Bitcoin Clarity

Kiara Bickers

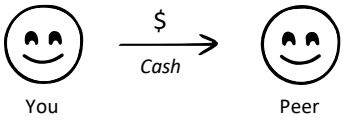
The Complete Beginners Guide to Understanding

Challenges in Understanding Bitcoin

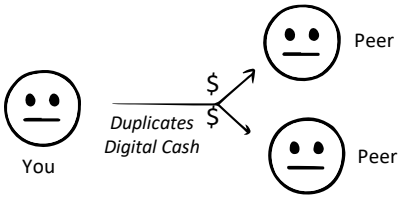
"If you don't believe me or don't get it, I don't have time to try to convince you, sorry."

– Satoshi Nakamoto, pseudonymous Bitcoin creator

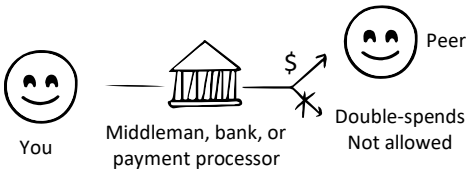
1.1 A one-to-one, peer-to-peer cash transaction:



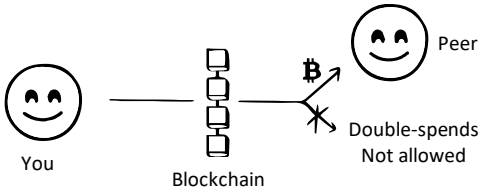
1.2 The same unit of digital currency being double spent:



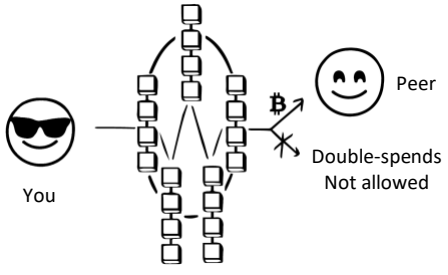
1.3 The payment processor solution:



1.4 Bitcoin's double-spend solution:

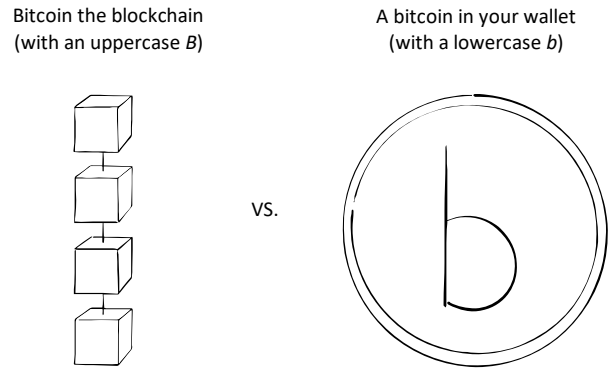


1.5 The peer-to-peer network of Bitcoin users:

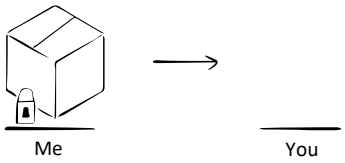


The peer-to-peer network of
independent blockchains in Bitcoin

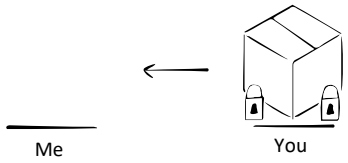
1.6 Bitcoin VS. bitcoin:



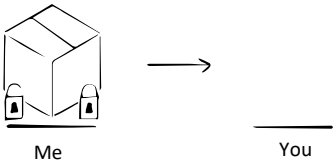
1.7 First, I put a secret in a box, lock it, then send the box to you.



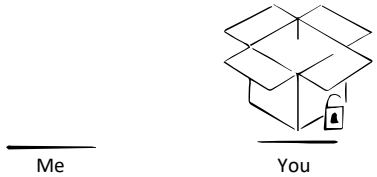
When you get the box, you put your own lock on it and then send the box, with both of our locks on it, back to me.



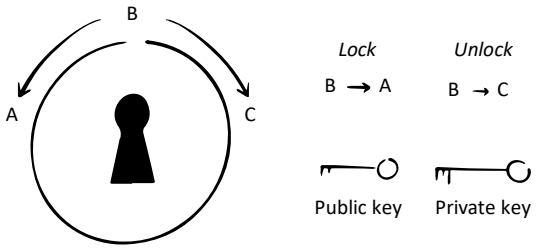
When I get the box, I take my lock off and send it back to you with only your lock on it.



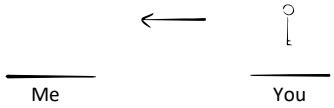
At this point only your lock is left on, so you can unlock the box and claim the secret for yourself.



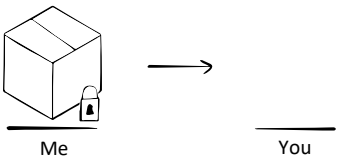
1.8 Public-key cryptography model:



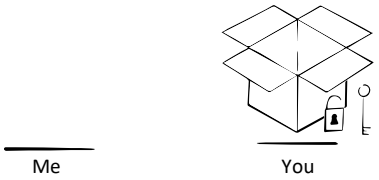
1.9 You send me a copy of your public key.



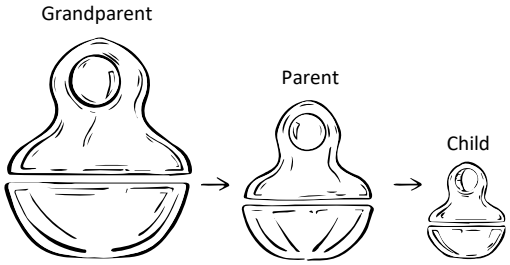
I put bitcoin in a box and lock it using your public key, then send the box back to you.



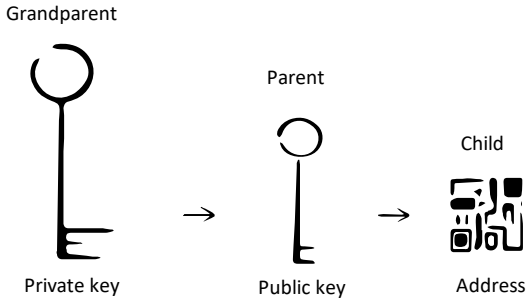
When you get the box, you open it with your private key and claim the bitcoin I sent you.



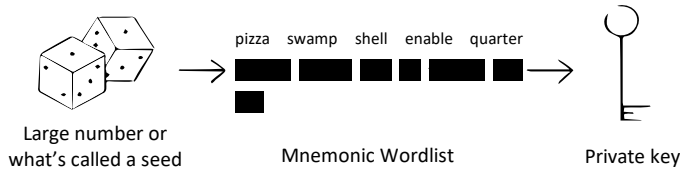
1.10 The inheritance of nested Russian dolls:



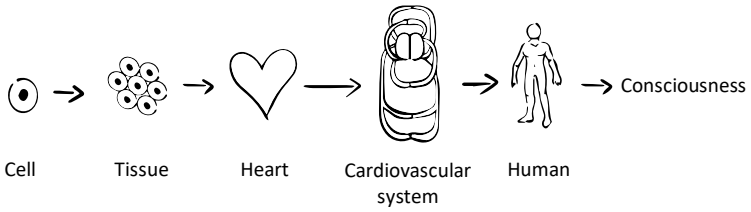
1.11 Key derivation from private keys to public keys to addresses:



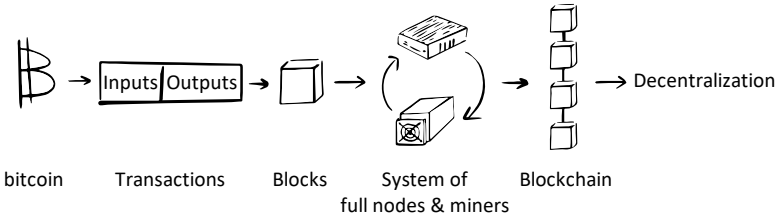
1.12 Bitcoin private keys represented in several different ways:



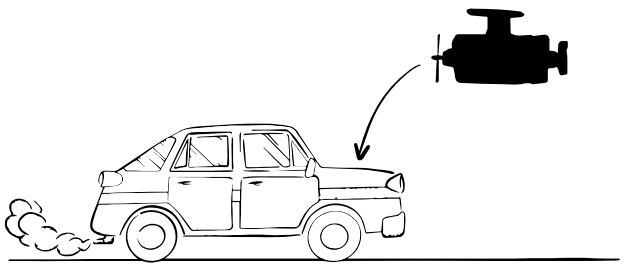
1.13 Consciousness is the basic emergent property of organisms:



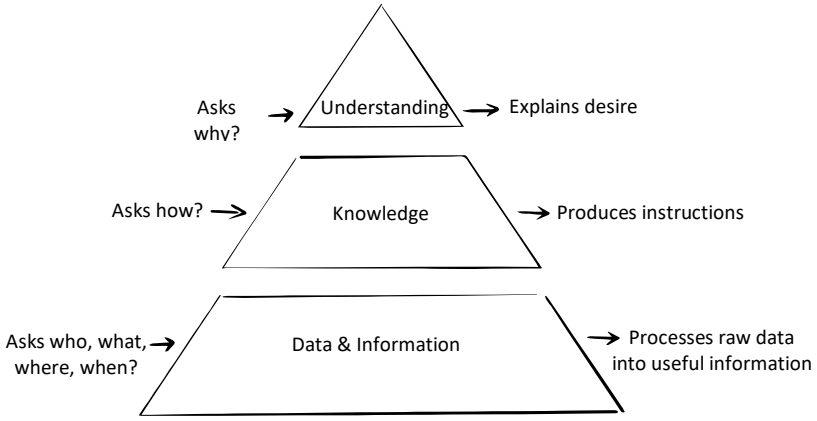
1.14 Decentralization is the fundamental emergent property of Bitcoin:



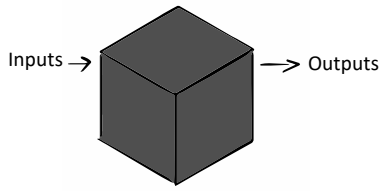
1.15 Systems thinking How VS. Why:



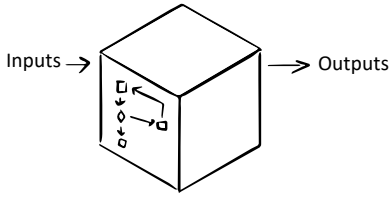
1.16 The difference between knowledge and understanding:



1.17 Black box thinking:



1.18 Black box thinking exposed:

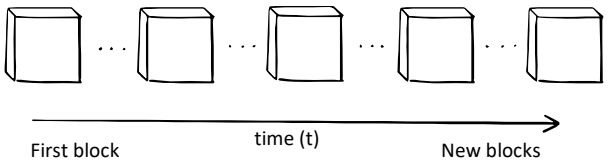


A Trust "less" Timechain

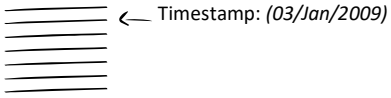
"Care must always be taken when generalizing, and it's important to remember that no two different things are the same—even when we call them the same name; especially when what counts depends so tremendously on the details."

– Greg Maxwell aka gmax, Bitcoin developer

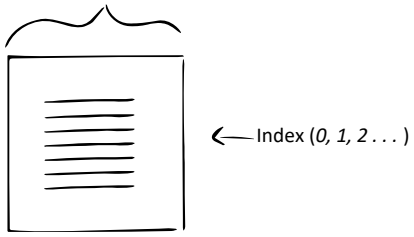
2.1 Bitcoin as a Blockchain:



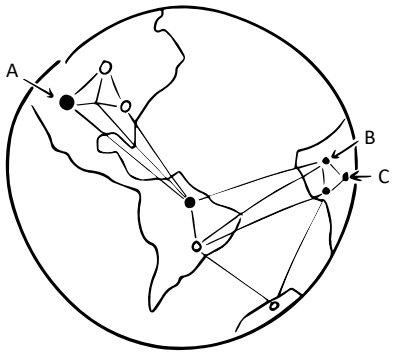
2.2 If transactions were individually timestamped:



2.3 A timestamp applied to the entire block:

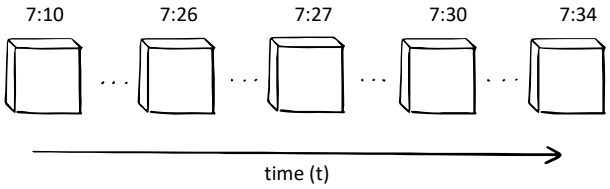


2.4 Consider the physical distance between computers:

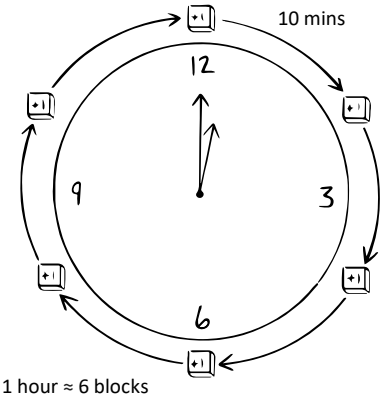


Transaction Order /	Alice's Node /	Bob's Node /	Charlie's Node
Transaction 1	A → B	B → A	B → A
Transaction 2	B → A	A → B	A → B

2.5 Timestamps are applied to each block in the blockchain:

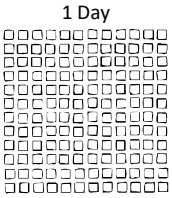


2.6 The blockchain visualized as a timechain:

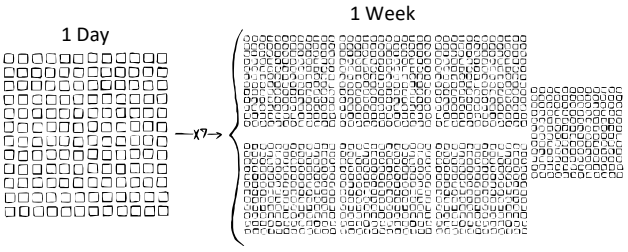


10 min blocks, results in roughly six blocks every hour.

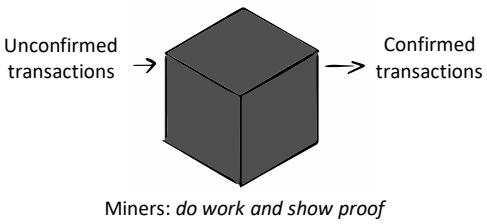
2.7 On average, 144 blocks are added to the blockchain every day:



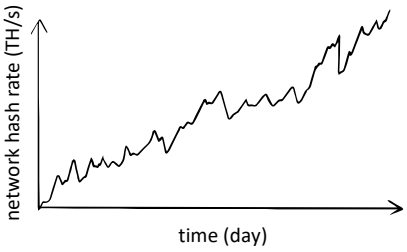
2.8 And 1008 blocks on are added to the blockchain every week:



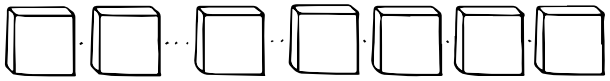
2.9 The role of miners in Proof-of-Work:



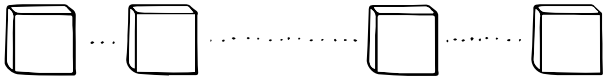
2.10 A graph of network hash rate over time:



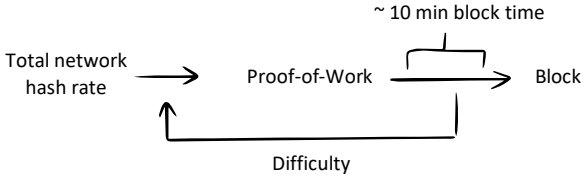
2.11 If a bunch of miners join the network at once, the time between blocks is closer, and transactions are processed more quickly:



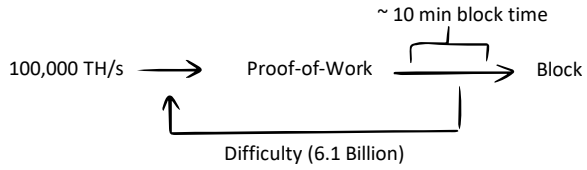
2.12 If a bunch of miners leave the network at once, the time between blocks is further apart, and transactions are processed more slowly:



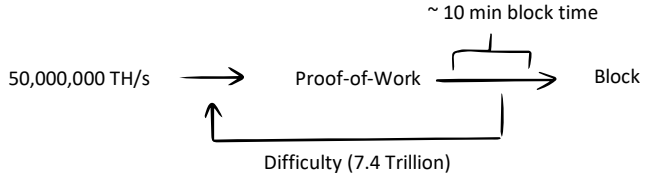
2.13 The control loop in the timechain:



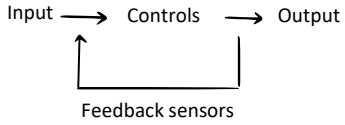
2.14 Network hash rate from the year 2014:



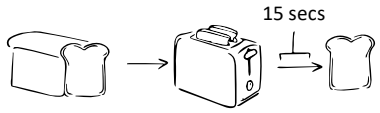
2.15 Network hash rate from the year 2018:



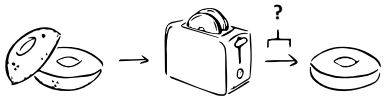
2.16 The generalized feedback control loop:



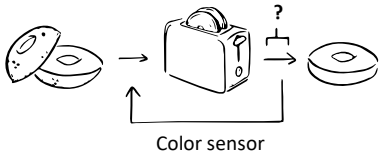
2.17 We can look to the humble toaster as one visual example of a feedback control loop system:



2.18 But you can imagine a situation where you want to toast different types of bread, a frozen waffle, or a bagel:



2.19 By closing the feedback loop with a color sensor, we can remove the need for a timer and repeated adjustments to the timer:



Information Integrity: Balance and Validation

"When I write code, I encode my values, just like when someone makes art or music."

– Amir Taaki aka genjix, Bitcoin developer

3.1 An example of single-entry accounting:

Date	Amount	Description
The sixth	II	Buttons
First of the month	~~IIII~~ II	Linen
Second of the month	II	Thread
~~Day of the full moon~~	~~IIII IIII IIII~~	~~Clothing~~

3.2 Both sides in the giving and receiving have to balance:

Debit *(Receiving & Wealth)*	=	**Credit** *(Giving & Income)*

3.3 Recording inventory purchases with double-entry accounting:

Date	Description	Debits	Credits
06 Nov	To: Inventory (Buttons)	2	
	By: Capital		2
01 Dec	To: Inventory (Linen)	7	
	By: Capital		7
02 Dec	To: Inventory (Thread)	2	
	By: Capital		2

3.4 Recording a sale entry with double-entry accounting:

Date	Description	Debits	Credits
12 Dec	To: Cash	15	
	By: Revenues (Sales)		15
	To: Cost of Goods Sold	4	
	By: Inventory		3
	By: Sales tax liability		1

3.5 From this, you can calculate the business' net profit:

Net Profit = Revenue – Cost of Goods Sold
Net Profit = $15 Revenue – $4 Cost of Goods Sold
Net Profit = $11

3.6 He formalized the double-entry system into an accounting equation:

Debit	=	Credit
Expenses: Utilize it		Loans: Repay it
Losses: Waste it		Liabilities: Repay it
Assets: Save it		Equity: Pay it
Assets	**=**	**Liabilities + Capital**

3.7 From the accounting equation, you can calculate owner's equity:

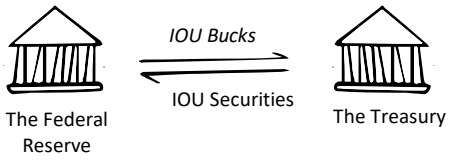
Assets = Liabilities + Owner's Equity
$30 Assets = $4 Liabilities + $26 Capital
Owner's Equity = $26 Capital

3.8 The balance sheets of The Fed and The Treasury:

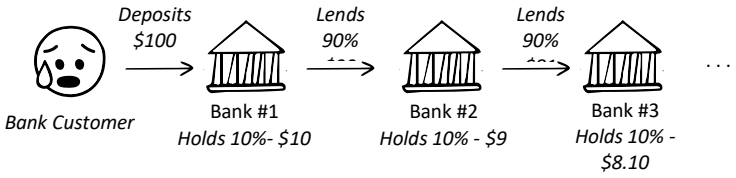
The Federal Reserve	
Debits (Assets)	Credits (Liabilities)
IOU Securities	
	IOU Bucks

The Treasury	
Debits (Assets)	Credits (Liabilities)
IOU Bucks	
	IOU Securities

3.9 The illusion at the heart of the value of dollar:



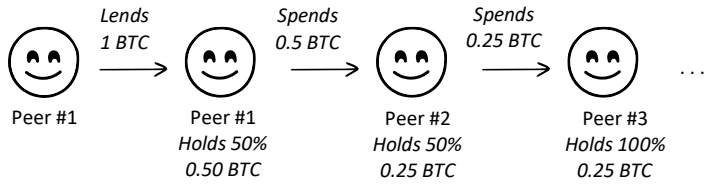
3.10 How the fractional reserve banking system creates money:



Bank #1	
Debits (Assets)	Credits (Liabilities)
$10 Reserves	
$90 Loans	
	$100 Deposits

Bank #2	
Debits (Assets)	Credits (Liabilities)
$9 Reserves	
$81 Loans	
	$90 Deposits

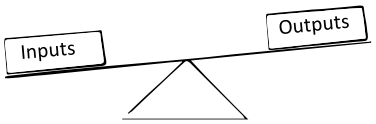
3.11 How Bitcoin Peer-to-Peer lending could be done:



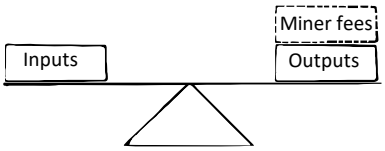
3.12 The blockchain for the three successive transactions:

	Inputs	→	Outputs
Transaction #1	1.00 BTC		1.00 BTC
Transaction #2	1.00 BTC		0.50 BTC 0.50 BTC
Transaction #3	0.50 BTC		0.25 BTC 0.25 BTC

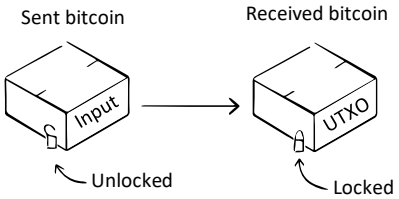
3.13 Each transaction is balanced according to these three rules:



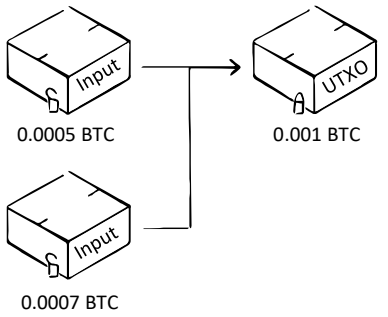
3.14 Miner fees implicitly balance the transaction's inputs and outputs, but do not show up explicitly in the transaction:



3.15 Bitcoin is transferred as inputs and outputs in a transaction:



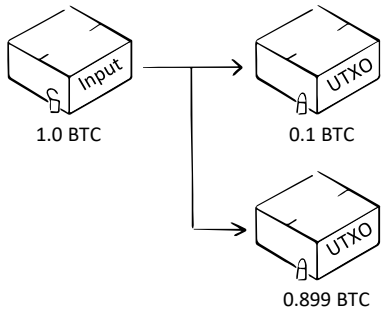
3.16 Combining UTXOs to send funds:



0.001 BTC is sent to your friend

0.0002 BTC excess is implicitly allocated for the miners

3.17 Splitting a UTXO to send funds:

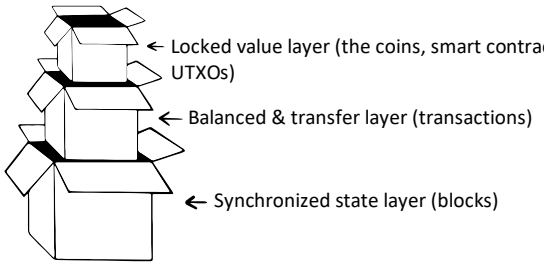


0.1 BTC is sent to your family

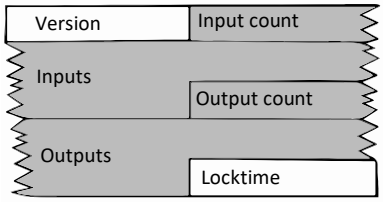
0.001 BTC is implicitly allocated for the miners

0.899 BTC remaining change is sent back to an address you control

3.18 Similar to how transactions are the container for UTXOs, blocks are the containers for confirmed transactions:



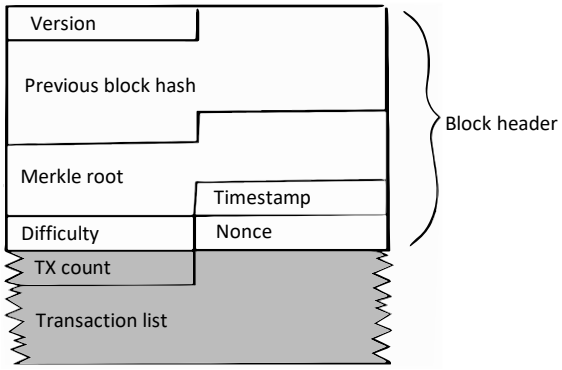
3.19 At the low-level raw data, this is the structure of a transaction:



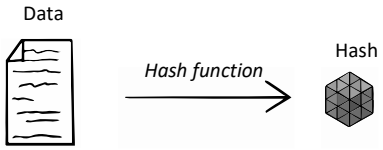
Represents 4 bytes

Gray fields are data with variable size that can be expanded into greater detail.

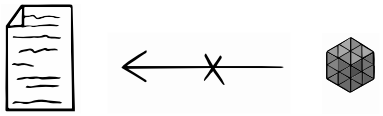
3.20 This is the structure of a raw data in a block:



3.21 A text file (data.txt), hashed to a fixed and unique output:

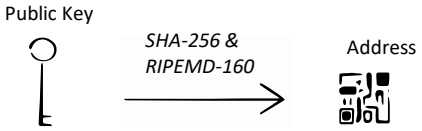


Hash functions are defined by working only in one direction:

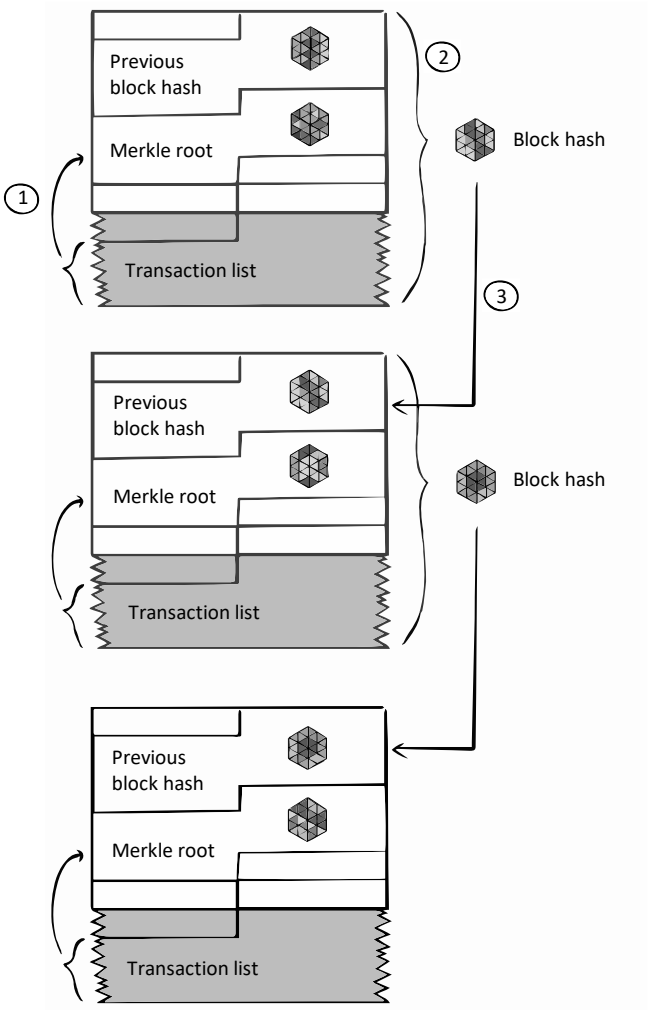


If even a single character is changed, if any data is added or removed, the same hash function will produce an entirely different hash:

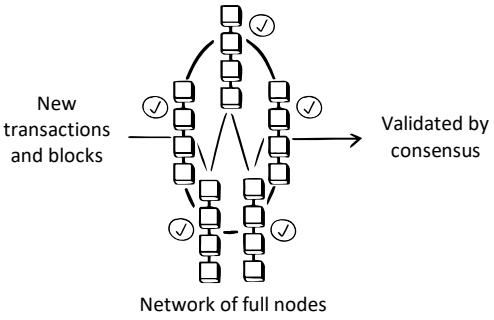
Hashes are used in a number of different ways in bitcoin, one of which is to turn a public key into a smaller, more shareable address:



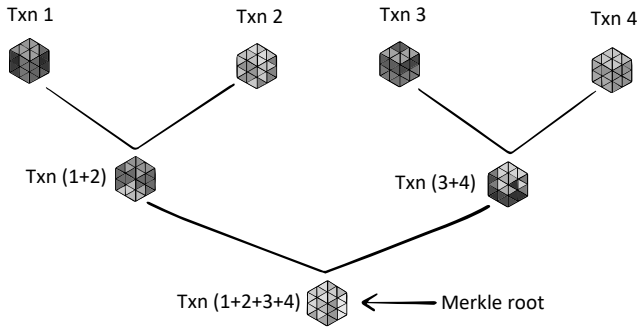
3.22 Hash functions create the chain in the blockchain:



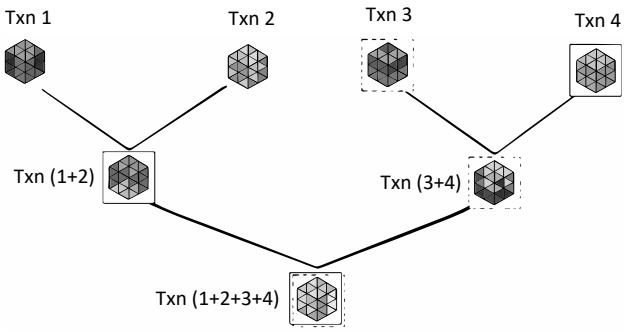
3.23 Full nodes enforce consensus rules on transactions and blocks:



3.24 Transactions hashed together in a Merkle tree:



3.25 Partial validation of transactions done by light nodes:

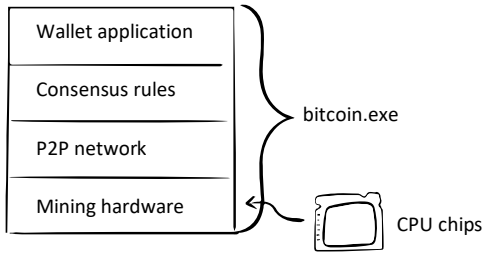


Information Propagation

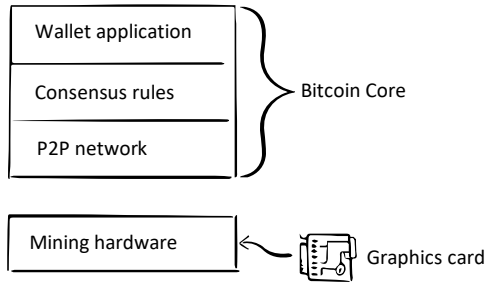
"Every participant in the network needs to verify that this operation is valid, that it is applicable to the local state, and that we can actually confirm it. . . . Now, that clearly doesn't scale. Simply the fact that we have to distribute this massive amount of data gives us a huge problem."

– Christian Decker, Bitcoin developer

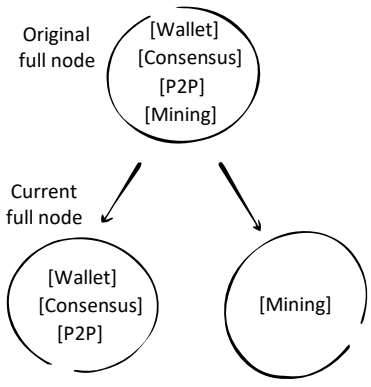
4.1 The first Bitcoin client:



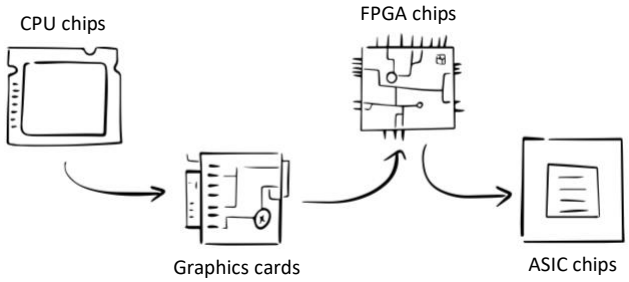
4.2 The Bitcoin split from mining functionality:



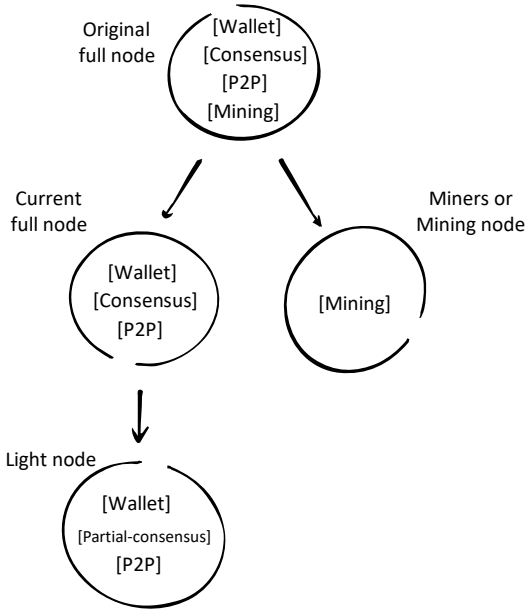
4.3 The split between the original full nodes and miners:



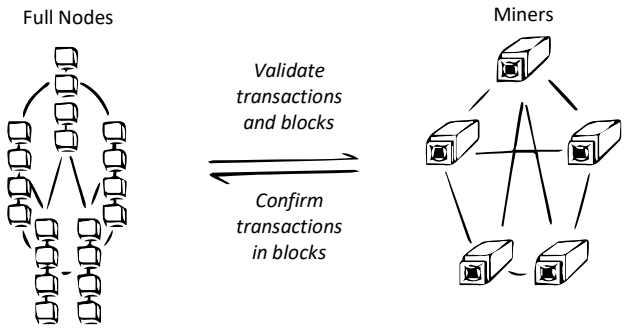
4.4 Miner hardware evolution:



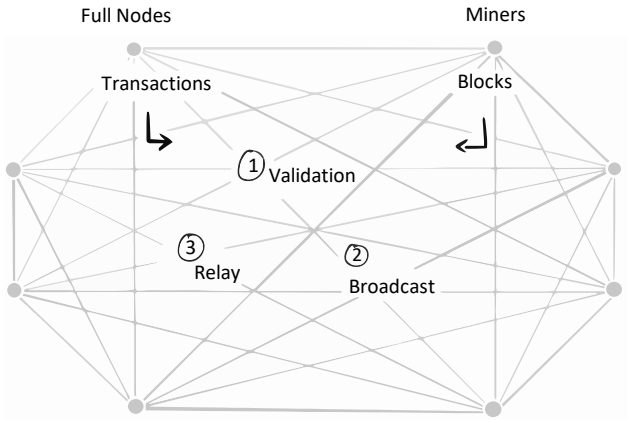
4.5 The evolution from a full node to the light node split:



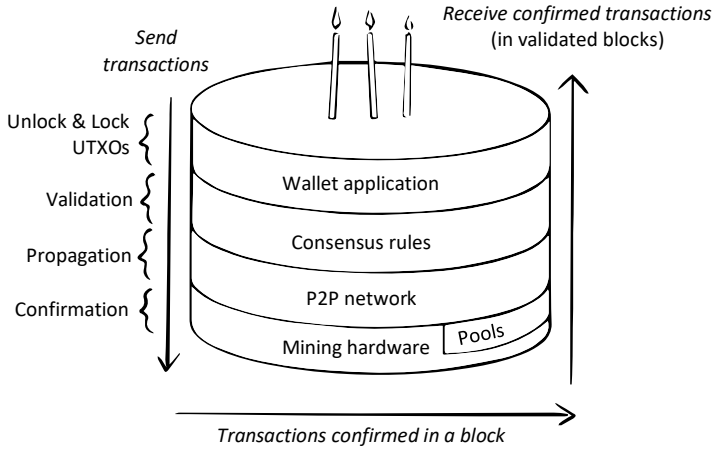
4.6 Two types of Bitcoin nodes:



4.7 The flow of transactions and blocks between miners and full nodes:



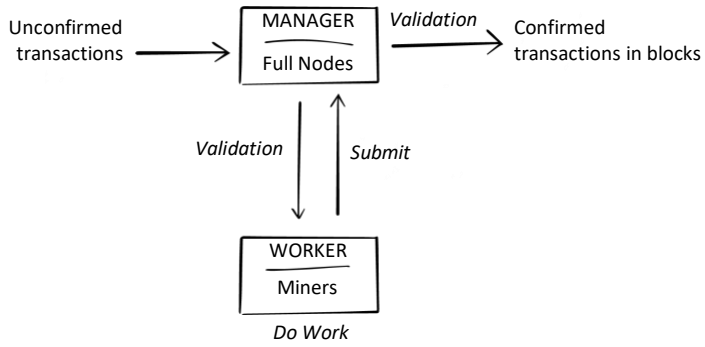
4.8 The flow of transactions and blocks through each layer of Bitcoin:



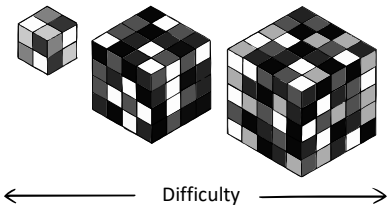
Confirmation, Not Consensus

"Simply put: I don't believe there are simple solutions for complex problems."
– Marek Palatinus aka Slush, inventor of the Bitcoin mining pool concept

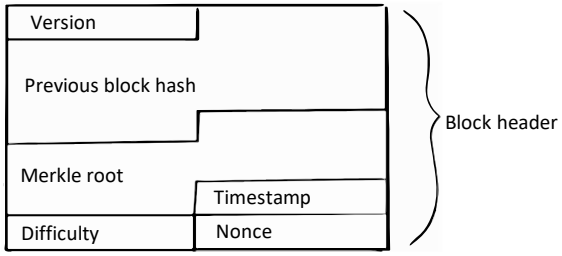
5.1 The manager-worker relationship between full nodes and miners:



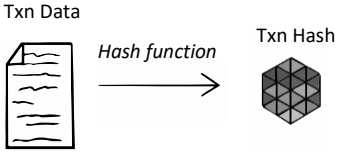
5.2 Proof-of-Work as a puzzle with varying levels of difficulty:



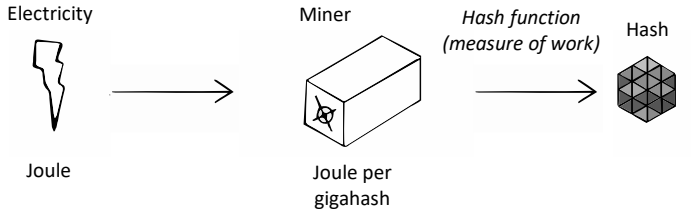
5.3 The nonce value, winning mining solution, in the block header:



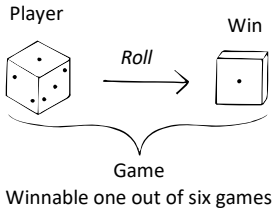
5.4 A transaction data hashed to a fixed and unique output:



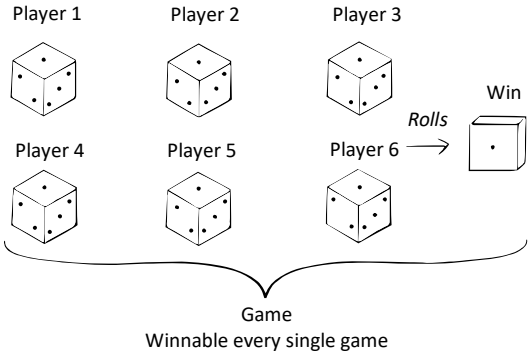
5.5 The units of work converted in the process of mining:



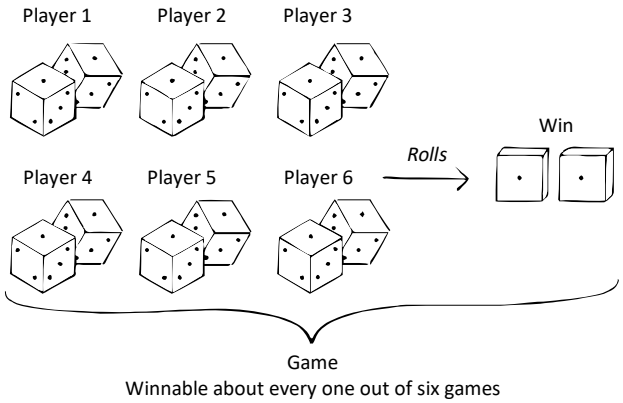
5.6 A single player dice game:



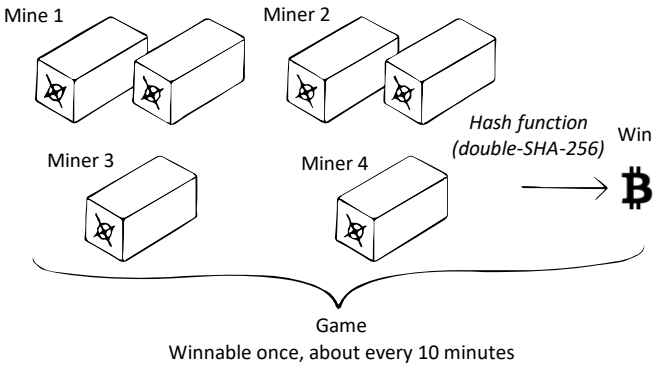
5.7 An easy dice game with more players:



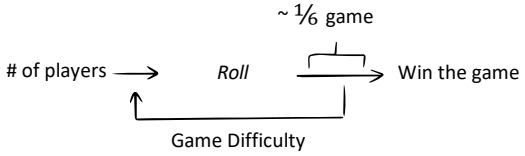
5.8 A harder dice game with more players:



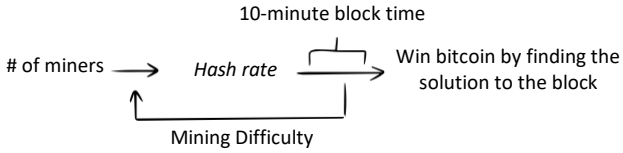
5.9 The game represented with mining pools instead of dice:



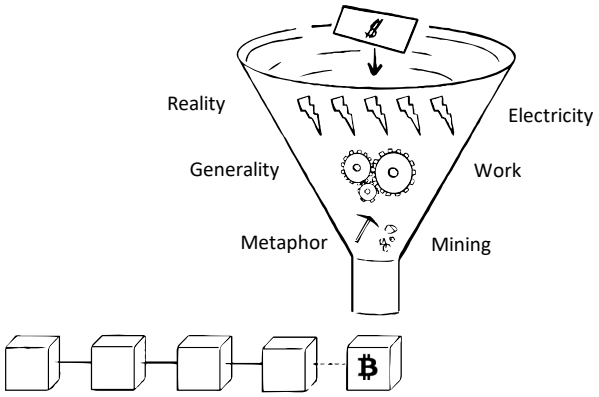
5.10 A dice game with a feedback control loop:



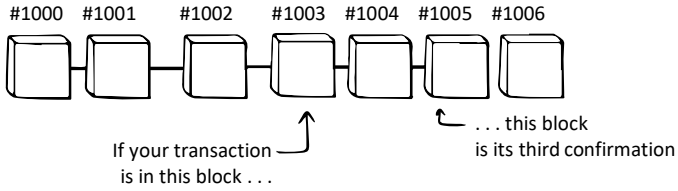
5.11 Proof-of-Work with a feedback control loop:



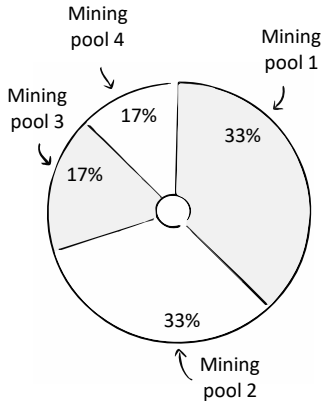
5.12 The process of converting value from off-chain to on-chain:



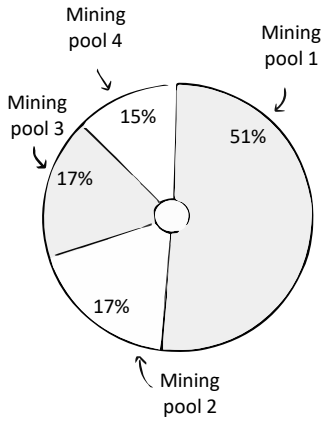
5.13 An example of three block confirmations:



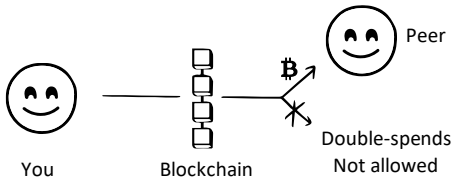
5.14 An example of bitcoin mining pool distribution:



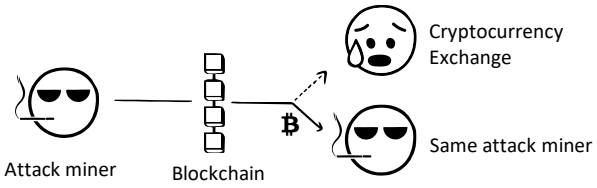
5.15 An example of a mining pool with 51% of the network hash power:



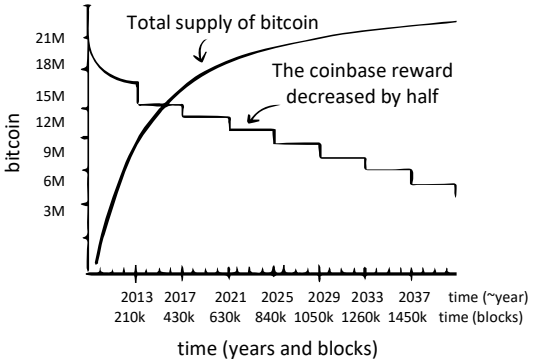
5.16 Recall that the blockchain prevents double spend attacks:



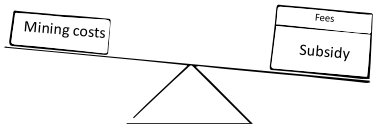
5.17 A miner double spending an exchange on the blockchain:



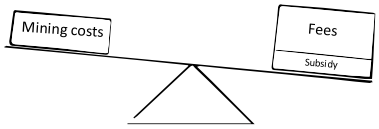
5.18 Bitcoin's monetary inflation rate:



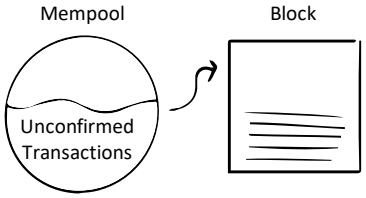
5.19 The network incentive for miners with the coinbase subsidy:



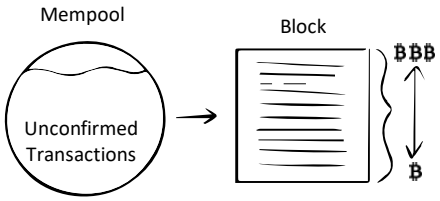
5.20 Incentive for miners when the network shifts to rely on fees:



5.21 With few transactions in the mempool:



5.22 With more transactions in the mempool:

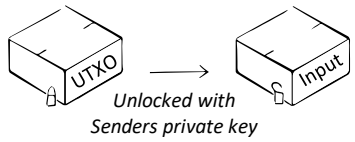


Smart Contracts: Locking and Unlocking

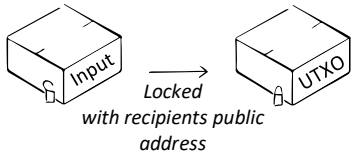
"What is the meaning and purpose of 'security'? How does it relate to the relationships we have? I argue that the formalizations of our relationships—especially contracts—provide the blueprint for ideal security."

– Nick Szabo, inventor of the smart contract concept before Bitcoin

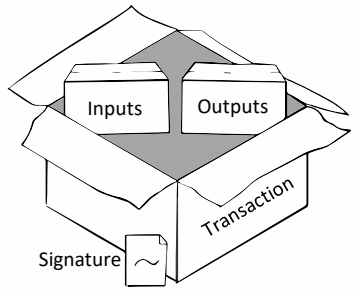
6.1 When you're sending bitcoin to a friend, your UTXO is unlocked with your private key and used as the input for the transaction.



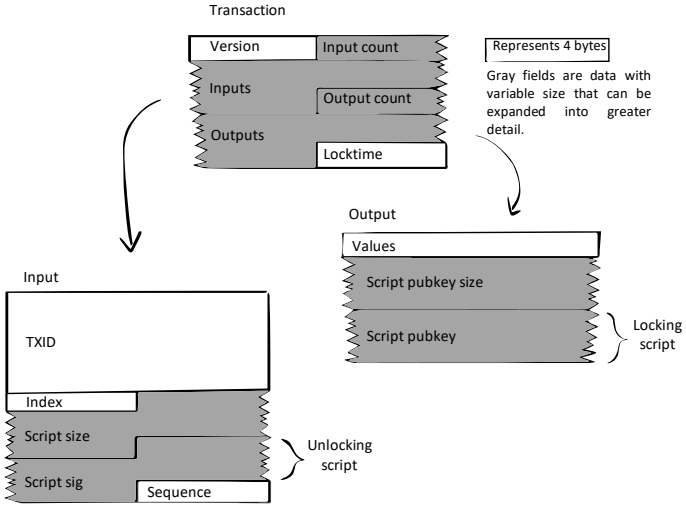
6.2 Your friend's bitcoin address re-locks the bitcoin at an address they control and creates the output (a new UTXO) in this transaction.



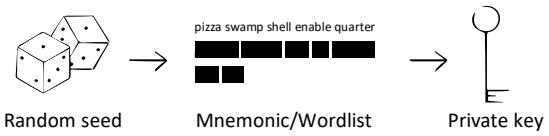
6.3 And then, a signature signs the transaction (loaded into the input unlocking script) to ensure that the inputs and outputs can't be swapped out in transit.



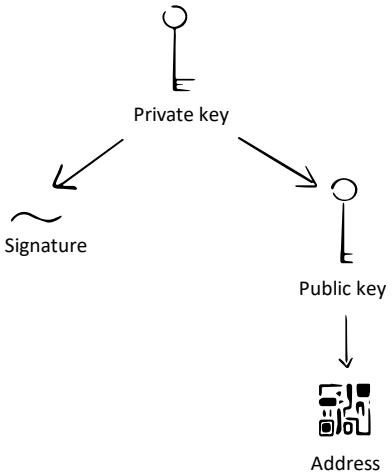
6.4 A lower-level representation of Bitcoin shows how scripts are loaded into the inputs and outputs of a transaction:



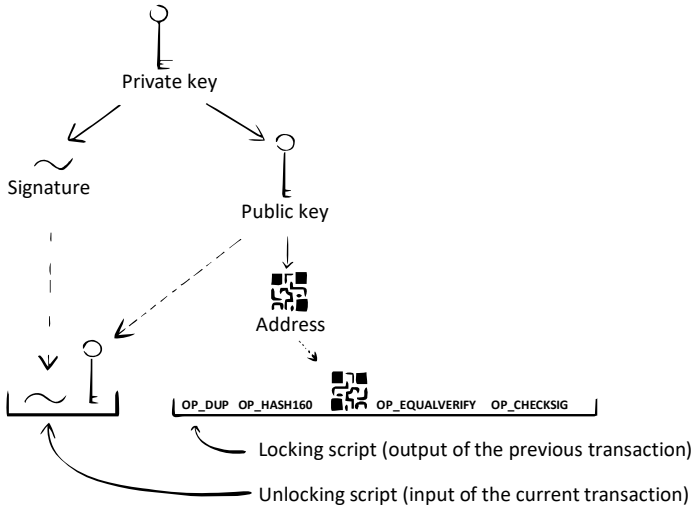
6.5 Bitcoin key generation:



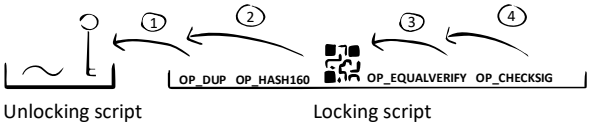
6.6 Bitcoin key derivation:



6.7 The sender's unlocking script in a P2PKH transaction:

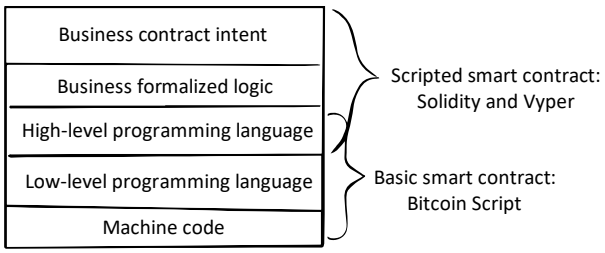


6.8 The validation of the unlocking script is computed:

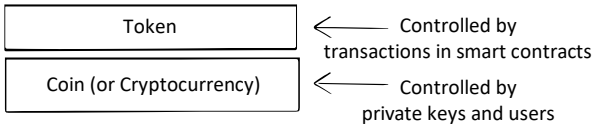


1. The script duplicates the public key:
   OP_DUP( ) =
2. The public key is hashed to an address:
   OP_HASH160( ) =
3. The computed script hash is checked against the locks script hash:
   OP_EQUALVERIFY( ) = ✓
4. Lastly the script checks the signature against the public key:
   OP_CHECKSIG ( ) = ✓

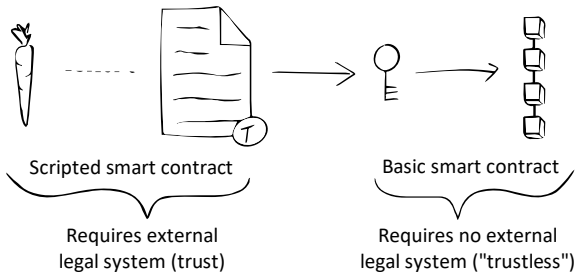
6.9 The abstraction stack of smart contracts:



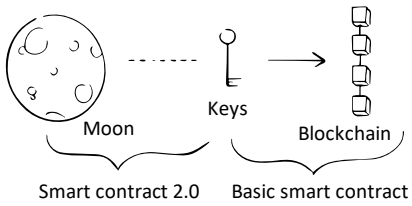
6.10 The most common type of scripted smart contract is a token issuance on top of a cryptocurrency:



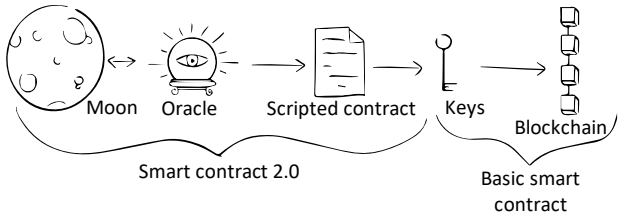
6.11 A tokenized asset has no control over the physical asset it represents:



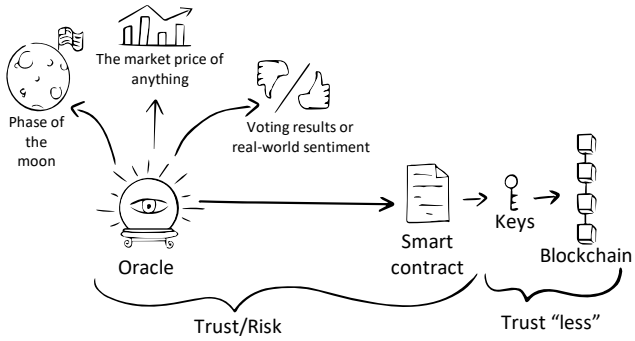
6.12 The blockchain has no access to off-chain data:



6.13 The oracle "solution" to external data on the blockchain:



6.14 All external data on the blockchain passes through trusted oracles:



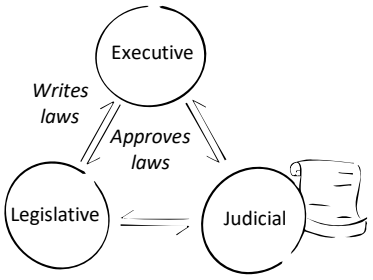
Governance

"[T]he United States can pay any debt it has because we can always print money to do that."
– Alan Greenspan, former chair of the Federal Reserve of the United States

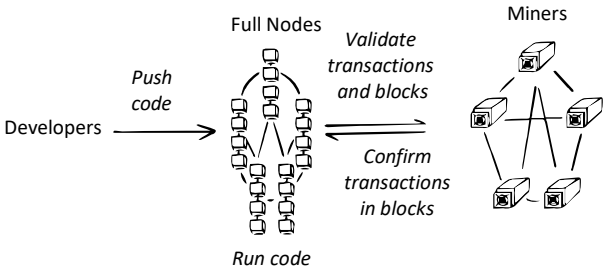
"You have to really stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it. Maybe somebody else can."

– Also Alan Greenspan

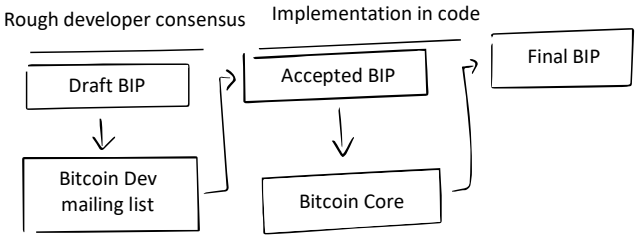
7.1 The balance of powers in a democratic republic:



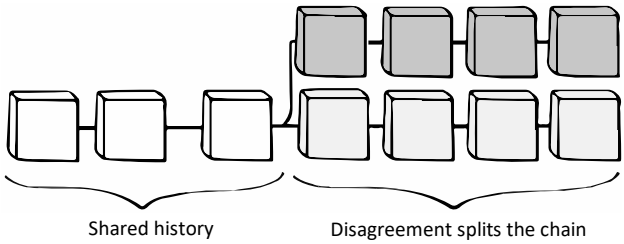
7.2 Bitcoin has its own interpretation of the balance of powers:



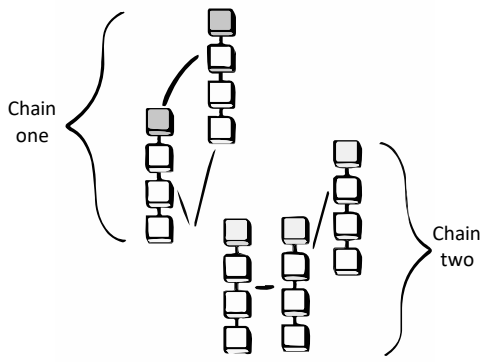
7.3 The process of changing Bitcoin with BIPs is as follows:



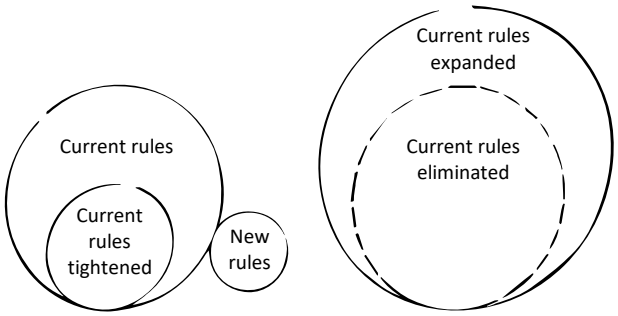
7.4 A disagreement on the chain causes a chain split:



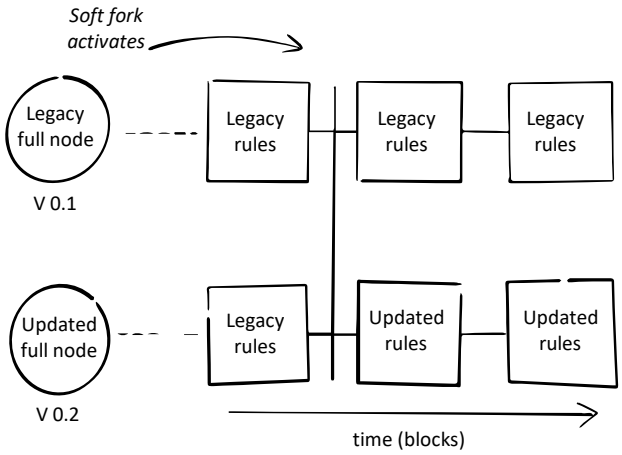
7.5 Chain splits divide the network:



7.6 The logic of a soft fork: **The logic of a hard fork:**



7.7 A soft fork's chain continuity with over about 60% of nodes upgraded:

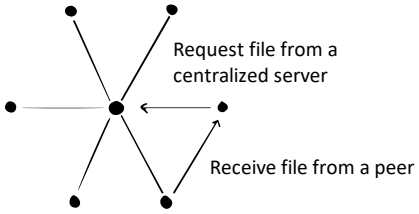


Approximating Decentralization

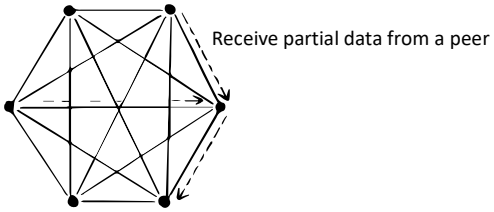
"Bitcoin is in the crucial stages of development. Its code can evolve in several directions. It's under threat from those who don't understand it; it's under threat from those who do understand it."

– Johnny Dilley, Bitcoin contributor

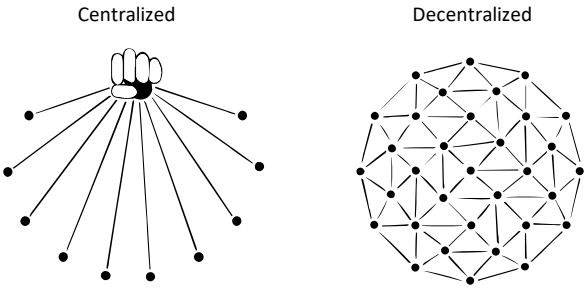
8.1 Napster's system architecture:



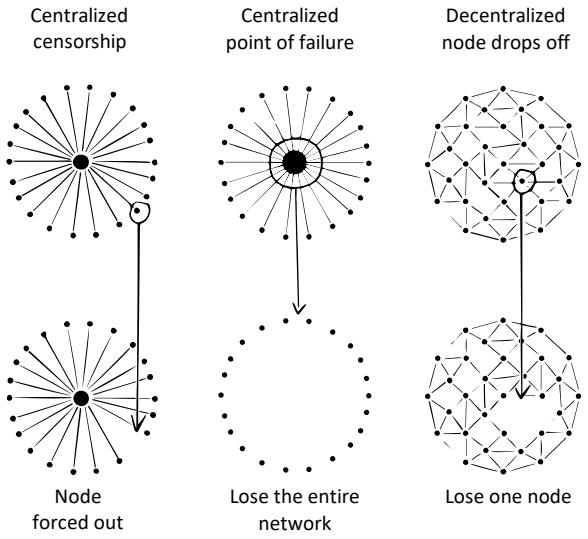
8.2 BitTorrent's system architecture:



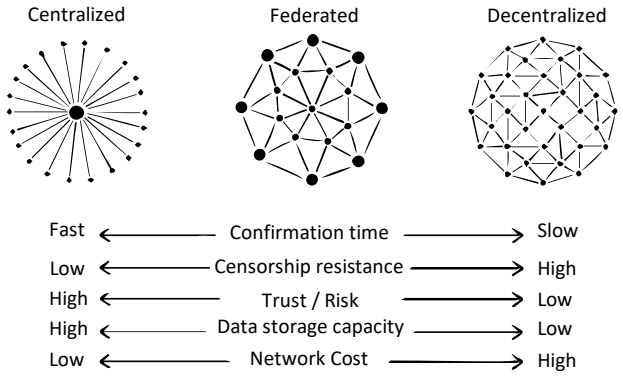
8.3 The controllability of these two systems:



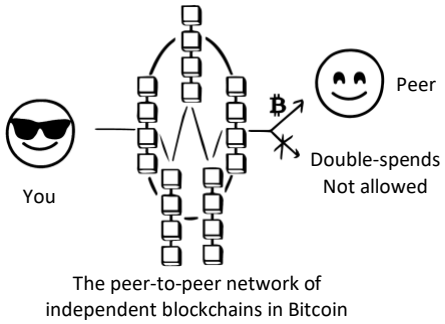
8.4 Decentralized networks are not easily censored or taken down:



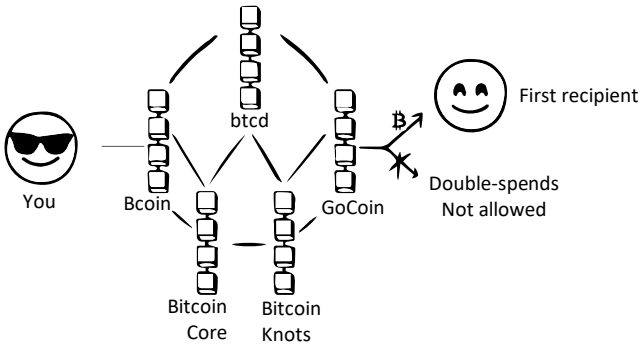
8.5 A scale of centralization:



8.6 Client and developer centralization on Bitcoin Core:



8.7 Client and developer decentralization with separate full node implementations:

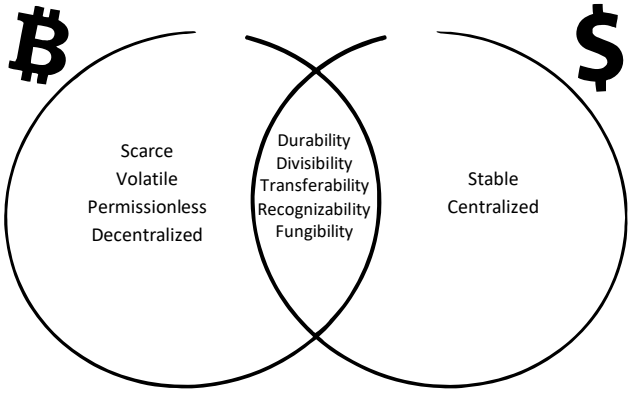


The Properties of Money

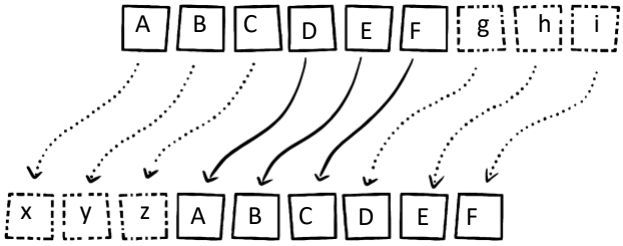
"It is impossible to grasp the meaning of the idea of sound money if one does not realize that it was devised as an instrument for the protection of civil liberties against despotic inroads on the part of governments. Ideologically it belongs in the same class with political constitutions and bills of rights."

– Ludwig von Mises, Austrian economist

9.1 Bitcoin VS. USD:



9.2 The Caesar Cipher:

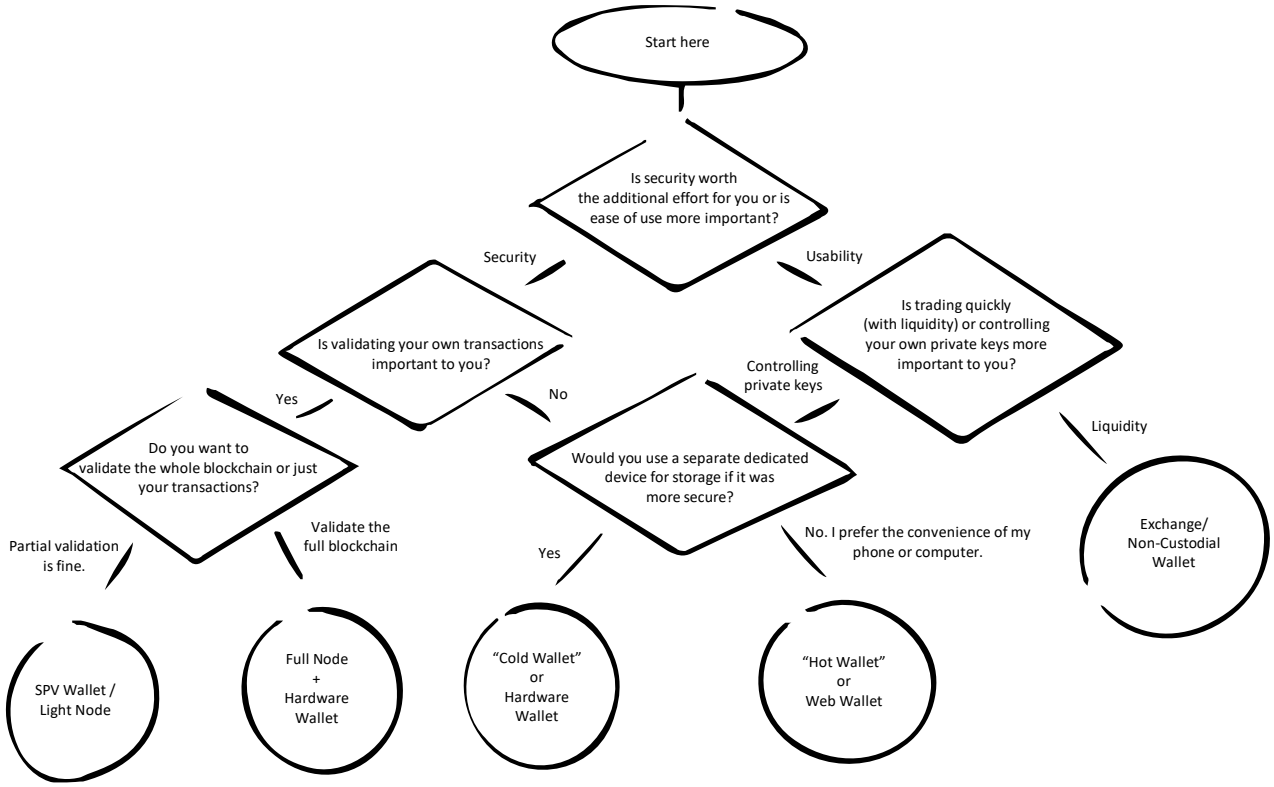


Getting Started

"I think it's important to recognize that not everyone needs this technology. Also, the technology is not ready for everyone. It is still difficult to use, difficult to secure, it's difficult to operate in a convenient way. The user interfaces are very poor, require a high level of technical expertise to operate, even more so to operate securely. And so, why do you need it in your life?"

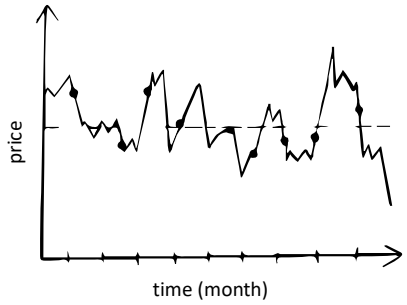
– Andreas Antonopoulos, author of Mastering Bitcoin

10.1 The right wallet for you:

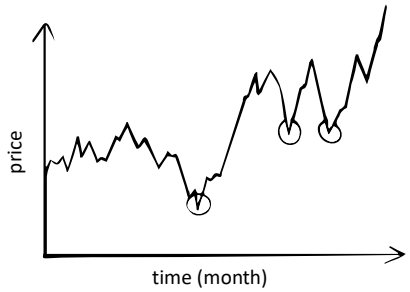


Yes.

10.2 Dollar Cost Averaging



10.3 Trading or "Buying the Dip"



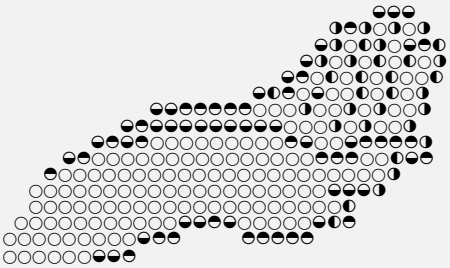
Markets

"Money is a bubble that never pops. It's a consensus hallucination."
– Naval Ravikant, angel investor, podcaster, and serial entrepreneur

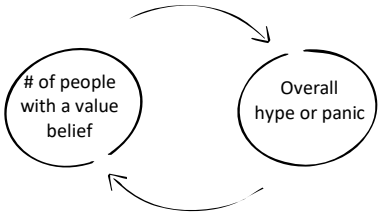
11. 1 If each circle represents one person's *belief* about an asset's value:

○

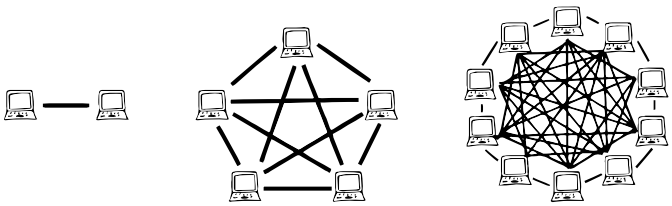
11.2 The invisible hand reflects the *beliefs* of the market in *action*:



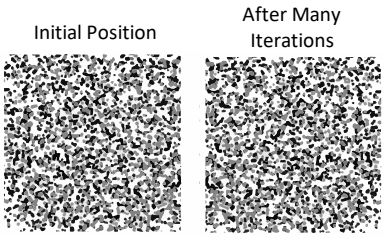
11.3 The hype panic cycle:



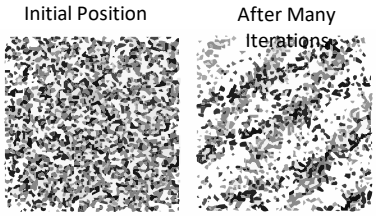
11.4 Metcalfe's value increase with n^2:



11.5 An example of random motion:



11.6 An example of chaotic motion:



11.7 Chaos VS. Randomness:

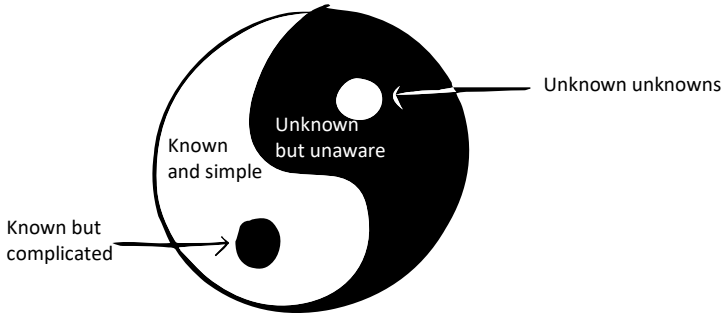
Randomness has no order or predictability in it at all.

Chaos always has some order in it.

11.8 The category of unknown unknowns in the Knowledge Matrix:

Known	Known knowns Things we are aware of and understand.	Known unknowns Things we are aware of but don't understand.
Unknown	Unknown Things we understand but are not aware of.	Unknown unknowns Things we are neither not aware of nor understand.
	Known	Unknown

11.9 The knowledge matrix mapped over the yin and yang symbol:

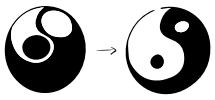


11.10 Unknown unknowns:

11.11 But as you learn about it, you push the boundary of unknown chaos out and sort the chaos into order:

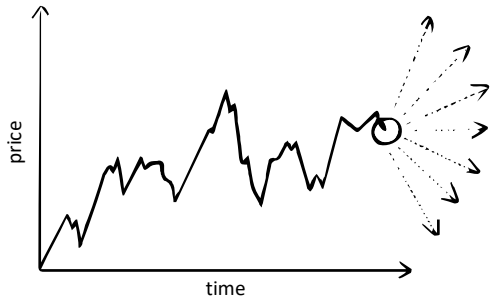
- Known and simple: Bitcoin is a digital currency.
- Known but complicated: Bitcoin makes digital currency and P2P payments possible with a decentralized ledger and proof-of-work.
- Unknown knowns: No idea how Bitcoin's cryptography works.
- Unknown unknowns:

11.12 The more you transform the unknown into the known, the more information you have to accurately estimate the value of an asset:

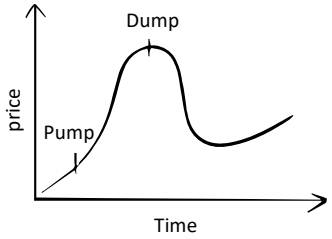


- Known and simple: The US, China, and Japan are the primary users of Bitcoin.
- Known but complicated: Fee pressure is a good estimate of utilization.
- Unknown knowns: Bitcoin wallets don't correlate with bitcoin users 1 to 1. But if I could know how many unique users there were across all the exchanges, I could get a better measure of the size of the network.
- Unknown unknowns:

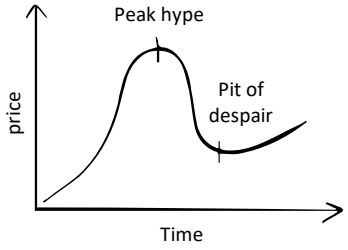
11.13 The market moves only three ways: up, down, or sideways:



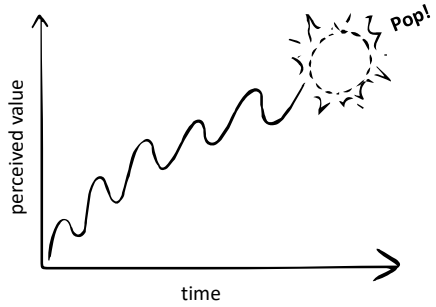
11.14 The pump-and-dump:



11.15 The result of buying into peak hype:



11.16 What people are asking when they ask, "Is Bitcoin a bubble?" is, "Should I run from it or should I hype it?"



CHAPTER 12

Mindset

"A person's worth is measured by the worth of what he values."

— Marcus Aurelius, Roman emperor, and Stoic philosopher

People tend to measure value by price:

```
฿ = $10,000
```

Value measured in the time it takes to capture it:

```
The time it took to earn a bitcoin or $10,000.
฿ = $10,000 at $25 an hr = 400 hours
```

Value measured relative to the value of other assets:

```
The salesperson had to sell four cars to buy 1/10th of a bitcoin.
Sales commission = $250 per car, $1000 = 0.10 BTC
```

What hustlers call the flip, fancy people call an arbitrage opportunity:

```
You find ● at a garage sale, undervalued at $25.
You buy it, resell it for $1,000 online, and profit $975.

Value captured in arbitrage:
Buy: ● = $25
Sell: ● = $1,000
----------
Profit: $975 minus time spent = 0.0975 BTC
```

An investor analyzes the value of an asset based on its periodic return in the short term, or its increased potential value in the long term:

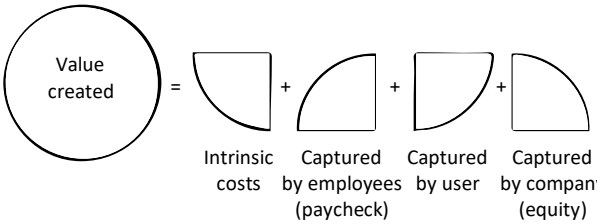
```
Value captured in investment overtime:
Rental income = $500 a month and $6000 annually

Potential future value of real estate investment:
Current valuation x 3% a year
```

Yet when some people see a material thing they want in the world, they see only one half of the value equation:

```
฿ ≈
```

12.1 Creating and capturing value in the form of equity or a paycheck:



Too much of a good thing? Never. I have ambitions to write more books, make more videos, and do whatever I can to get you more educated and entertaining Bitcoin content. You can check that out at YouTube, BitChute, or getbitcoinclarity.com.

If you enjoyed this book and found any nuggets within it valuable, please share it and consider leaving a review on Amazon or Goodreads. If you're feeling philanthropic, throw it in the BTC tip jar below:

bc1qh3xakg0s6zazz6tgyefu8965yd4uqyk0zas4dx