Introduction to Information Security
14-741/18-631 Fall 2021
Unit 5, Lecture 4: Intro to Cryptocurrencies

Hanan Hibshi hhibshi@andrew

Part I: Overview

Most Common Types of Cryptocurrencies

- **Bitcoin**
  - Most famous and recognizable
- **Bitcoin cash**
  - Introduced in 2017; faster; block size is 8 MB
- **Litecoin**
  - Shorter transaction time; lower fees; faster processing
- **Ethereum**
  - Smart Contracts; Focuses on decentralized applications
- **Ripple** (Not blockchain based; meant for larger corporations)
- **Stellar** (money transfers; non-profit;)
- **NEO** (Ethereum competitor)

Bitcoin Primer (1/2)

- **A peer-to-peer digital payment system**
- **Completely decentralized digital currency**

  - **No central mint** to produce currency
  - **No central bank** to verify transactions
    - Verification needed for digital currencies, are duplication of coins simply means "copying bits"
      - Without verification double-spending is possible
      - Physical currencies avoid this by using physical security features
  - Once confirmed, transactions are **irreversible**
  - Predictable, capped, currency supply

- **Key innovation in Bitcoin: coin production and verification is done by network consensus**

Bitcoin Primer (2/2)

- **There is actually no notion of a "coin"**
  - Although Casascius provides neat physical artifacts
    - Those are technically one-time use wallets

- **Bitcoins are exchanged from "wallet" to "wallet"**
- **Transactions are at the heart of the protocol**
- **Wallets are represented by addresses (e.g.,** 1VayNert… **)**
  - (An address is essentially the public key of the wallet)

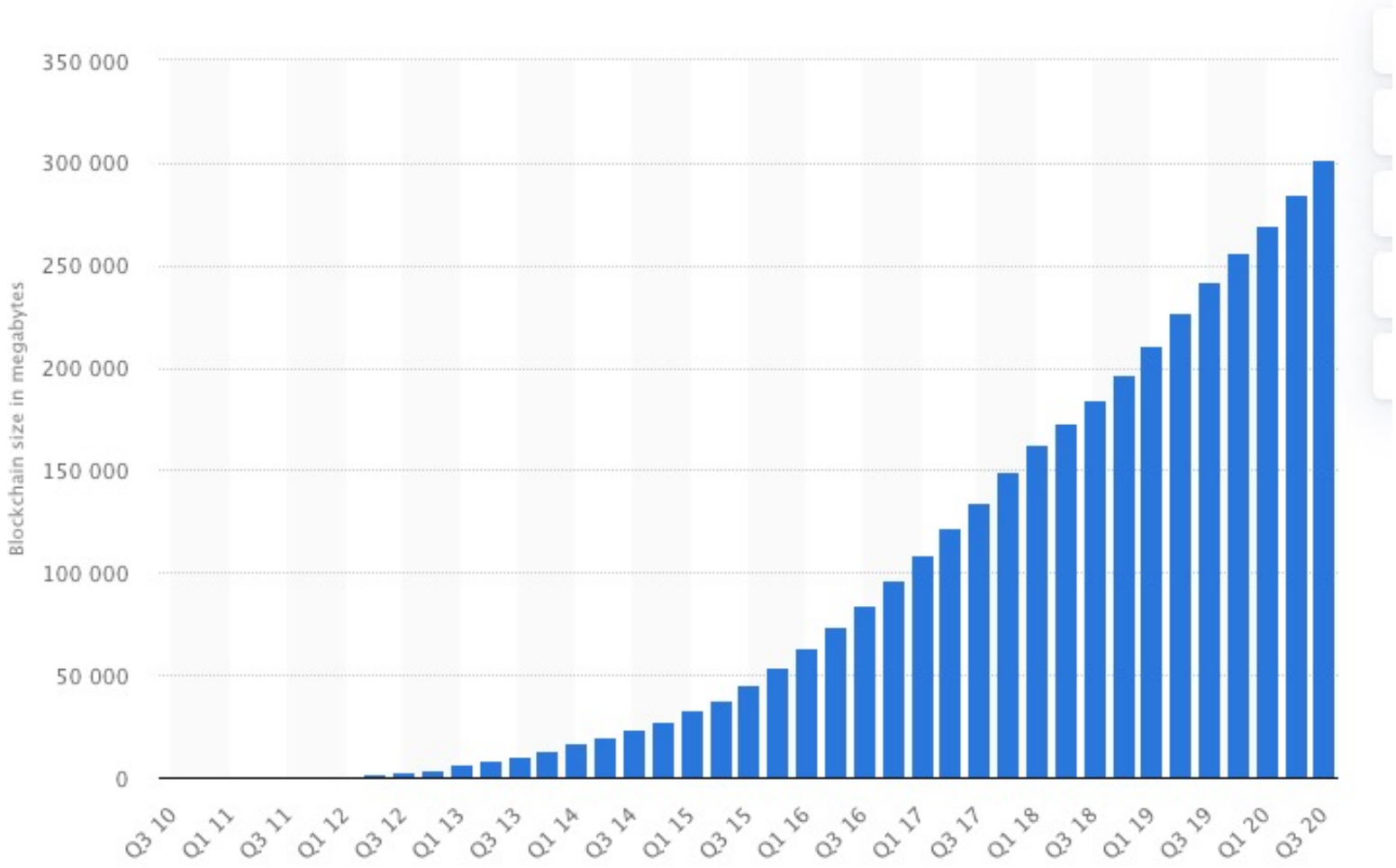
Bitcoin Transactions

- **Alice wants to send 1 BTC to Bob**
  - She picks a transaction (or a group of transactions) that she has previously been the recipient of and that cumulatively contain at least 1 BTC
  - She then appends Bob's wallet address to the transaction and digitally signs it
- **When Bob subsequently wants to spend the 1 BTC, all he has to do is to repeat the operation**

Preventing Double-Spending

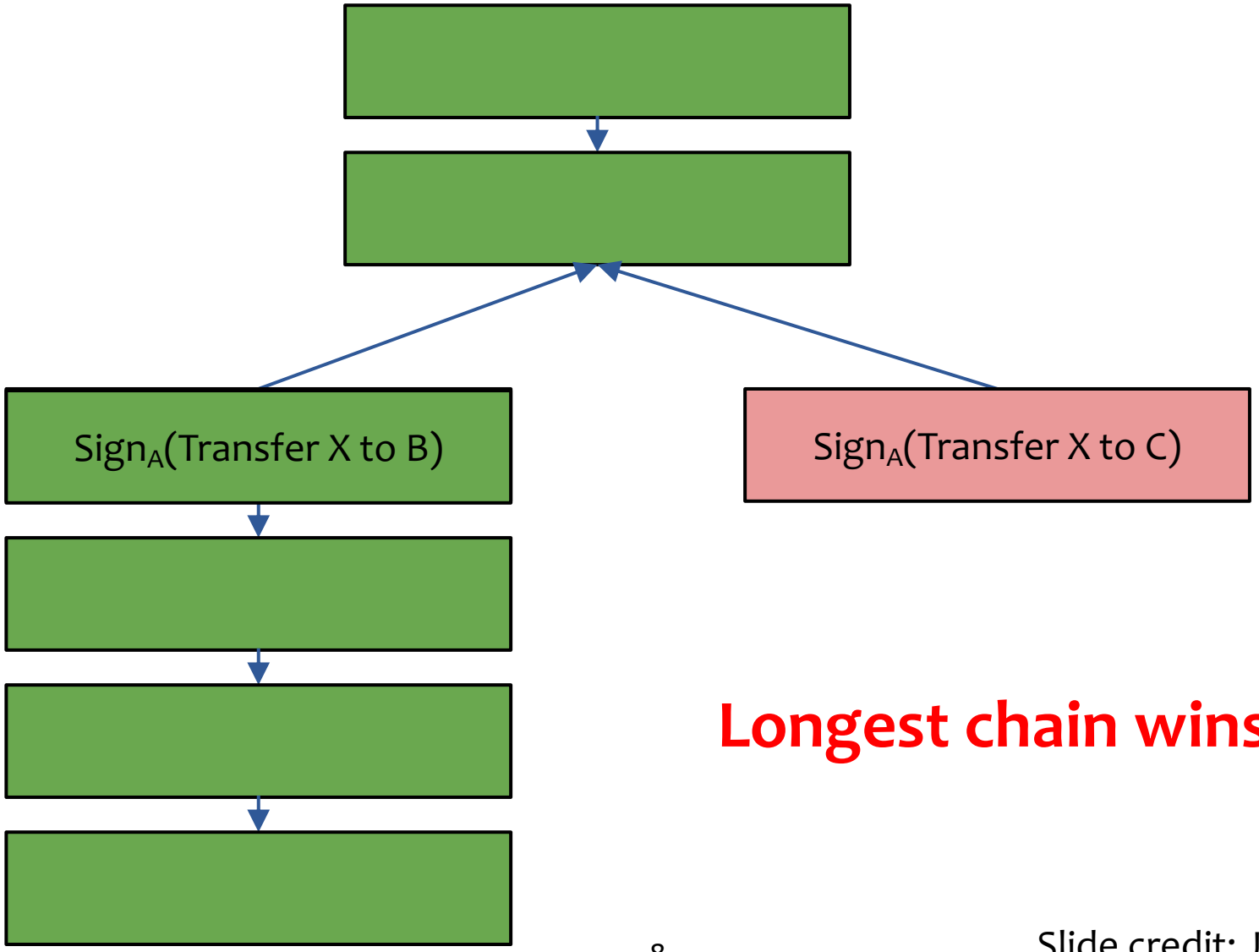
- **Bob now has 1 BTC**
  - He wants to send it to Charlie…
  - … while keeping it for himself at the same time
- **To prevent this Bob (and Alice before him) has to broadcast the transaction to everybody in the Bitcoin network**
- **Then other peers can verify that the transaction is not a double-spend**
- **Once this is done, the transaction is embedded forever in a public ledger**

Bitcoin Ledger Size



Details: Worldwide; 2010 to 2020

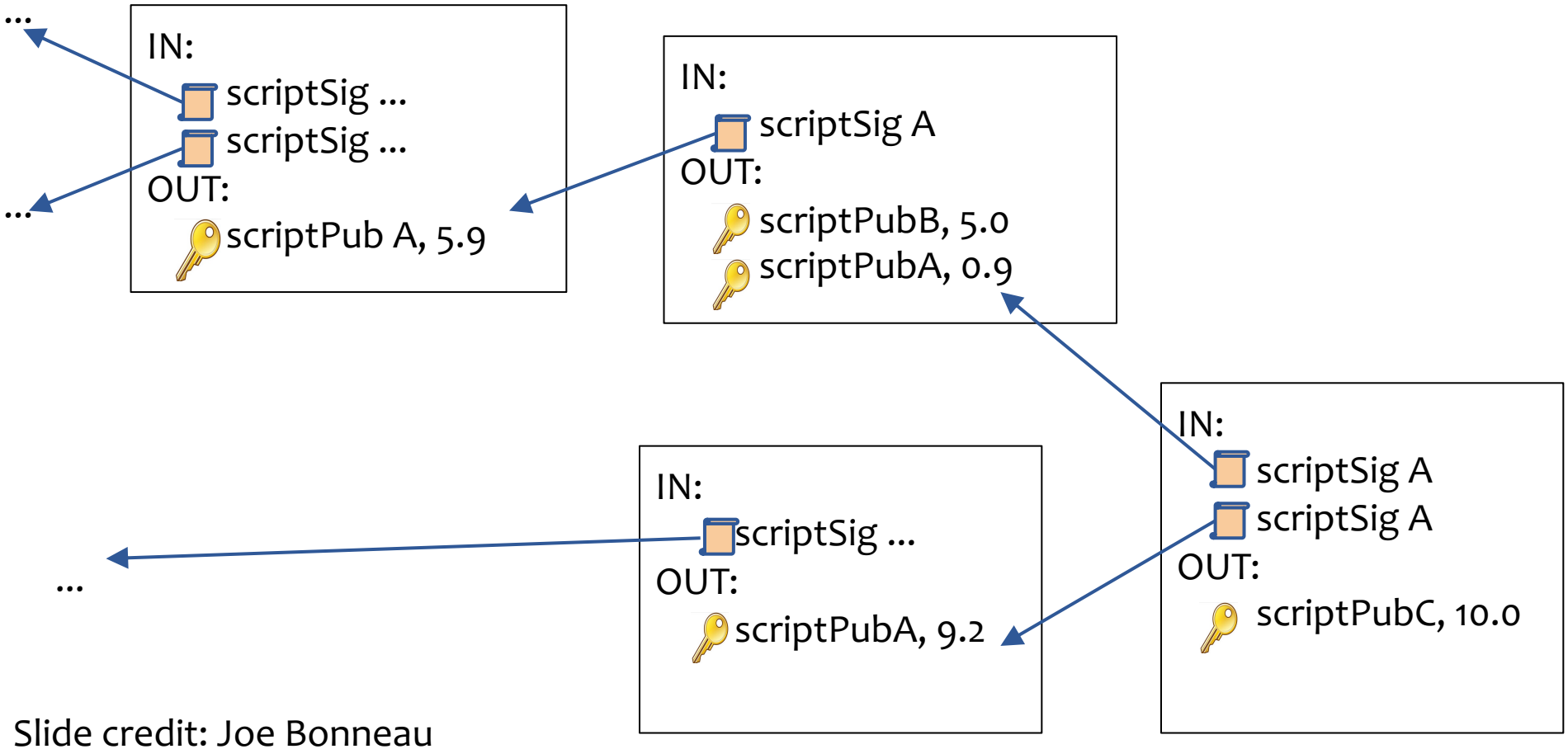
Preventing Double Spending



Longest chain wins

Slide credit: Joe Bonneau

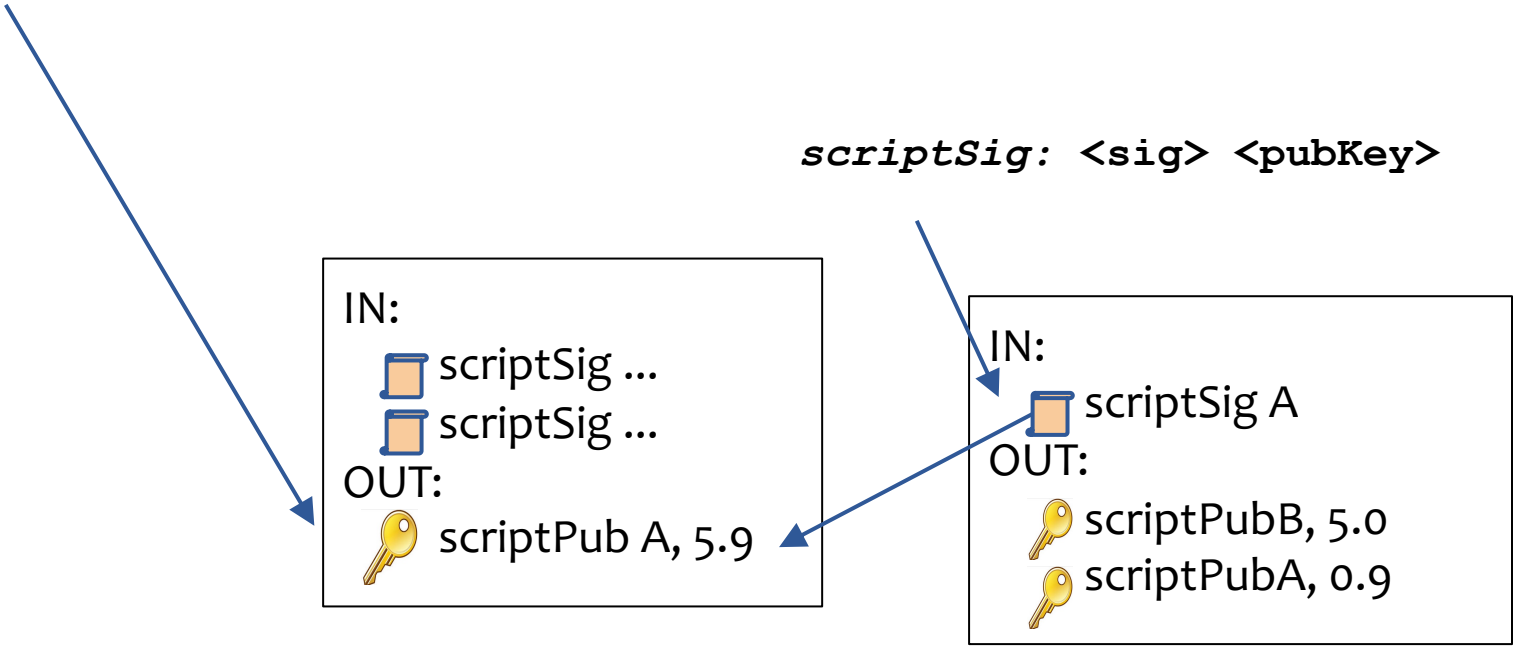
Bitcoin is Transaction-Based



Slide credit: Joe Bonneau

Bitcoin Transactions Specify Scripts

scriptPubKey: **OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG**

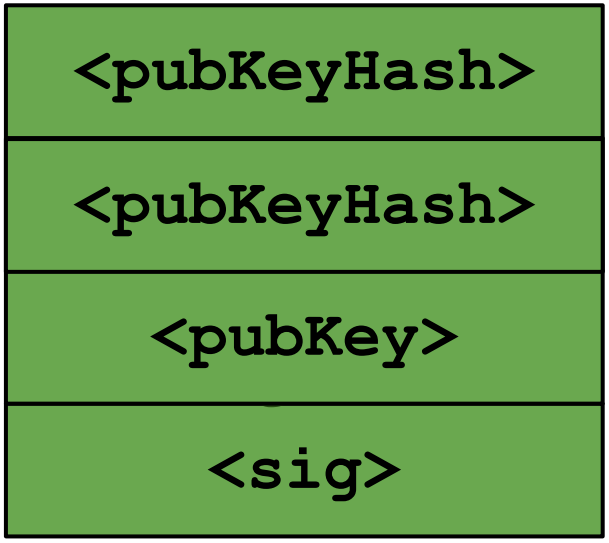


Redemption script:

```
<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```

Slide credit: Joe Bonneau

Bitcoin Transactions Specify *Scripts*



```
<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```


Slide credit: Joe Bonneau, full details here

Bitcoin Script Features

- multiple signatures
- escrow
- time locking
- commitment opening
- ...

- smart contracts?

Slide credit: Joe Bonneau

Part II: Mining Bitcoin

Coin Production

- **Coin production is embedded in the verification process**
- **Verifiers ("miners") verify batches of transactions at once**
  - In exchange for which they are allowed to add a "creation" transaction to the batch and give themselves a fixed amount of money
    - 50 BTC originally, 12.5 BTC as of 7/9/2016, divided by two every so often, drop to 6.25 BTC estimated 5/22/2020
  - Verification is combined with a "proof-of-work" scheme to ensure
    - That transactions have proper timestamping
    - That currency production is rate-limited

Proof-of-Work /Mining Incentives

- **Miners essentially solve a cryptographic puzzle, essentially**

$$\text{find } x \text{ such that } H(x) < y$$

- **There is no good algorithm to solve this (*H* is a cryptographically secure hash function)**
  - **Brute-force:** try $x=0$, $x=1$, $x=2$, $x=\ldots$
  - The lower y, the harder the puzzle

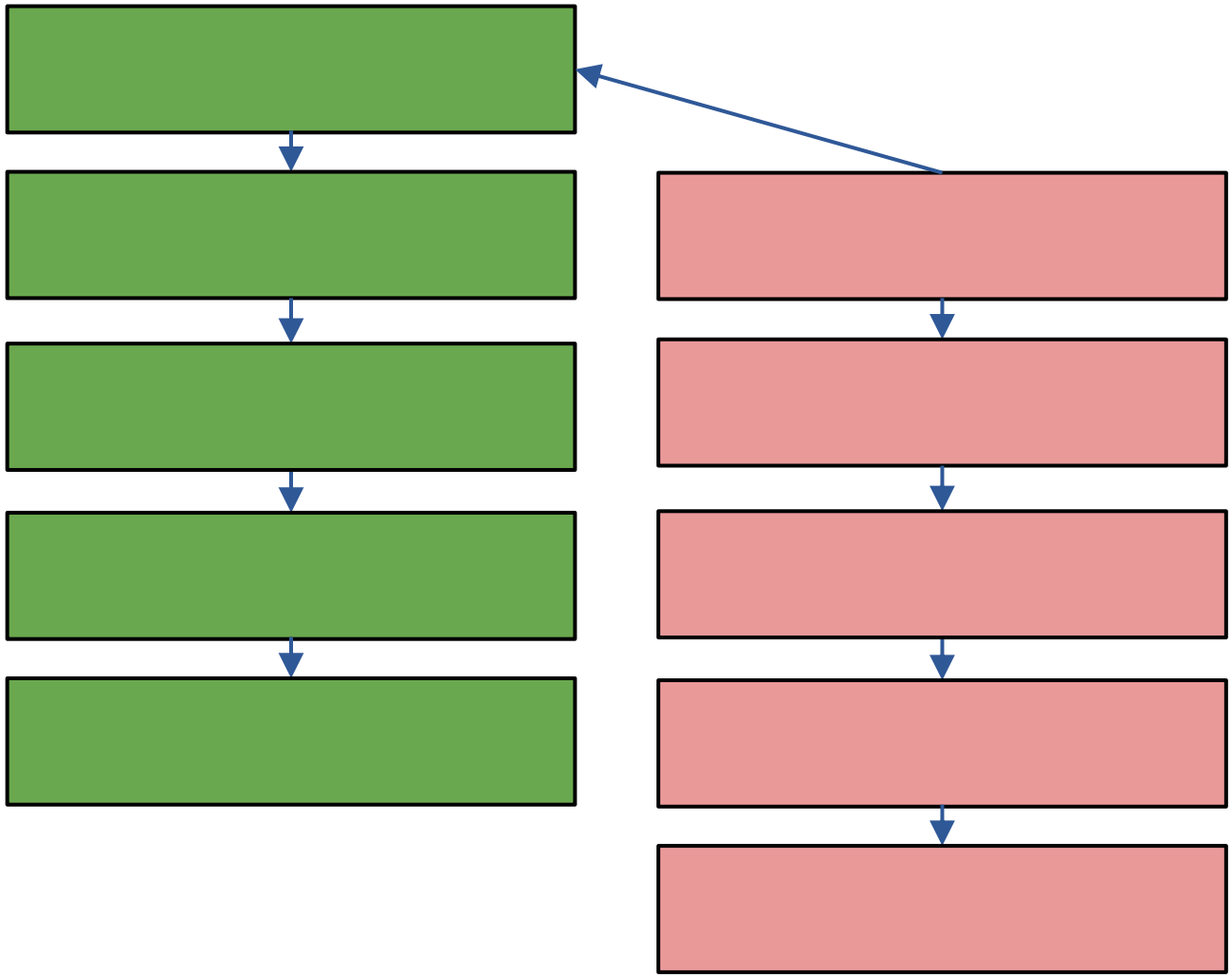
- **Difficulty is tunable and is (by edict) designed to be inversely proportional to the total computational power of the network**

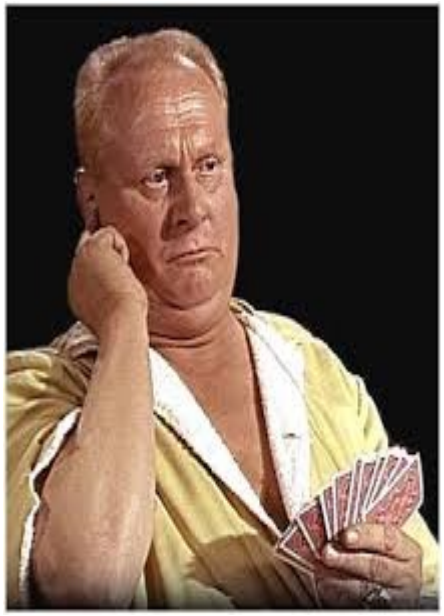
- **The goal is to have one block every ten minutes**
  - Predictable supply of currency (independent of the difficulty)
  - **But this limits how quickly transactions can be verified**
    - At least 10 minutes, usually 60 minutes is recommended

Transaction Fees

- **In addition to the bonus they get for mining, miners get "transaction fees"**
  - Leftover "change" voluntarily left in transactions
- **Because the bonus is decreasing over time, the expectation is that transaction fees will increase over time to make up for lost mining revenue**

51% Attacks

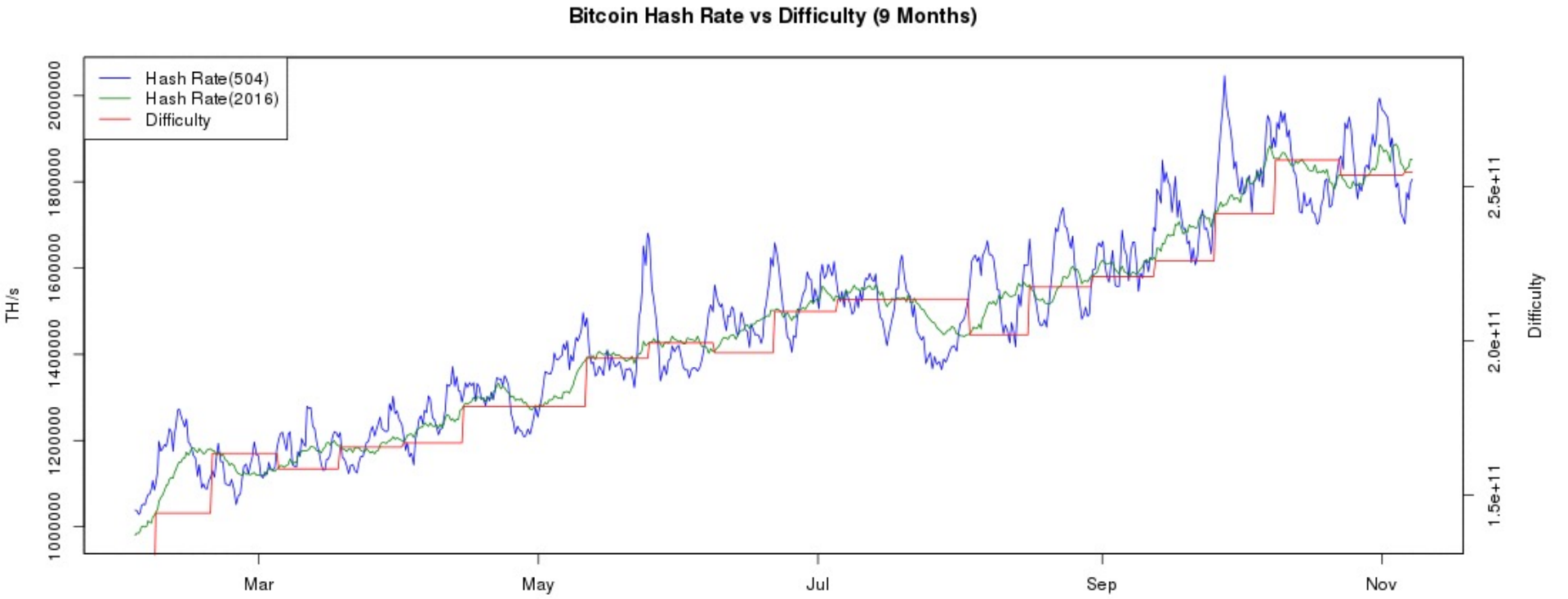




Goldfinger Attack?

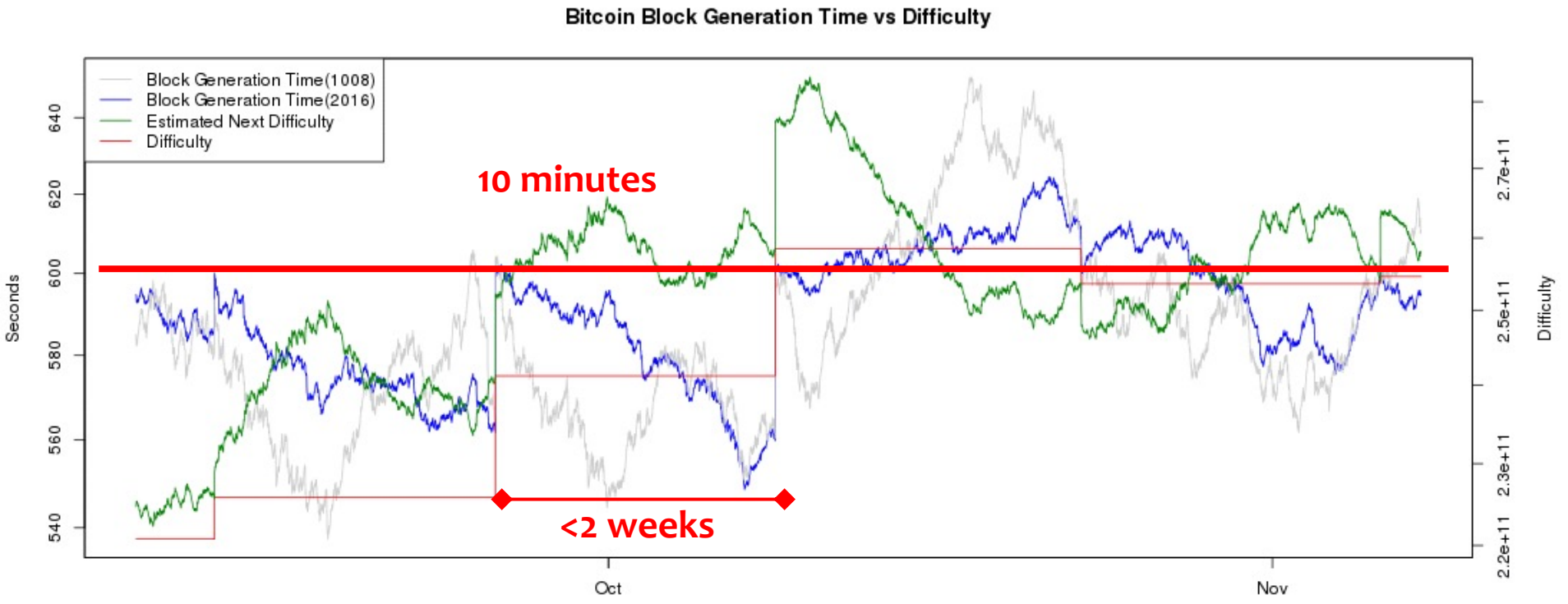
Slide credit: Joe Bonneau

Mining Difficulty



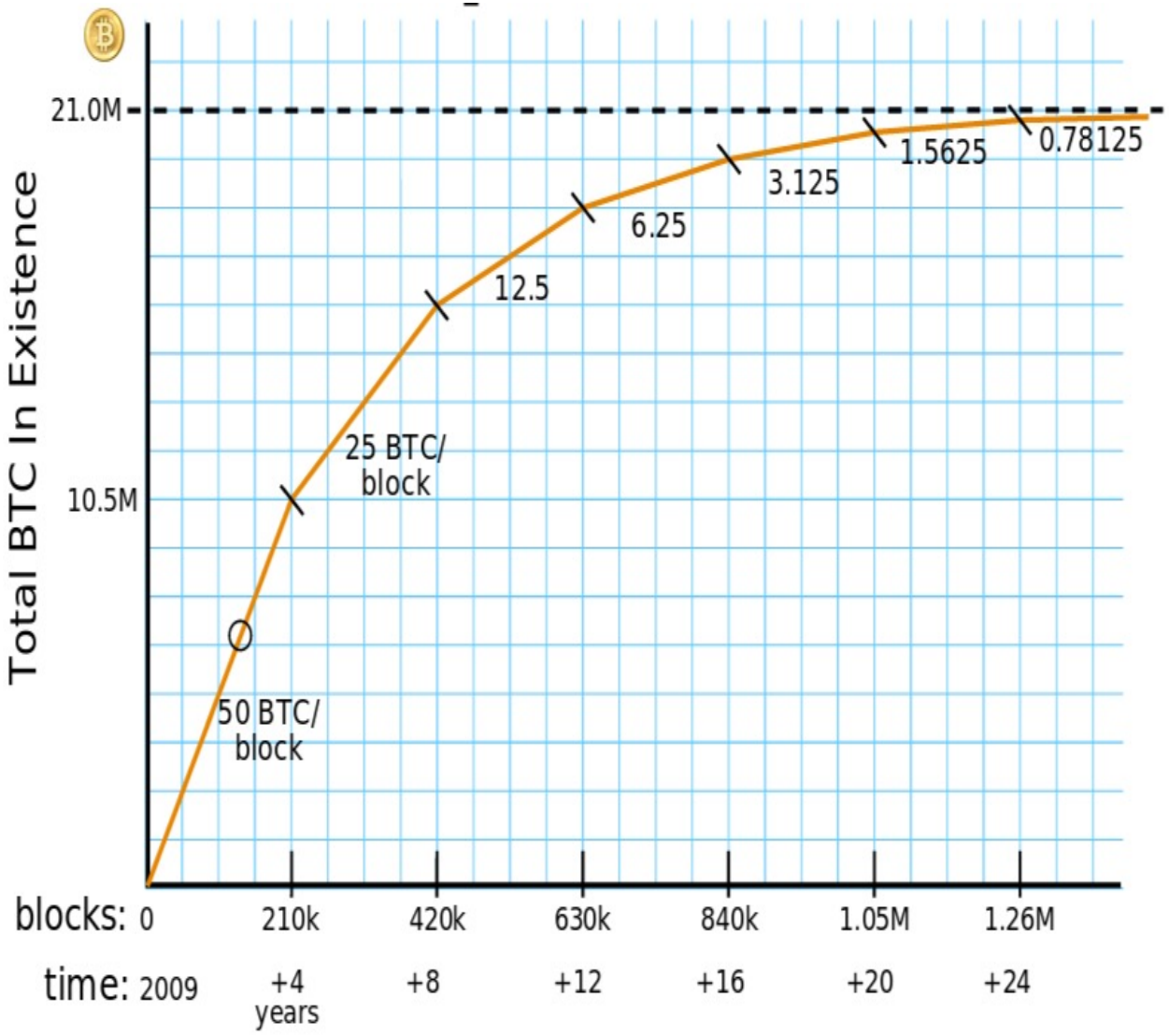
bitcoinwisdom.com

Difficulty Adjustment



bitcoinwisdom.com

Mining Rewards



Courtesy:
Brian Warner

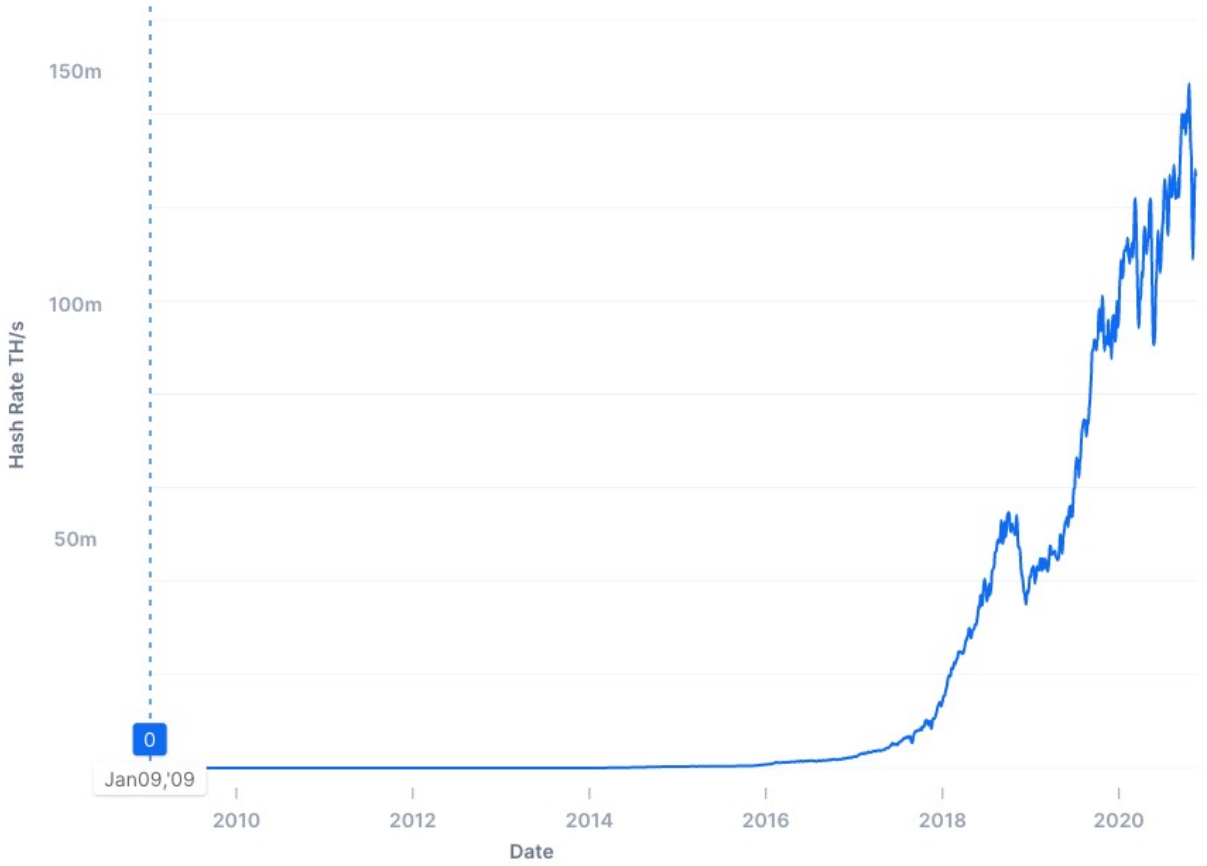
Total Network Capacity

- **Feb 2019: $2^{74.4}$ hashes per block (every 10 minutes!)**
- **Consuming >> 4.2GW continuously **
  - *Assuming ~10,000 MegaH/J (AntMiner S9)
- **2^{75} hashes in 2015… in one hour!**
- **Computation of power is very hard to do nowadays – see https://digiconomist.net/bitcoin-energy-consumption**
- **Recent historical perspective:**

Year	2017	2018
Total # of hashes	$2^{87.37}$	$2^{89.89}$
~power*	**> 0.6 GW (5.4 TWh/yr)**	**> 3.6 GW (31 TWh/yr)**
Profit	> US $1.6B	**> US $4.7 B**

Slide credit: Nicolas Christin

Bitcoin Hash Rate



Source: https://www.blockchain.com/charts/hash-rate

Bitcoin Mining Hardware

TerraMiner™ IV – 2TH/s Networked ASIC Miner

$5,999

Shipping June 2014

300 GH Bitcoin Mining Card

The Monarch BPU 300 C

$1,497.00

Qty: 1 ADD TO CART

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.

THE LEOPARD

DETAILS :

- **2,5 TH/s**
- Dimensions: 15" x 13.3" x 13.7" (38cm x 34cm x 35cm)
- 28nm ASIC technology
- Silent Cooling
- In-built WiFi Connection (without Antenna)
- Less than 750 watt (0.3 per GH)
- 1 Year Guarantee

- $ 5.800

COMES WITH :

1. Power Supply
2. Free Remote Power Outlet & Smartphone App
3. Free User Guide
4. Free Personal Assistance for Setup

SHIPPING :

- Worldwide, Express
- Included in the price
- Available: 100 Units: Shipping April (Week 3)

Slide credit: Joe Bonneau

Should I Mine Bitcoins?

Chilkoot pass,
Klondike 1898

Slide credit: Joe Bonneau

Mining Pools

Mint(25, K_{POOL})

0x0000000000000003f89...

0x000000000000a877902e...

0x000000000001e8709ce...

0x00000000000490c6b00...

0x0000000000007313f89...

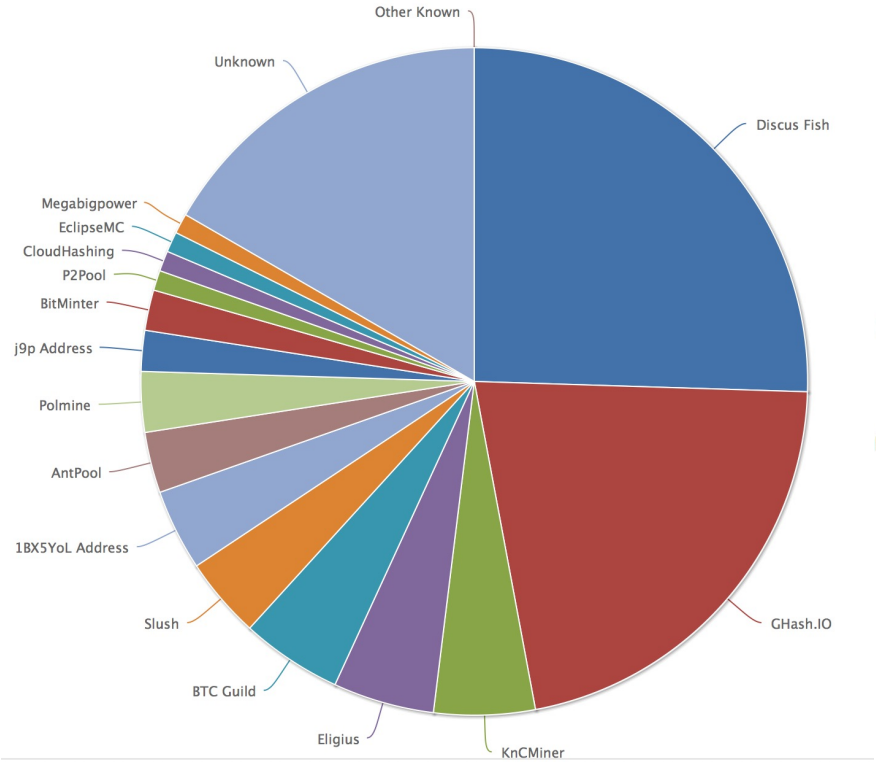
0x0000000000000003f89...

0x00000000000045a1611f...

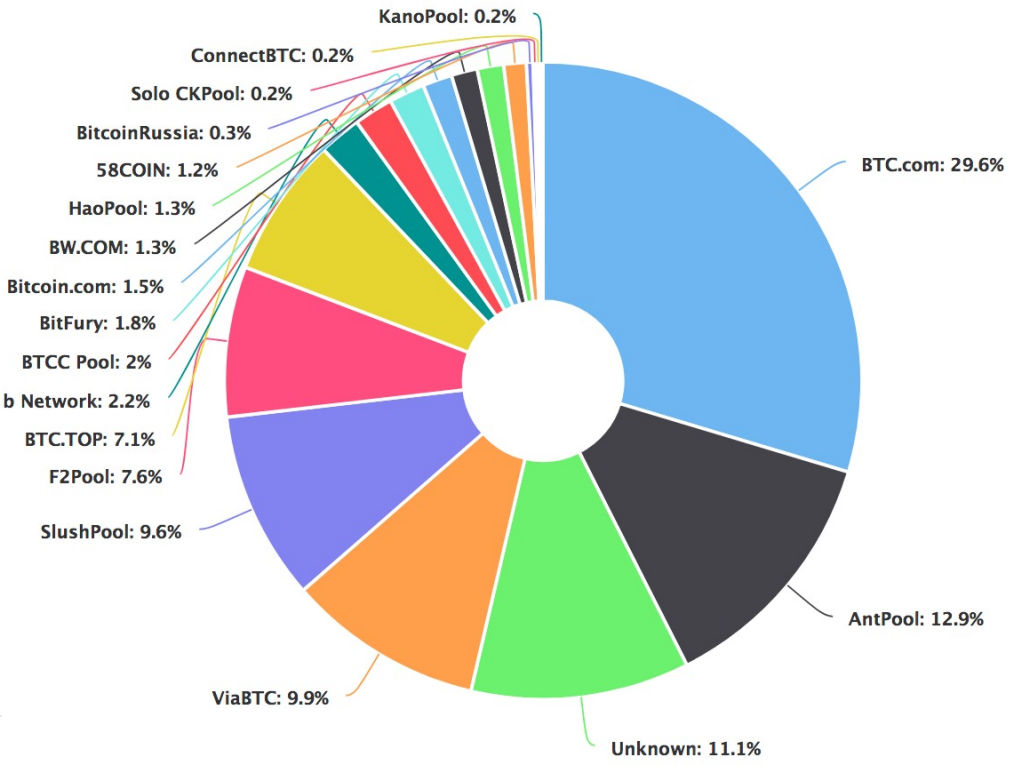
Slide credit: Joe Bonneau

Mining Pools

2013



2018



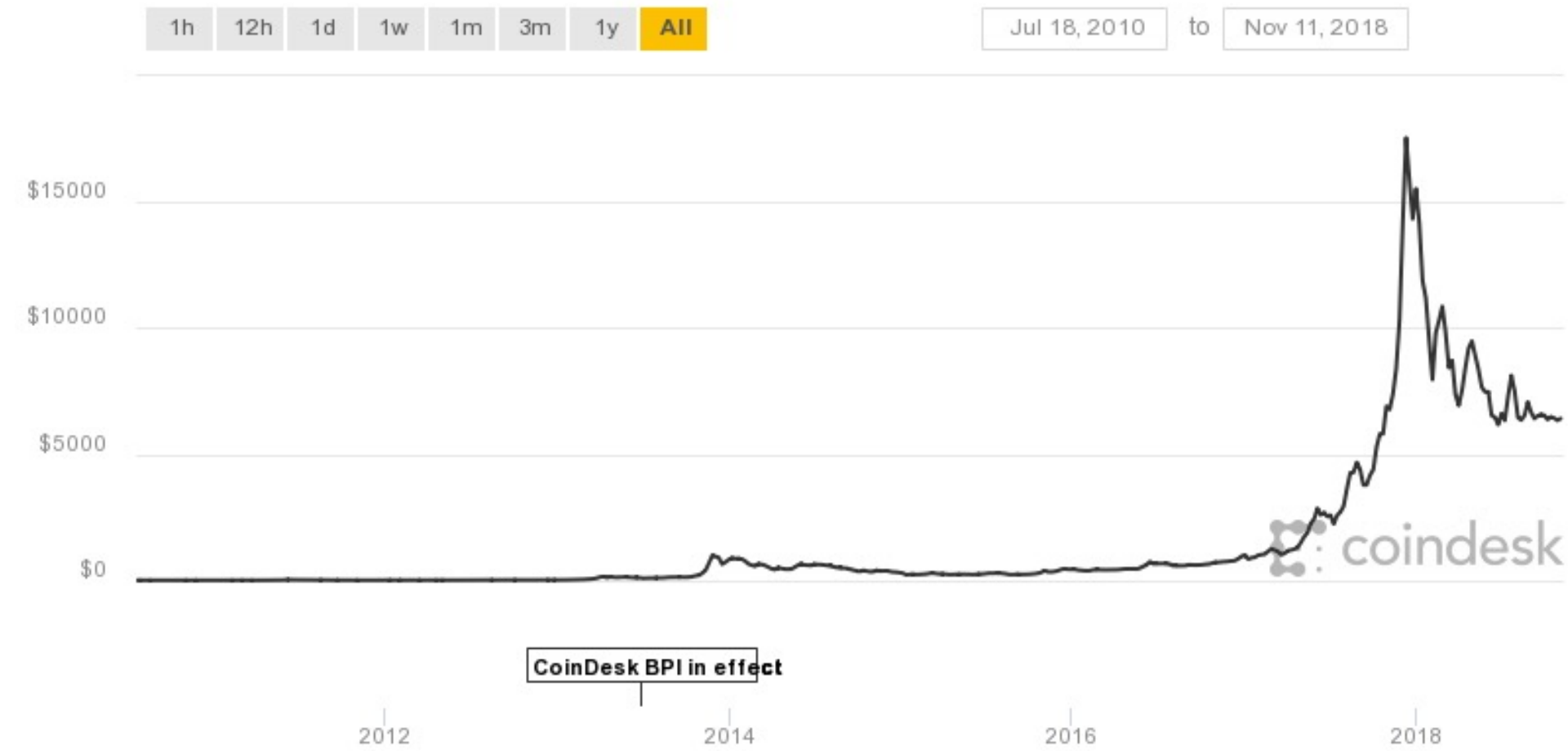
Part III: Using Bitcoin

Getting Bitcoin

- **Become a miner**
  - Nowadays only profitable if dedicated (ASIC) hardware
- **Buy at an exchange**
  - CampBX, Bitstamp, BTC-e, Coinbase…
  - (Mt.Gox before they went bankrupt)
  - Very **high concentration** on exchanges through which money is exchanged
    - Exchanges fail pretty often…
  - Increasingly scrutinized by regulator
- **Buy from individuals**
  - Satoshi Square in NYC

Main Bitcoin Uses

- **As a speculative instrument**
  - People invest in BTC, betting on its rising value
  - Dominant use thus far



Main Bitcoin uses

- **As a currency**
  - Only currency accepted on underground marketplaces (Silk Road, Evolution,…)
    - (Except for LiteCoin, which is a clone of Bitcoin)
    - Because of its "anonymity properties"
    - Still relatively modest
      - Entire Silk Road revenue represented in 1st half of 2012 about $15M/annum
  - Gambling, poker sites
    - Large number of transactions, volume not very high
  - Other uses still in their infancy
    - Campaign contributions, online stores (e.g., Overstock), etc.

silkroadvb5piz3r.onion/silkroad

Startpage

Silk Road

anonymous market

messages 0 | orders 0 | account ฿0.00

Search Go

Shop by Category

- Drugs *11,247*
  - Cannabis *2,664*
  - Dissociatives *269*
  - Ecstasy *1,262*
  - Opioids *667*
  - Other *551*
  - Precursors *102*
  - Prescription *2,447*
  - Psychedelics *1,213*
  - Stimulants *1,551*
- Apparel *341*
- Art *3*
- Biotic materials *2*
- Books *912*
- Collectibles *14*
- Computer equipment *74*
- Custom Orders *89*
- Digital goods *630*
- Drug paraphernalia *330*
- Electronics *103*
- Erotica *626*
- Fireworks *15*
- Food *9*
- Forgeries *158*
- Hardware *27*
- Herbs & Supplements *11*
- Home & Garden *11*
- Jewelry *90*
- Lab Supplies *53*
- Lotteries & games *53*

Royal Customers 10G

฿1.66

Decanoate250, (1 x 10ml = 2.500mg)

฿0.39

XTC Pills MDMA 175mg x500

฿19.28

100g Dimethoxbenzaldehyde

฿1.45

LECKERMANN WEEKLY SKUNK IS BACK STRONG

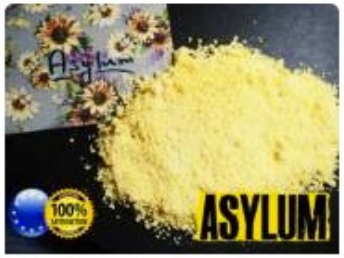
฿0.52

Good Quality Soap Bar | 126g(4.5oz) | UK Vendor

฿2.78

Modafinil 200mg - 300 Pills

฿2.65



0.2g DMT Freebase

฿0.48

1g cocaine high premium quality FLEX - high grade

฿1.32

How Was Anon Market Able to Survive?

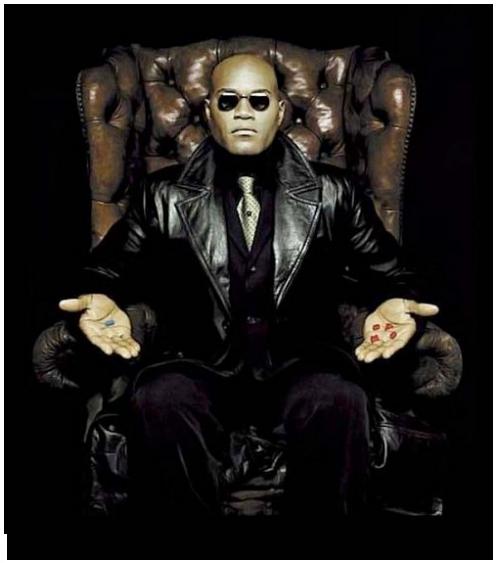
- **Tor "hidden service"**
  - Tor = peer-to-peer network that conceals IP addresses of traffic sources by bouncing traffic around peers
  - Website uses Tor to connect to the Internet
  - **Only** accessible through Tor
    - .onion address as opposed to .com, .org, .net
  - Server is very hard to locate for an attacker

- **Bitcoin for payments**
  - Peer-to-peer, decentralized currency
  - Some anonymity (no identity bound to wallets)
    - However the entire chain of transactions is public

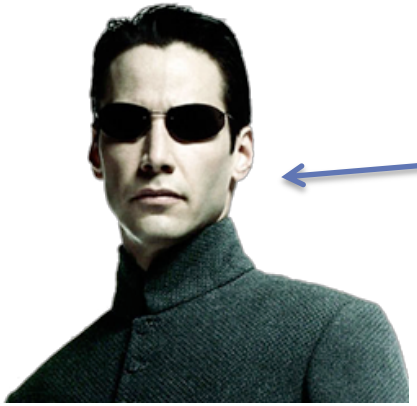
- Marketplace provides escrow mechanism to guarantee transaction completion
  - For buyers: Registration free, open to anyone
  - For sellers: Relatively modest account fee (refunded after a number of successful transactions)

Escrow Transactions

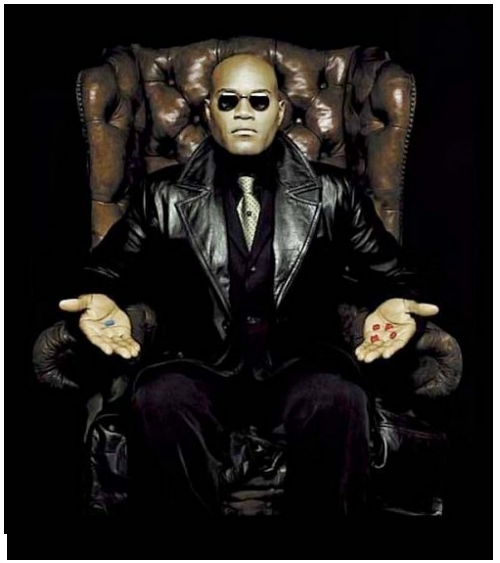
"I'll take the red pill"



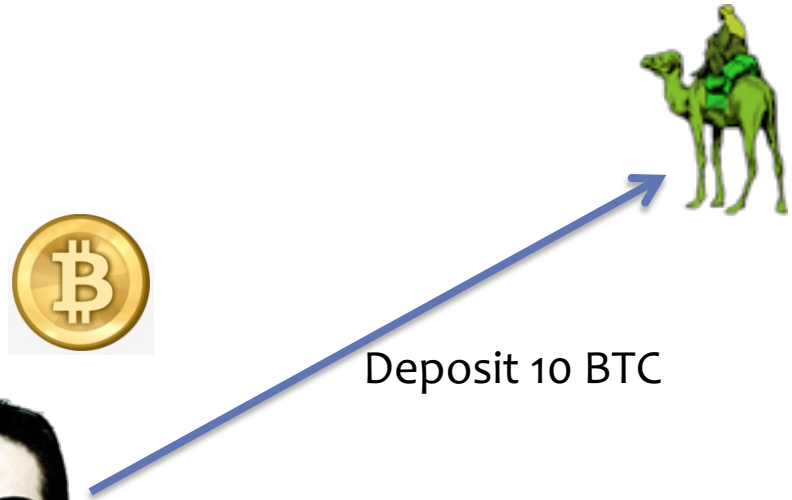
Escrow Transactions

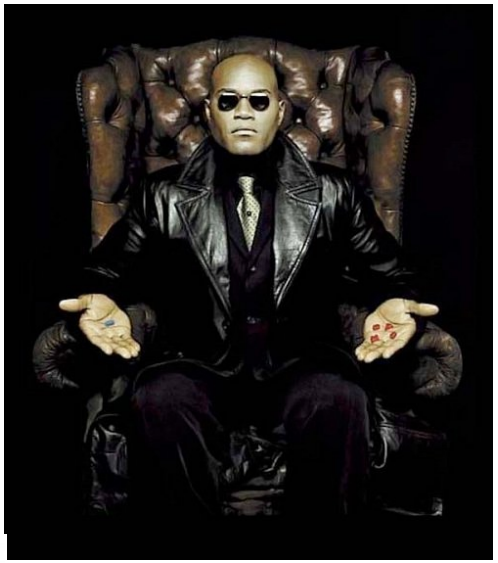


"The red pill is 10 BTC"



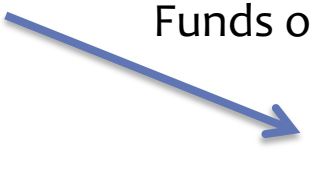
Escrow Transactions

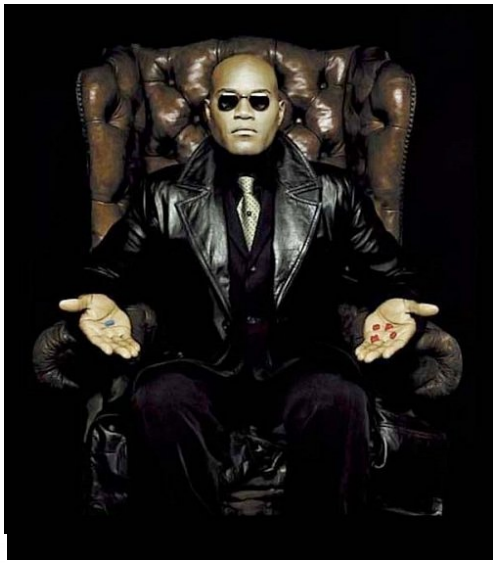




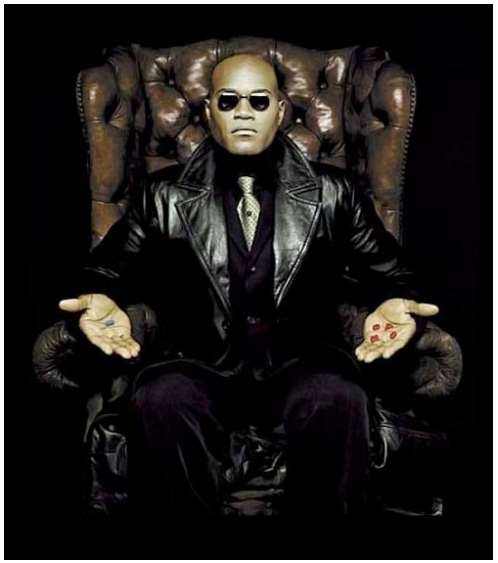
Escrow Transactions

Funds ok

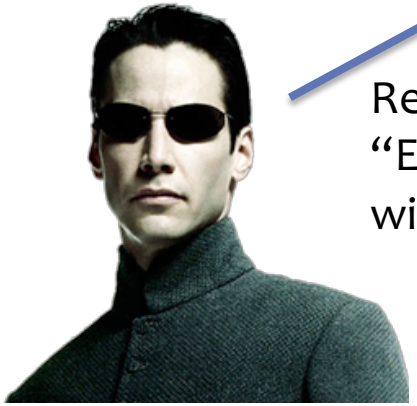




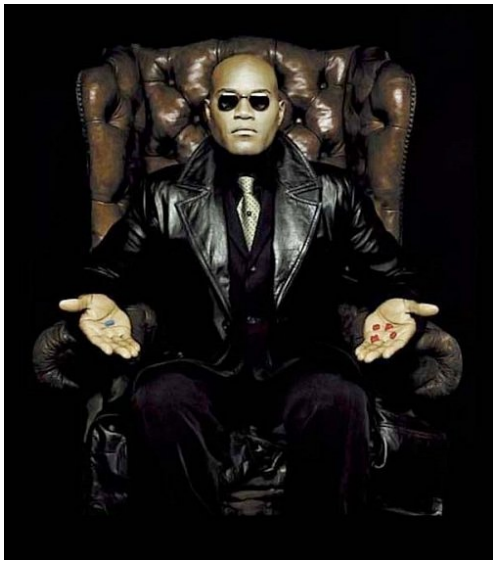
Escrow Transactions



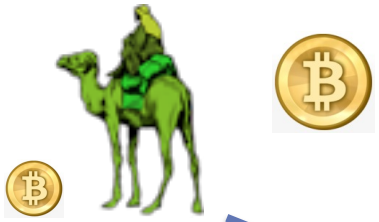
Escrow Transactions



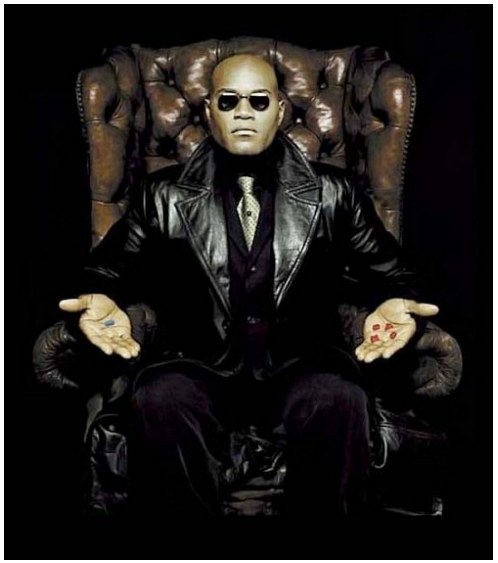
Received
"Excellent seller, would do business with again"



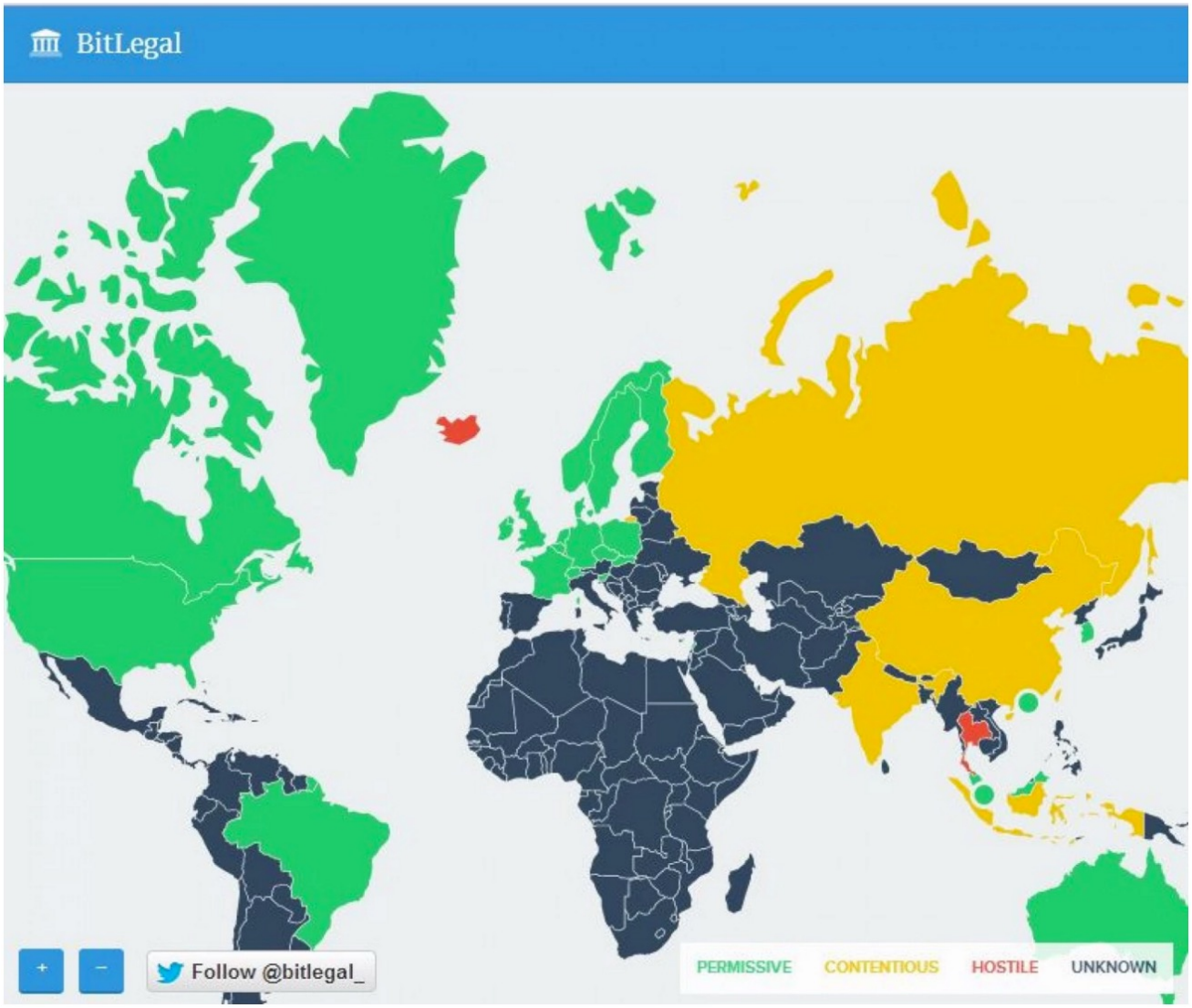
Escrow Transactions



Deposit 9 BTC



Bitcoin Regulation



Bitcoin Regulation

- **Is Bitcoin a currency, a commodity, or a security? Is Bitcoin a payments network, a protocol, or a digital bank of sorts**
- **Against**
  - No protections for consumers (Mt. Gox lost 850,000 bitcoins).
  - Used by criminals in dark markets
- **For**
  - Freedom
  - Transformative technology
- **New York becomes the first state to regulate bitcoin**
  - BitLicense Regulatory Framework

Part IV: Anonymity?

Pseudonymity vs Anonymity

- **Wallets are public/private key pairs**
  - Can create as many as you want
  - Think of them as zero-cost pseudonyms
- **There is no central authority issuing Bitcoins or vetting transactions**
- **This means Bitcoin is anonymous, right?**

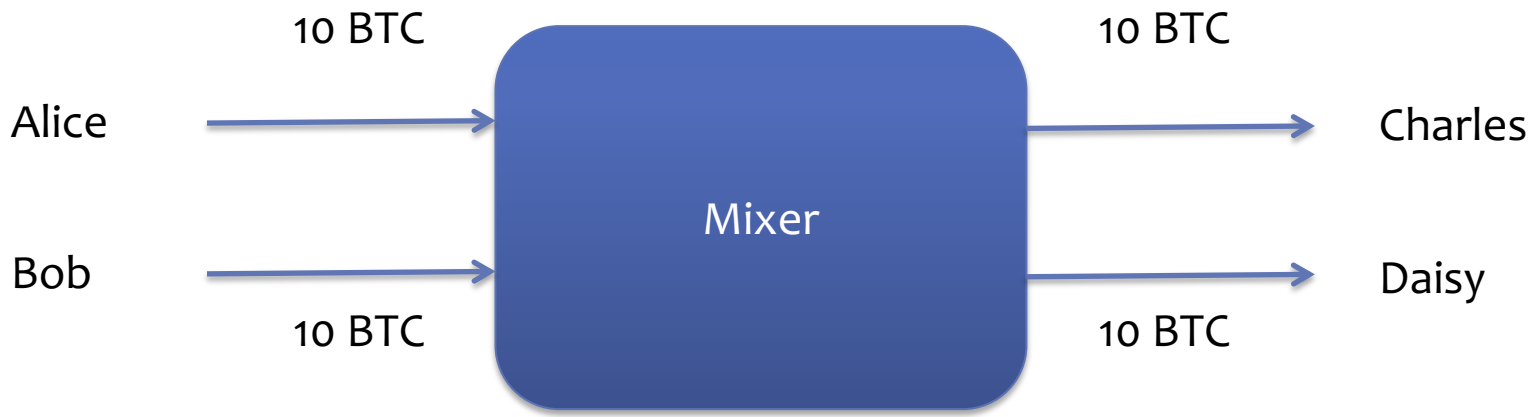
NO!

Bitcoin Tracing

- **Anonymity here implies un-linkability of transactions**
- **The entire ledger of all transactions is available, forever**
  - Technically in a compressed form, but transaction chains can all be reconstructed
- **Even if you add intermediary dummy steps wallets, linking the source and the destination of a transaction may be done by graph analysis…**
  - Something that computer scientists know how to do!
    - Reid & Harrigan, 2011
    - Shamir & Ron, 2012
    - Meiklejohn et al., 2013
- **Families of wallets can be pooled together as belonging to the same actual user…**
- **…and if somehow you can get the user's identity, the game is over**

Anonymizing Bitcoin

- **Mixers**



- **Did Alice give 10 BTC to Charles or Daisy?**

Anonymizing Bitcoin

- **Mixers in practice**

- **Need to also introduce arbitrary delays**
- **Introduction of change addresses, etc**
- **Mixer can be dishonest!**

Anonymizing Bitcoin

- **It's unclear how good existing Bitcoin mixers are**
  - Key difference with message mixing (Tor, mixnets)
    - You can't implement arbitrary "padding" – money has to go somewhere eventually
  - Possible measure: taint
    - Amount of money that can be traced back to a given source
  - Recent research (Meiklejohn et al.) suggests existing mixers are not effective or downright dishonest
- **Open problem: is it possible to design a (distributed) mixing algorithm that provides strong unlinkability guarantees?**

Ethereum Smart Contracts

Ethereum

- **2014: Whitepaper released, crowdsale**
- **Crypto-currency and more**
- **Similar to bitcoin**
  - Use public blockchain as ledger
  - Each block contains several transactions
  - Proof of work
- **Different from bitcoin**
  - Transactions can include Turing-complete programs that run when blocks are processed (Solidity language)
  - Helps developers build de-centralized applications

Transaction & Contracts: Accounts

- **Externally owned accounts (similar to wallet in Bitcoin)**
- **Contract accounts (controlled by smart contract programs)**
- **Send *ether* to contracts, send money from contracts to externally owned accounts**
  - examples in the homework

For more readings: https://ethereum.org/en/developers/docs/smart-contracts/

A Smart Contract

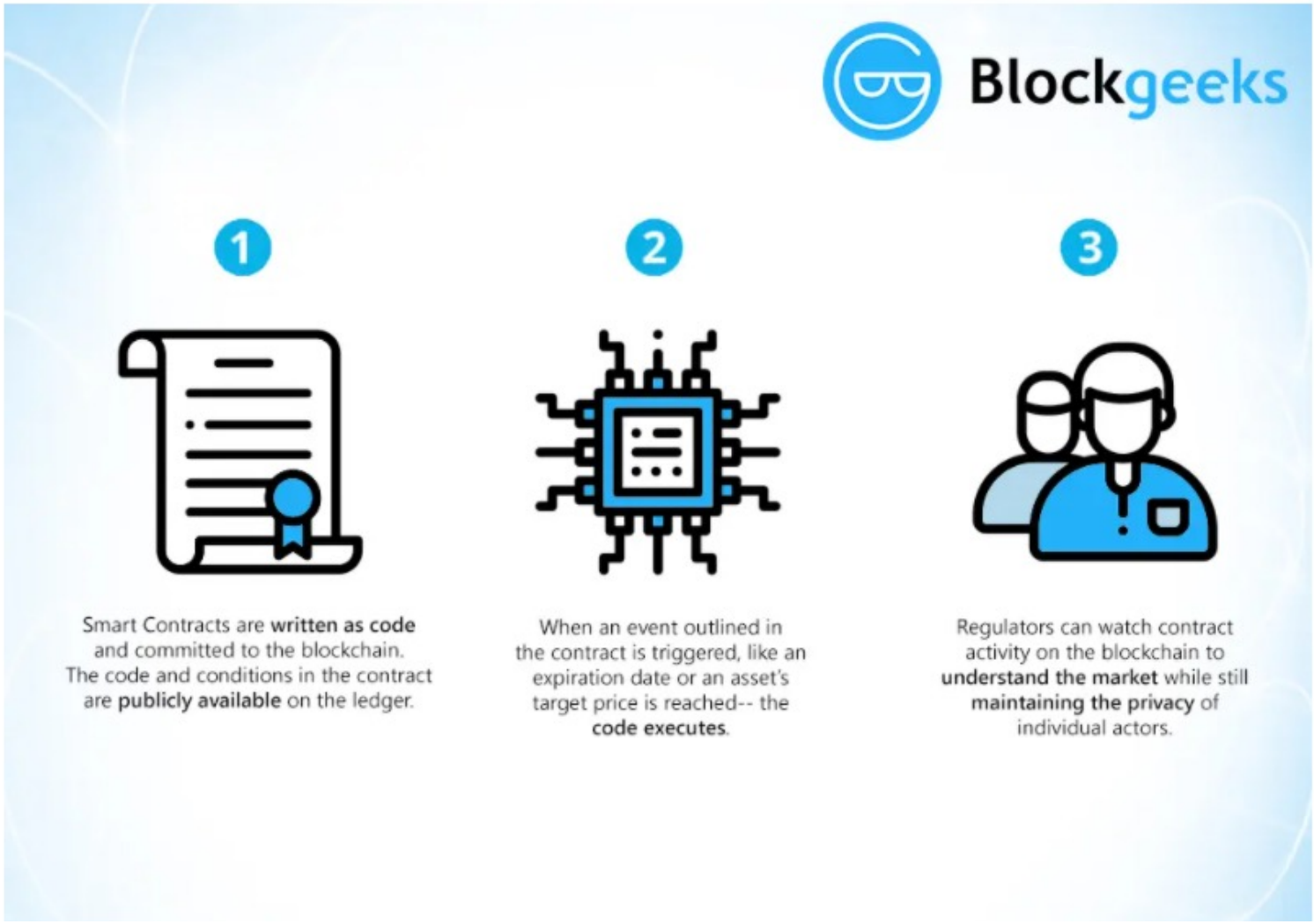
- **A program that runs on the blockchain**
- **Collection of code (its functions) and data (state)**
- **They have a balance and can send transactions**
- **Not controlled by the user**
  - Instead, deployed to the network
  - Run as programmed
- **User accounts interact with a smart contract**
  - Submitting transactions that execute a function defined on the smart contract
- **Can define rules and enforce rules via code**

For more readings: https://ethereum.org/en/developers/docs/smart-contracts/

Transaction & Contracts: Gas

- **What if someone writes a contract that never terminates?**
- **Gas: fuel for executing transactions and contracts**
  - Submitting transactions and contracts to the blockchain has an associated "gas" cost paid in Ether based on the complexity of the operations.

Why Smart Contracts?



Source: https://blockgeeks.com/guides/smart-contracts/

Solidity: Basics (v0.5.12)

```
contract Coin {
        // The keyword "public" makes those variables easily readable from outside.
        address public minter;
        mapping (address => uint) public balances;

        // Events allow light clients to react to changes efficiently.
        event Sent(address from, address to, uint amount);

        // This is the constructor whose code is  run only when the contract is created.
        constructor() public { minter = msg.sender; }

    // Sends an amount of newly created coins to an address; can only be called by the contract creator.
        function mint(address receiver, uint amount) public {
            require(msg.sender == minter);
            require(amount < 1e60);
            balances[receiver] += amount;  }
        // Sends an amount of existing coins from any caller to an address.
        function send(address receiver, uint amount) public {
            require(amount <= balances[msg.sender], "Insufficient balance.");
            balances[msg.sender] -= amount;
            balances[receiver] += amount;
            emit Sent(msg.sender, receiver, amount); }
}
```

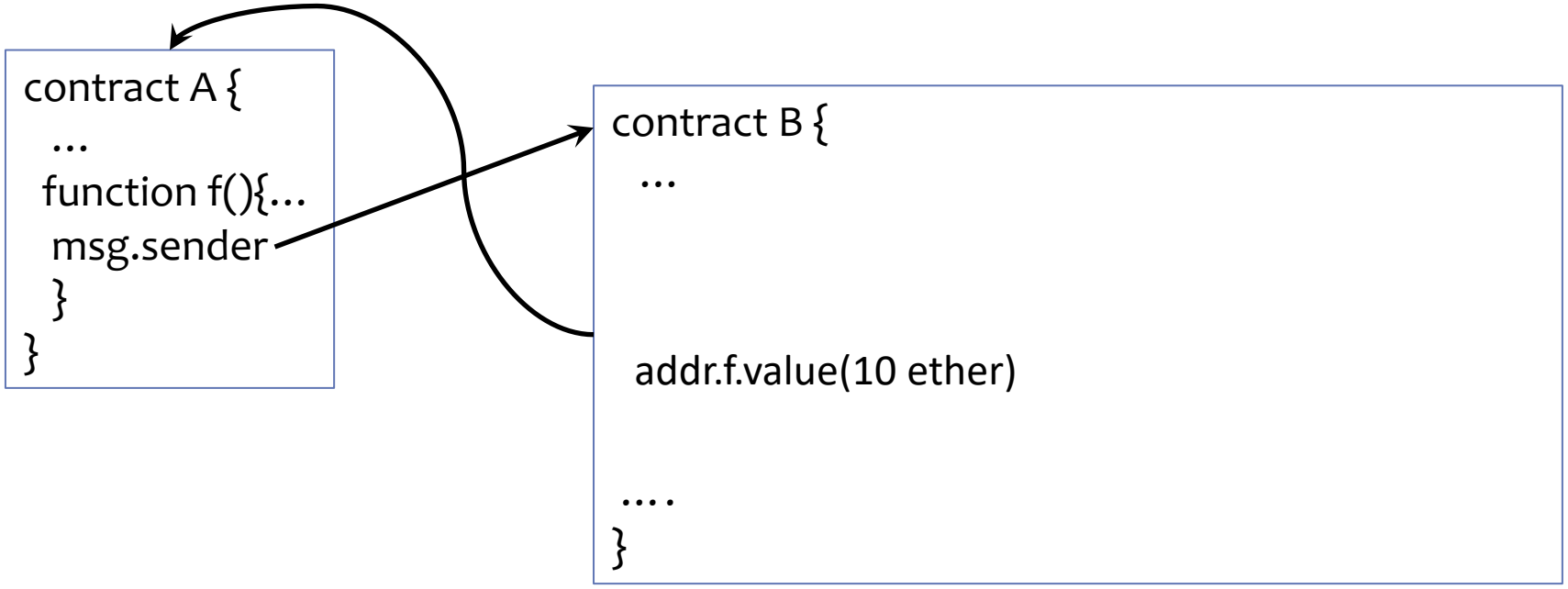
160-bit value, no arithmetic operations

permanently stores address of the contract creator

Only creator can call mint

Only maximum amount of tokens

Transactions & Contracts: distributed applications

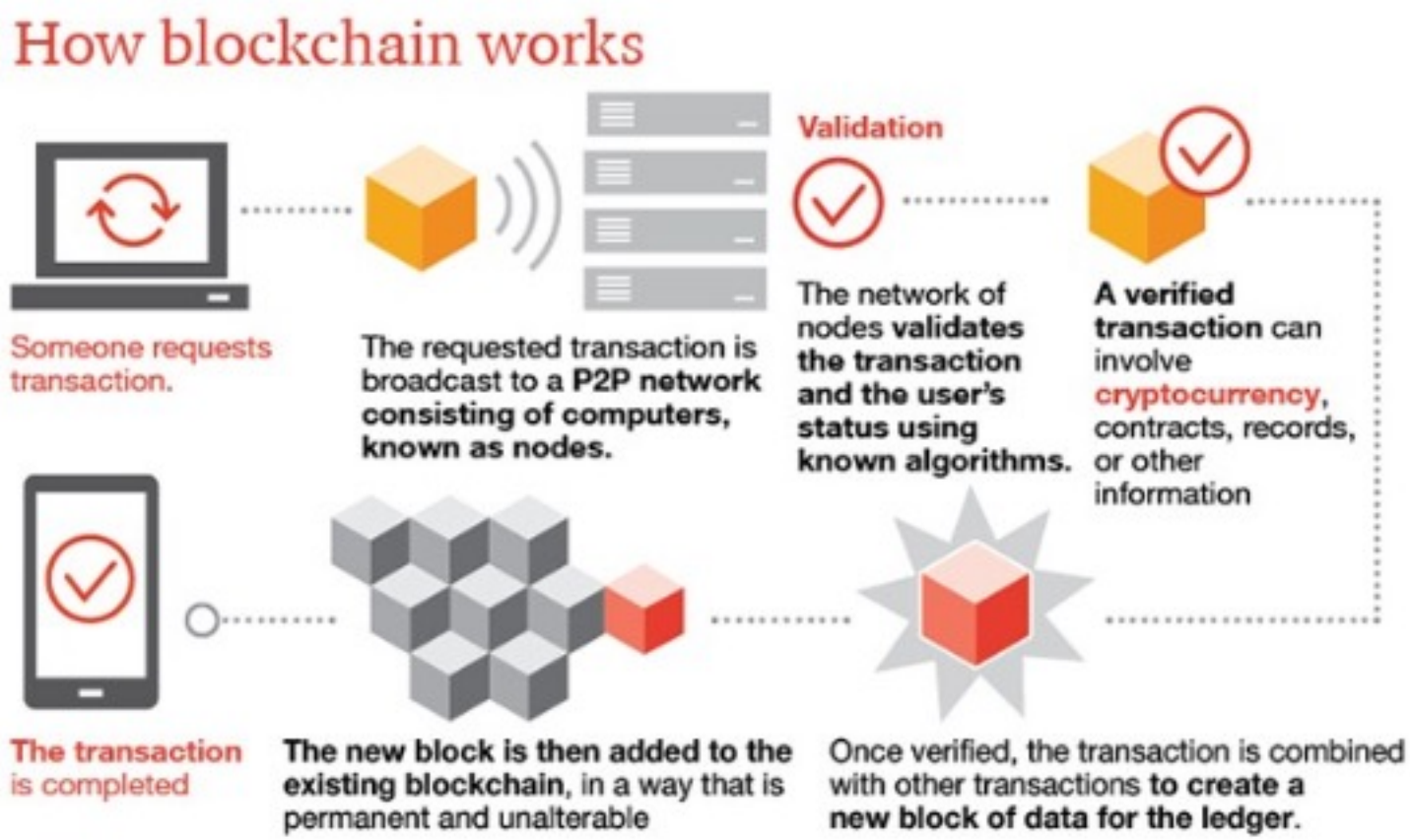


Solidity: Fallback Functions

- **A contract can have exactly one unnamed function, which is called fallback function**
  - function(){….}
- **It is called when**
  - a function f is called but f does not match any function name in the contract
  - Or no function name is supplied
- addr.call.value(x)()
  - Invoke the fallback function at addr and send x ether to it

The Blockchain Technology

Blockchain Overview



Source: pwc, United States

New Application for Blockchain

- **Research in interest into good applications of Blockchain and smart contracts**
  - Autonomous cars
  - Financial services (reduce transaction costs)
  - Voting (cast votes electronically, immediate verifiable results)
  - Healthcare
    - Share patient information with multiple providers
    - Preserve privacy

Memory-Based Proof of work

- **Goal: performance is less sensitive to hardware specs**
- **Computation speed is bound by main memory accesses**
- **Example Algorithms**
  - CryptoNight
    - Released in 2013 as part of CryptoNote blockchain
    - Memory hard-loop; sequence of random reads and writes in a scratchpad (small memory area)
    - Fits on CPU cache
  - Ethash
    - Used by Ethereum.
    - Memory hard-loop randomly reads DAG area (memory slices larger than scratchpad)
  - Cuckoo Cycle
    - Solves a PoW puzzle that finds cycles or other structures in large random graphs

Proof-of-Stake

- **Current common consensus algorithm is proof of work(PoW)**
  - Energy consumption
  - No penalty for fraud
  - Miners increase processing power to improve their chances
- **Proof-of-Stake**
  - More energy efficient
  - Removes the high-powered computing from the consensus algorithm
  - More complicated
    - security?
  - “Validators” set aside a certain amount as collateral

How PoS Works

- **“Validator” instead of “miner”**
- **The validator has an economic state**
  - The “stake” their funds on the blocks that they believe are valid
- **Validators take turns to propose and vote**
  - Votes are weighed by size of collateral amount
- **Anyone can become a validator**
  - If and only if they hold some ether as collateral amount
- **An algorithm determines the validators to be chosen for a block**
- **Validators no longer increase processing power**
  - Increase “stake” to improve chances
- **Verifying bad (fraudulent) blocks can result in loss of stake**

Takeaway Slide

- **Bitcoins, Ethereum and other cryptocurrencies are applications of crypto**
  - Decentralized Peer-to-peer digital payment systems
- **Eventually, the blockchain technology is now attractive to other applications**
- **Security challenges**
  - Attacks (e.g. 51%)
  - Anonymity
  - Others?
- **Other challenges include**
  - Computation recourses
  - Environmental impact
- **Proof-of-work and proof-of-stake**
  - An ongoing area of research and development