Bitcoin and Cryptocurrencies

- Lecture 3: Bitcoin Mechanics & Optimizations: A Technical Overview

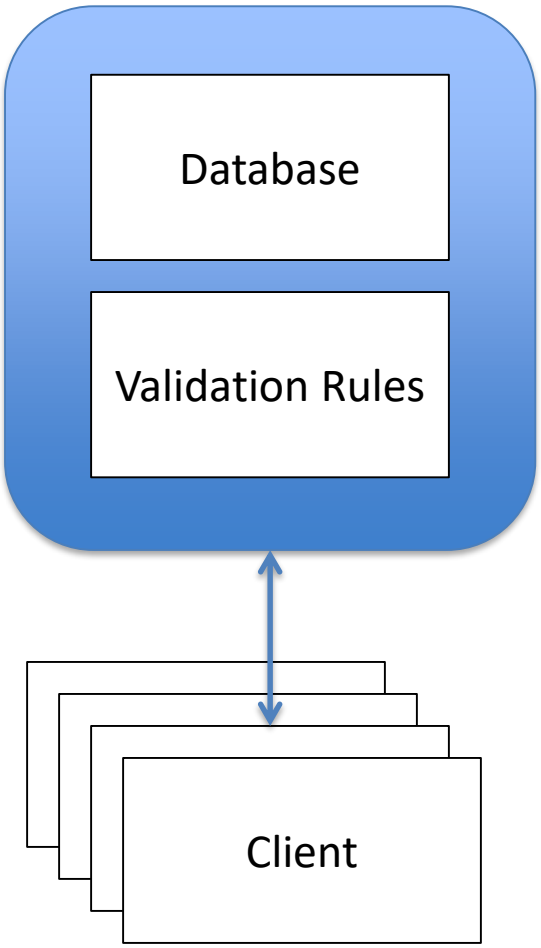
- Professor Radjabov Mukhammad

Goals

- Get to a technical understanding of:
  - Blockchains
  - Bitcoin
  - Smart contracts
- Why they are important and how cryptography enables these mechanisms

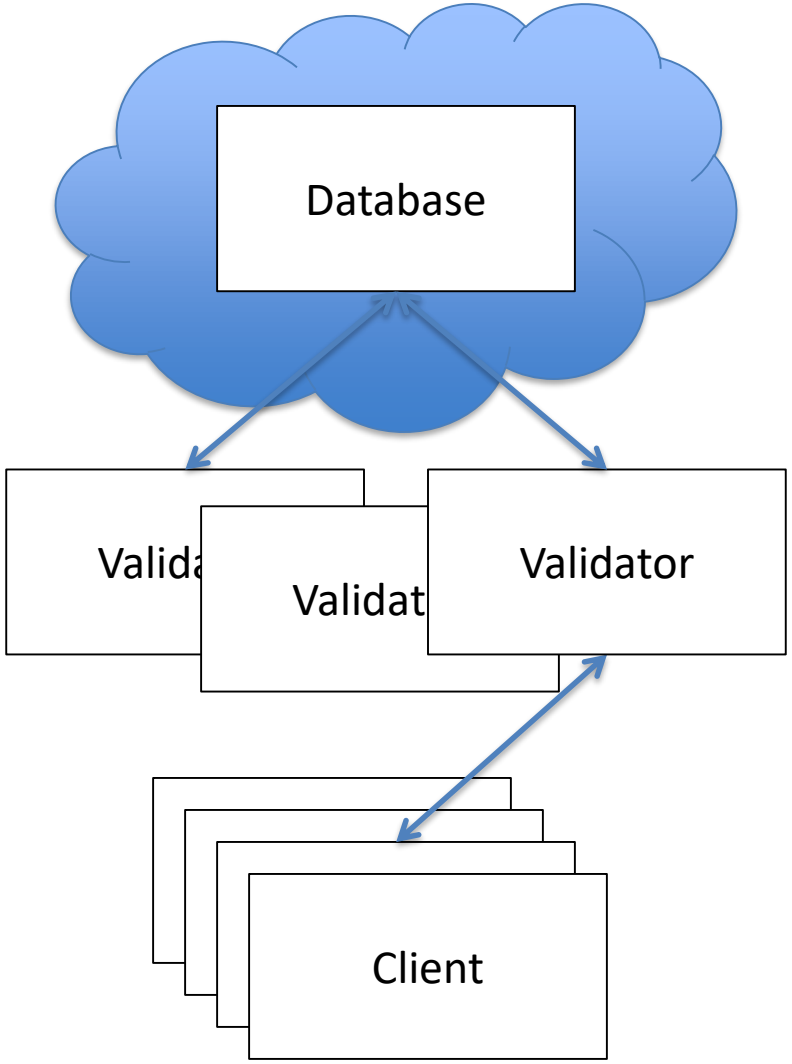
Note: This will be somewhat BTC heavy, but most rules apply to private chains.

What do blockchains replace?



- Access protected writes to an authoritative database
- Transactions, timestamping, contracts, etc.

What do blockchains replace?



- Authoritative access control replaced with distributed consensus
- Database state dependent upon majority agreement of update validity

Why?

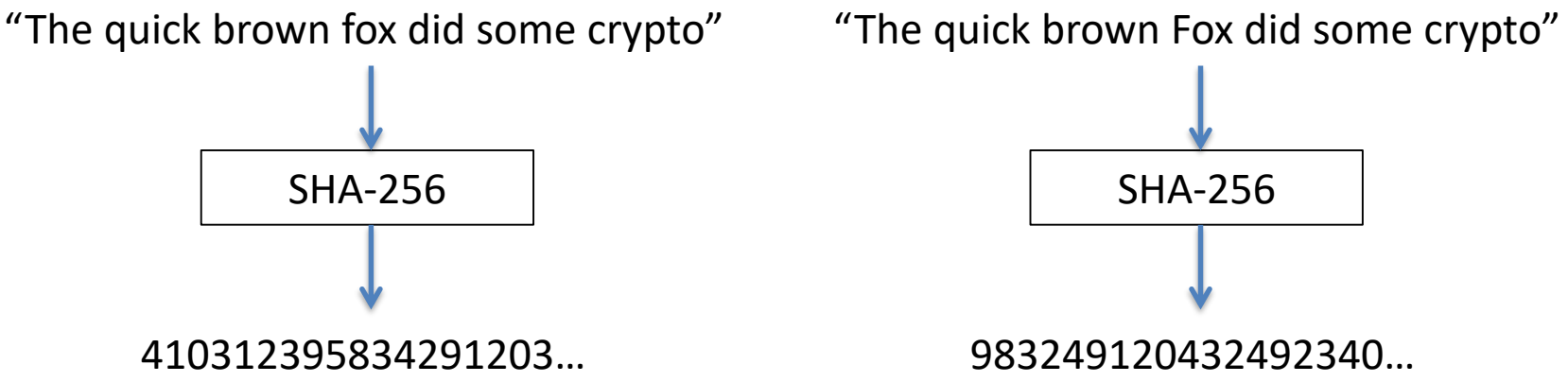
- Authority seems to work pretty well
- Distributed consensus can allow:
  - Distrustful parties to maintain clean state
  - Completely unambiguous rules about validity
  - Removing authentication and identity as essential
  - Perhaps solves other problems also….

Welcome to Cryptoland

- Ugh. Do I *have* to learn all this detail?
- Yes. The laws of crypto are the laws of blockchains and bitcoin. Not understanding this will lead to bad intuitions about what this stuff can and cannot do.
- Luckily, only need to understand two laws of cryptography (and believe that people are motivated by incentives, I guess)
- We'll do this by building increasingly complex games that simulate parts of bitcoin and blockchains.

Ingredient #1: Hashes

- A hash function (like SHA-256) takes a block of data in, and produces an effectively random fixed size integer.
- Any change to the input randomizes it



Hash-based Proof of Work

- Can't compute an input from an output
- To find a hash with N zeros at the start of the input, requires 2^N computations…proves computational work
- If we hash an incrementing "nonce" as the hash input, we can go looking for zeros:

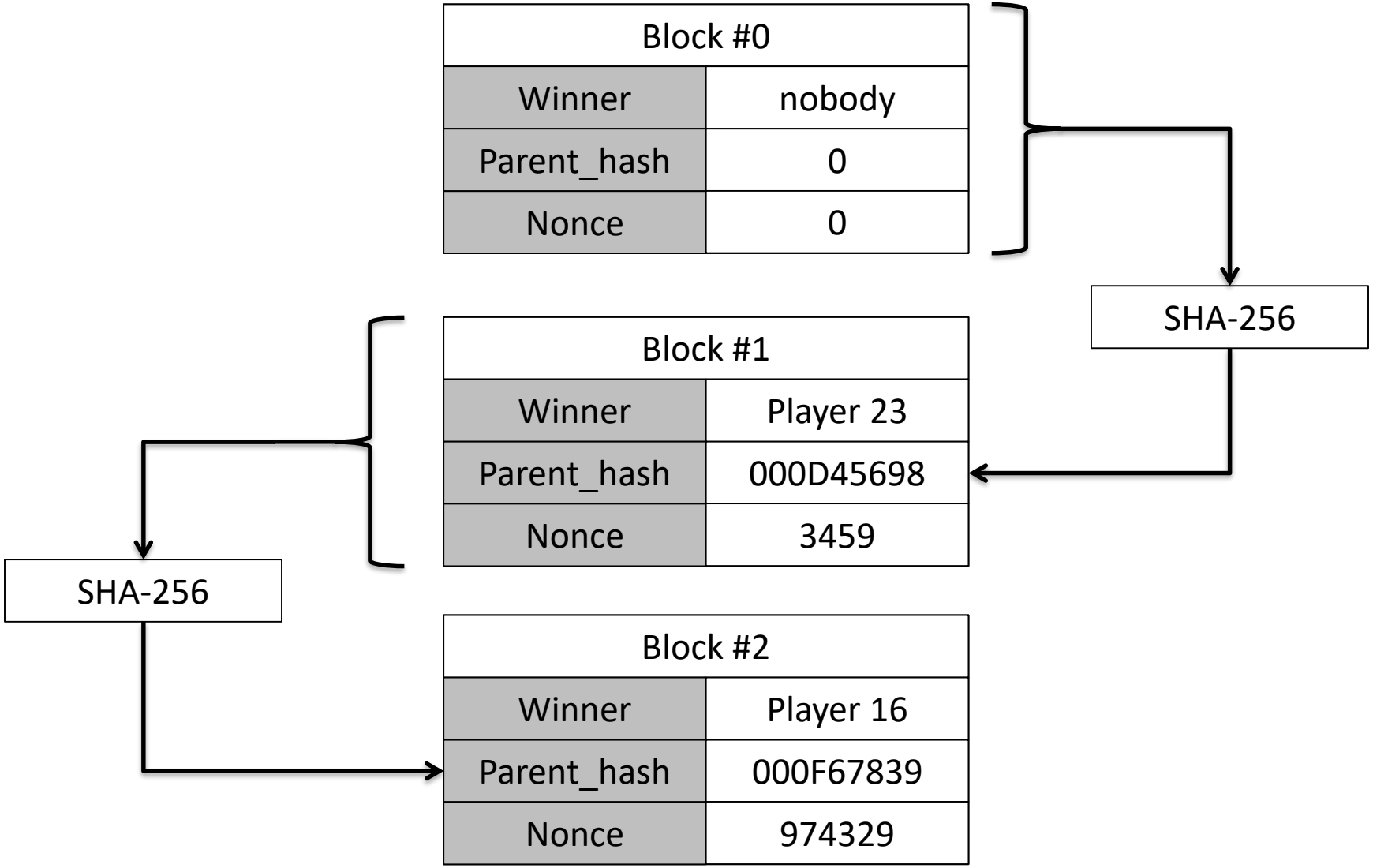
in 3e-05 seconds, nonce = 0 yielded 0 zeros. value = 4c8f1205f49e70248939df9c7b704ace62c2245aba9e81641edf…
in 0.000138 seconds, nonce = 12 yielded 1 zeros. value = **0**5017256be77ad2985b36e75e486af325a620a9f29c54…
in 0.000482 seconds, nonce = 112 yielded 2 zeros. value = **00**ae7e0956382f55567d0ed9311cfd41dd2cf5f0a7137…
in 0.014505 seconds, nonce = 3728 yielded 3 zeros. value = **000**b5a6cfc0f076cd81ed3a60682063887cf055e47b…
in 0.595024 seconds, nonce = 181747 yielded 4 zeros. value = **0000**af058b74703b55e27437b89b1ebcc46f45ce55d6….
in 3.491151 seconds, nonce = 1037701 yielded 5 zeros. value = **00000**e55bd0d2027f3024c378e0cc511548c94fbeed0e….
in 32.006105 seconds, nonce = 9913520 yielded 6 zeros. value = **000000**77a77854ee39dc0dc996dea72dad8852afbde6….
in 590.89462 seconds, nonce = 186867248 yielded 7 zeros. value = **0000000**225060b16117b23dbea9ce6be86ac439d….
in 4686.171007 seconds, nonce = 1424462909 yielded 8 zeros. value = **00000000**2dd743724609a9f57260e2492908d….

We can now make this into a distributed "game"

Game #1 – The Chain Race

- A parameter N sets the difficulty of the game
- Players get a list of blocks, with:
  - A block number
  - A winner number
  - A nonce value
  - A hash of the previous block
  - A hash of the current block with N zeros
- Players accumulate points by creating blocks
  - Hash the previous block
  - Find a hash of the new block with enough zeros
  - They then transmit this block to everyone

Game #1 – The Chain Race



The Nonce / Hash Loop

- The algorithm to make a new block:

1. Verify the hashes of all the previous blocks
2. Build a new block with a random nonce
3. Hash the new block. Does it have N zeros?
   - No? Go back to Step 2
   - Yes? Send your new block to everyone!

- Note that as a result of step #1, you can find out how many points anyone has by counting how many blocks they have won

How hard is the game?

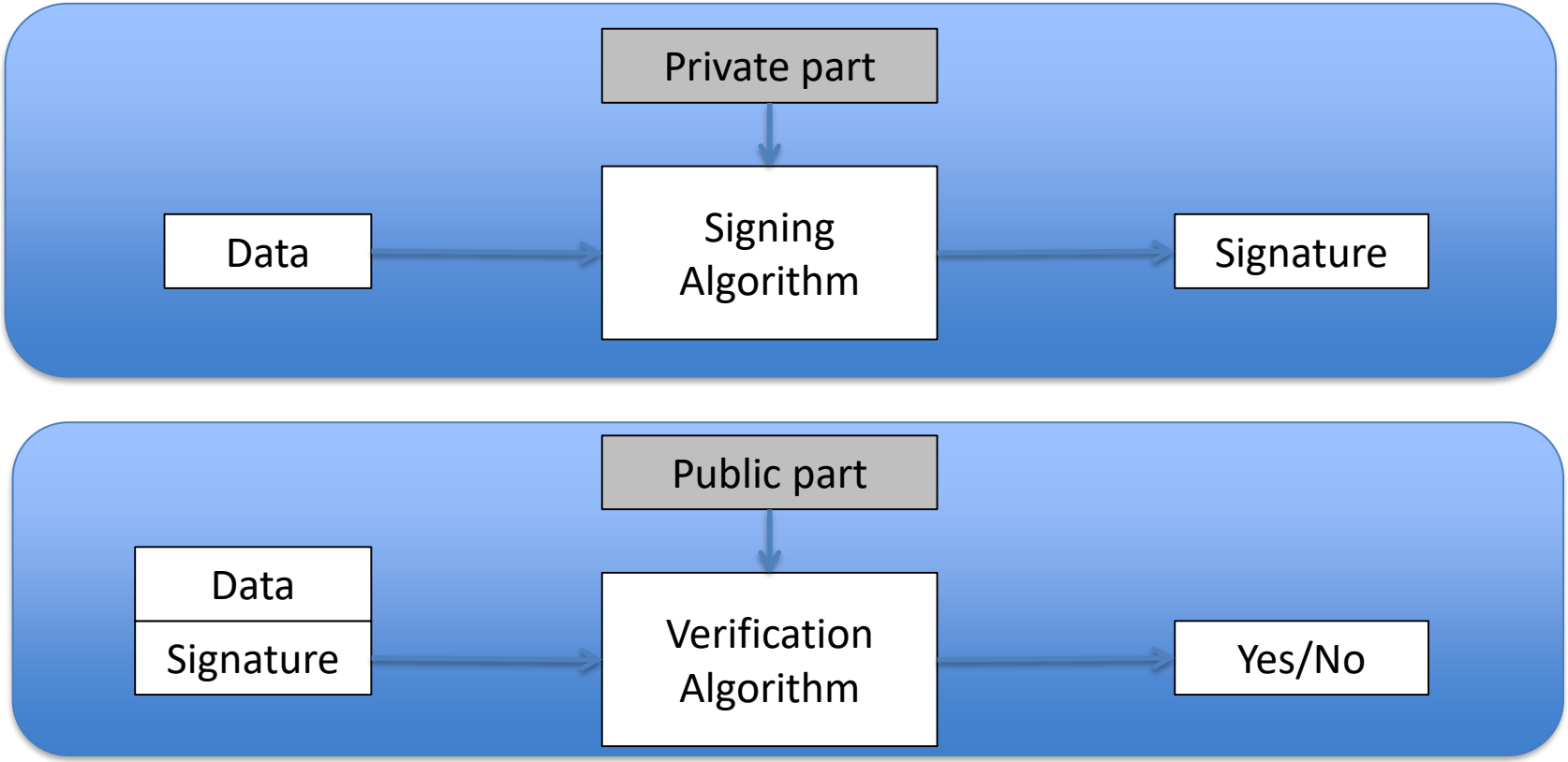
- For N zeros, because the SHA-256 output is effectively random, getting zero bits = same as flipping a coin and getting N heads in a row
- For N zeros, have to try $2^N/2$ nonces…
  - N=1 …. Try 1 nonce
  - N = 16 … Try 32768 nonces
  - N = 32 … Try 2 billion nonces
- Winning a block proves the player did work

What about cheaters?

- One way to cheat: make up a fake hash!
- What happens then?
  - Step 1 in the algorithm will fail for all the other players.
  - Other players will not use your block, making it not part of the chain

Ingredient #2: Signatures

Signing key	
Public part	454F4D3E1..
Private part	56F23F2D..



Trading points

Make player ID = public key

We can now make trades by signing messages and sending them to everyone

Signed trades are:

- Unalterable
- Verifiable by anyone
- From key to key, not tied to a "real" identity

Trade #8423	
From	Public_key1
To	Public_key2
Amount	50 points
SIgnature	345349354

Trade #8424	
From	Public_key2
To	Public_key3
Amount	50 points
SIgnature	734589345

Game #2 – The Race with Trades

Block #0	
Winner Key	nobody
Parent_hash	0
Nonce	0

Block #1	
Winner Key	045F45F…
Parent_hash	000D45698
Nonce	3459

Block #2	
Winner Key	8234DB4…
Parent_hash	000F67839
Nonce	3459

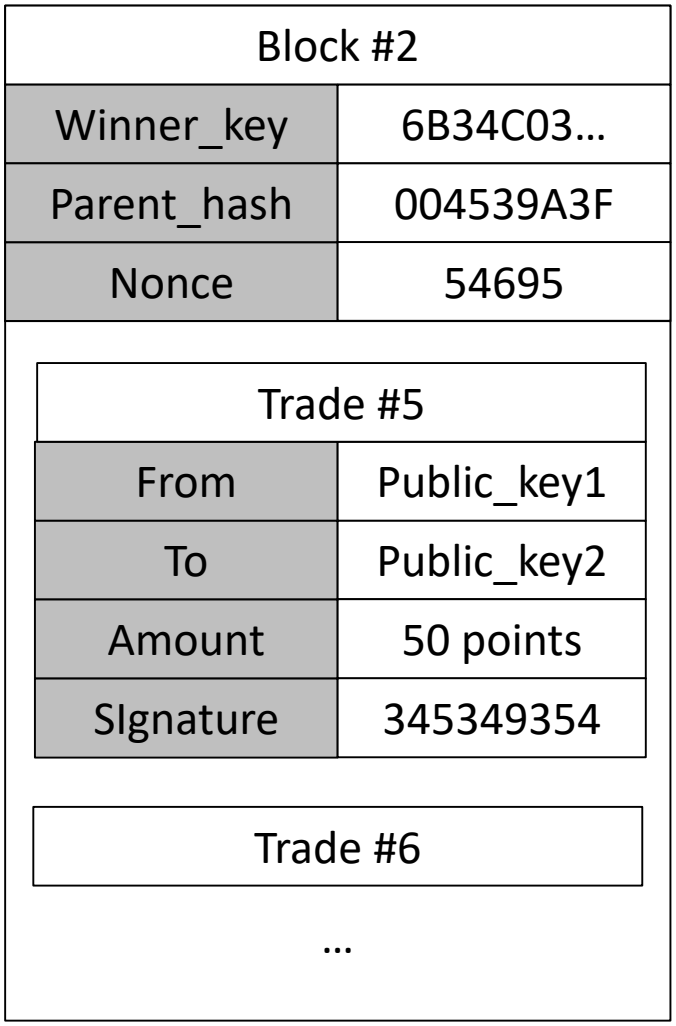
Trade #8423	
From	Public_key1
To	Public_key2
Amount	50 points
SIgnature	345349354

Trade #8424	
From	Public_key2
To	Public_key3
Amount	50 points
SIgnature	734589345

Cheating!

- Can’t alter transactions, but sneaky players could trade extra points by sending more trades than they have points to cover
- “Overtrading” not resolvable, because don’t have an absolute unalterable source of time
- Let’s fix this in game #3…
  - Critical insight: Put the trades in the blocks.

Game #3 – No-cheating Social



Game #3 is magic…

- Players expend effort to get points
- Players can trade points securely
  - Signatures prevent alteration of trades
  - Signatures authenticate the origin of trades
- Players can detect overtrading
  - Players will decline to extend the game on blocks with overtrades
  - If they do, they are wasting effort, since other players will not extend the game on their blocks

Game #3 Problems

- Why bother to put trades in your block?
- Lets solve this by adding a fee in transactions
  - Incent players to add transactions by giving them points per trade added
  - Two ways to get points!
- Why limit trades to players?
  - Let players send points to anyone with a public key….
  - This is now a global transaction system

Game #4 – Simplified Bitcoin

- Players = “miners”, points = “bitcoins”
- Transactions send value (bitcoins) from key to key
- The chain race game (blockchain) prevents overspending without a central authority
- Game rules = bitcoin node code, changes by miner consensus
- Player consensus replaces authority
  - Number of coins (limit to 21 million)
  - Reward per block
  - How difficulty grows

Transition to transactions

- Note that player/miners can interact with non-players
- Once a point is created, the recipient can create a transaction to any public key
- Now can extend to trades with non-miner/players
- All points still originate with some block/miner

Anatomy of a Block

Block #404234

Summary	
Number Of Transactions	459
Output Total	3,812.78908631 BTC
Estimated Transaction Volume	815.7381711 BTC
Transaction Fees	0.1059914 BTC
Height	404234 (Main Chain)
Timestamp	2016-03-25 15:52:47
Received Time	2016-03-25 15:52:47
Relayed By	BitFury
Difficulty	165,496,835,118.23
Bits	403088579
Size	704.855 KB
Version	4
Nonce	311538175
Block Reward	25 BTC

Hashes	
Hash	000000000000000000221e92ec5f42f4ccf8ba7ad71020e9dcbeed3f5e484b2f8
Previous Block	0000000000000000060e89871b8a2e9a769ec031ac3fc1da24d00886d5a8f256
Next Block(s)	0000000000000000005687e47a1fa3936b3c7eca894920b30d4904f42faa1df75
Merkle Root	3bef11b868b850a27ca176d8c4a5fb465f71771f9b46ba272dbf6f53d4e1550b

Network Propagation (Click To View)

(from blockchain.info, a great resource for bitcoin info)

Block Transactions

Transactions

4d0452c4fe98178875ede72319ca3162389edd43a22690ebcd49938bbcffd37c			2016-03-25 15:52:47
No Inputs (Newly Generated Coins)		1DrK44np3gMKuvc... (Bitfury)	25.1059914 BTC
			25.1059914 BTC
ed93695feee71a0d115d84e3bfbd759eebc03c3f707b9fdfec6fed3514d204ec			2016-03-25 15:51:26
1BJaAgMK9F31HpTB8yePe69zEqR6cTg9eS		1Lie2o1tAjKxHgRMkFVmJZUMgFbsjummks	1.1269325 BTC
			1.1269325 BTC
53cd4fbc48378eb686873f0f8b1d5cc34dfd0099bcc4cfb46069649fb18fe0e7			2016-03-25 15:51:55
17wLMV3wgDFCn4LQxQsDLrD6KvvVMZSuBi		15PUBY3omSex2kkBNBfEwextZvhRWYevNA 17zLoiL1EEdHkgdpNuagG1vq7Fa6UMyK2h	8.7 BTC 3.37028336 BTC
			12.07028336 BTC

Where are the rules?

- The laws of Bitcoin (or any blockchain) are in the miner nodes
  - Whatever 51% of the miners are running will win
- The source to the node are the law
- How do you change rules?
- What happens if:
  - The crypto breaks?
  - We want to add more coins?
  - We want to change the block format?

Attacks

- What happens if the majority of the players defect?
  - 51% attacks – can extend bad blocks
- How large a body needs to defect?
  - Depending on network, can be 30% or less
  - Sybil attacks

Operational Realities

- Assumes cheap storage and networking
  - Nodes store every transaction ever
  - Transactions and blocks are broadcast
  - Might limit scale...
- Transactions are slow
  - To verify a transaction, have to wait for a public block
- Control of private keys is crucial
  - Lose your private key = unspendable coins
  - Steal your private key = steal coins
  - Blacklisting keys breaks the game
    - Builds a central control locus

Bitcoin Today

- How much player power:
  - Global hashing power just passed 1 Exahash/sec
  - 1,000,000,000,000,000,000 SHA-256 ops/sec
- How many transactions:
  - Approx 185,000 transactions / day
  - About 383,000 BTC exchanged / day
- 1 BTC =~ $420 USD

What a Petahash looks like

Hashnest.com

Hardware Cryptography?

- Is there a place for secure hardware?

Keepkey.com

Beyond Bitcoin

- Transactions don't have to just be transactions
- Transactions can contain:
  - Executable code
    - In fact, BTC transactions are scripts
    - Scripts specify when outputs can be spent
  - Contracts
    - Set conditions for allowing outputs to move
  - Random data to be timestamped
    - "Colored coins" – add data to a transaction
    - Transaction is recorded, so can be a hash of a document or other external data

Private Chains

- Change the game to require signed blocks
- Limit miners to some authorized set
- Useful for adding other rules or preventing block “takeovers”
- Approach being used to trade securities on a blockchain
- Same crypto physics apply….

For More Information

- Blockchain.info – a view onto the BTC chain
- Ethereum.org – blockchain programming
- Hyperledger.org – standards for blockchains
- R3CEV.com – bank consortium for chains
- Bank of England Distributed Ledgers
  - http://www.bankofengland.co.uk/banknotes/Pages/digitalcurrencies/default.aspx

For a deeper understanding

- Google “Princeton Bitcoin Book” – a free and excellent technical exploration of everything in this presentation
- Associated Coursera course

Reference

- The Bitcoin Standard: The Decentralized Alternative to Central Banking – Illustrated, April 24, 2018 by Saifedean Ammous
- The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)
- Blockchain Bubble or Revolution: The Future of Bitcoin, Blockchains, and Cryptocurrencies – June 12, 2019 by Neel Mehta (Author), Aditya Agashe (Author), Parth Detroja (Author)
- Cryptocurrency Investing For Dummies – March 6, 2019 by Kiana Danial
- Cryptocurrency Mining For Dummies– Illustrated, December 5, 2019 by Peter Kent
- Cryptocurrency Mining: A Complete Beginners Guide to Mining Cryptocurrencies, Including Bitcoin, Litecoin, Ethereum, Altcoin, Monero, and Others – February 21, 2018 by Crypto Tech Academy (Author)