto:LABOON@CS.PITT.EDU))

LECTURER, COMPUTER SCIENCE DEPARTMENT, UNIVERSITY OF PITTSBURGH