Bitcoin Protocol and Consensus: A High Level Overview

Lecture Overview

- Bitcoin basics, much more detailed
- Consensus Build-up
- Mining Overview

Basic Concepts - What is Bitcoin?

- Cryptocurrency
  - Cryptocurrency: "A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank."
  - Built upon a combination of computer science, cryptography, and economics
- Bitcoin is a cryptocurrency
  - “Bitcoin” can refer to:
    - Bitcoin (uppercase) - the protocol, software, and community
    - bitcoins (conventionally lowercase) - the unit
- Community terminology
  - **"crypto"** – cryptocurrencies
  - **Public - "private blockchain"** - private blockchains, permissioned ledgers, large financial institutions
  - "**blockchain**" - umbrella term

Implications of blockchain technology

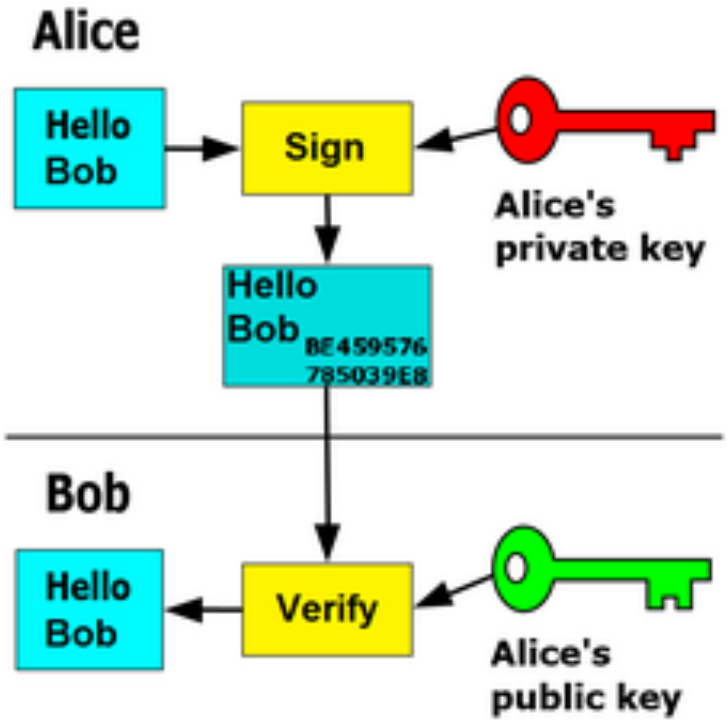
- Altcoins (Dash, Dogecoin, Litecoin)
- Bitcoin 2.0 / Ethereum - applying blockchains outside of finance
- Remittances - circumvent traditional banking infrastructure
  - Send money anywhere in the world for 5 cents
- Be your own bank - 100% uptime
- Current hot topics: Governance and “blockchain”
  - Block size debate
  - Banks taking interest in financial implications
- Private blockchains - reduce costs + settlement times in traditional banking infrastructure

Basic Concepts - Identity in Bitcoin

- Send money between pseudonyms
  - pseudonym == address == public key

- Cryptographic primitives
  - digital signature scheme (ECDSA: Elliptic Curve Digital Signature Algorithm)
    - public key/private key pair; like email address + password
  - one-way hash function (SHA-256)

Asymmetric Encryption-Public / Private Key Cryptography



Courtesy of Wikipedia: https://en.wikipedia.org/wiki/Public-key_cryptography

Basic Concepts - Identity in Bitcoin

- Bitcoin is hidden in the large amount of public keys
  - Users can generate arbitrarily many key pairs
  - Example Address: 1FtQU9X78hdshngJiCBw9tbE2MYpx87eLT
  - 2^160 possible addresses (1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976 addresses)
  - Grains of sand on earth: 2^63
  - 2^126 is actually only 0.0000000058% of 2^160

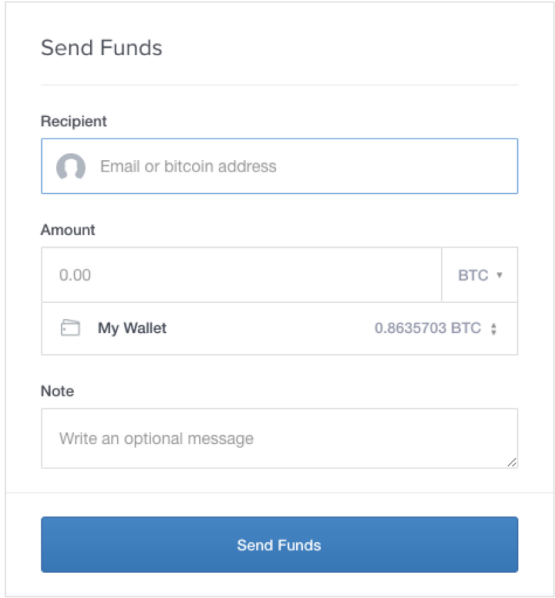
https://www.bitaddress.org

https://bitref.com/

A Bitcoin Transaction - Basic Version

- Bitcoin exists as software
  - Transactions are conducted through wallet software
  - Wallet creation generates a Bitcoin address
- To receive money, you share your address
  - Sender specifies address and amount
- The transaction is broadcast to the network, where "miners" verify it and add it to the transaction history

1LNnJDNTUXYUfmbiVcngKGg52N8TKNPw6J



Coinbase interface

- https://www.blockchain.com/
- www.coinbase.com
- https://koineks.com/
- https://www.btcturk.com/

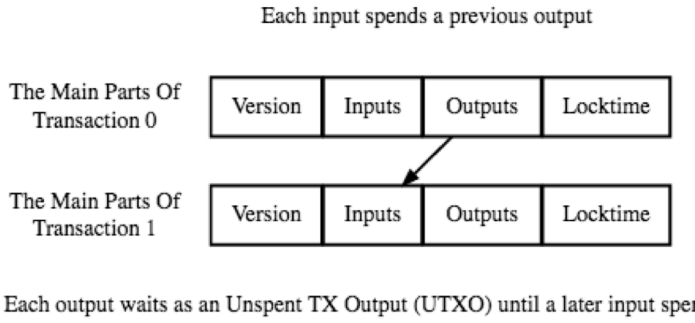
One-way hash function (SHA-256)

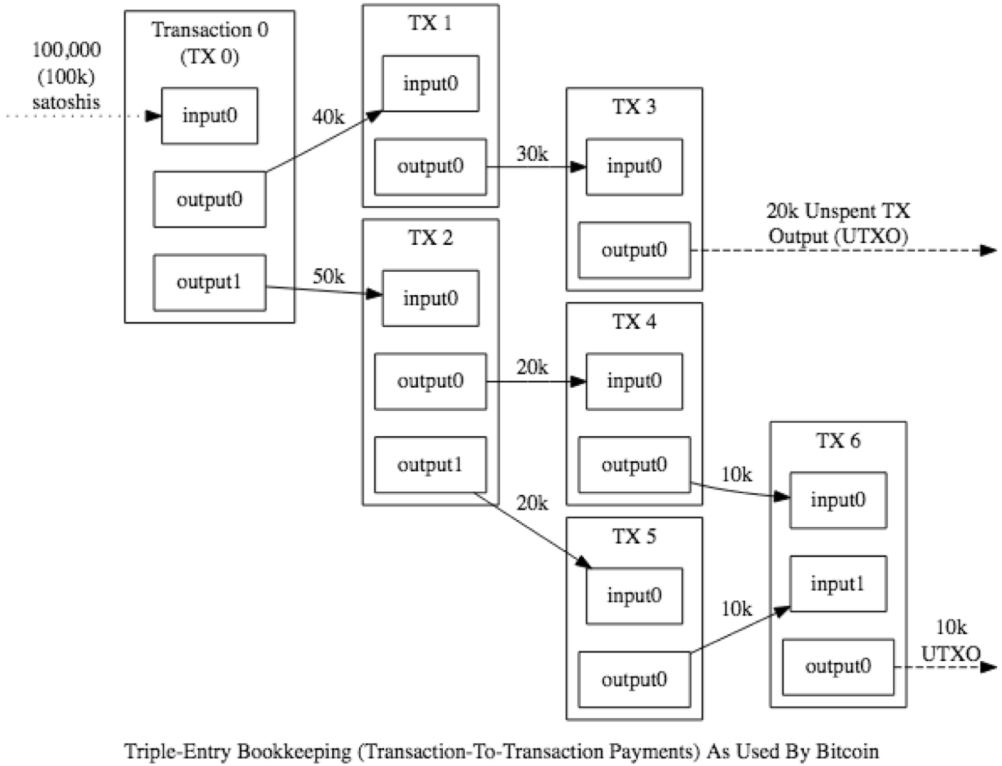
- The **SHA** (Secure Hash Algorithm) cryptographic hash function
- A cryptographic hash - a signature for a text or a data file.
- **SHA**-**256** generates an almost-unique, fixed size **256**-bit (32-byte) hash.
- Hash is a one way function – it cannot be decrypted back.
- https://www.movable-type.co.uk/scripts/sha256.html

Basic Concepts - Transactions

Source: Bitcoin Developer Guide

- Maps inputs addresses to output addresses
  - Outputs can only be spent once
- Typical tx: one input, two outputs
- Fees are implicit





Basic Concepts - UTXO analogy

UTXOs stands for "Unspent Transaction Outputs"

- Global set of unspent bitcoins
- "I'm spending THIS bitcoin," not "I'm spending A bitcoin."

Analogous to Rai Stones of the Yap Islands

- Rai Stones never moved
- Instead: Agreed on change of ownership

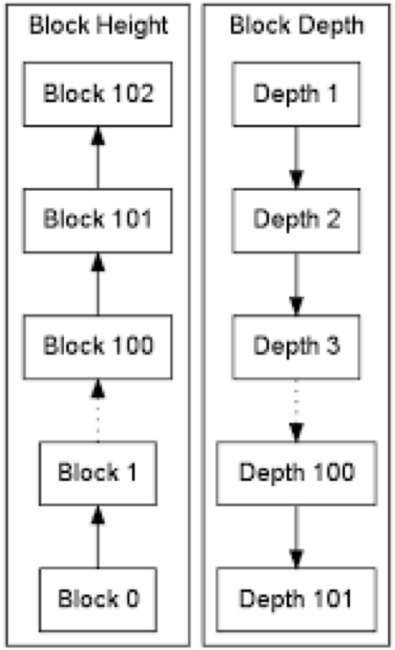
Source: Wikipedia

Basic Concepts - Blocks + Blockchain

Blocks

- Contains an ordered bunch of transactions
  - Timestamps the transactions, are immutable
- Each block References a previous block
- Each block has height and depth (confirmations)
  - Currently 599k blocks
  - https://bitinfocharts.com/bitcoin/

Blockchain=The entire series of blocks 'chained' together



Block Height Compared To Block Depth

Source: Bitcoin Developer Guide

Transaction View information about a bitcoin transaction

447cb6623db32b5f28c94ac1055180207 5f053208fe995204a145197e2904bb9

3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v (44,000 BTC - Output)	3LrLWTSdd69oZVVQ6dtWaAAaBLn7N3rRjz - (Spent)	333.33328889 BTC
	3QkXtcSWJA9w77eCujnMBKDWFe7F7zwxTg - (Spent)	333.33328889 BTC
	3Qd7hXZoZ1iyXZznrbdUwUQBxHMmujdqhJ - (Spent)	333.33328889 BTC
	3ECJwvx9VgfotcUuEJMVNvmWnTGVMk179L - (Spent)	333.33328889 BTC
	3BuQmbmdce3e31GEovq5SgowLdfMgJzLDE - (Spent)	333.33328889 BTC
	3NwKLjJjzXSnBFQWokXRgBG3JeuF3bsnfE - (Spent)	333.33328889 BTC
	3GEaT8ZRXELcjMSFvGro6eZcC5S1LSLZuN - (Spent)	333.33328889 BTC
	35DVAzDtZDKAU94kFT9sxoscnuLCTxgwYc - (Spent)	333.33328889 BTC
	3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v - (Unspent)	38,000 BTC
	35mwqShnStDro6uEB4bmsgbyBo8en6Byfm - (Spent)	333.33328889 BTC
	39pvSqfNcUosc8RGVWxyzKM3ny96a3uSkW - (Spent)	333.33328889 BTC
	39QNJSgQg5JnBXAtbF8ezkDn72VqWdPZPJ - (Spent)	333.33328889 BTC
	3L9qAGBQLbXkFAB2GpijnJXPScSVjuiJio - (Spent)	333.33328889 BTC
	37WSkANPVUQ8uuktf8hv671CejRtBtQ4tJ - (Spent)	333.33328887 BTC
	3EEwPZZ6pYRJSotCz9RBoVYPRnoWyGWEka - (Spent)	333.33328889 BTC
	3C4ABC7iPcAAKBh6SJXfvUSDBew3abCtw3 - (Spent)	333.33328889 BTC
	3HpQozfTzoXAsHf87m2mwJXUQ14LVtLgK4 - (Spent)	333.33328889 BTC
	337RfngTLRTpU7RT9sKWQWDdmfcdmWnugi - (Spent)	333.33328889 BTC
	3P2eoKr3vAeZhJcTzon3VFkv5r7DqSXW9G - (Spent)	333.33328889 BTC
		43,999.9992 BTC

Summary	
Size	1055 (bytes)
Received Time	2016-08-30 11:45:03
Included In Blocks	427512 (2016-08-30 11:51:09 + 6 minutes)
Confirmations	854 Confirmations
Relayed by IP	5.39.93.85 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	44,000 BTC
Total Output	43,999.9992 BTC
Fees	0.0008 BTC
Estimated BTC Transacted	333.33328887 BTC
Scripts	Hide scripts & coinbase

https://www.blockchain.com/explorer

Byzantine Generals Problem

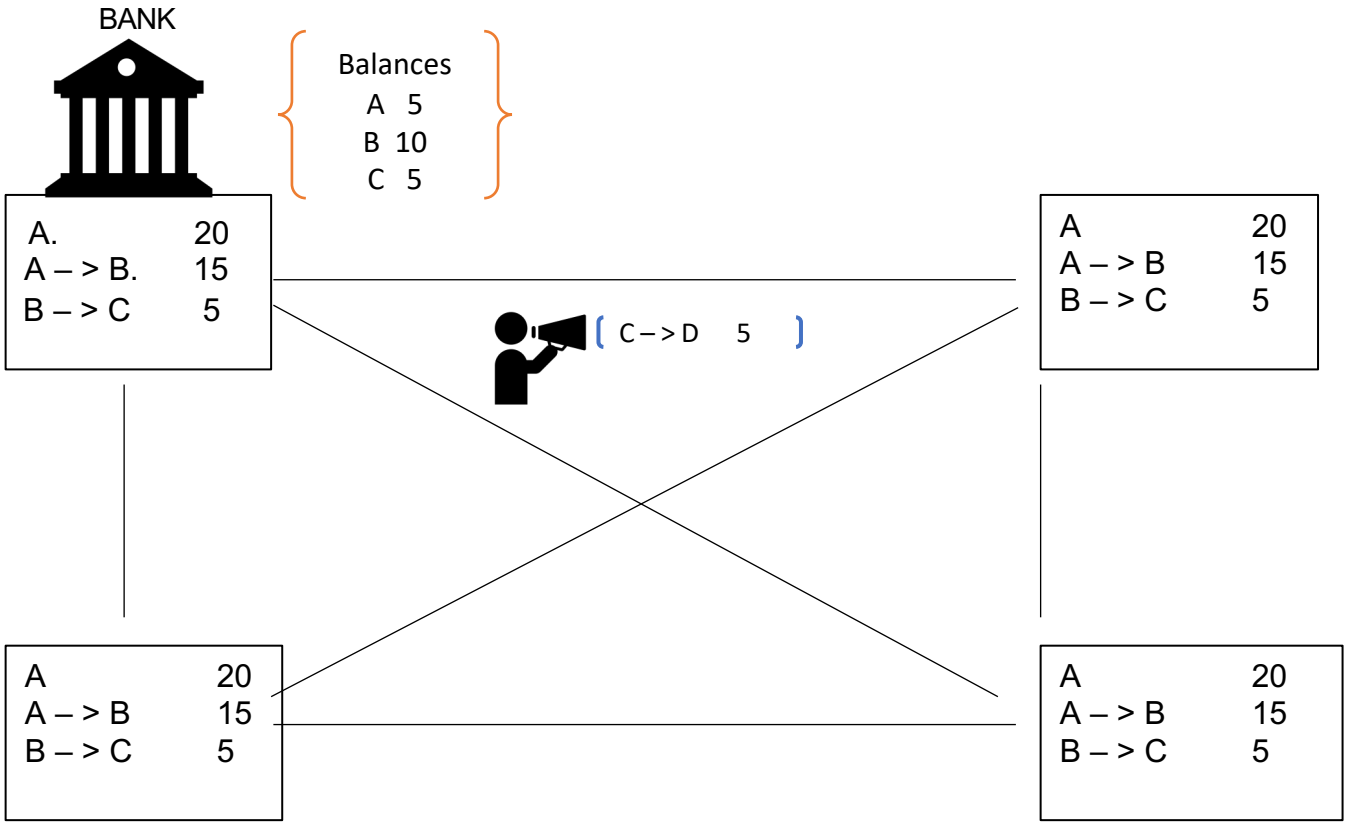
Group of generals surrounding a city must vote and agree on a plan of action

Constraints:

- Generals are physically separated; must use messengers
  - Messengers may fail
- Generals may be loyal or intentionally traitorous
- Assume **majority** of generals are loyal
- "Byzantine Fault Tolerance" achieved if **loyal** generals have unanimous agreement on strategy

In Bitcoin, this is an agreement on the history of transactions

Bitcoin Basics
High Level Overview



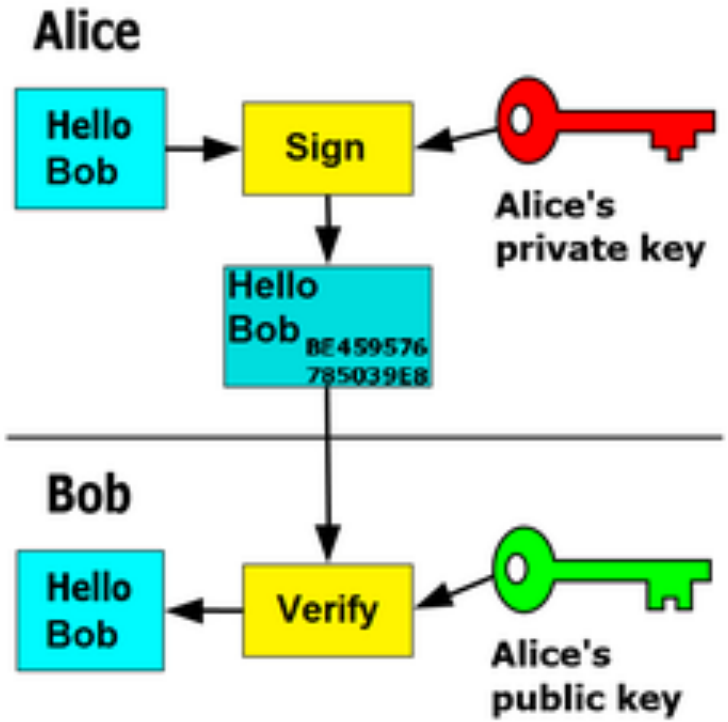
Problems?

1. Does C own 5 units of money?
2. Is the sender really C?

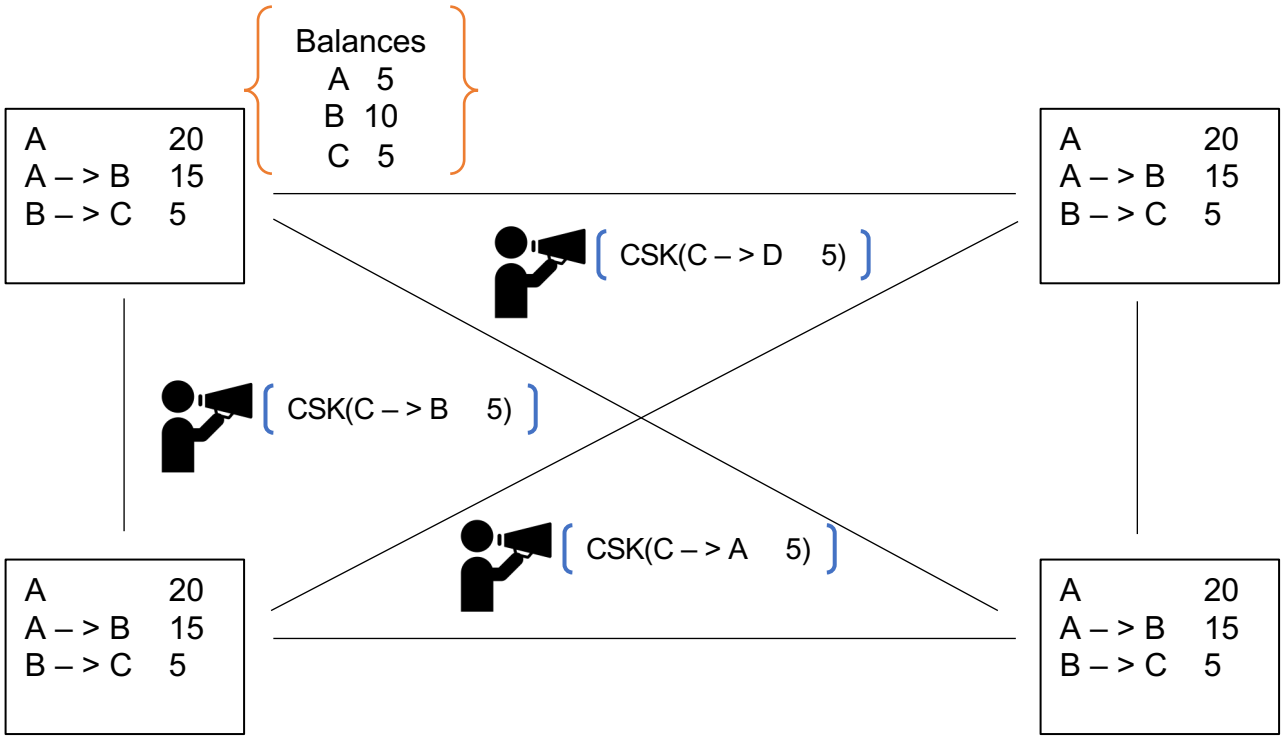
Solution

Asymmetric Encryption
Public / Private Key Crypt.

Asymmetric Encryption-Public / Private Key Cryptography



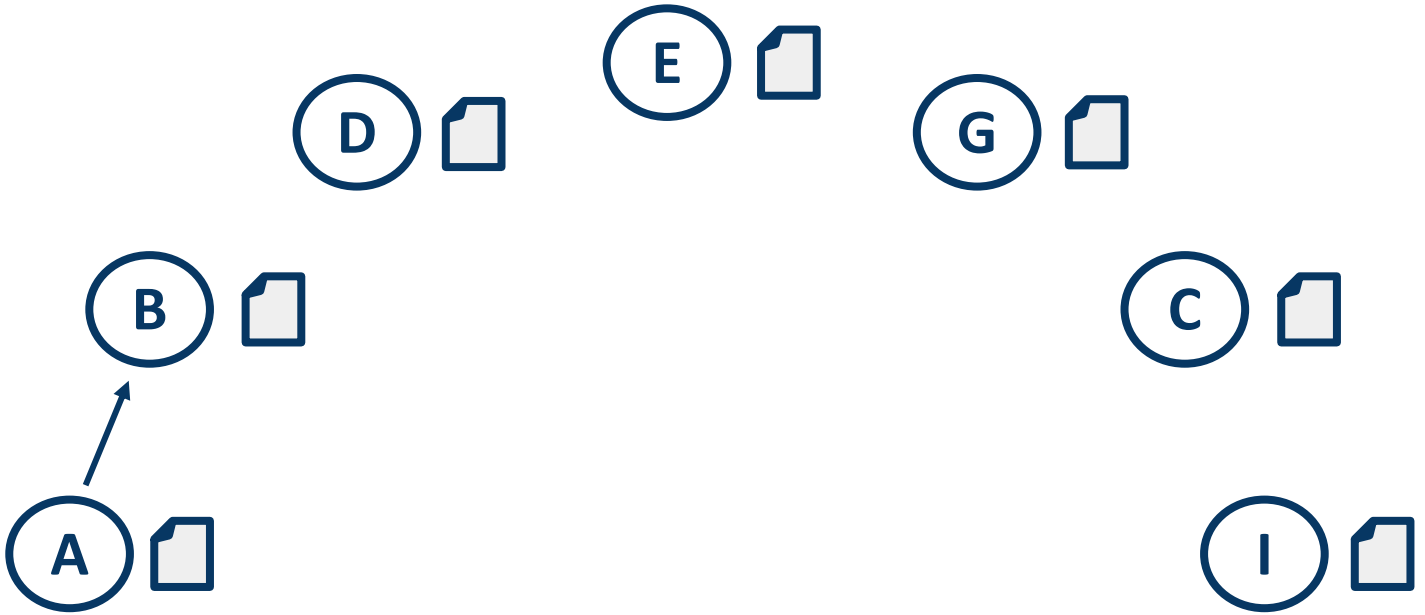
Courtesy of Wikipedia: https://en.wikipedia.org/wiki/Public-key_cryptography



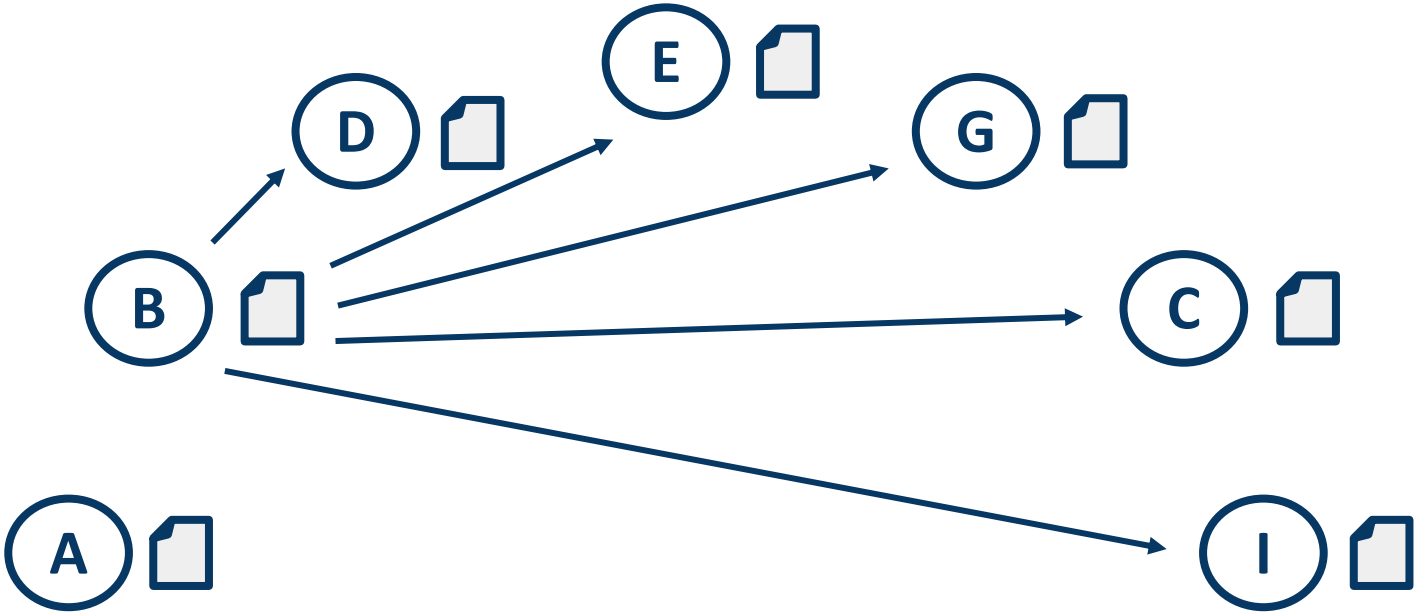
Problems?

1. Can C send the same Money twice?
Double Spending

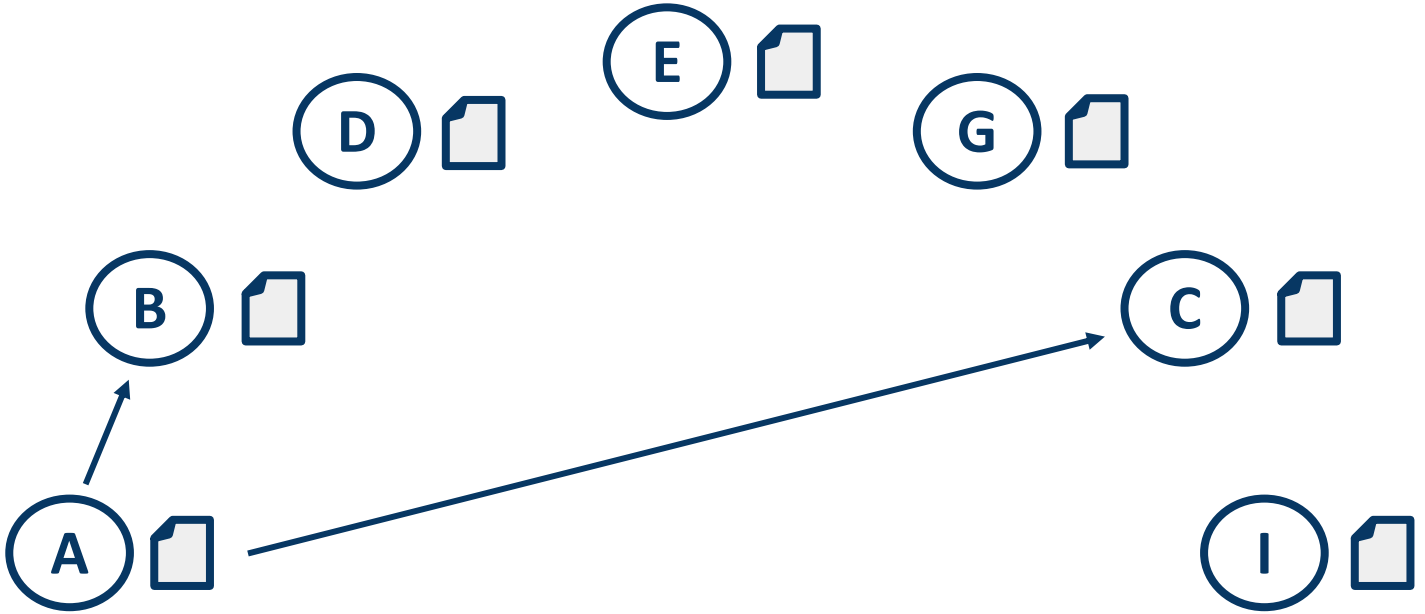
Alice sends her transaction to Bob



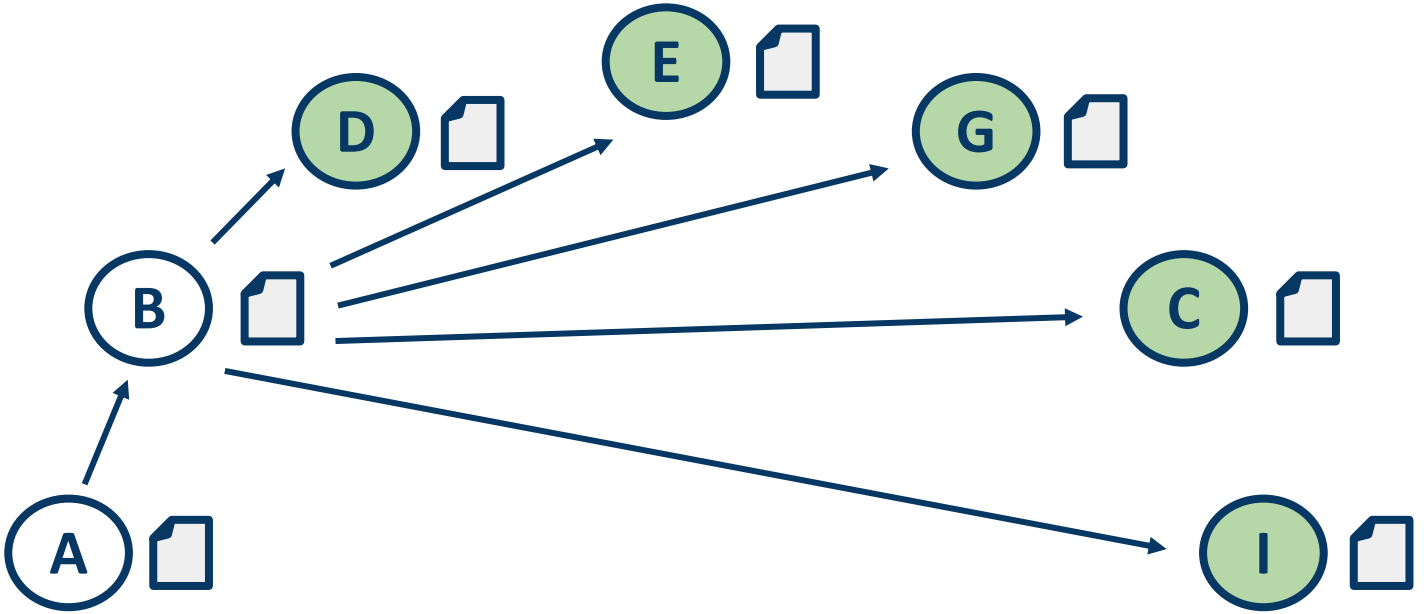
Bob announces the transaction to the world



Alice double spends on Bob and Charlie

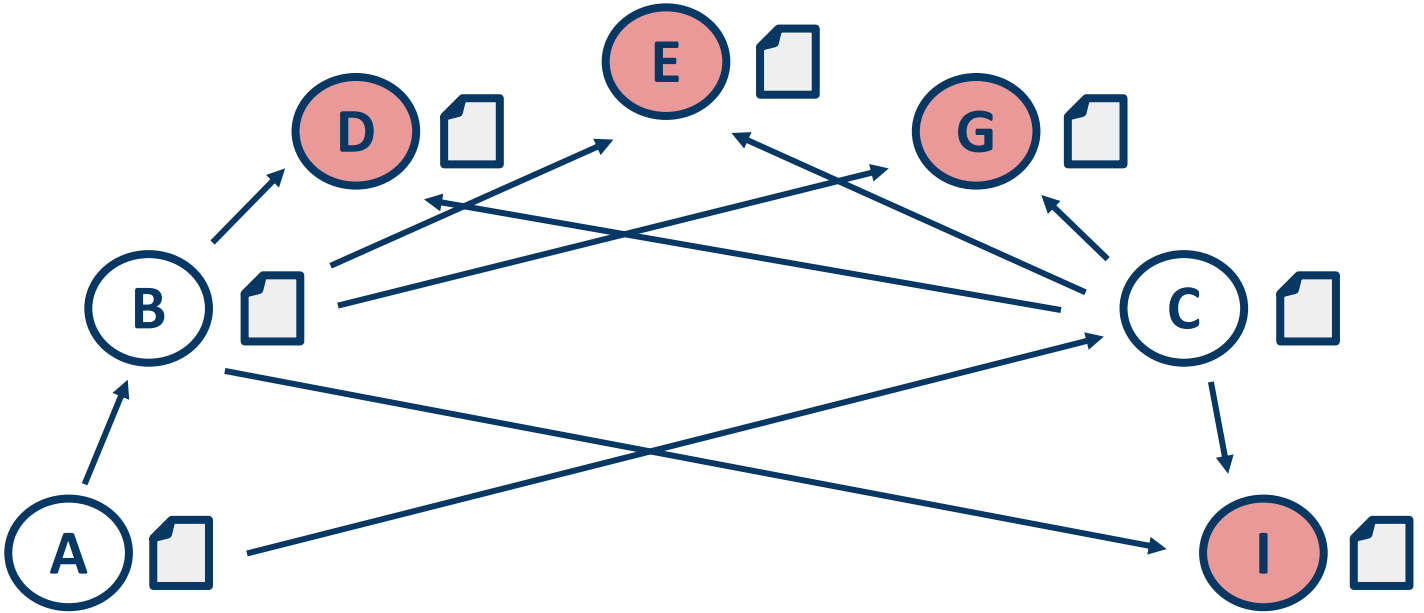


Everyone verifies transactions

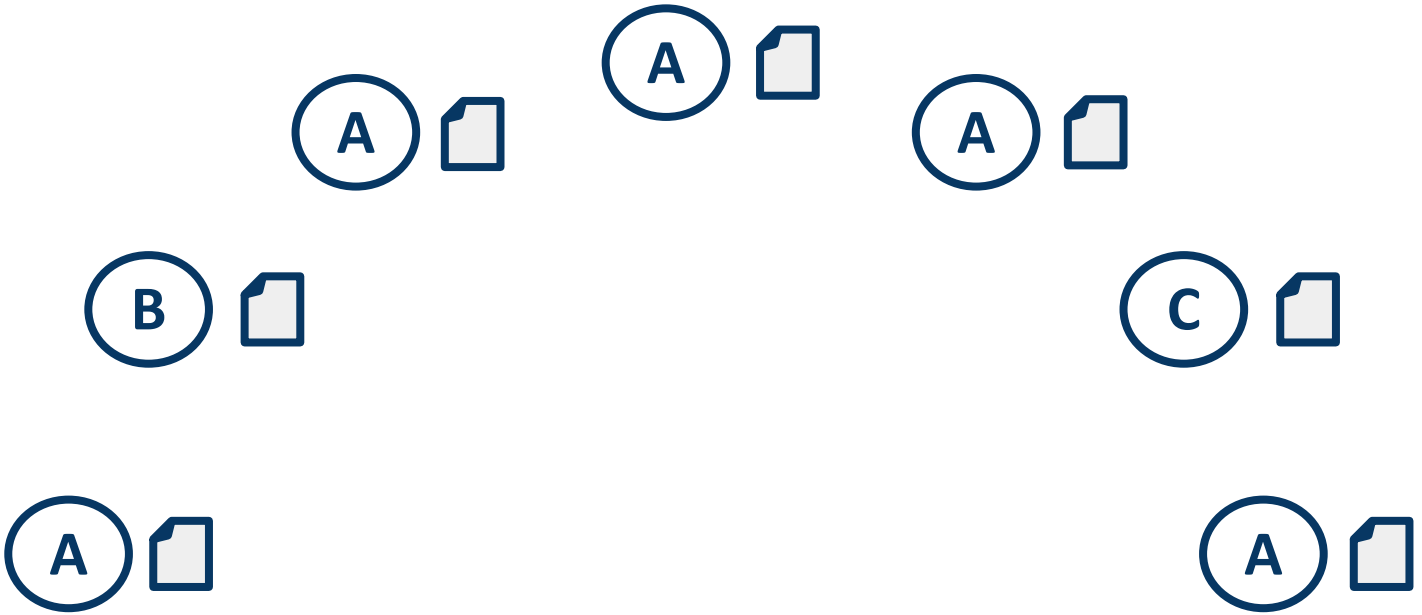


Alice is prevented from double spending

What is wrong with this? Can A still act evil?

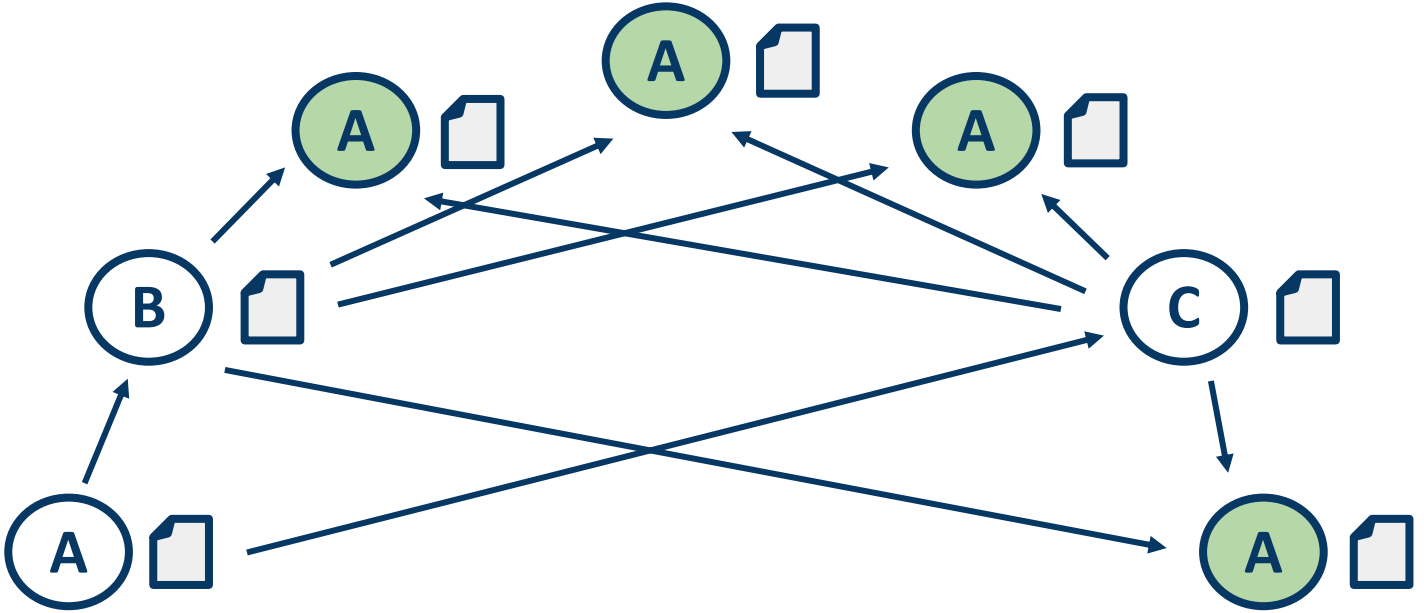


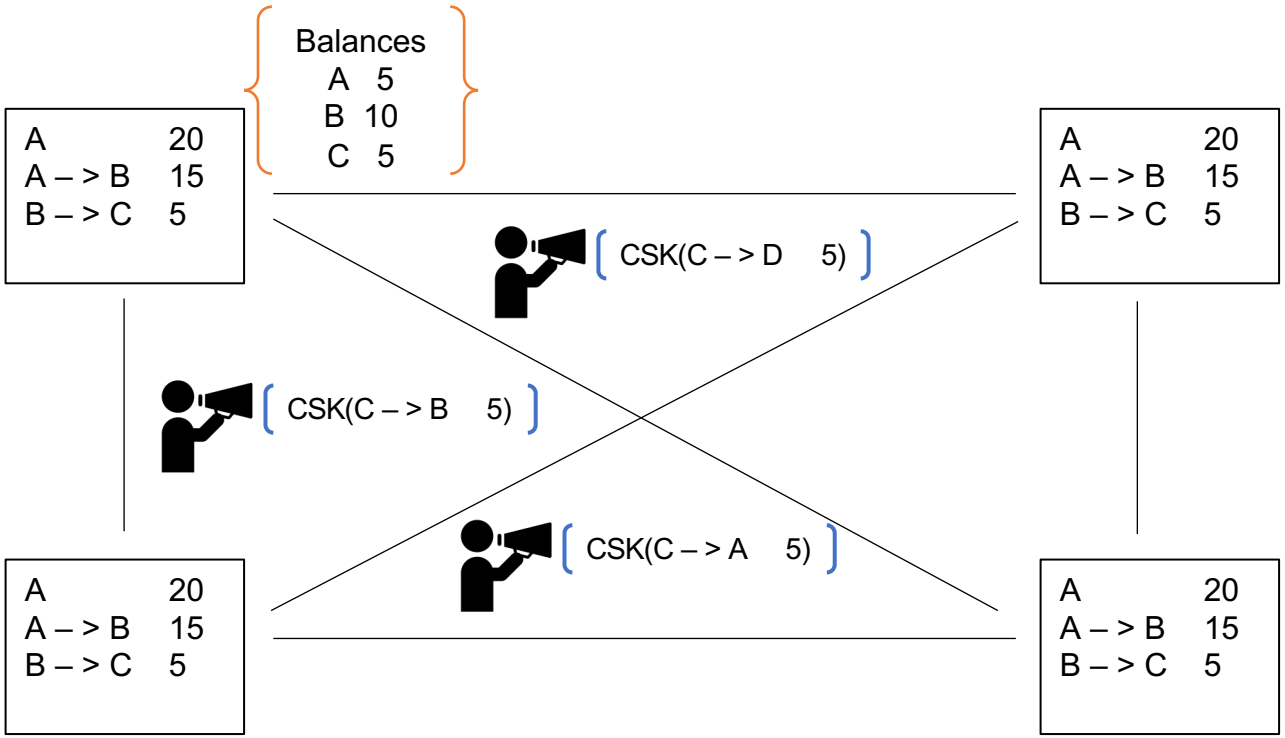
Alice sets up multiple identities



Alice double spends with her multiple identities

Sybil Attack: Done by creating many fake identities





Problems?

1. Can C send the same Money twice?
Double Spending

Solution

Consensus in the network
Proof of Work

Proof of Work

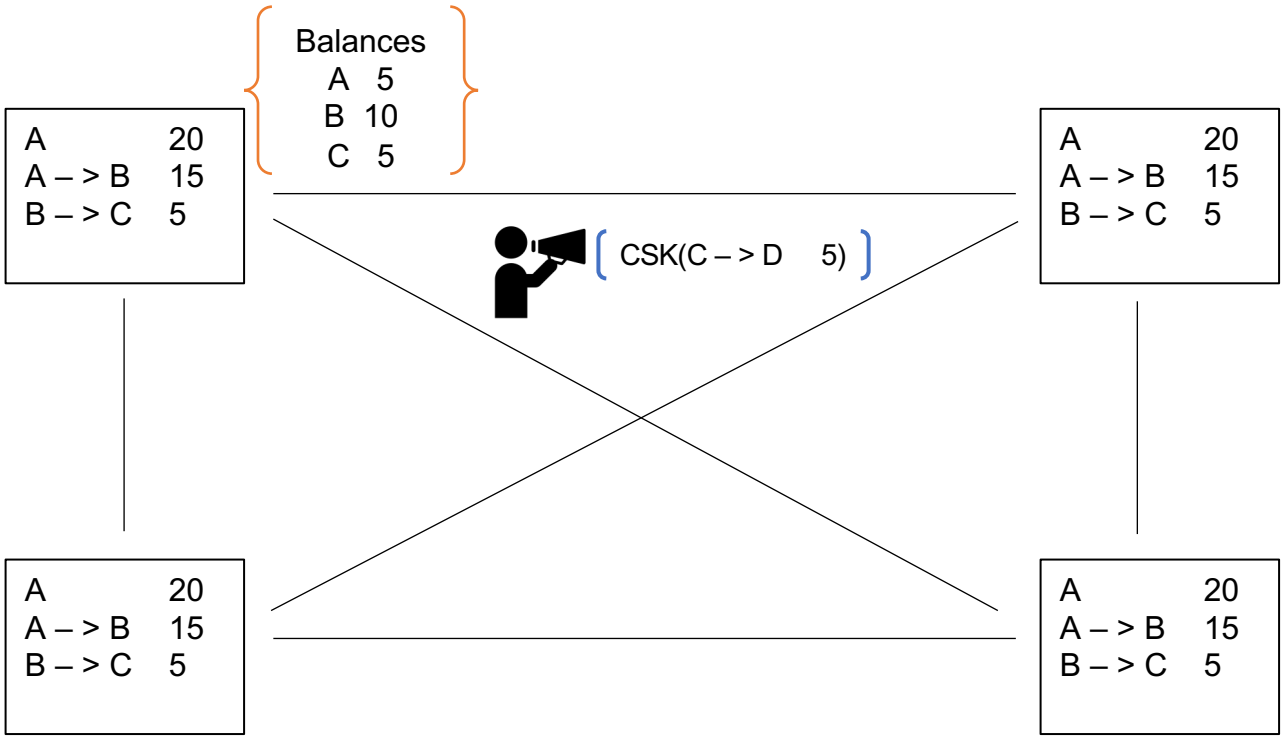
A **proof of work** is a piece of computation which is difficult (costly, time-consuming) to solve but easy for others to verify and which satisfies certain requirements

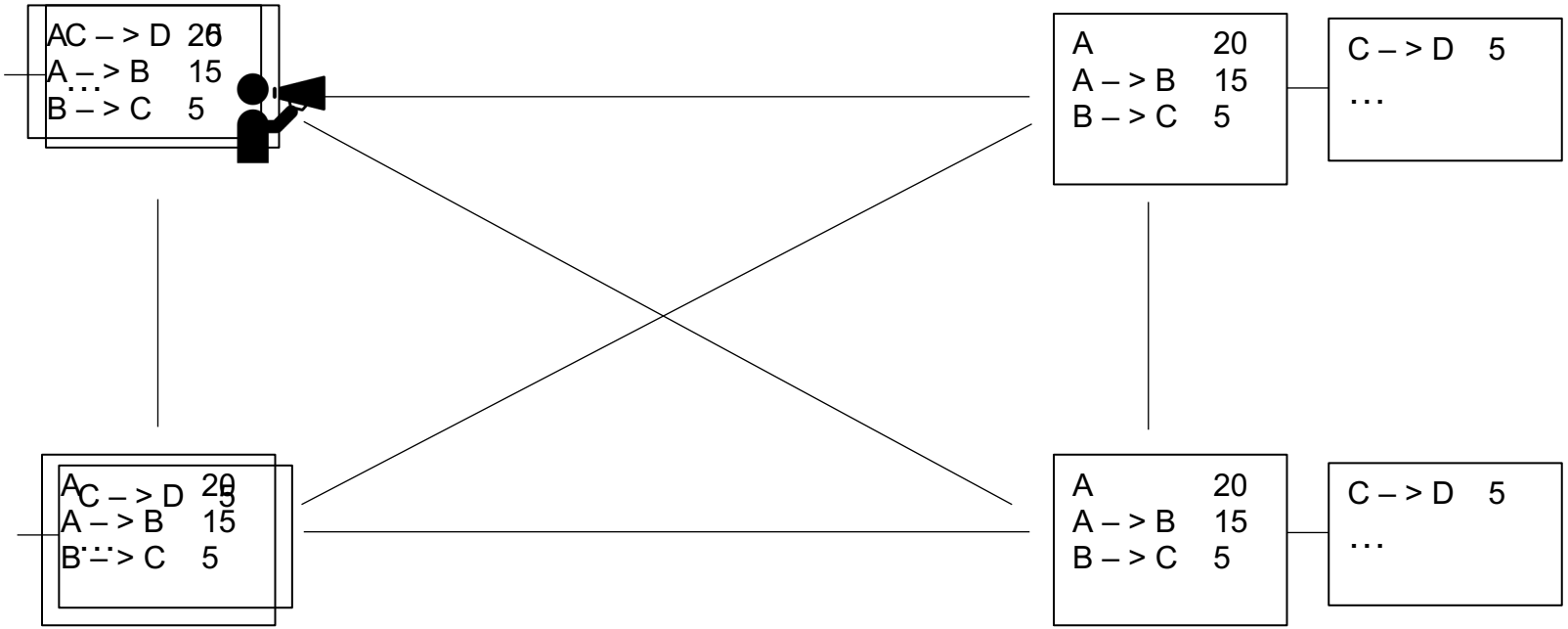
$$a_0 = f(x)$$
$$a_0 < \text{TARGET}$$

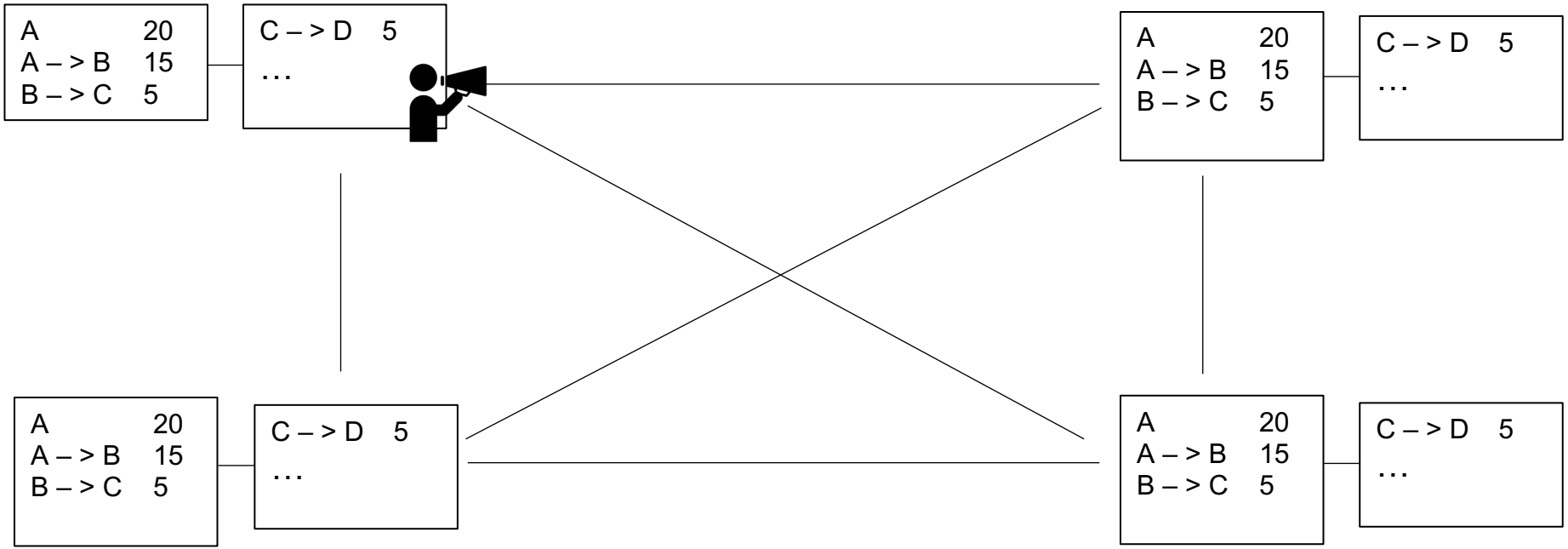
```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
      header = makeBlockHeader(transactions, coinbase_nonce);
      for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
            if (SHA256(SHA256(makeBlock(header, header_nonce))) <
      TARGET)
                  break; //block found!
      }
      coinbase_nonce++;
}
```

Figure 5.6 : CPU mining pseudocode.

Image source: Mastering Bitcoin


Balances
A 5
B 10
C 5
A 20
A – > B 15
B – > C 5
CSK(C – > D 5)
A 20
A – > B 15
B – > C 5
A 20
A – > B 15
B – > C 5
A 20
A – > B 15
B – > C 5


AC – > D 20
A – > B 15
B – > C 5
…
A 20
A – > B 15
B – > C 5
C – > D 5
…
A 20
C – > D 20
A – > B 15
B – > C 5
…
A 20
A – > B 15
B – > C 5
C – > D 5
…


A 20
A – > B 15
B – > C 5
C – > D 5
…
A 20
A – > B 15
B – > C 5
C – > D 5
…
A 20
A – > B 15
B – > C 5
C – > D 5
…
A 20
A – > B 15
B – > C 5
C – > D 5
…

Summary

Version	Major feature	Value added
1	Signed messages announced to the network	Basis of entire system
2	Serial numbers	Uniquely identifiable transactions
3	The block chain	Shared record of transactions
4	Everyone verifies transactions	Increased security
5	Proof-of-work	Prevents double spending

Recap - The Innovation of Satoshi Nakamoto

Bitcoin was created by Satoshi Nakamoto in 2009

- First ever decentralized, trustless system for transactions
  - A low cost financial system that only requires an internet connection
- Nakamoto solved the Double Spending problem
  - Prevent someone from spending the same asset twice
  - Solution? The blockchain + PoW
  - Who helped secure the network were rewarded
  - Who tried to compromise the Bitcoin network had to make a massive financial investment to do so, with relatively little benefit

Dorian Satoshi Nakamoto
(not actually Satoshi Nakamoto-probably)

Sketch of Bitcoin Mining - Proof of Work

- Solution to the Byzantine Generals Problem: Proof-of-work (PoW)
  - “Miners” continuously compete to solve a very computationally difficult problem
  - Proof of work is an example of a "Byzantine consensus algorithm"
- Proof of work criteria:
  - Easy to verify
  - Hard to compute
- SHA-256 Hash function satisfies these
  - One-way hash function; can hash any arbitrary data
  - Pretty much random (very useful property)
- Example
  - SHA256("Donald Trump") == "e4f2e1f0e2ae4d3ce7018cf3b4f3577c99714bdc9f5a4ac28e3e7cb2c505db6c"
  - SHA256("Donald trump") == "6ad2fa6a5caaee9143578931456322c4433a92ae2af8f0d5c9b4f9bb080f49d6"

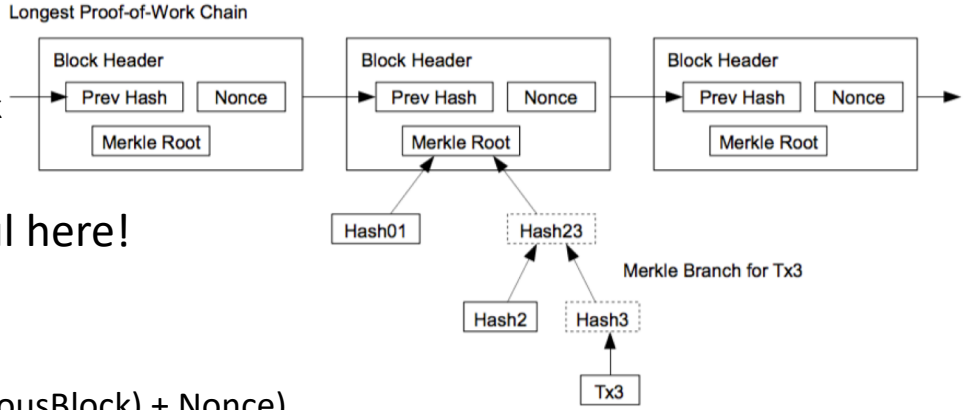
Sketch of Bitcoin Mining - Finding blocks

- Finding the PoW => 'found' a block; can add block to blockchain
  - Miner who found block adds "**coinbase transaction**"
    - contains mining reward (currently 12.5 BTC)
  - Miner broadcasts block
  - Other nodes verify, then add to their own copy of the blockchain
- Timeline + stats
  - This happens roughly every 10 minutes
    - Difficulty of the problem adjusted every 2 weeks
  - Block reward halving every 4 years
  - Bitcoin is in limited supply - 21 million bitcoins by 2140
    - Deflationary
  - 17.3 million bitcoins currently in circulation today
  - ~$142 billion market cap (10.2019)
  - Price is currently ~$6590 per bitcoin

Sketch of Bitcoin Mining - The Mining Problem

Components hashed together:

- Merkle Root
  - 'summary' of the transactions in the block
- Hash of previous block
- Nonce
  - Randomness of SHA-256 is useful here!



Formally:

- Output = SHA-256(Merkle Root + SHA-256(PreviousBlock) + Nonce)
- Solution (Proof-of-work): an output that contains a requisite number of leading 0 bits
  - The number of 0 bits is the **difficulty**
  - Difficulty adjusts every every 2016 blocks* to regulate block creation
    - *technically every 2015 blocks

Sketch of Bitcoin Mining - 51% Attacks

Major assumption of Bitcoin:

No more than 51% percent of the network is dishonest

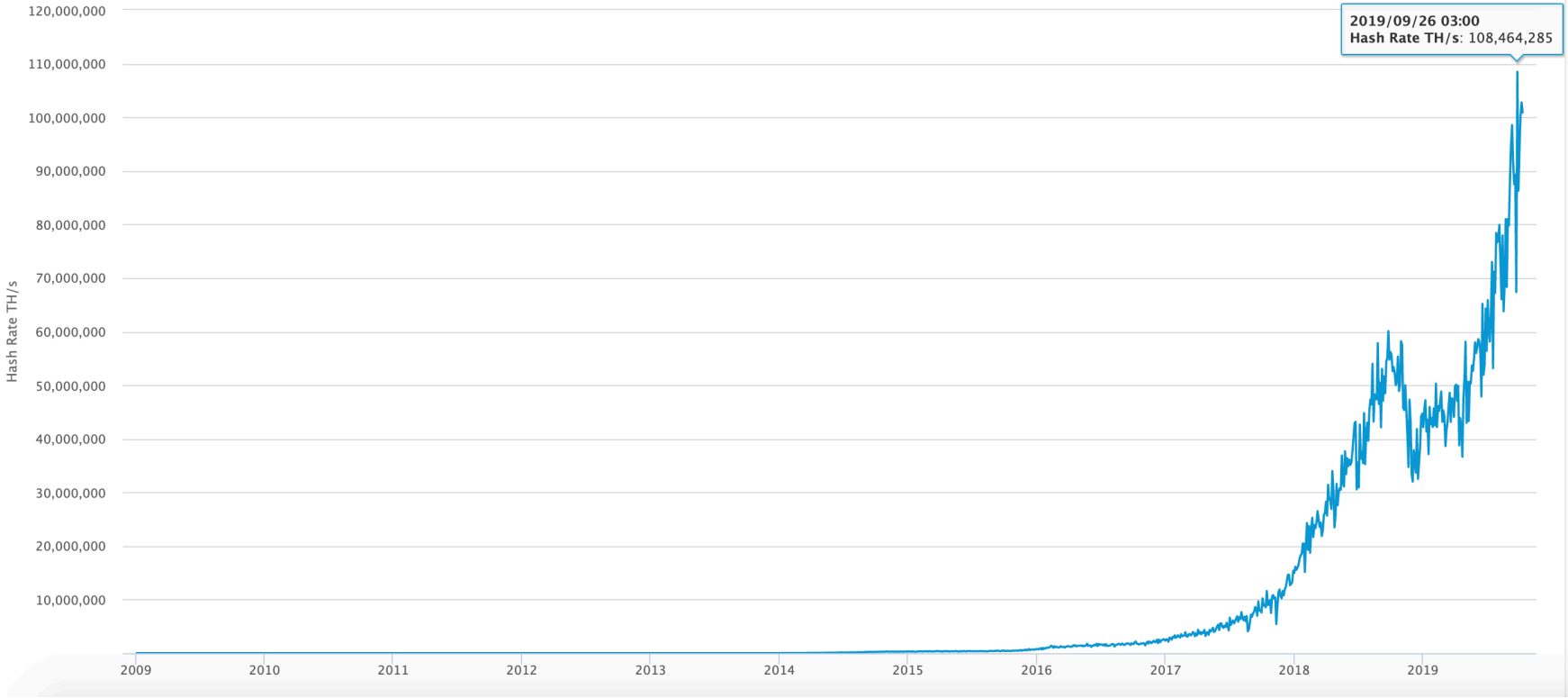
An honest majority will always form the longest proof-of-work chain

51% Attack: Attempt to overwhelm the mining power of the network

Hash Rate

The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.

Source: blockchain.com



Sketch of Bitcoin Mining - Summary

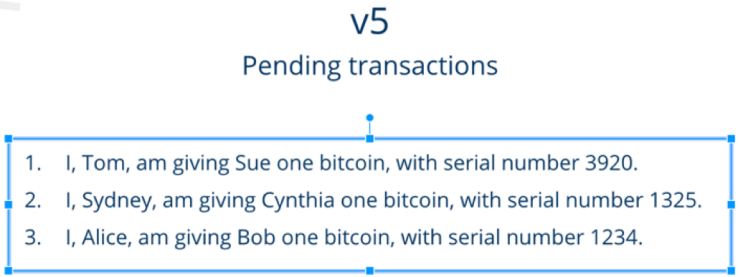
Functions as:

- A minting mechanism that ensures coins are distributed in a fair way
- An incentive for people to help secure the network
- Key component that enables you reach consensus in a decentralized currency

Bringing it all together - Back to a transaction

- I want to send money to Sunny
  - Sign transaction
  - Broadcast to network
- Miners receives transaction, adds to “**zero-conf pool**”
  - Verify transaction: i.e. signature matches, enough money,
- Miner finds PoW, broadcasts block
  - Block propagates; others verify
- Miners work on the next problem

Slide by Viget



Demo

- https://anders.com/blockchain/

Next class – Bitcoin Mechanics

Suggested Readings:

- Blockchain Demo: https://www.youtube.com/watch?v=_160oMzblY8
- Princeton Textbook 5.1-5.4 (pg. 131 - 157)
- Bitcoin Wallets Explained

http://cryptorials.io/bitcoin-wallets-explained-how-to-choose-the-best-wallet-for-you

References

Slides mainly adopted from

- Blockchain @ Berkeley : https://blockchain.berkeley.edu/
- Blockchain @ Princeton : http://bitcoinbook.cs.princeton.edu/