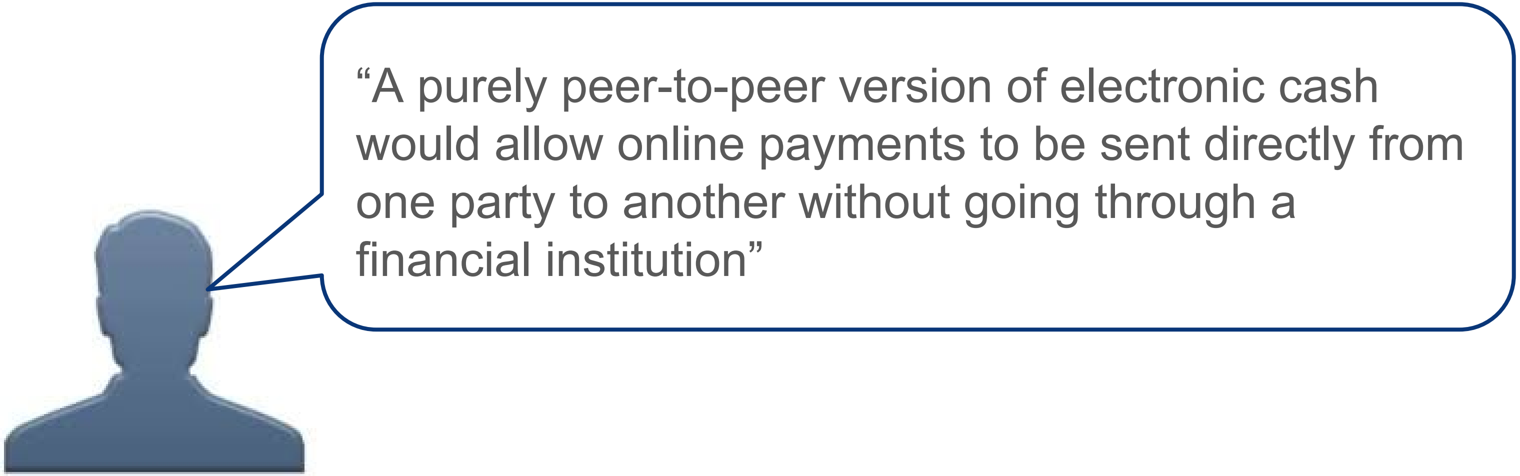
Mobile Tea

Bitcoin: Beyond the Hype

James Piechota, Vlad Shtokman, Tom Houman

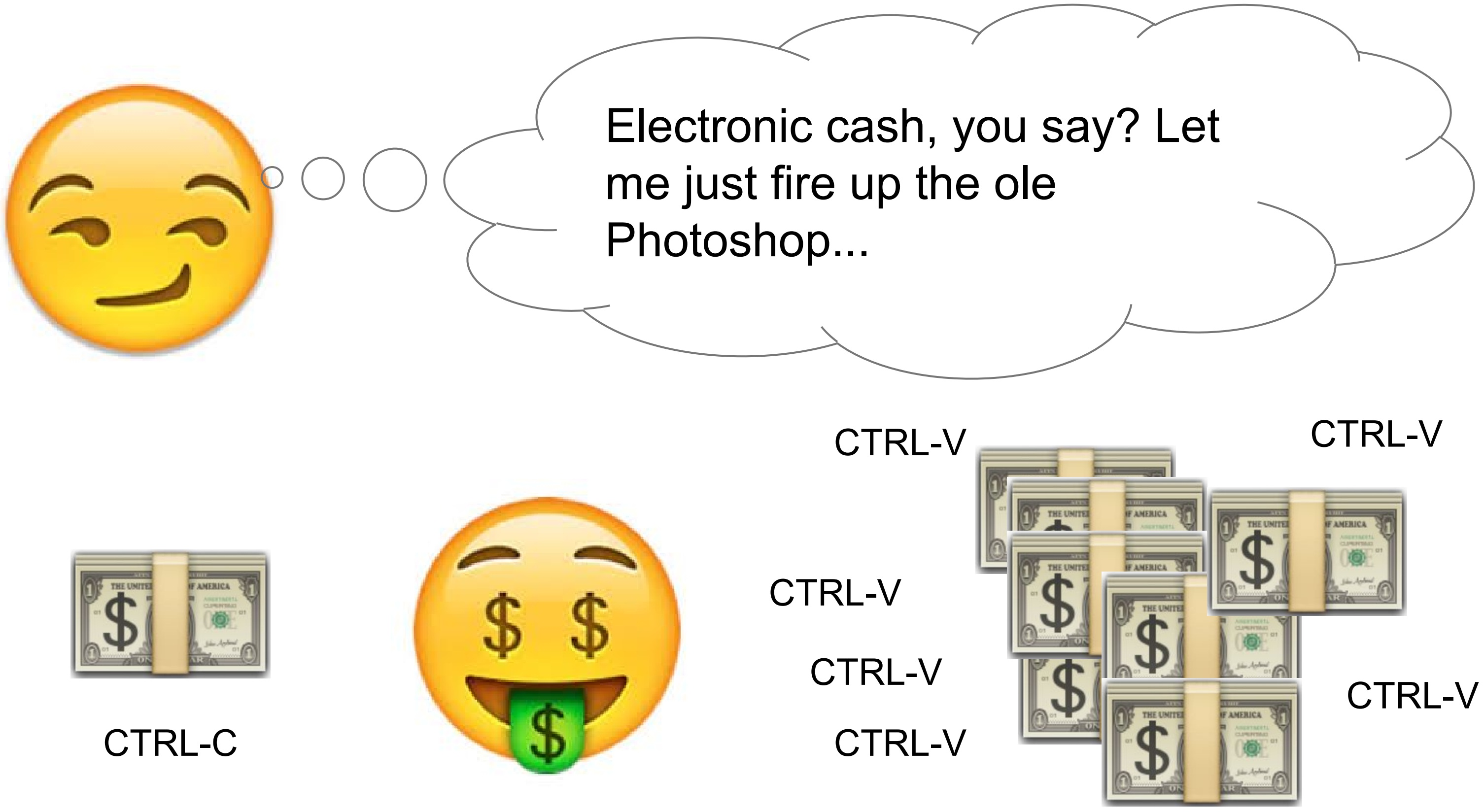
2017

Why bitcoin?



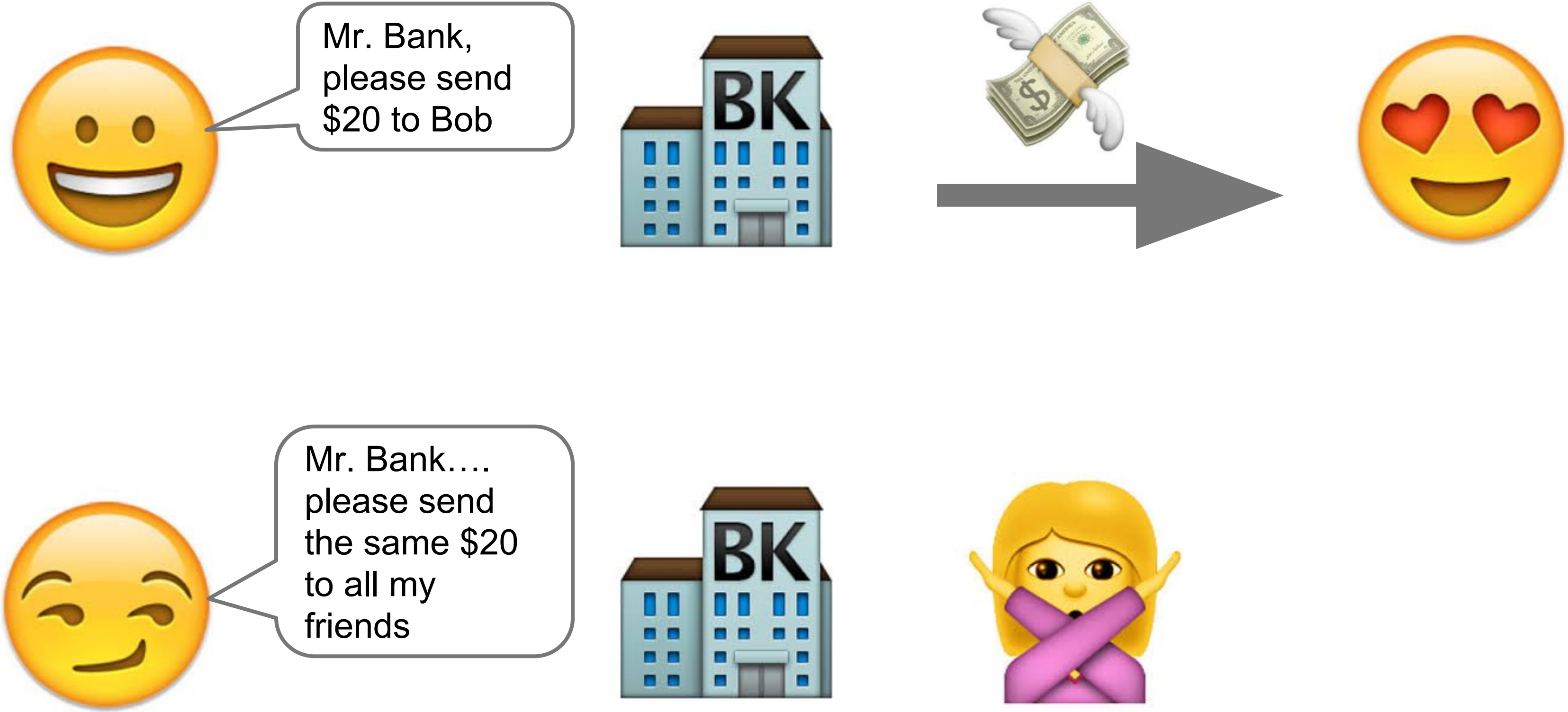
“A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution”

The challenge was preventing a “double spend”



Electronic cash, you say? Let me just fire up the ole Photoshop...

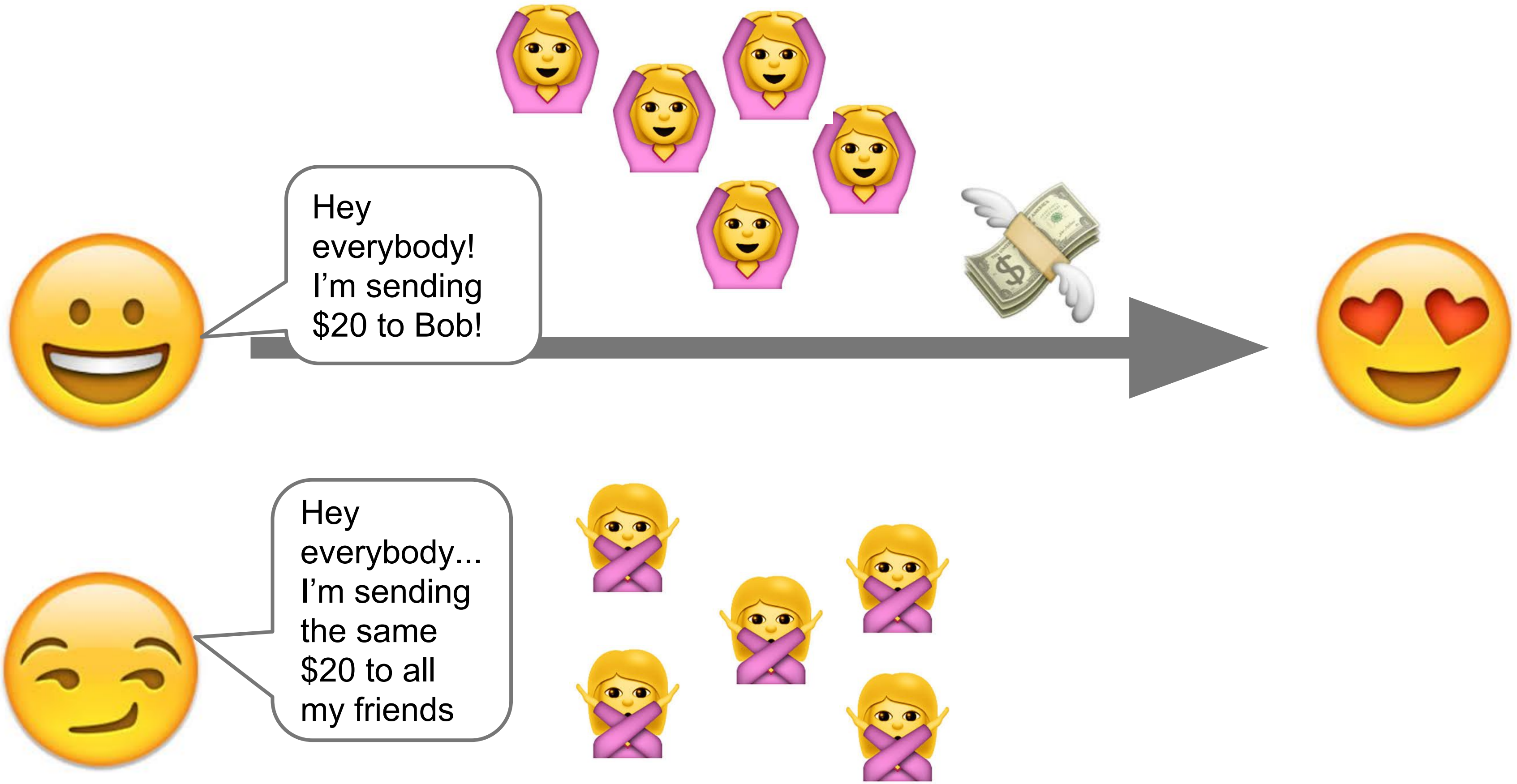
Traditional solutions rely on a central arbiter



Mr. Bank,
please send
$20 to Bob

Mr. Bank….
please send
the same $20
to all my
friends

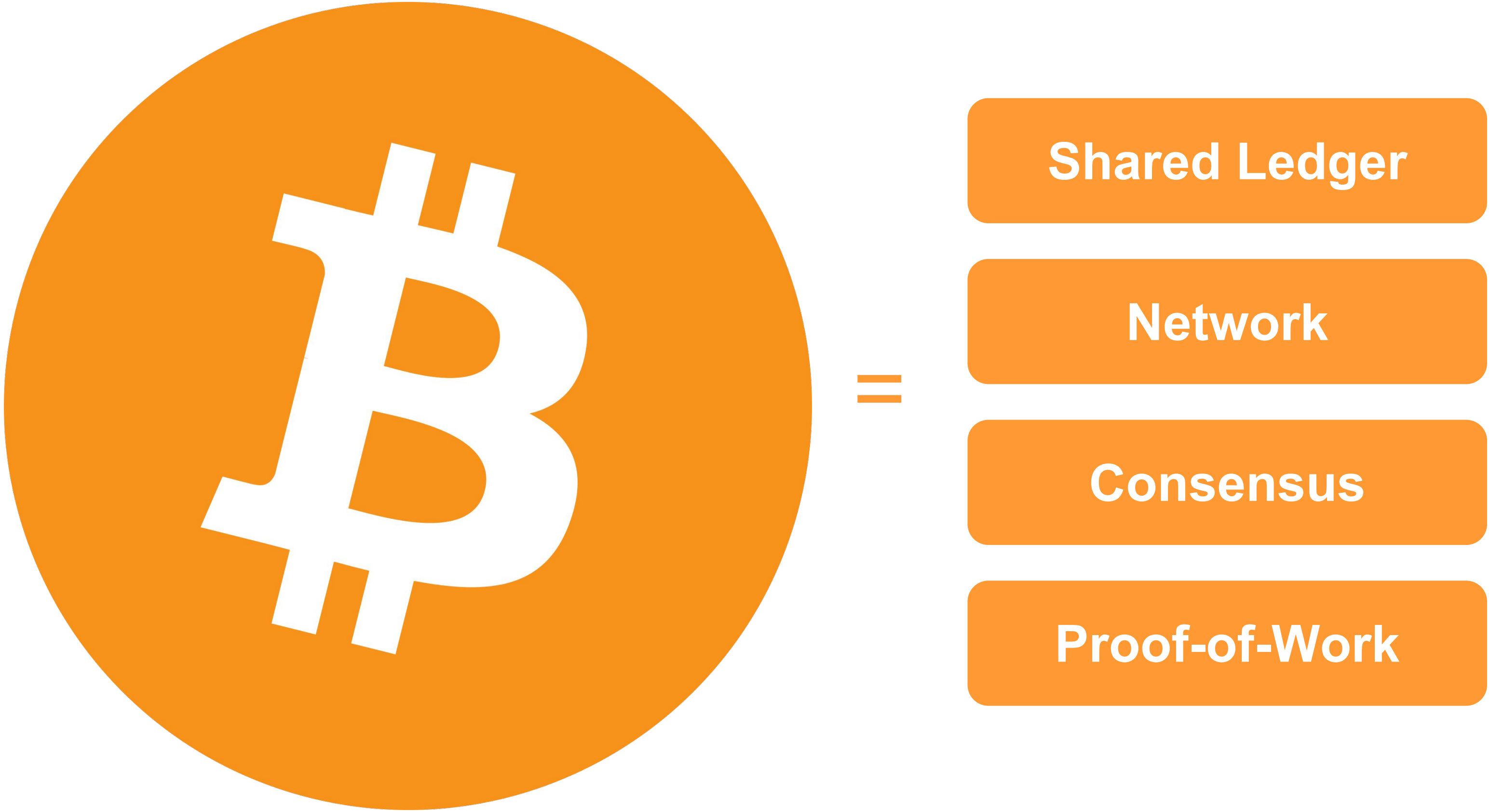
Bitcoin replaces “central arbiter” with “entire community”



Hey
everybody!
I’m sending
$20 to Bob!

Hey
everybody...
I’m sending
the same
$20 to all
my friends

How does Bitcoin do it?



=

Shared Ledger

Network

Consensus

Proof-of-Work

Shared Ledger

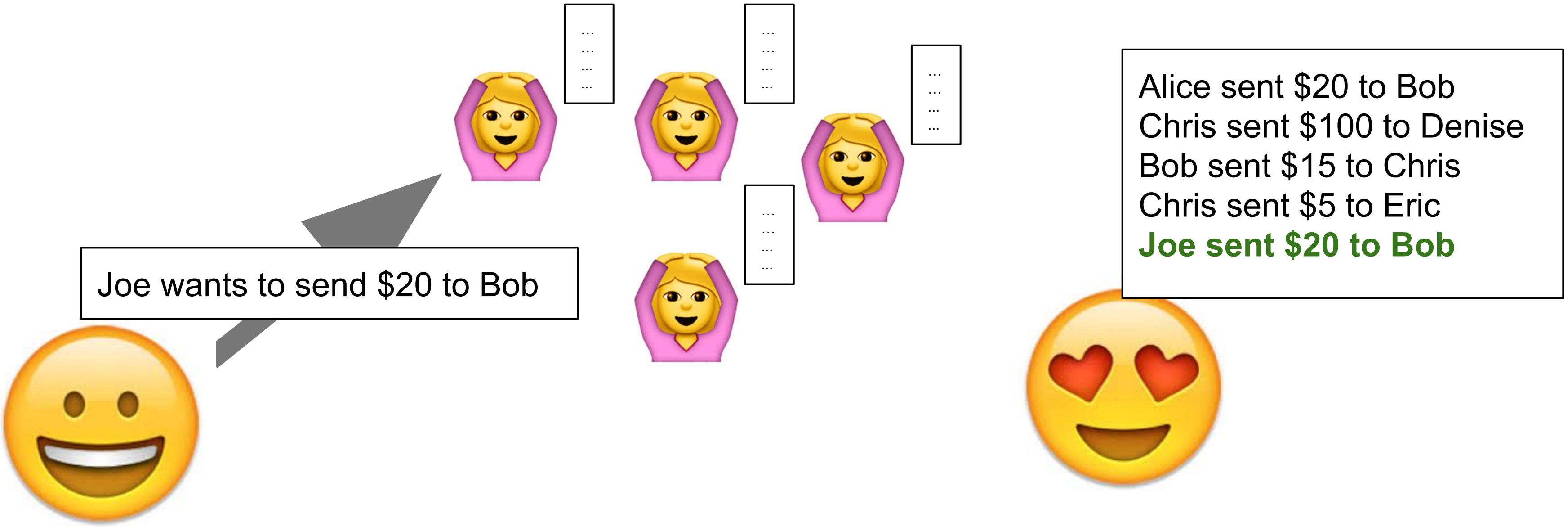
- All participants in the Bitcoin network store a copy of a “shared ledger”
- Shared ledger is a record of all transactions that have ever been made on the Bitcoin network:

Alice sent $20 to Bob
Chris sent $100 to Denise
Bob sent $15 to Chris
Chris sent $5 to Eric
...

- The shared ledger provides enough information to determine the balance of every Bitcoin account

Community validates all transactions

- A successful transaction is one that has been validated by the community and added to the shared ledger

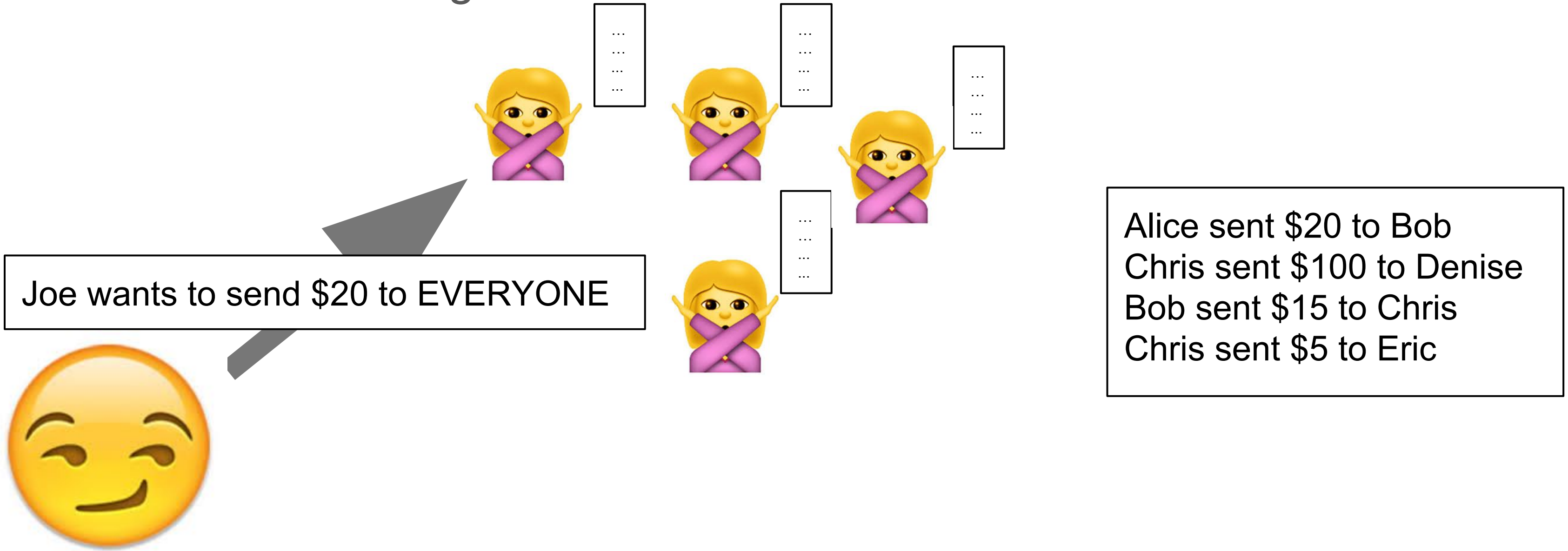


Joe wants to send $20 to Bob

Alice sent $20 to Bob
Chris sent $100 to Denise
Bob sent $15 to Chris
Chris sent $5 to Eric
Joe sent $20 to Bob

Community validates all transactions

- If the community deems a transaction is invalid (e.g. the sender does not have enough balance, or is not who they claim to be) it is not added to the ledger

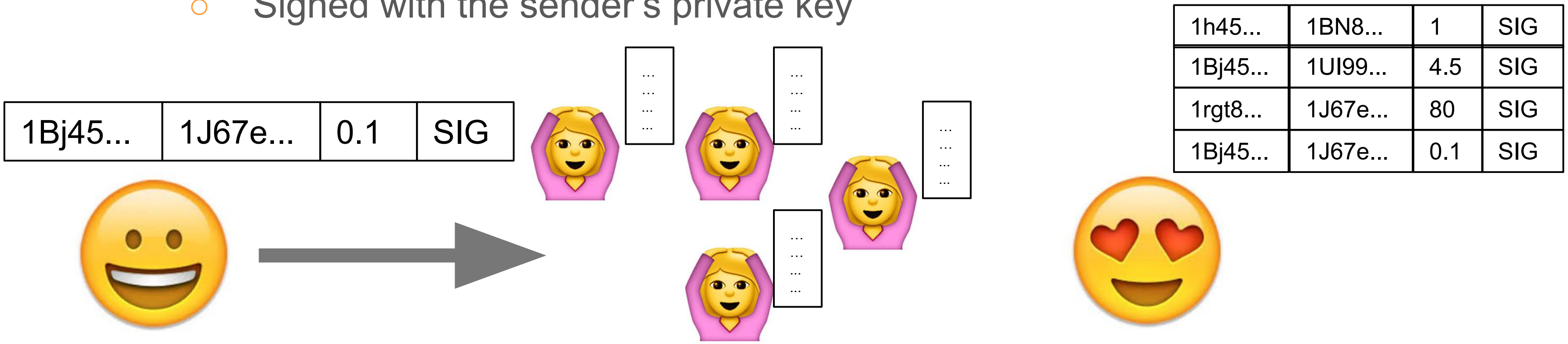


Joe wants to send $20 to EVERYONE

Alice sent $20 to Bob
Chris sent $100 to Denise
Bob sent $15 to Chris
Chris sent $5 to Eric

What is a transaction technically?

- Bitcoin relies on public key / private key pairs
- Instead of "user names" a transaction refers to a specially formatted "Bitcoin address" which is derived from a user's public key
- Transactions include fees
- A transaction is:
    - The address of the sender
    - The address of the recipient
    - The value being sent
    - Signed with the sender's private key



1Bj45...	1J67e...	0.1	SIG

1h45...	1BN8...	1	SIG
1Bj45...	1UI99...	4.5	SIG
1rgt8...	1J67e...	80	SIG
1Bj45...	1J67e...	0.1	SIG

Important: Protect Your Private Key

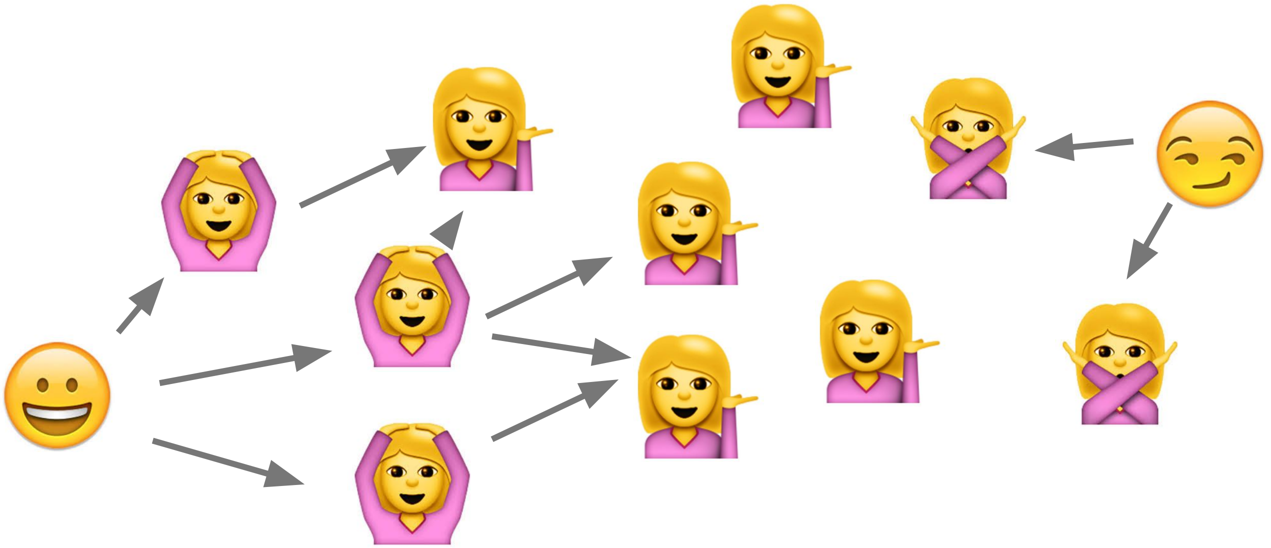
- A transaction is only valid if it is signed with the sender’s private key

If you lose your private key, **you can’t spend your money**
If someone steals your private key, **they can spend your money**

- We recommend you back-up your wallet’s private key offline so it can’t be stolen by a computer virus or lost by hard drive failure
  - Note: the Copay wallet “recovery phrase” is your private key
- Side note: wallets will often generate a new Bitcoin address every time you receive bitcoin
  - A way to help preserve anonymity

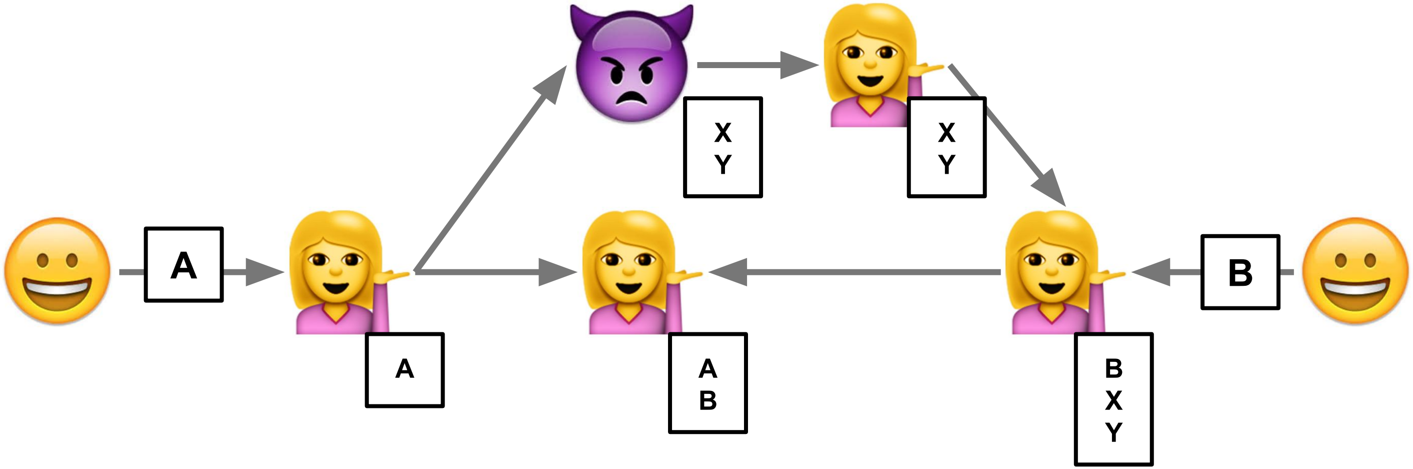
Network

- Bitcoin network is a collection of independent peers
- Data (e.g. transactions) travels from peer to peer
- Whenever a node receives a transaction it validates it against the shared ledger and either discards it as invalid, or propagates it further



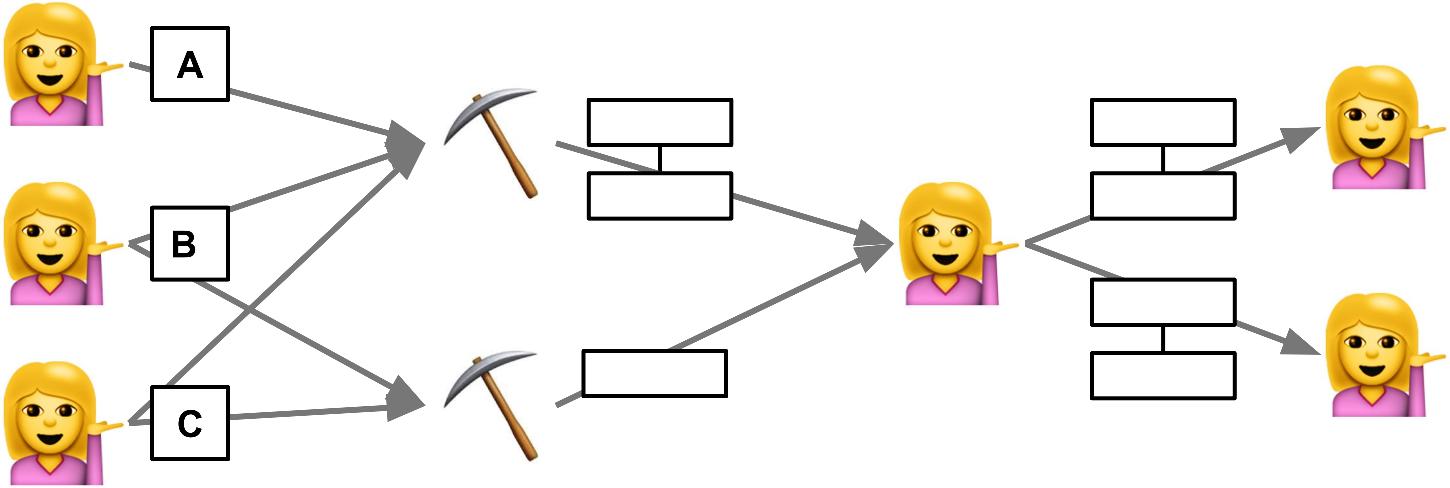
Consensus: how everyone agrees on the shared ledger

- Previous slides mention a “shared ledger”, but what happens if peers disagree on what exactly is in the ledger?
- For example:
  - Propagation delay might change the order different peers receive transaction
  - A malicious peer might purposefully omit or reorder transactions to their benefit



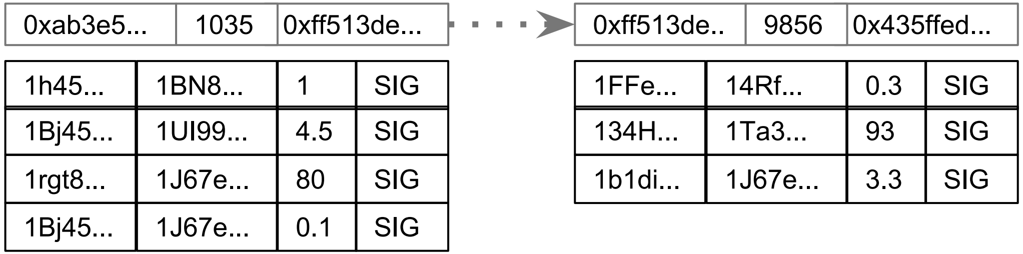
The longest block chain wins

- Special peers called “miners” bundle up transactions into a “block” and link those blocks into a “block chain”
- Honest peers who receive multiple block chains discard all but the longest chain



What is a block technically?

- A block is:
  - An ordered list of transactions
  - A reference to the previous block’s ID
  - A “nonce” value (a number chosen by the miner)
  - A specially constrained SHA-256 hash of all the data in the block (this hash also serves as the block’s ID)



0xab3e5...	1035	0xff513de...

1h45...	1BN8...	1	SIG
1Bj45...	1UI99...	4.5	SIG
1rgt8...	1J67e...	80	SIG
1Bj45...	1J67e...	0.1	SIG

0xff513de..	9856	0x435ffed...

1FFe...	14Rf...	0.3	SIG
134H...	1Ta3...	93	SIG
1b1di...	1J67e...	3.3	SIG

Final piece of the puzzle

- Final piece of the puzzle: if the longest blockchain is accepted by all peers, what’s to stop a malicious miner from quickly building a long blockchain and rewriting history?

💥 **Proof of Work** 🎉

Proof of work

- To create a new block, a miner has to make sure that the block hash has a certain number of leading 0's*.
- To achieve this, the miner has to find a nonce value that satisfies the requirements.
- The only way to find the right nonce value is by guess-and-check.
- Moreover, each block must reference the previous block.
- The above constraints result in the following:
    - Blocks are *very* difficult to mine.
    - Blocks can be mined only one at a time.
- The miner node that does create a block receives:
    - Transaction fees.
    - Coinbase reward - this is how new Bitcoin is injected into the system.

*The number of leading 0's is essentially what is known as the block difficulty.

51% attack

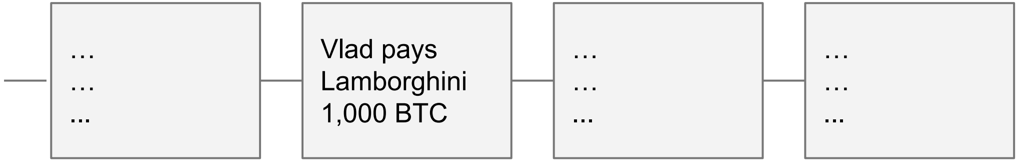
- The more mining power you have, the faster you will mine new blocks.
- If you control 51% of the mining power, you will mine new blocks faster than the rest of the network combined.
- Therefore, you will be able to create a chain that eventually overtakes the existing chain, and thus rewrite history, allowing you to double-spend. Remember, that the most difficult (i.e. longest) chain is considered to be the source of truth.

- *Has this happened? Not as far as we know.*
  - ghash.io mining pool exceeded 51% in July of 2014.

- *Can this happen today? Yes.*
  - *Top 3-4 mining pools usually have >50% mining power.**

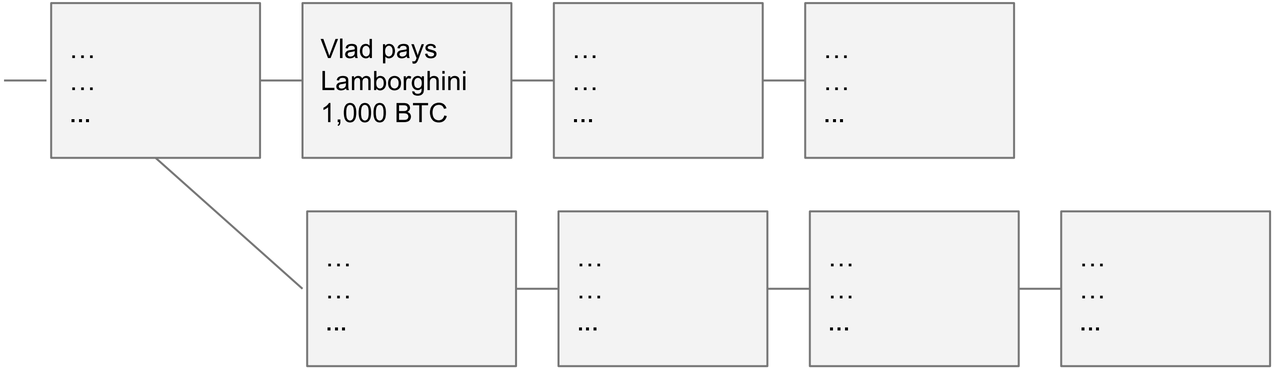
* *https://bitcoinchain.com/pools*

51% attack



Net: Vlad paid
Lamborghini
1,000 BTC

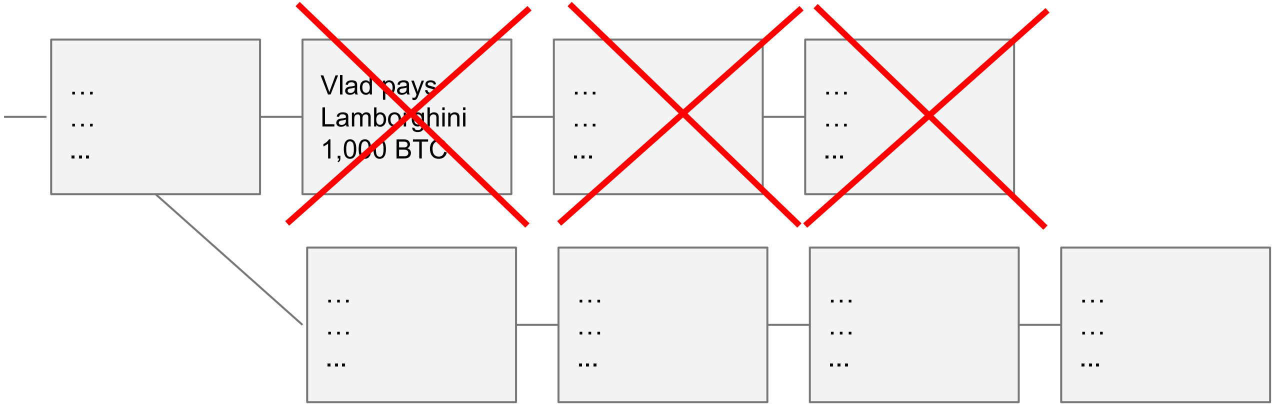
51% attack



Net: Vlad did not pay Lamborghini 1,000 BTC.

But has already received the car.

51% attack

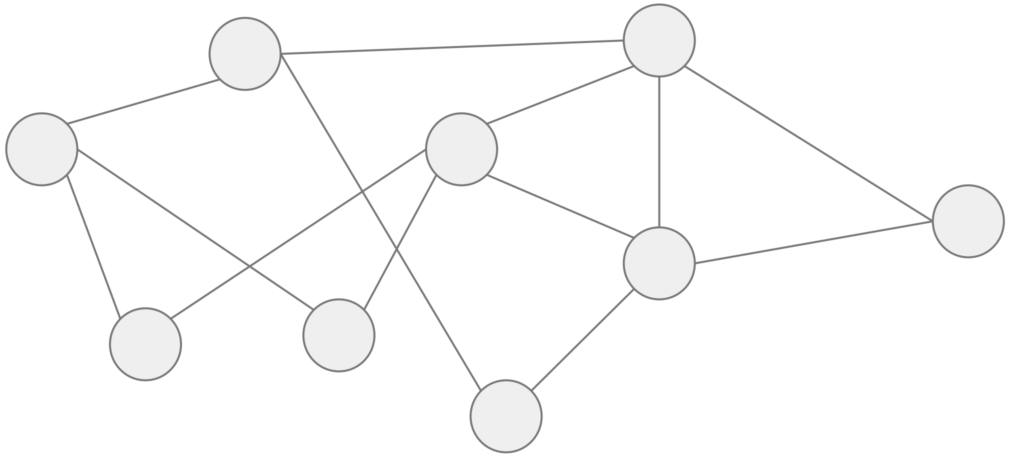


Net: Vlad did not pay Lamborghini 1,000 BTC.

But has already received the car.

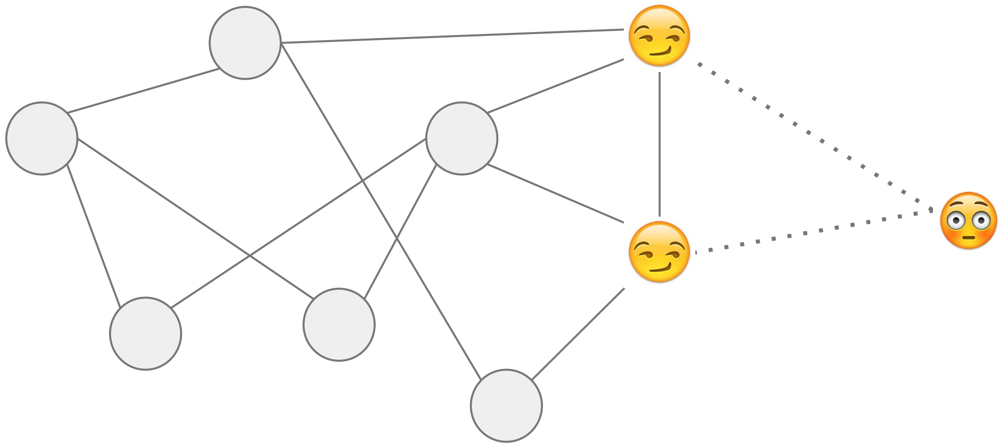
Network Partitioning Attack

- If you partition the network, cutting off a set of nodes, you can:
  - Withhold certain transactions from those nodes, distorting their view of history.
  - Withhold new blocks from those nodes, making their mining operations useless.



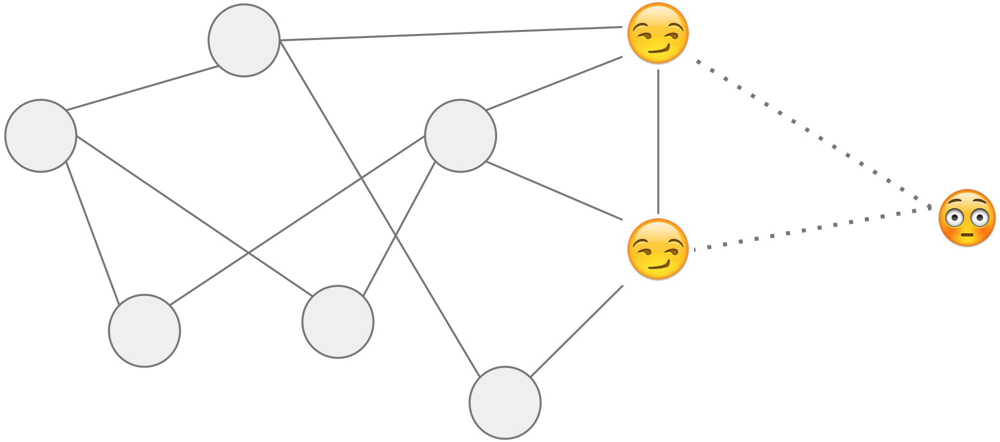
Network Partitioning Attack

- If you partition the network, cutting off a set of nodes, you can:
  - Withhold certain transactions from those nodes, distorting their view of history.
  - Withhold new blocks from those nodes, making their mining operations useless.



Network Partitioning Attack

- Standard internet problem - if the nodes you are connected to are lying to you, would you ever know something is up?
  - *Maybe.* Blocks will start to appear less frequently.
  - You also need to control a large number of malicious nodes to pull this off.
  - Alternatively, you need to know which nodes the target node is connected to.



Summary

- Transactions are recorded on the Blockchain - distributed public ledger.
- Consensus is reached by (slowly) mining one block at a time.
- Transactions and blocks are signed - prohibitively expensive to forge.
- Bitcoin is sent from address(es) to address(es).
- Accounts are controlled by knowing the associated private key.
- Lose private key - lose account control.
- Anonymity is not guaranteed (yet).
- New currency is injected with every block (until ~21,000,000 BTC).
- Attacks are possible (but unlikely).

Install a mobile Bitcoin app and we'll send you $1 in bitcoin!

1 Install the **Copay Bitcoin Wallet** from the Google Play Store or Apple App Store

2 Click through any popups and Terms of Use screens (if the terms are acceptable)

3 Once the wallet is loaded, click the **RECEIVE** button in the lower left corner

4 Click **BACKUP NOW** and record the 12 word **recovery phrase**. Ideally you'd record it somewhere safe (like on a piece of paper) for now you can just put it in your phone's Note App and transfer it to paper later.

5 Click **CONTINUE** and follow the instructions to verify you recorded the phrase correctly

6 Click **FINISH** and then click **RECEIVE** again

7 Congratulations! You now have a Bitcoin address! It is the long thing that looks like **1PW8UGTPYfXaAFPDkzkZBp1NFJczan65cY**

8 Visit http://bit.do/mobiletea and enter the address into the form!

Questions? Find Vlad S, James P, or Tom H and ask away!