ThoughtWorks®

CRYPTOCURRENCY

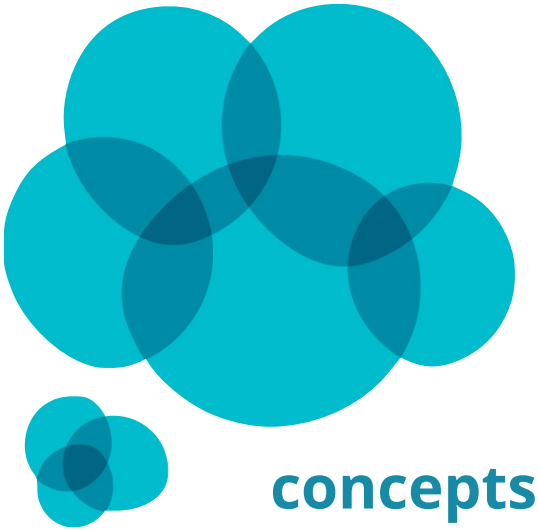
How It Works & Why It Matters

ThoughtWorks®

NEAL FORD

Director / Software Architect / Meme Wrangler

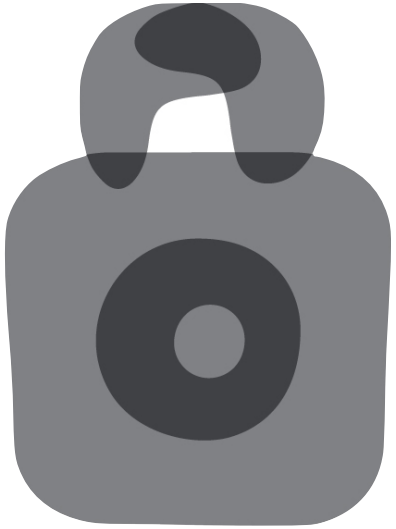
Agenda



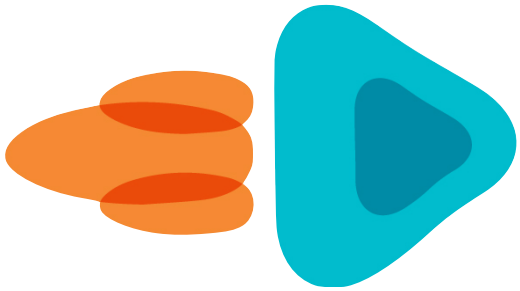
concepts

blockchain

transactions

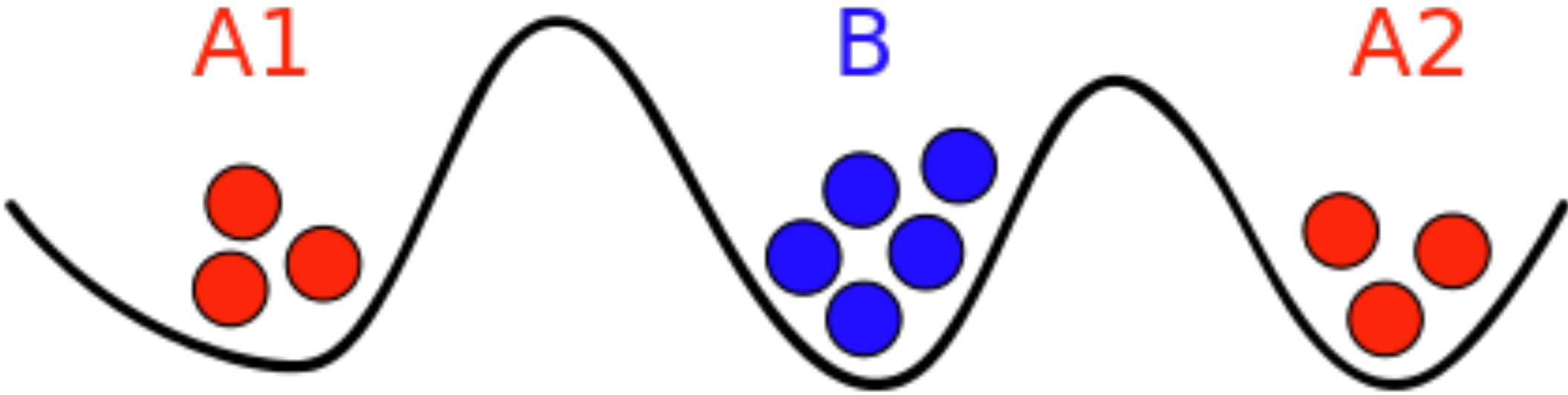


security



implications

Two Generals Problem



http://en.wikipedia.org/wiki/Two_Generals%27_Problem

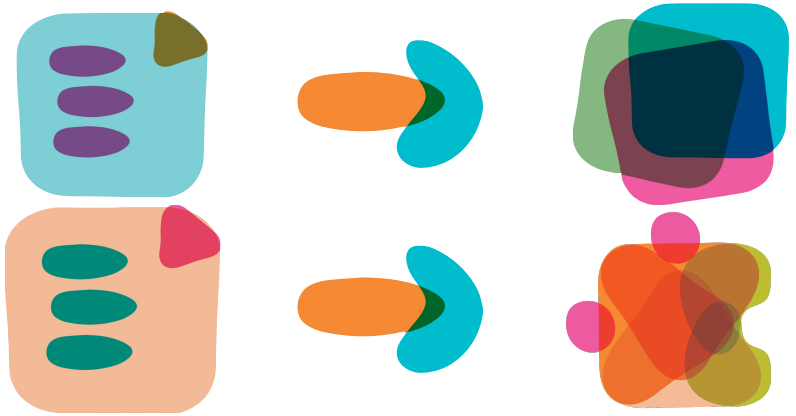
Cryptographic Hash Functions

easy to compute the hash value for any given message

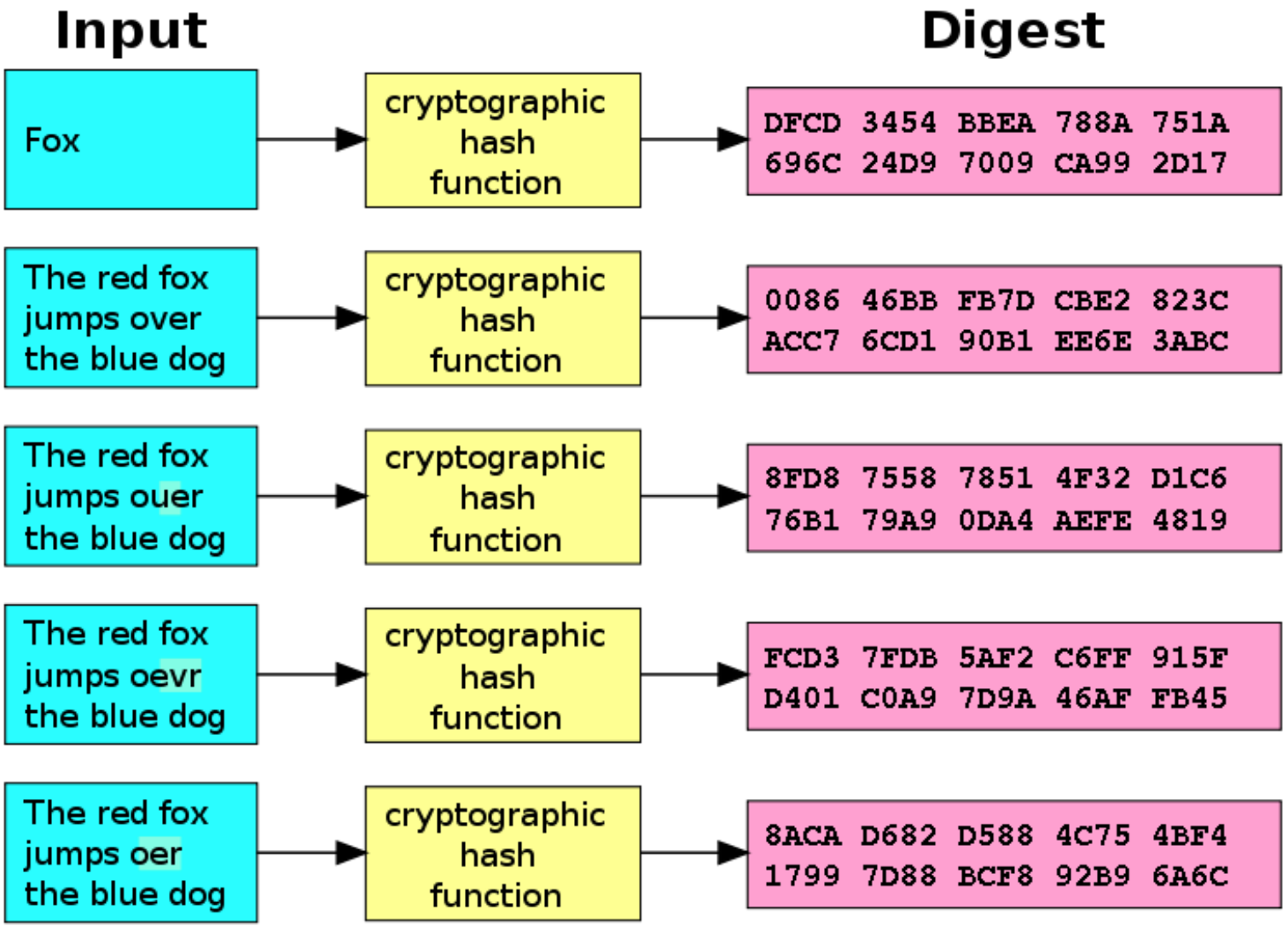
infeasible to generate a message from its hash

infeasible to modify a message without changing the hash

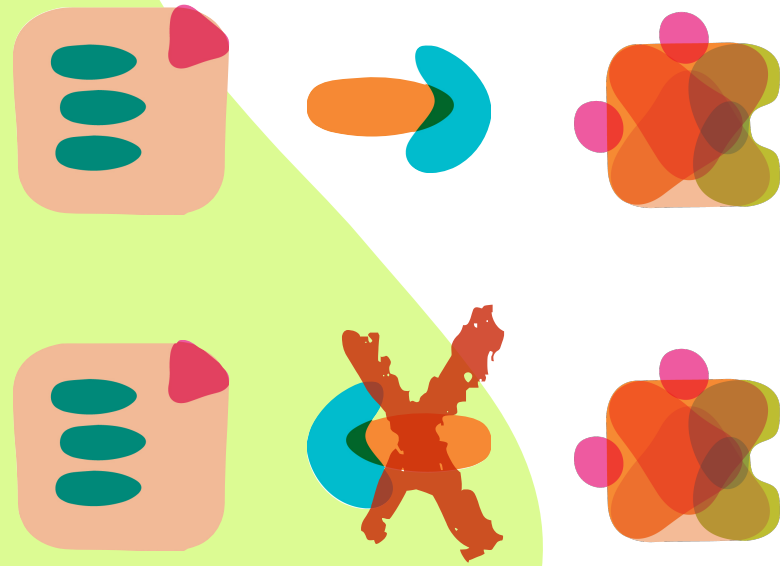
infeasible to find two different messages with the same hash



SHA-1 at Work


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Proof-of-work System



Proof of work

```
require 'digest'

s = Digest::SH
s << "Satoshi
puts s.hexdige
nonce = 0
loop do
  s << nonce.t
  puts s.hexdi
  break if s.h
  nonce = nonc
end
puts nonce
```

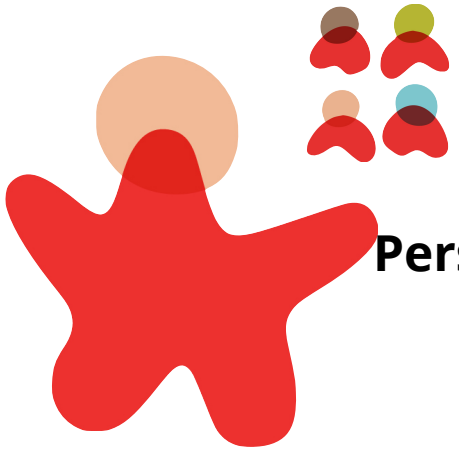
```
a0dc65ffca799873cbea0ac274015b9526505daaaed385155425f7337704883e
a8e6cfb0a4ddca931ed69eba4b22c161765bfe557b77e0c28ca697dac2bc9f25
7a61d466a1b78536610ebd946d4ad2661256e860ac530197d7ce239d0020225c
d1e8686864db9931ccd9c3e6f15326c25000fa0b8c902a383baa8ec6b4848d36
4b1508aa6bfa2f045cdf4eeca864b875639fb94ec04a6d139309729ae315190d
94a872ccbc276a9be9a8d836929e3f40a49c66352d1eadd10ba0f753f6b641b1
f6ea160208ad0c738e252092448b4d625b2591d960b2b9c32aa4d59bf44716ec
44ea80ff3cbe229c436b2474ceac312af3af080cc588a2ed1fc04eccd6ed4274
fa6e151c69032b0f7b7d4bd6de1f36452d2bbc566703be4c48472d986205418d
563cc13aa52be6a8bba3eeea0fc780e4164578fa6c3cb9be76f4fd1929e6449b
9e36fd9fb39392fd38f5fbabba822699a872e76ea77834f9ee50410f1f7a7f22
9102b0eaf4a7cd3672d81c62f1b0d6756d05ca53eb42aa07514ded6175c3f532
8cf8a465e0ba7d9672a190297edcfdb83df9d440e0bc3c4653556218d7a971c2
7a75a48c1511f32eb3bbc7313cc8ac62c11542e381785803be40aac0288d03af
fe595e3267dea562aeaa51522d61a266b000f29c4e235c009d5e8073b27d8d5e
50372ab66581561b38c213b318ddb9a8c83945e0fa269a6e81d37c6b0fb6615b
f0a73c72883744e1c41913af1f7cf064e14ed8e01e61519b8716d7492f8c77fa
8552c4d79b8dabaf41c5f1e089eb353885788caa5a1c33fe5141891c56992cab
c92e3f7f85187006dc9dab408cc667359bcff82b588d1fc22948f0b7407c8892
7241e8deb28ef142df42e048ab482dbb1a91a80658da8fe6c1e346dd900dafeb
7dc3ad5a16632e669d0e0bc882d139efa9f86e053f7a685d1dc0581d4583b9f0
77b54e3a280d4ba07c522ee3096a604840f13250e2afae48624c023d95eaeaaf
1749b3fc76a0e32e881075db1d771d0df0dead66c127fd69e26f122ad7589a37
0406b42df850c37fdb251b682a453611b701843b47db045880f530f4132dc958
22
```

Adding Work

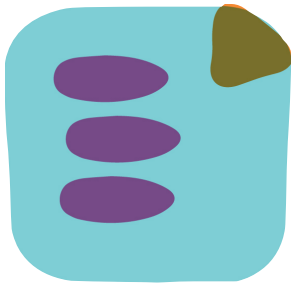
```ruby
require 'digest'

s = Digest::SHA256.new
s << "Satoshi Nakamoto"
puts s.hexdigest
nonce = 0
loop do
  s << nonce.to_s
  puts s.hexdigest
  break if s.hexdigest =~
  nonce = nonce + 1
end
puts nonce
```

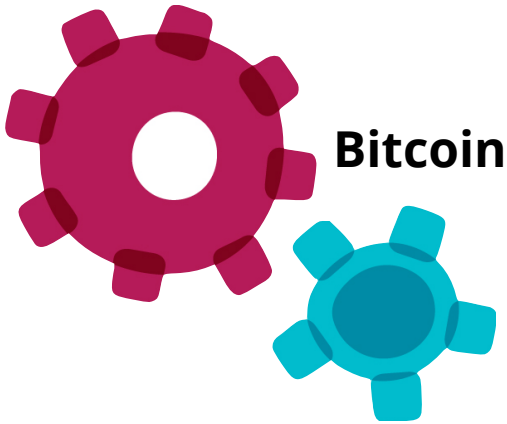
Satoshi Nakamoto



Person (or people)

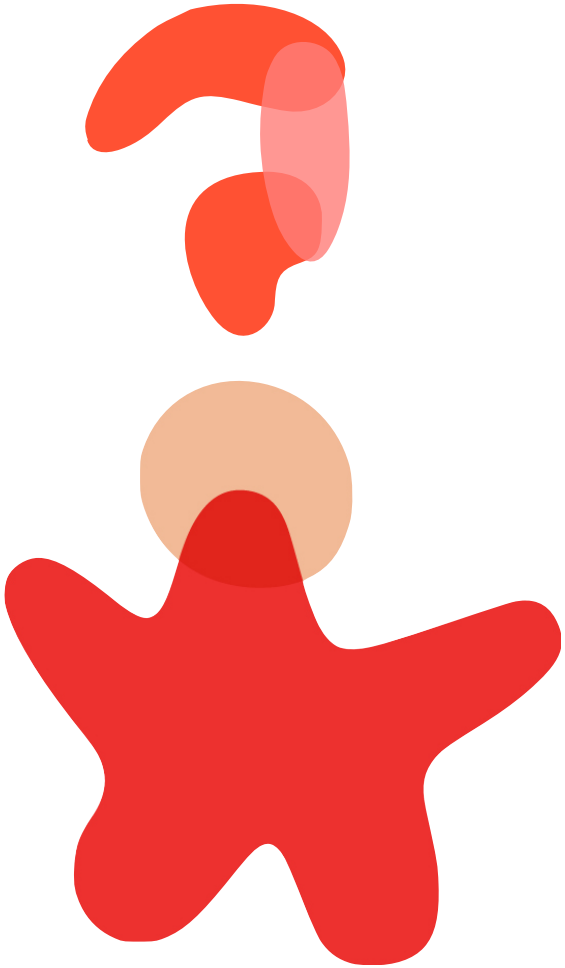


Published in 2008 on The Cryptography Mailing list at metzdowd.com



Bitcoin software in 2009.

Anonymity ?



Cryptocurrency is disruptive!

Banned by several governments

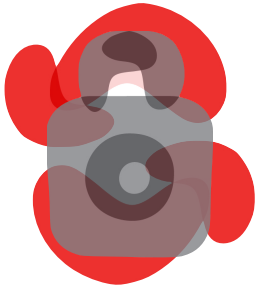
Foundation for other *distributed trust* applications

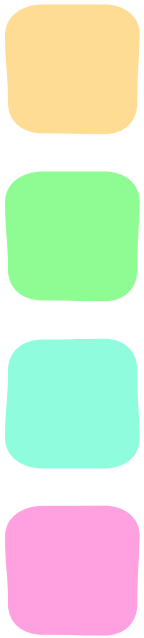
Implementation over Commodity

bitcoin

currency/commodity

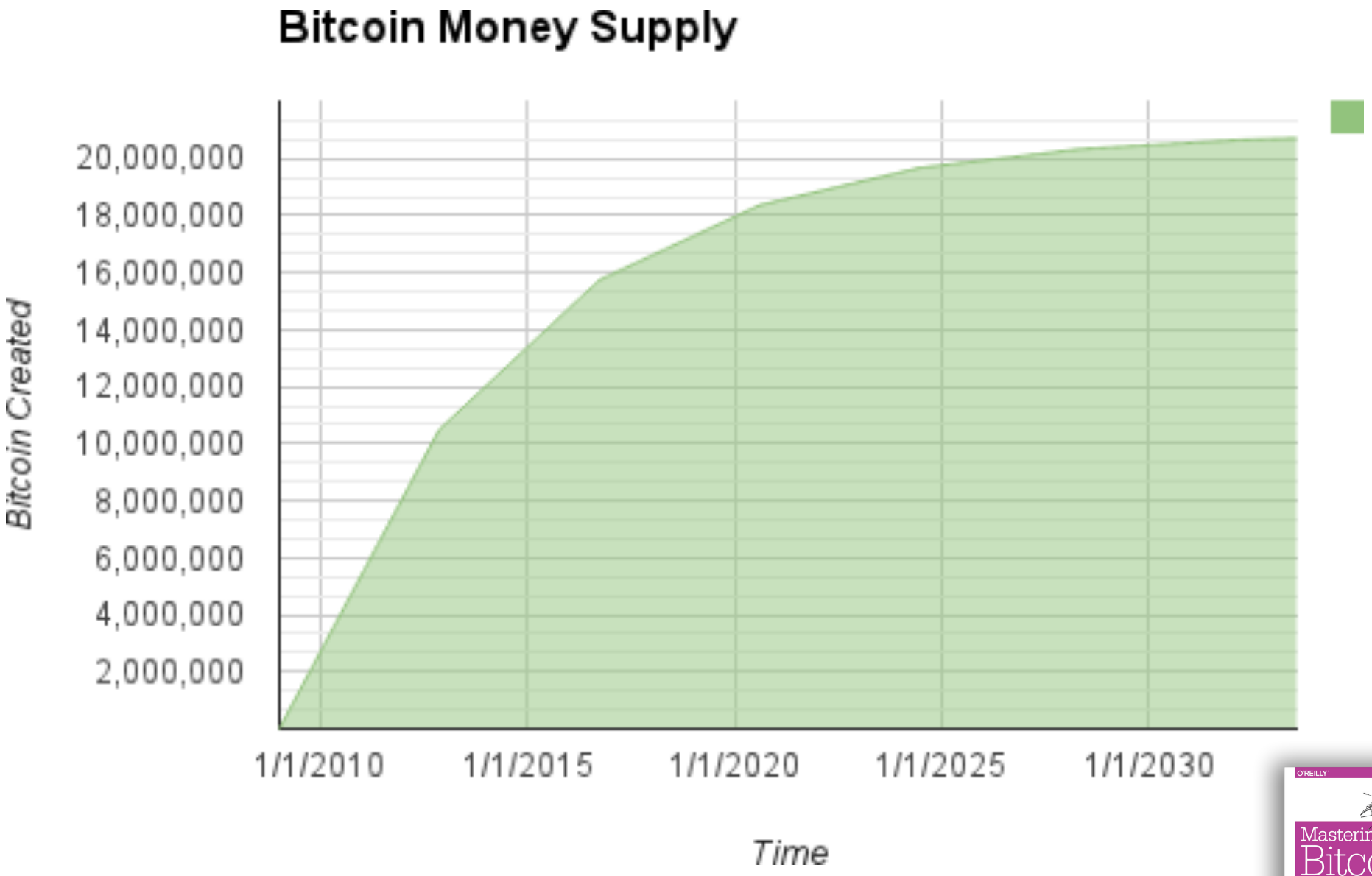
digital bearer instrument

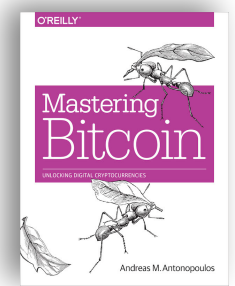




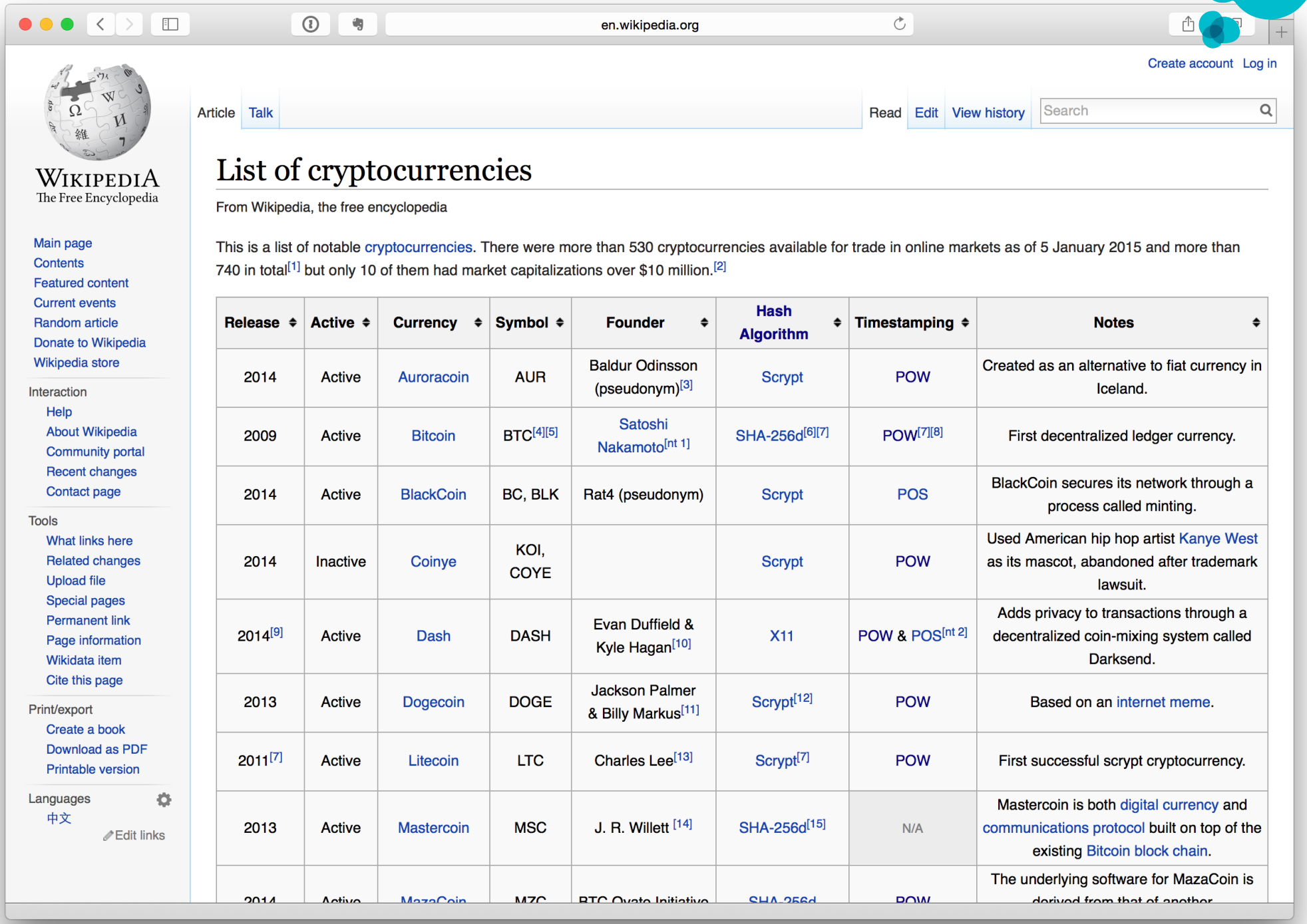
distributed trust

Deflationary Currency





Variations



en.wikipedia.org

Create account Log in

WIKIPEDIA
The Free Encyclopedia

Article Talk | Read Edit View history | Search

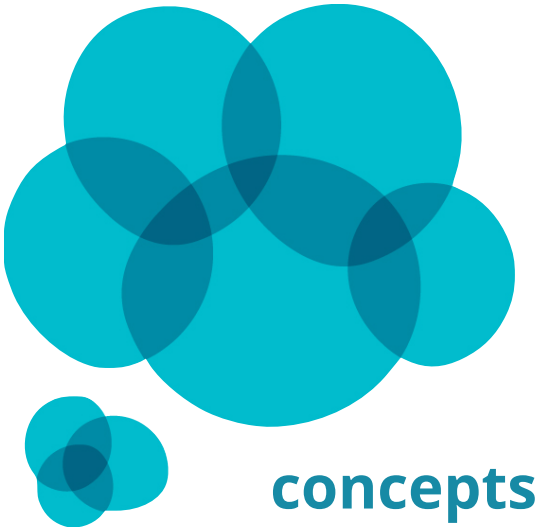
List of cryptocurrencies

From Wikipedia, the free encyclopedia

This is a list of notable cryptocurrencies. There were more than 530 cryptocurrencies available for trade in online markets as of 5 January 2015 and more than 740 in total[1] but only 10 of them had market capitalizations over $10 million.[2]

Release	Active	Currency	Symbol	Founder	Hash Algorithm	Timestamping	Notes
2014	Active	Auroracoin	AUR	Baldur Odinsson (pseudonym)[3]	Scrypt	POW	Created as an alternative to fiat currency in Iceland.
2009	Active	Bitcoin	BTC[4][5]	Satoshi Nakamoto[nt 1]	SHA-256d[6][7]	POW[7][8]	First decentralized ledger currency.
2014	Active	BlackCoin	BC, BLK	Rat4 (pseudonym)	Scrypt	POS	BlackCoin secures its network through a process called minting.
2014	Inactive	Coinye	KOI, COYE		Scrypt	POW	Used American hip hop artist Kanye West as its mascot, abandoned after trademark lawsuit.
2014[9]	Active	Dash	DASH	Evan Duffield & Kyle Hagan[10]	X11	POW & POS[nt 2]	Adds privacy to transactions through a decentralized coin-mixing system called Darksend.
2013	Active	Dogecoin	DOGE	Jackson Palmer & Billy Markus[11]	Scrypt[12]	POW	Based on an internet meme.
2011[7]	Active	Litecoin	LTC	Charles Lee[13]	Scrypt[7]	POW	First successful scrypt cryptocurrency.
2013	Active	Mastercoin	MSC	J. R. Willett [14]	SHA-256d[15]	N/A	Mastercoin is both digital currency and communications protocol built on top of the existing Bitcoin block chain.
2014	Active	MazaCoin	MZC	BTC Ovate Initiative	SHA-256d	POW	The underlying software for MazaCoin is derived from that of another

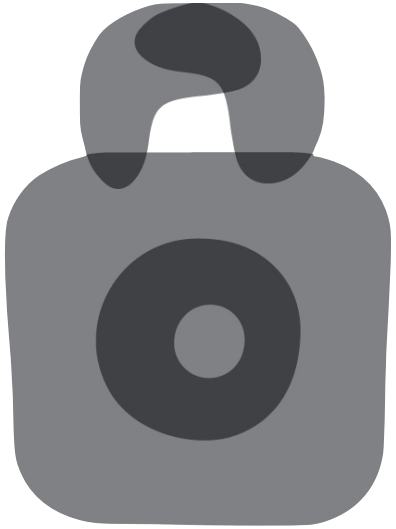
Agenda



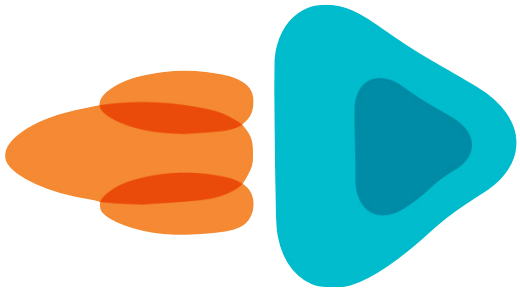
concepts

blockchain

transactions



security

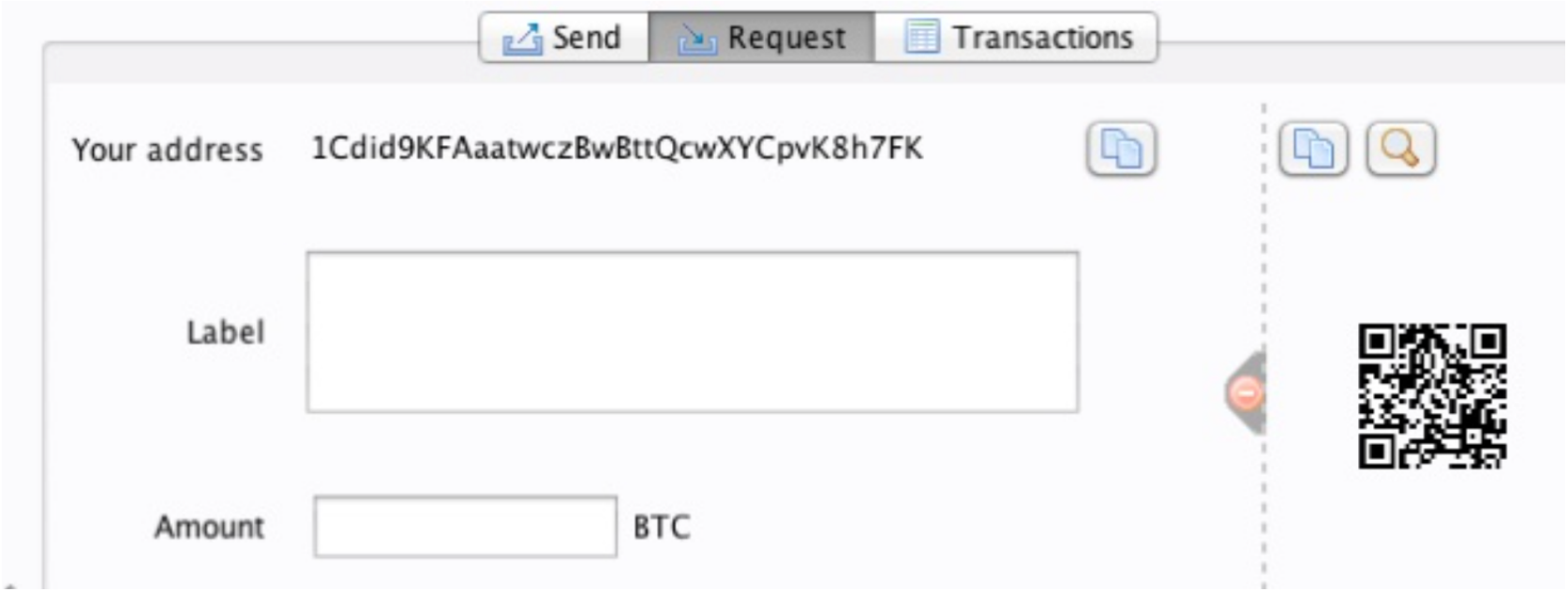


implications

BitCoin Wallet

bitcoin.org

Bitcoin Address



like email...

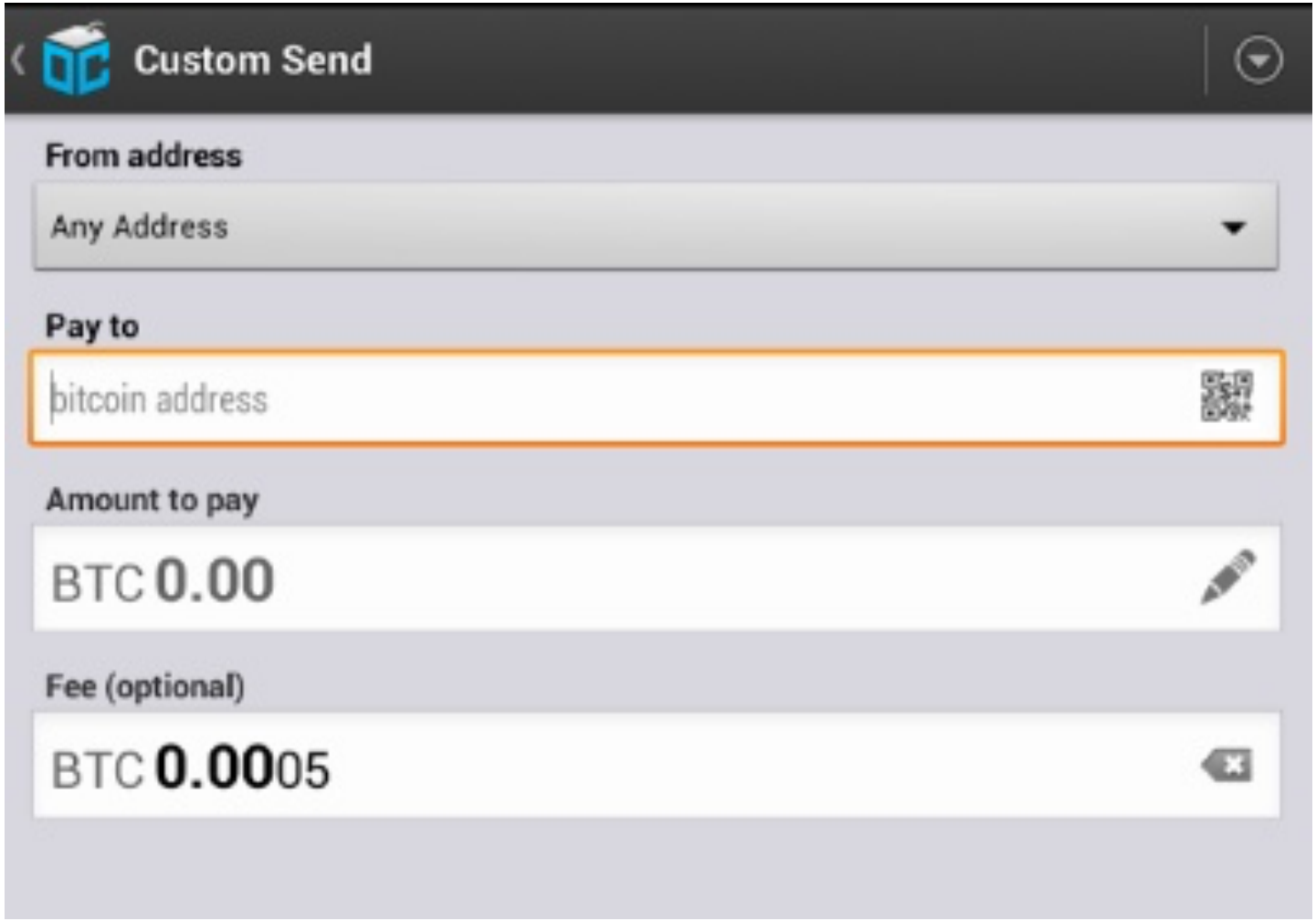
people can send stuff

UN-like email...

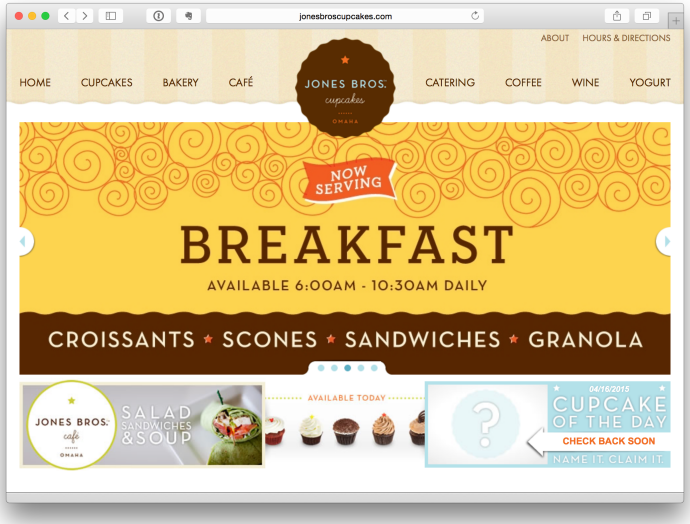
as many as you want

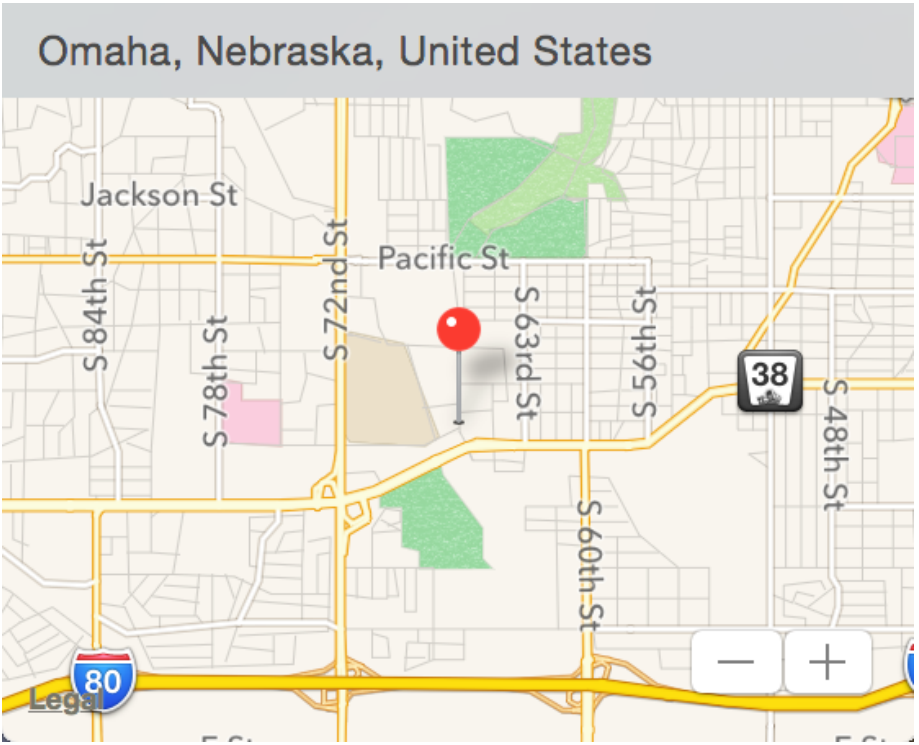
a wallet is a collection of addresses

Sending Bitcoin



Bitcoin ATM


jonesbroscupcakes.com
ABOUT
HOURS & DIRECTIONS
HOME
CUPCAKES
BAKERY
CAFÉ
JONES BROS. cupcakes
CATERING
COFFEE
WINE
YOGURT
NOW SERVING
BREAKFAST
AVAILABLE 6:00AM - 10:30AM DAILY
CROISSANTS ★ SCONES ★ SANDWICHES ★ GRANOLA
JONES BROS. cafe
SALAD SANDWICHES &SOUP
AVAILABLE TODAY
04/16/2015
CUPCAKE OF THE DAY
CHECK BACK SOON
NAME IT. CLAIM IT.

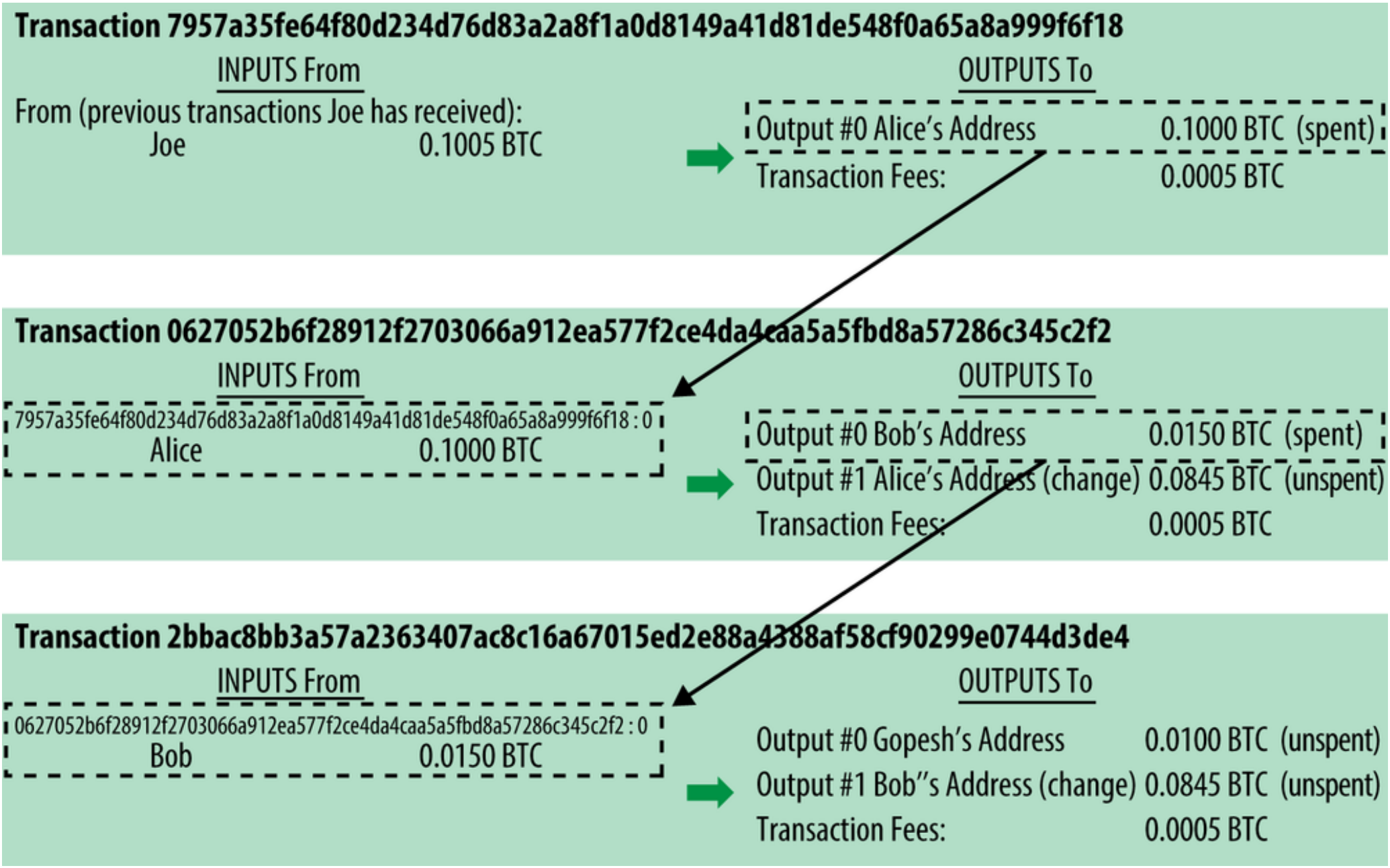

Omaha, Nebraska, United States
Jackson St
Pacific St
S 84th St
S 78th St
S 72nd St
S 63rd St
S 56th St
S 60th St
S 48th St
38
80
Legal


expresscoin
BTM
BITCOIN TELLER MACHINE
1 BTC
273.82 USD
START
Select Language / Selecciona Idioma
English
Español
www.zenbox.us
Printer
Cash Acceptor
Cash Dispenser
zenBox
Harmoniously

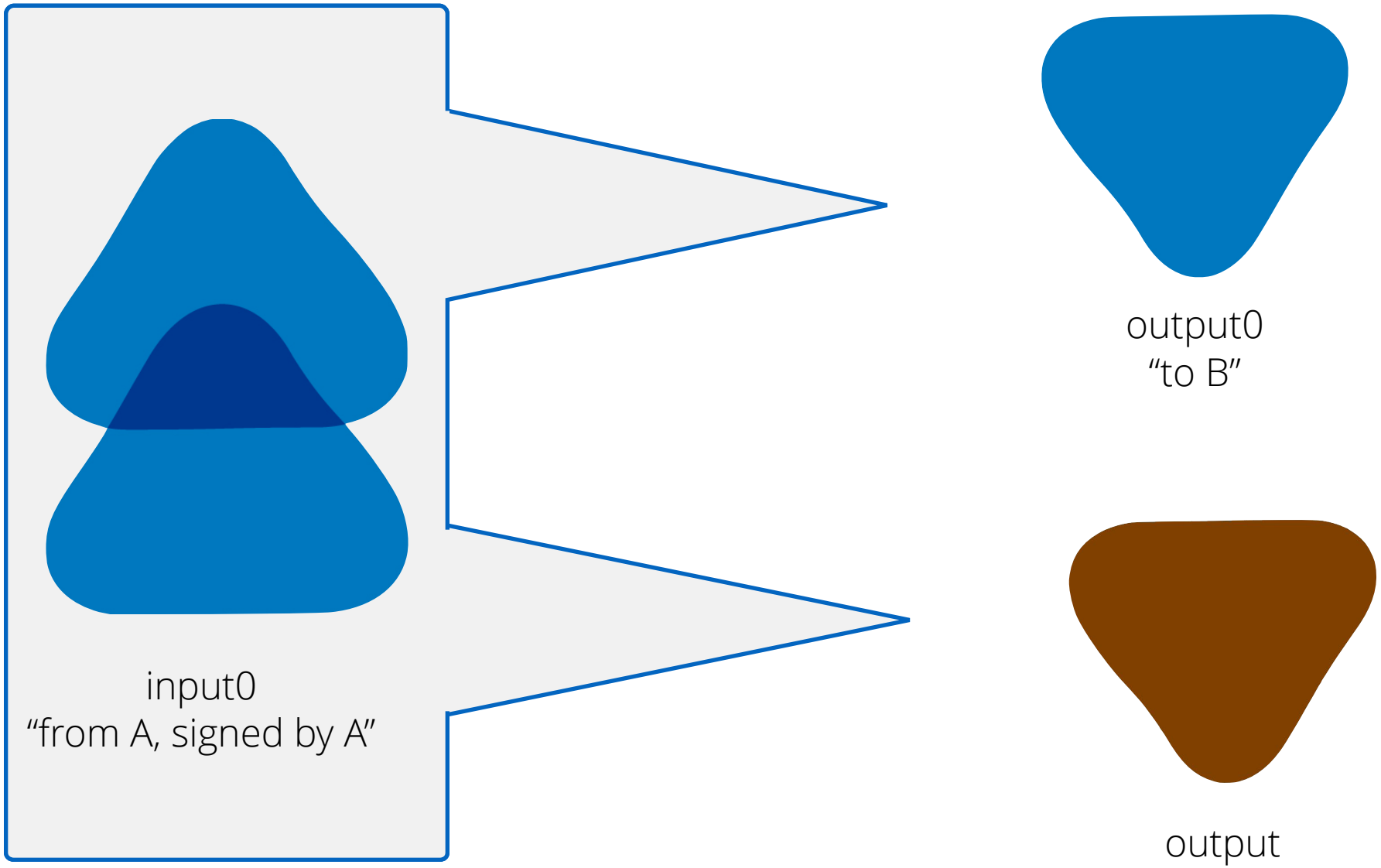
Buy a Cup of Coffee

bitcoin:1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA?
amount=0.015&
label=Bob%27s%20Cafe&
message=Purchase%20at%20Bob%27s%20Cafe

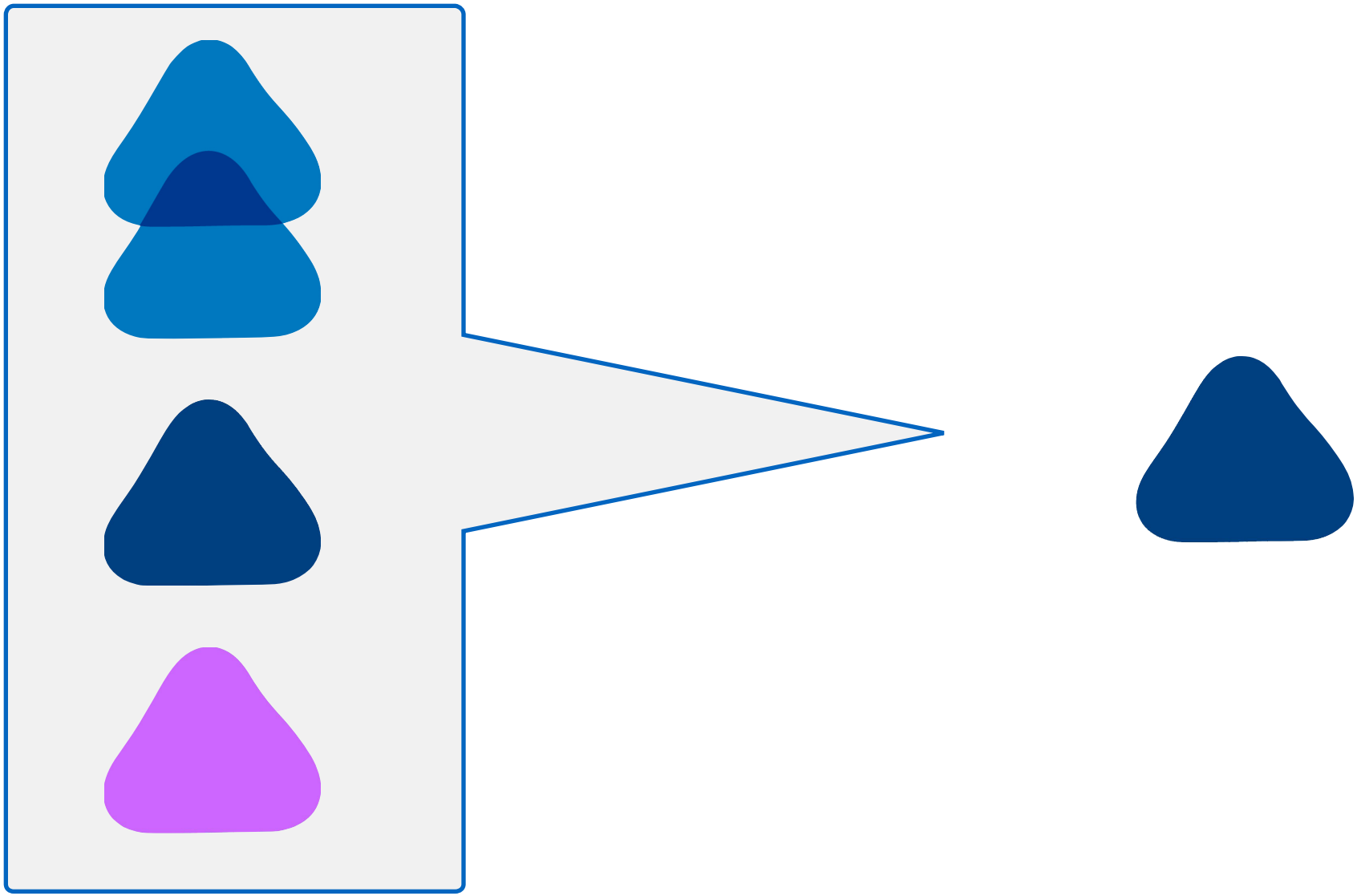
Transaction Chain



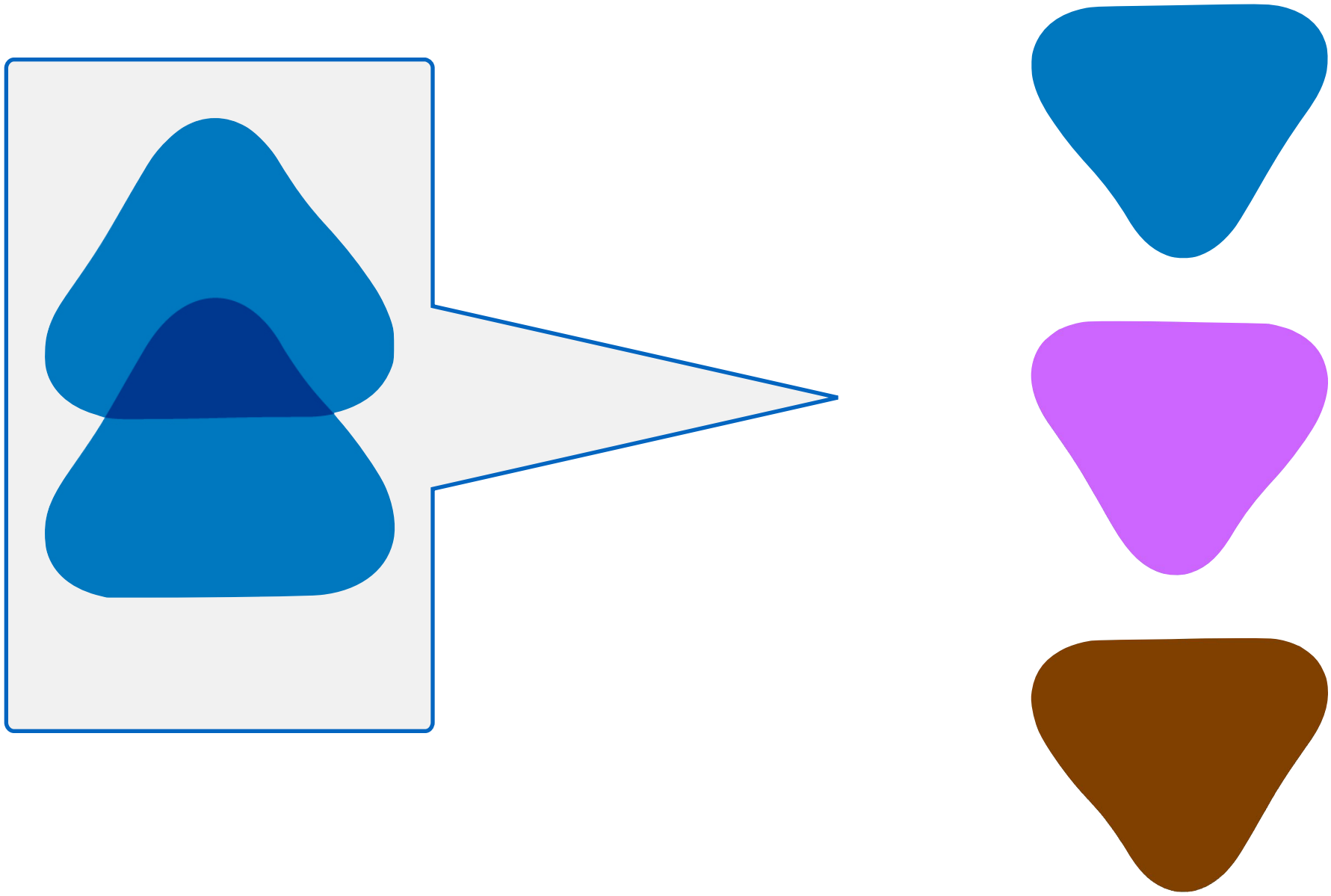
Common Transaction



Aggregate Transaction



Distributing Transaction



Committing

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

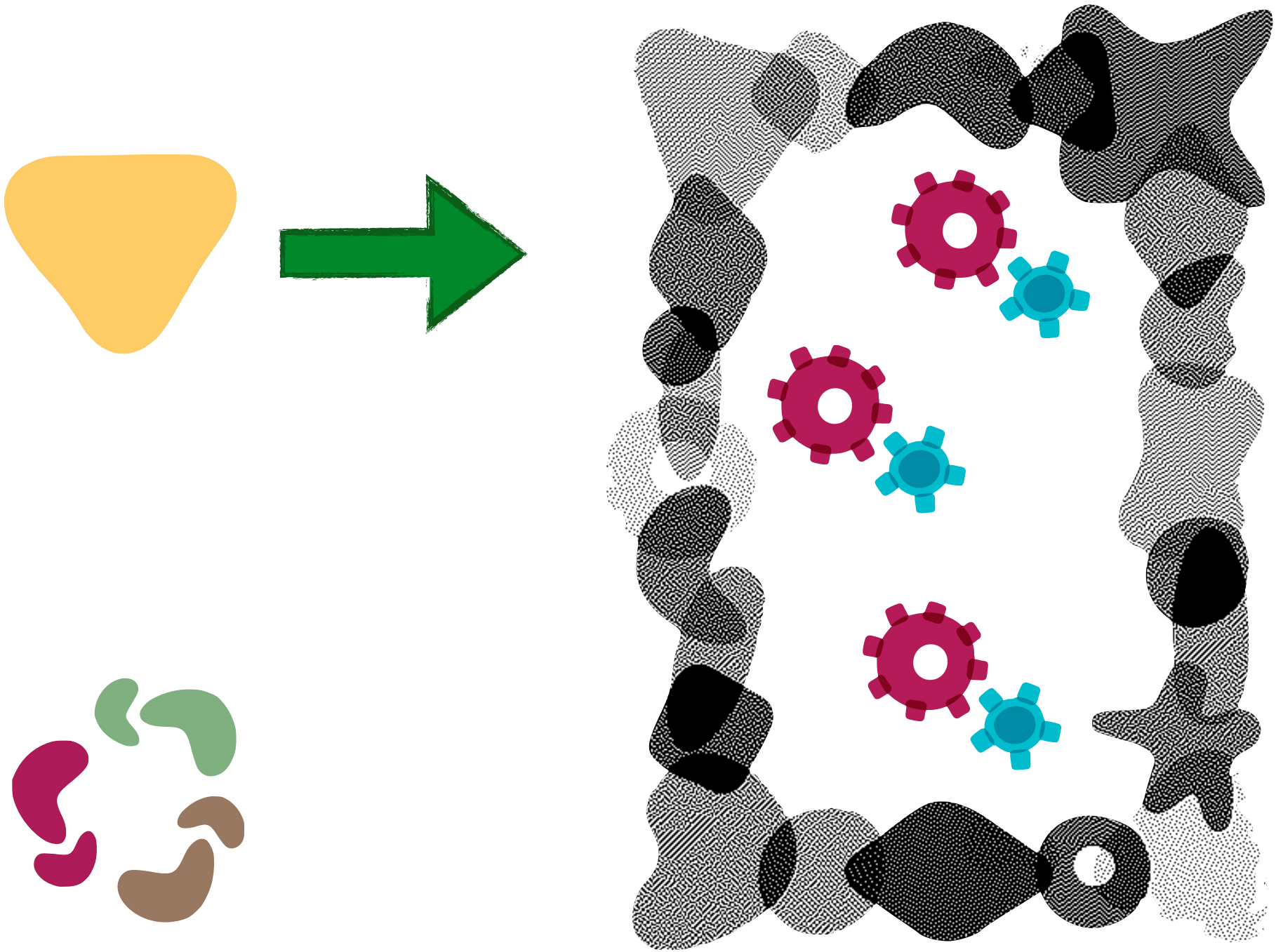
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

97 Confirmations | 0.0995 BTC

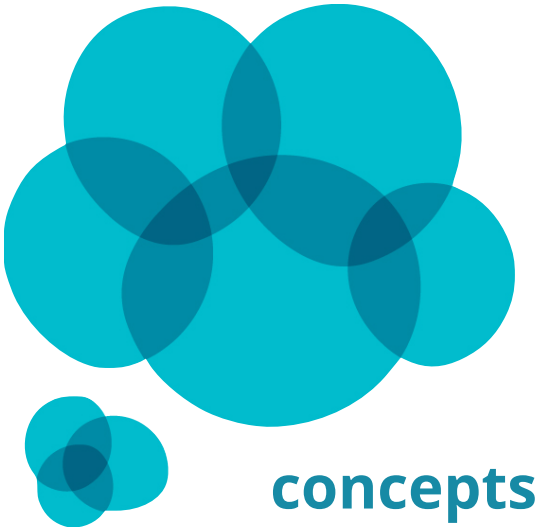
Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

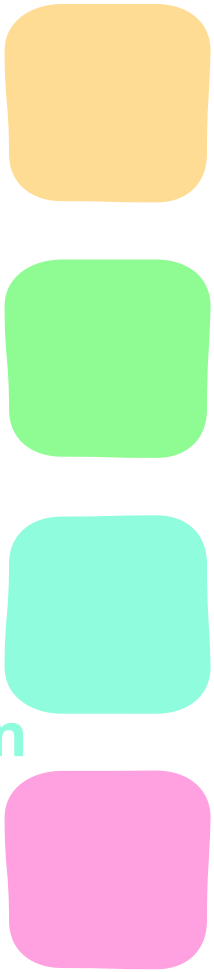
Add a Transaction to the Ledger



Agenda

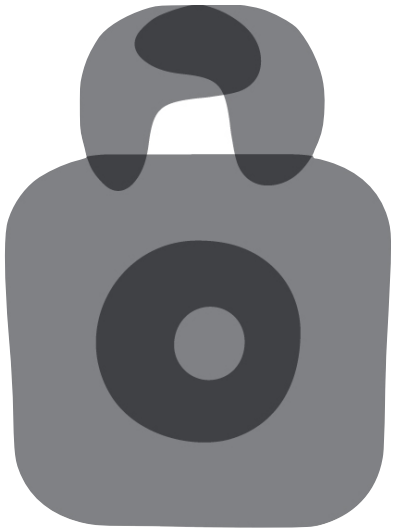


concepts

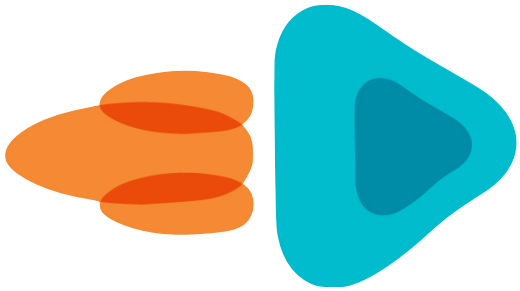


blockchain

transactions

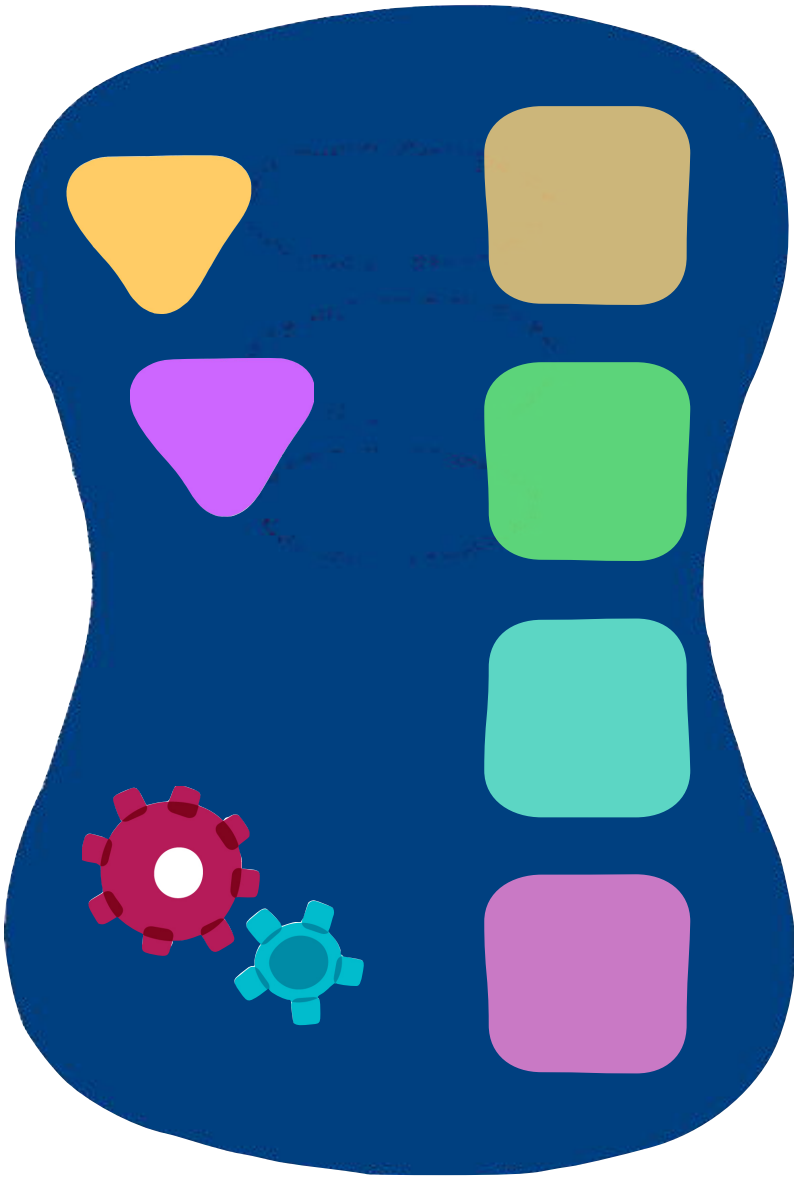


security



implications

Mining

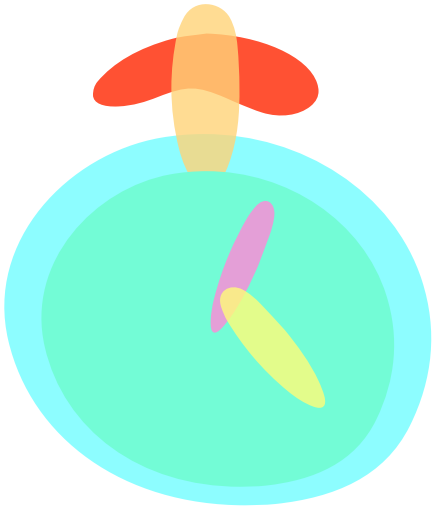


Mining is the process by which new bitcoin is added to the money supply

new bitcoin

transaction fee

Difficulty Targeting & Retargeting



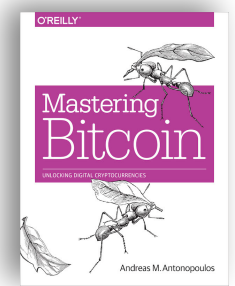
BitCoin blocks are generated every 10 minutes (on average)

expanded to accommodate increasing computing power

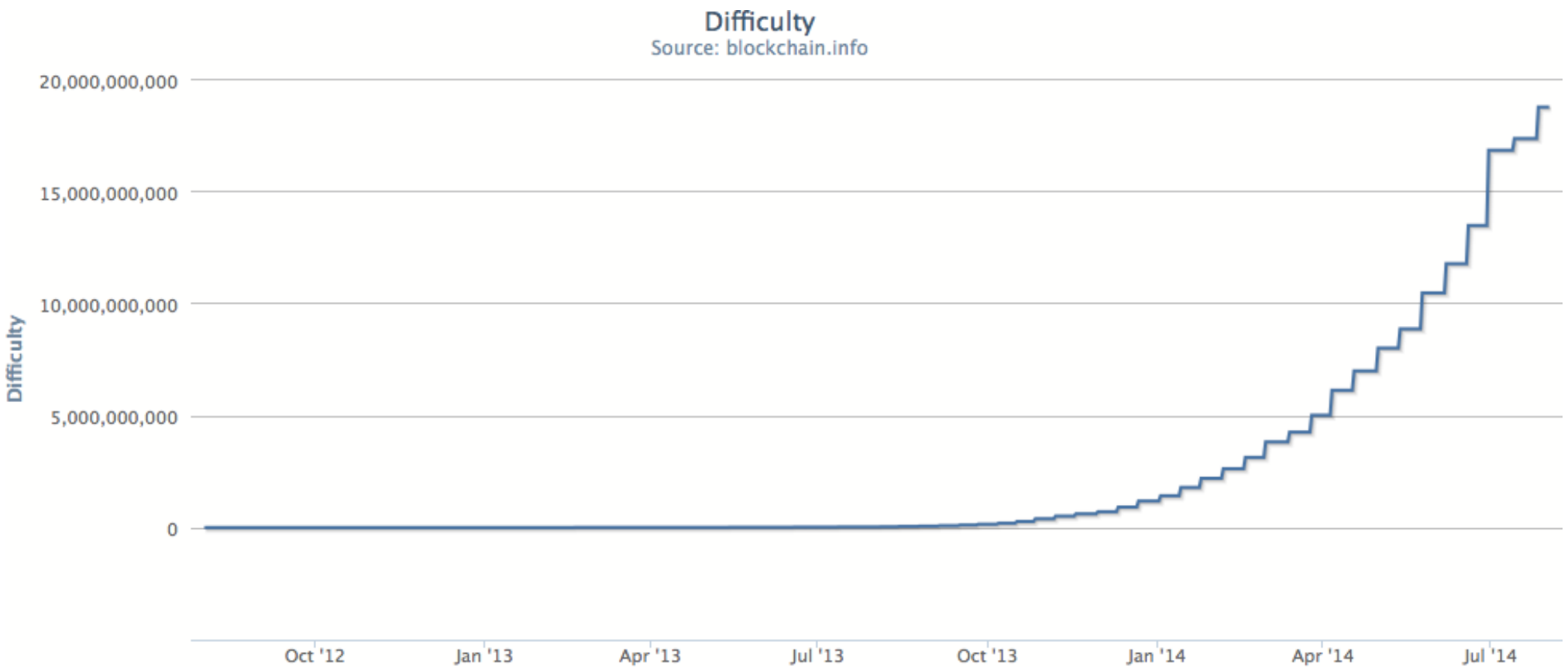
New Difficulty = Old Difficulty * (Actual Time of Last 2016 Blocks / 20160 minutes)

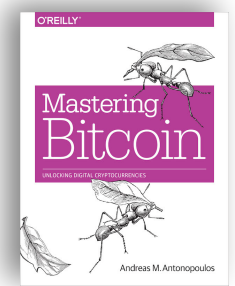
The actual cost of bitcoin mining is how much electricity you burn to achieve success.

Mining Trends

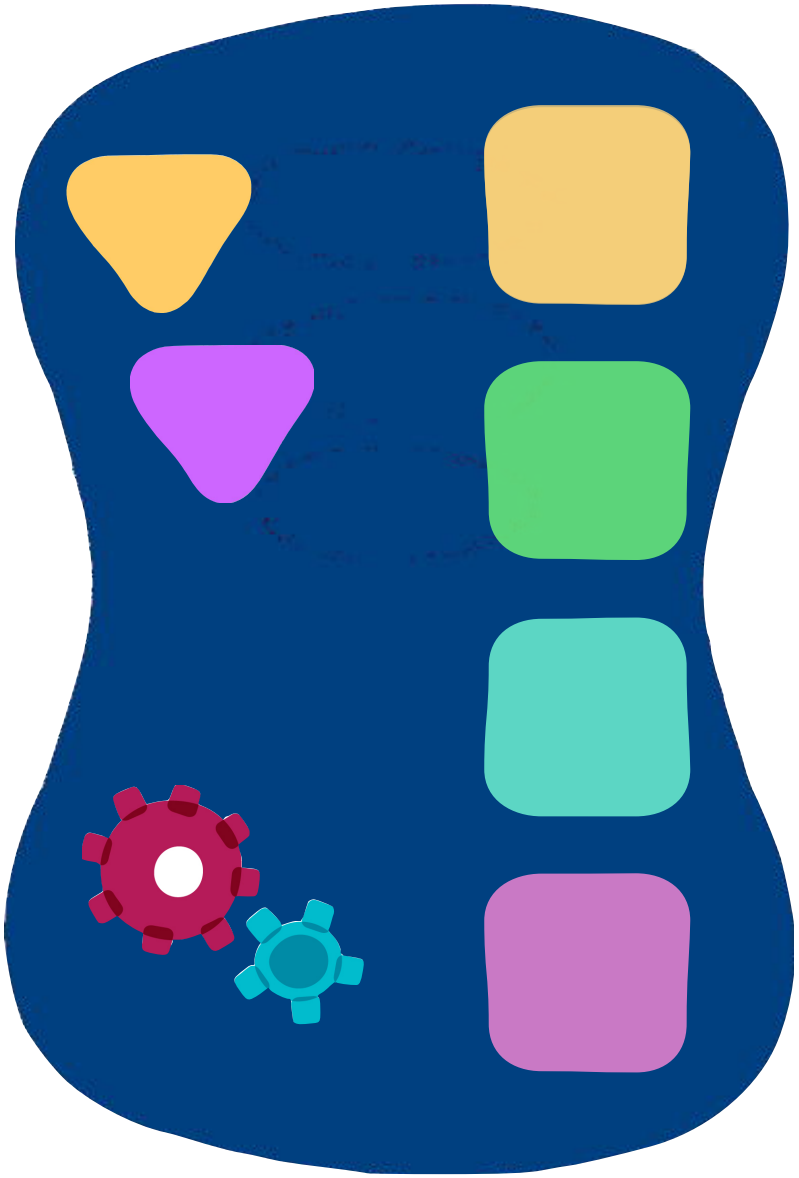


Escalating Difficulty



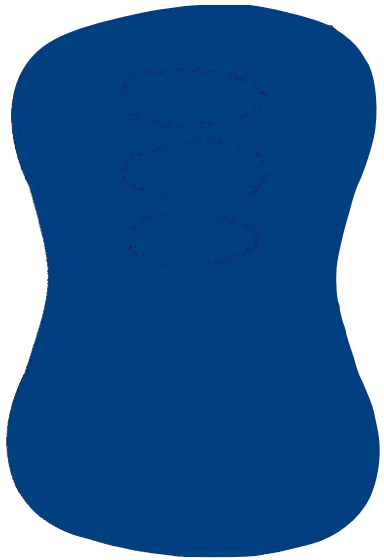


Mining

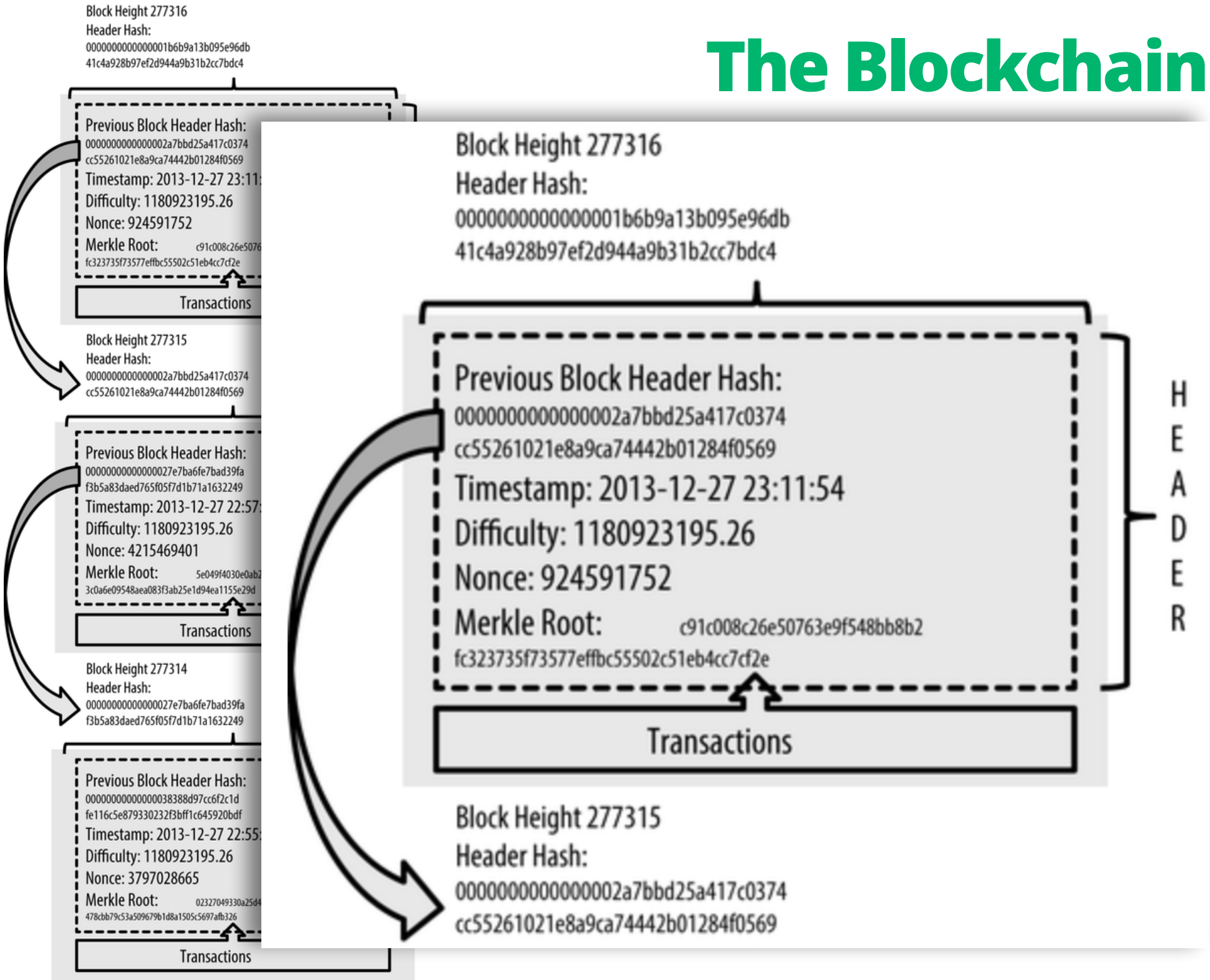


Mining

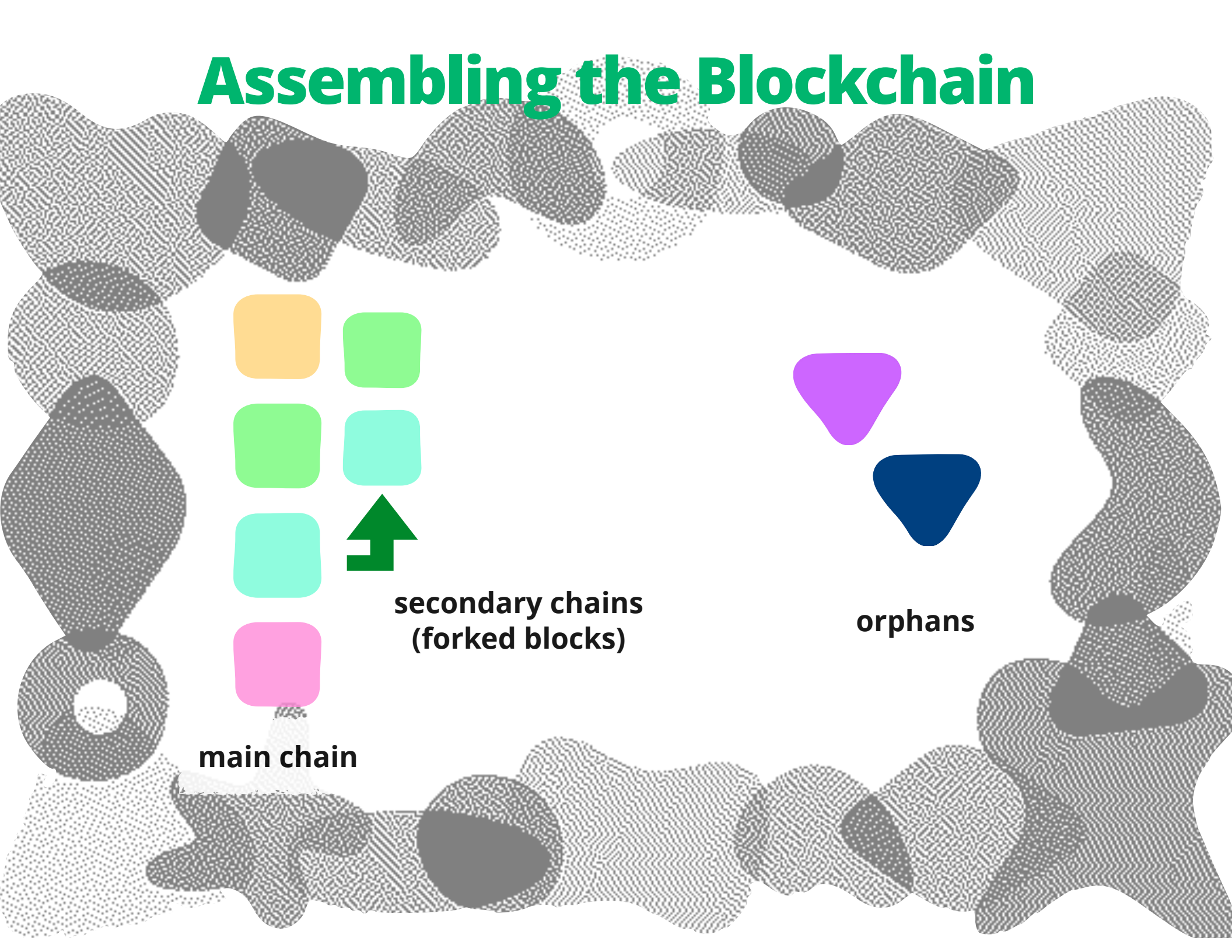
$$\text{Priority} = \frac{\sum(\text{Value of input} * \text{Input Age})}{\text{Transaction Size}}$$



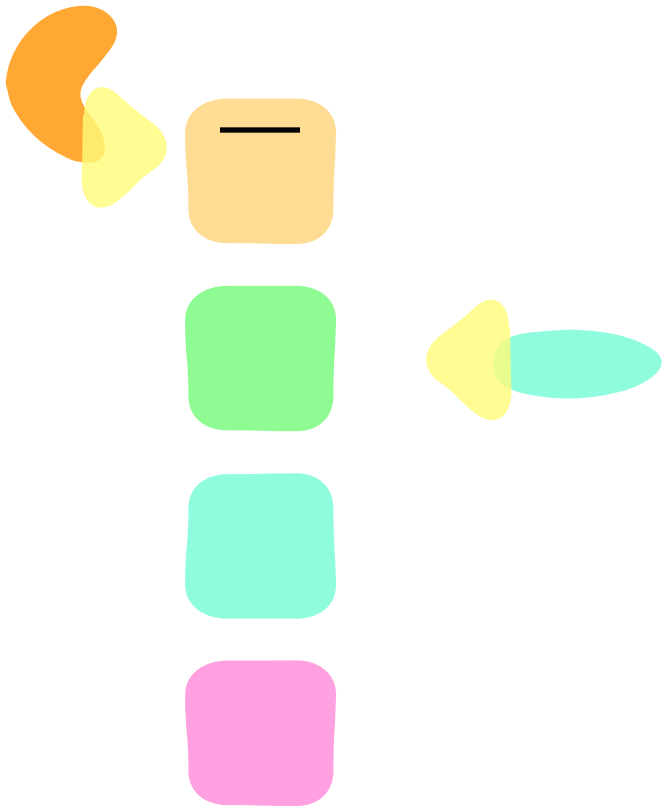
The Blockchain

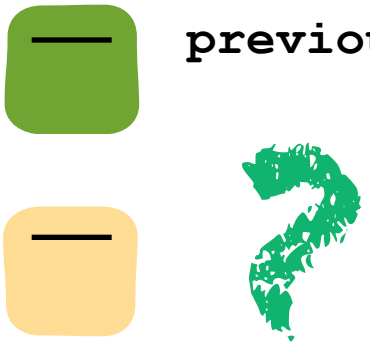


Assembling the Blockchain



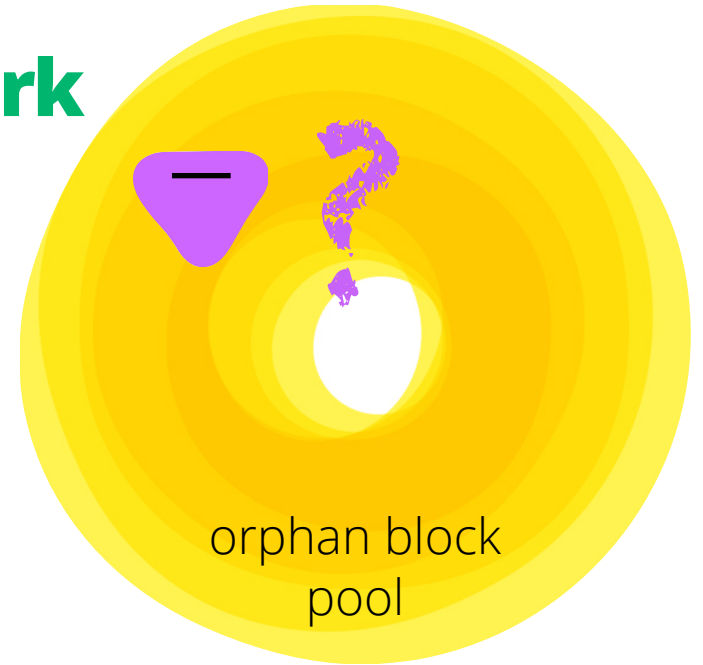
Adding to the Blockchain



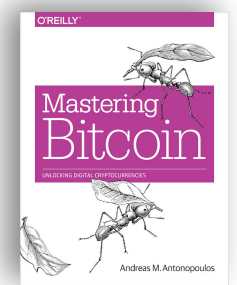


`previous block hash == parent`

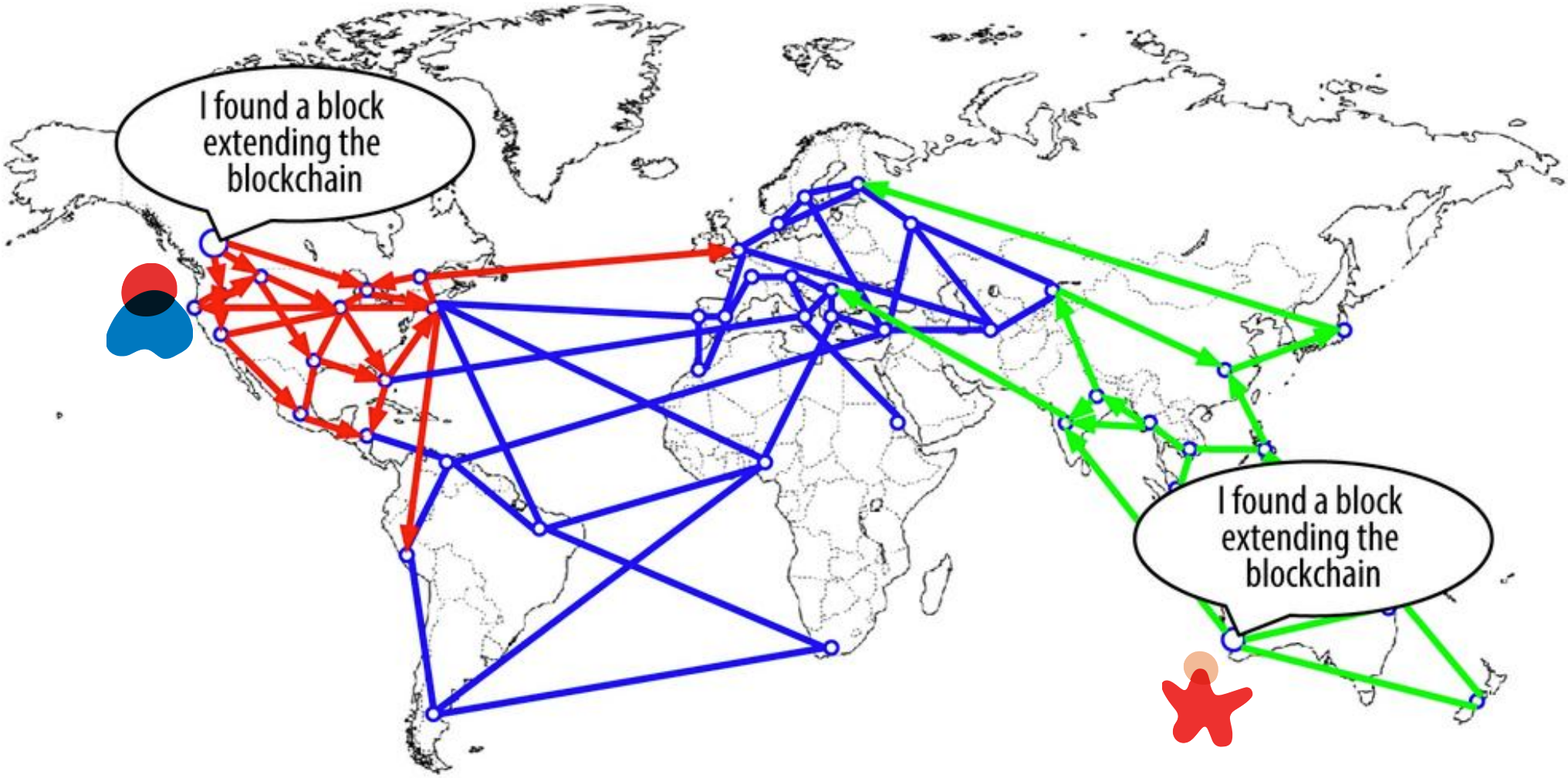
Blockchain Fork

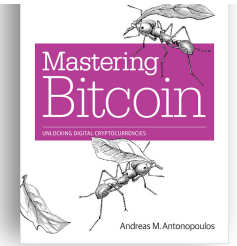


Blockchain Fork

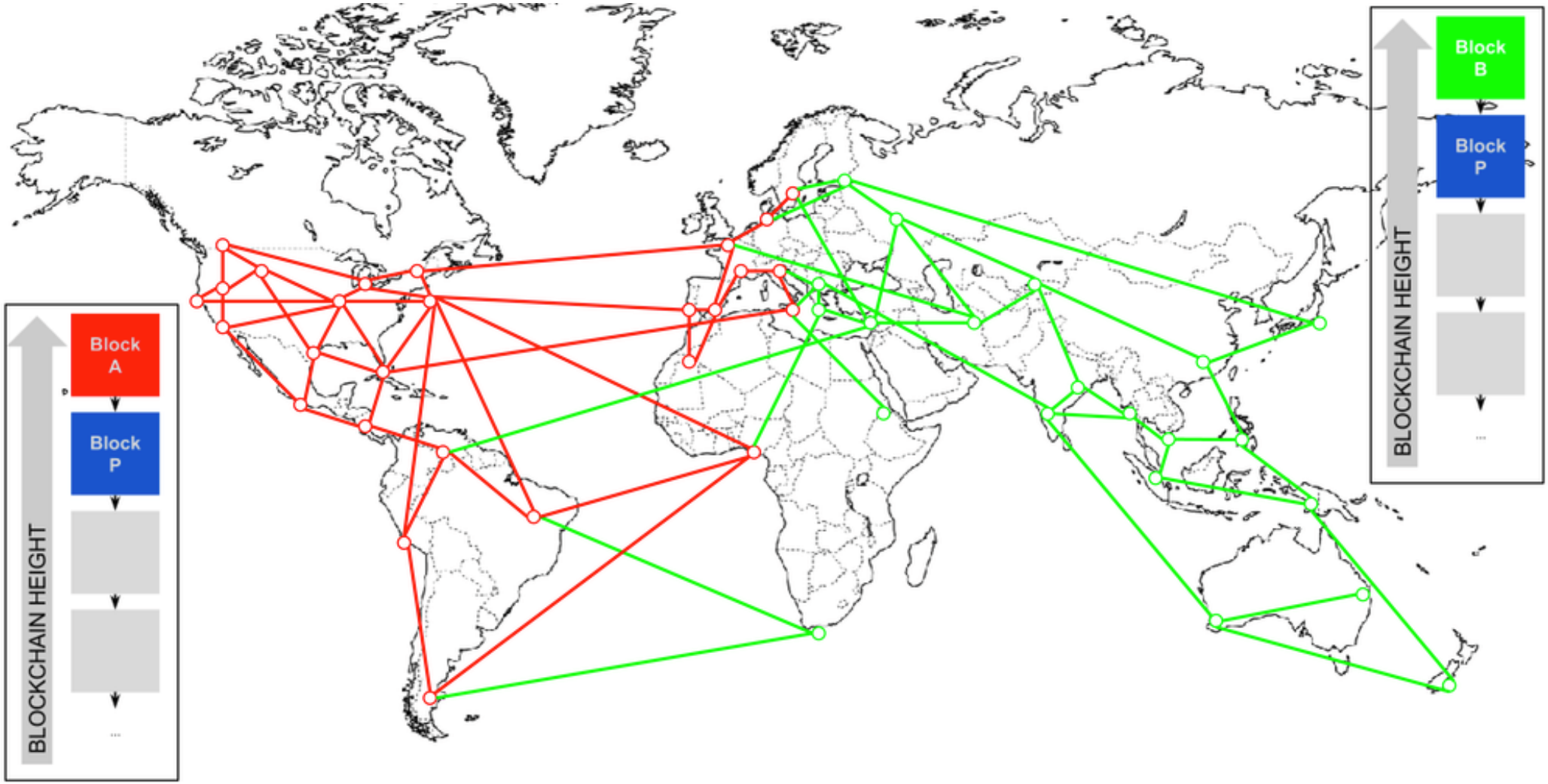


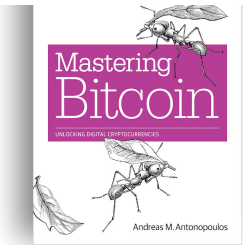
Blockchain Fork



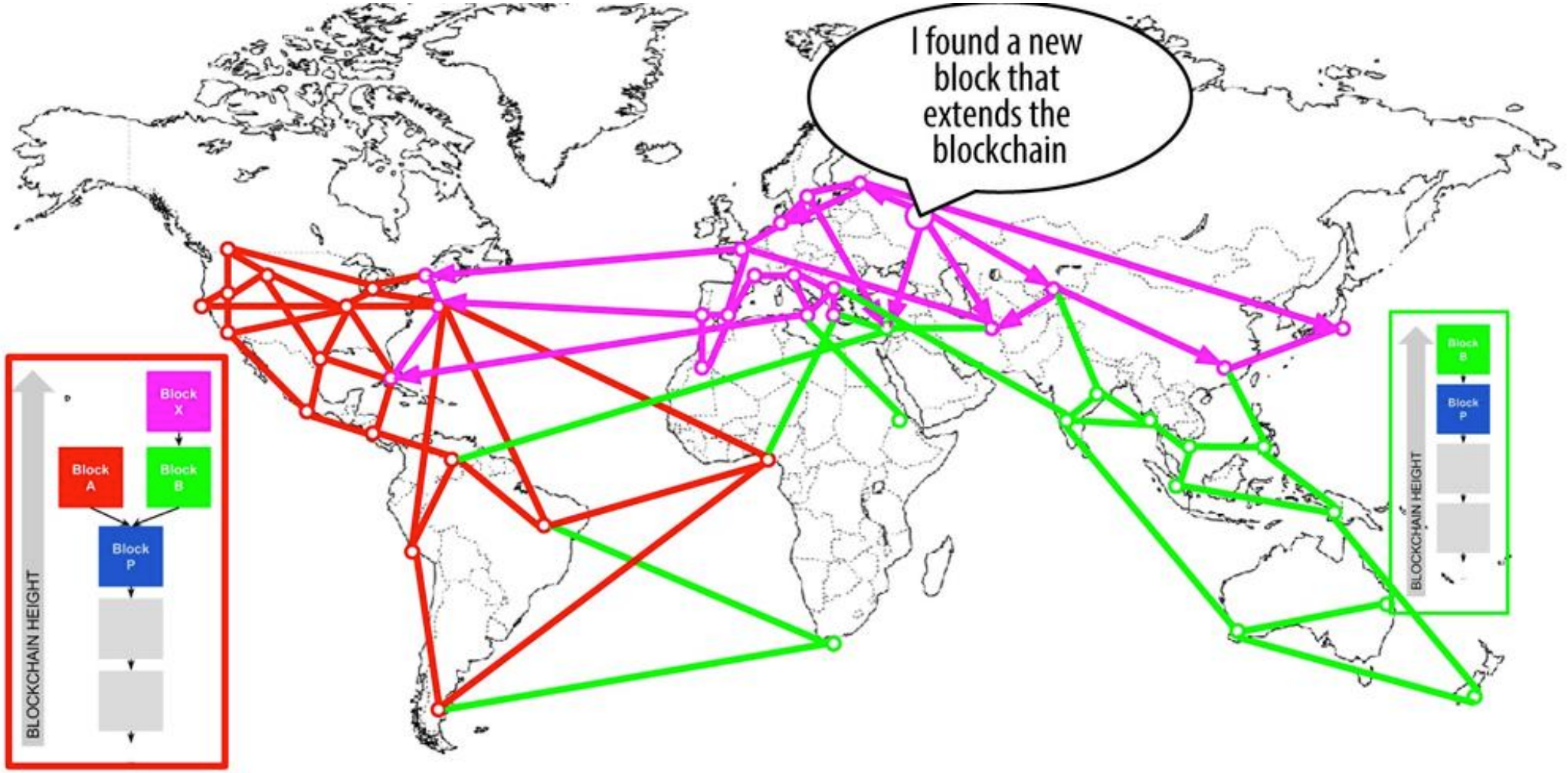


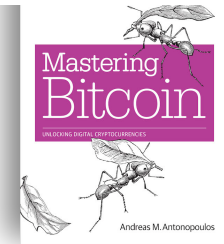
Blockchain Fork



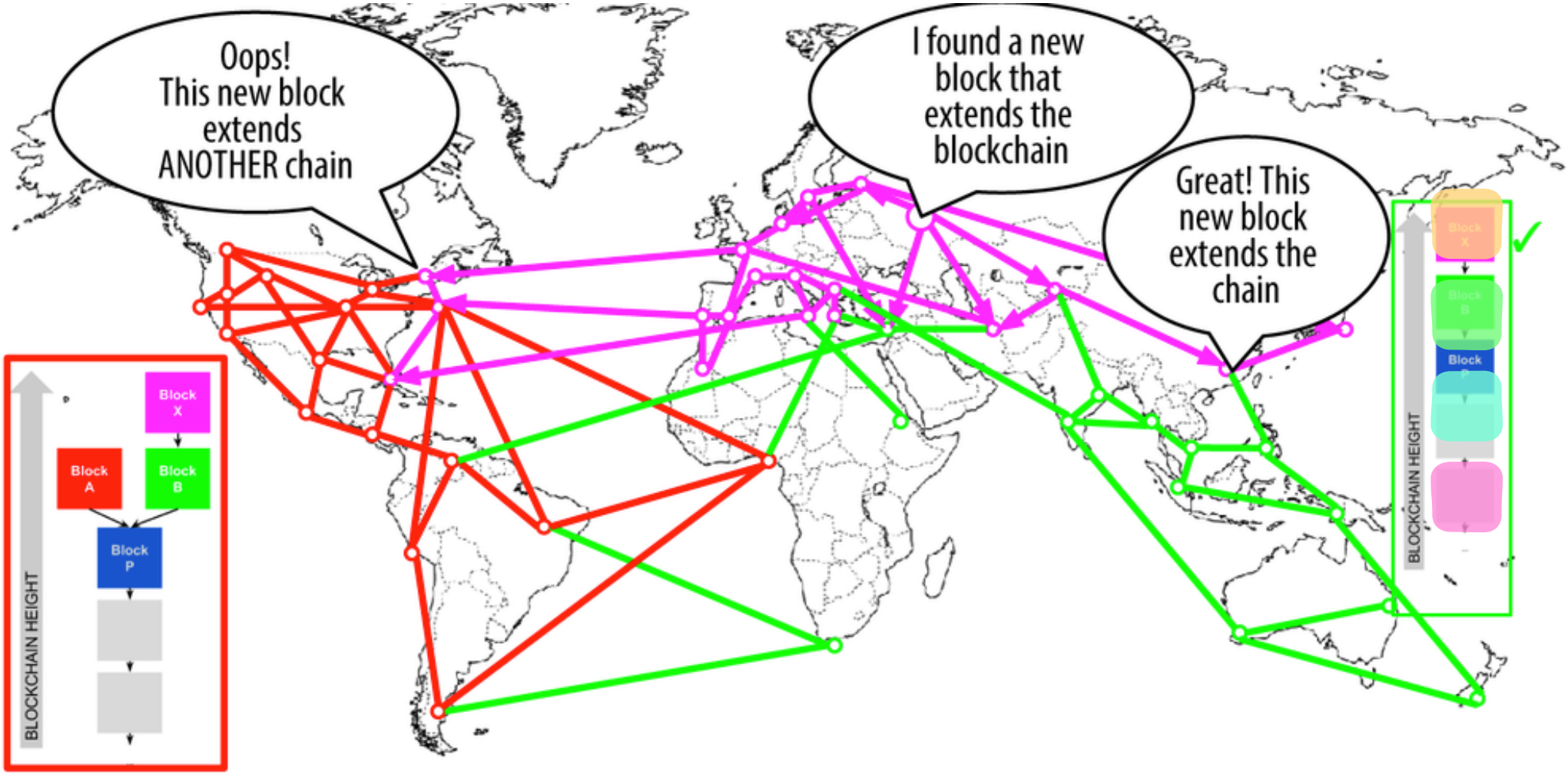


Blockchain Fork

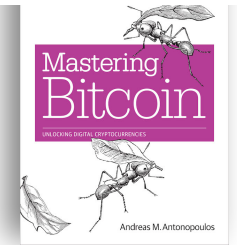




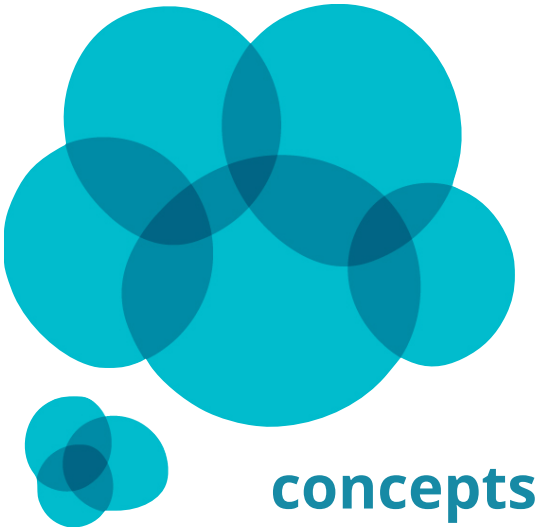
Blockchain Fork



When in doubt, look for the most work



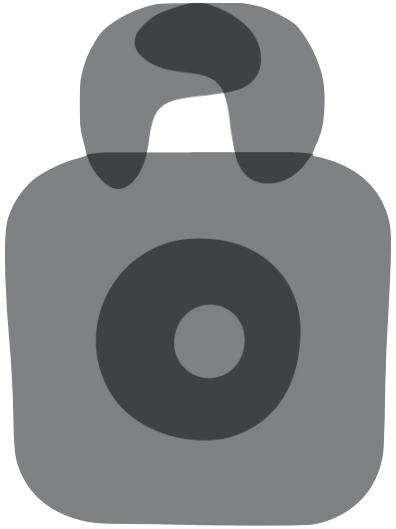
Agenda



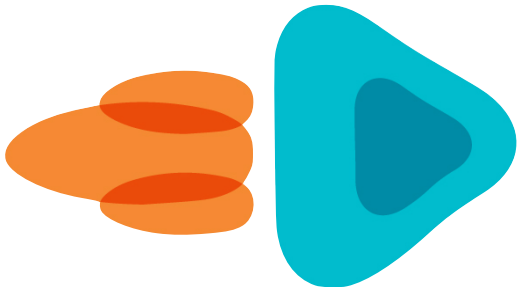
concepts

blockchain

transactions

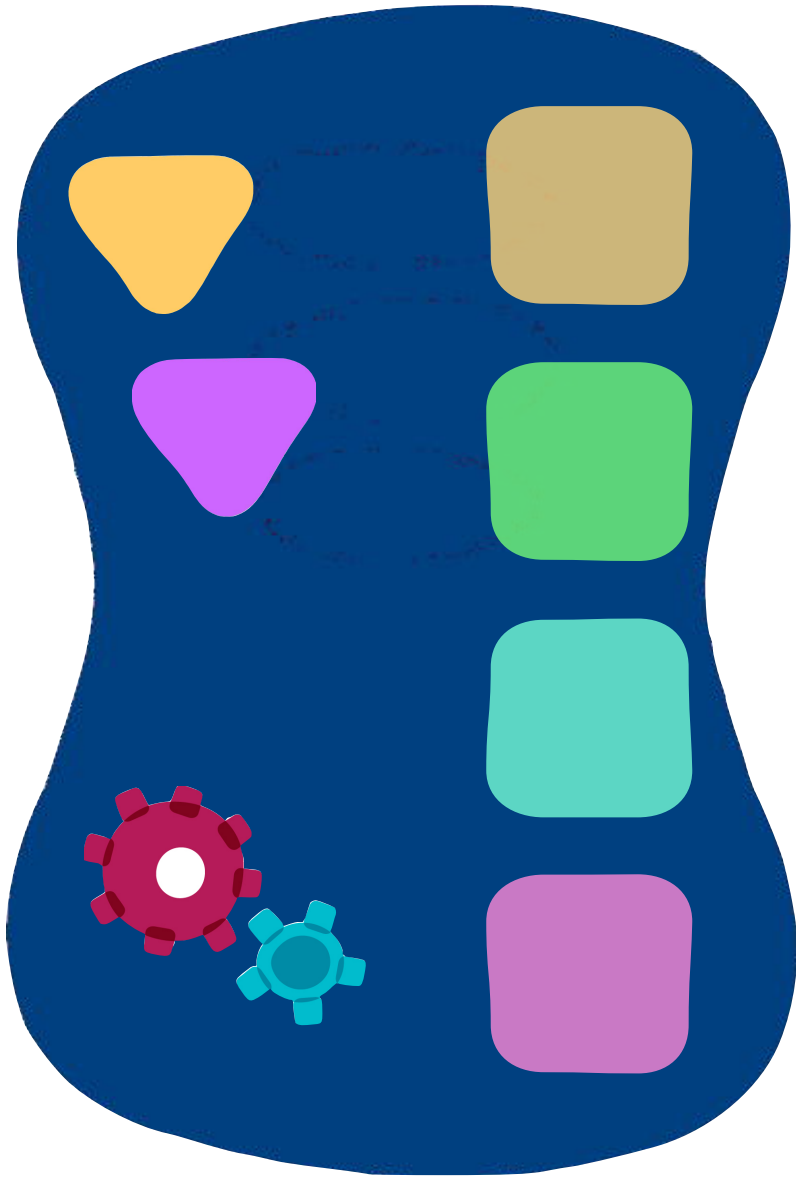


security



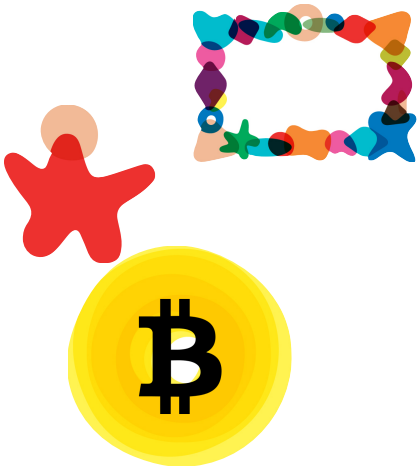
implications

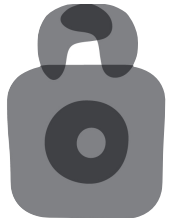
Validating a Block



- The block data structure is syntactically valid
- The block header hash is less than the target difficulty (enforces the proof of work)
- The block timestamp is less than two hours in the future (allowing for time errors)
- The block size is within acceptable limits
- The first transaction (and only the first) is a coinbase generation transaction
- All transactions within the block are valid using the transaction checklist discussed in Independent Verification of Transactions

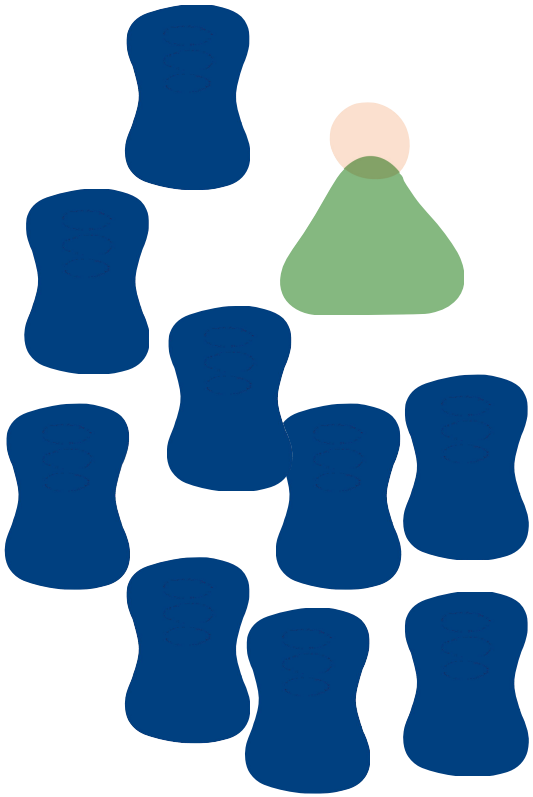
Consensus Attacks





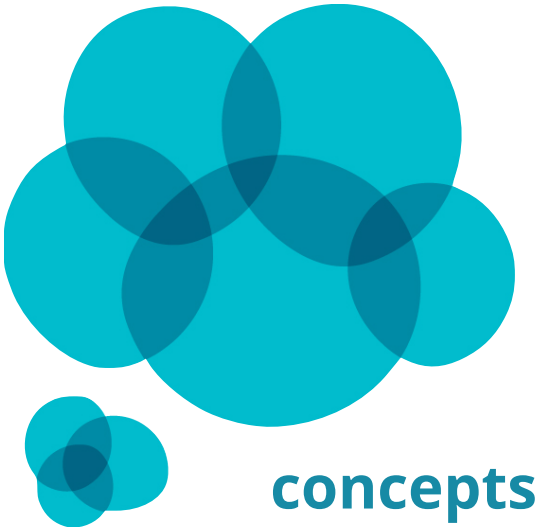
"51 %" attack

For big transactions, wait for 6 new blocks (~ 1 hour)



the older the transaction,
the more immutable it is

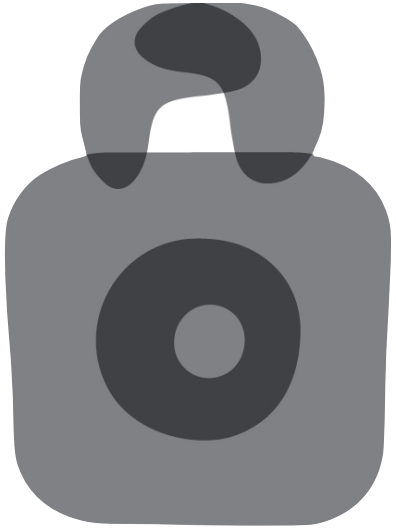
Agenda



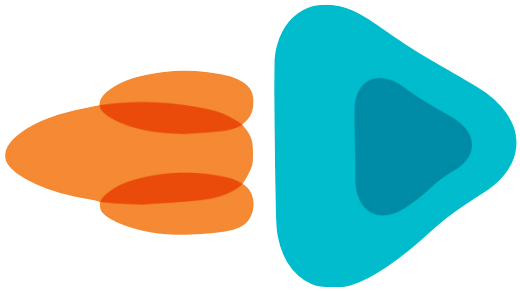
concepts

blockchain

transactions



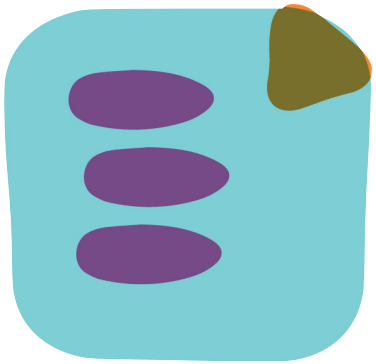
security



implications

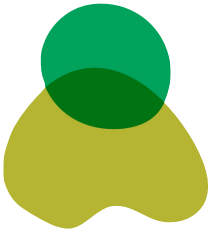
Implications

currency

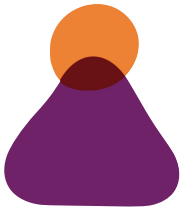


contracts

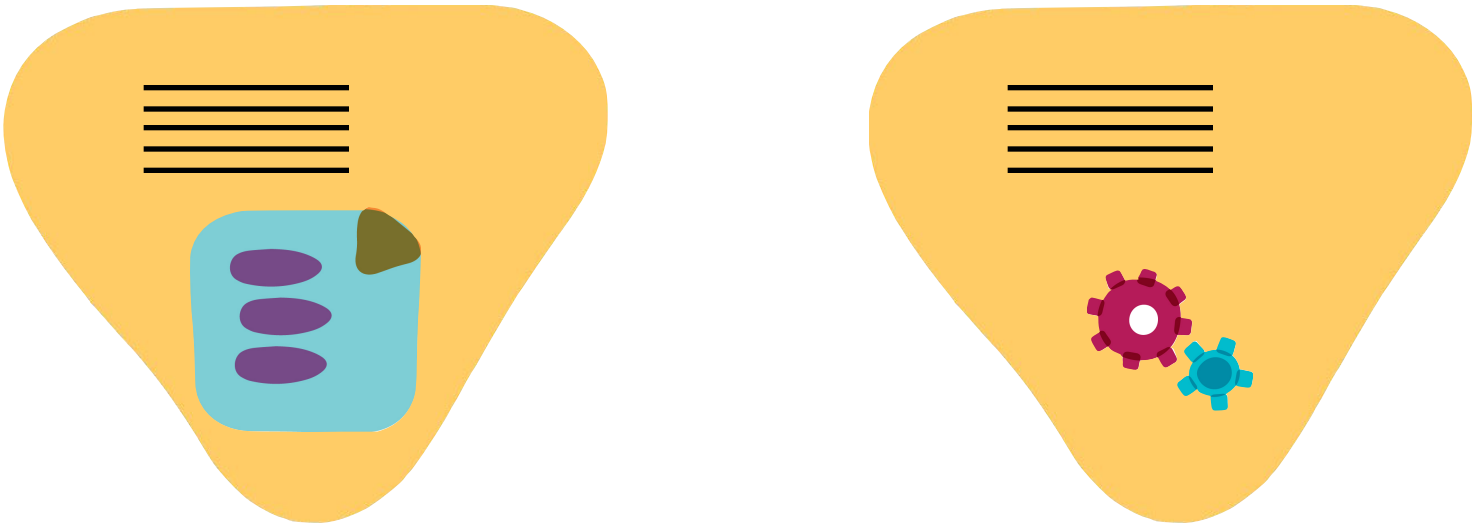
reputation index



voting



Content Binding

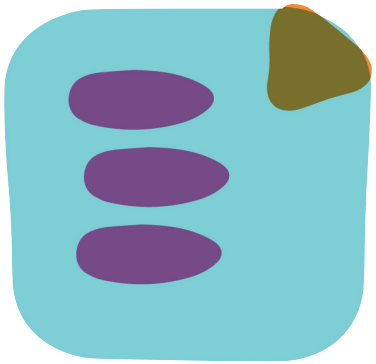


Transaction fees include size

Bigger payload == bigger fee

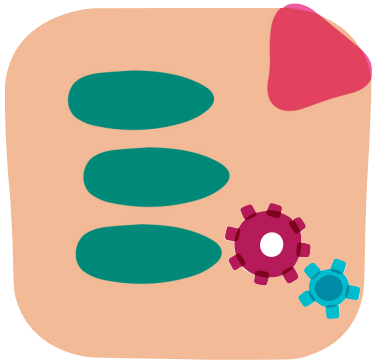
Implications

currency



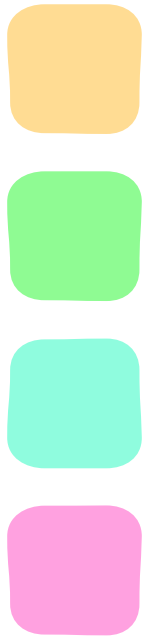
contracts

reputation
index



contracts
w/
conditions

voting

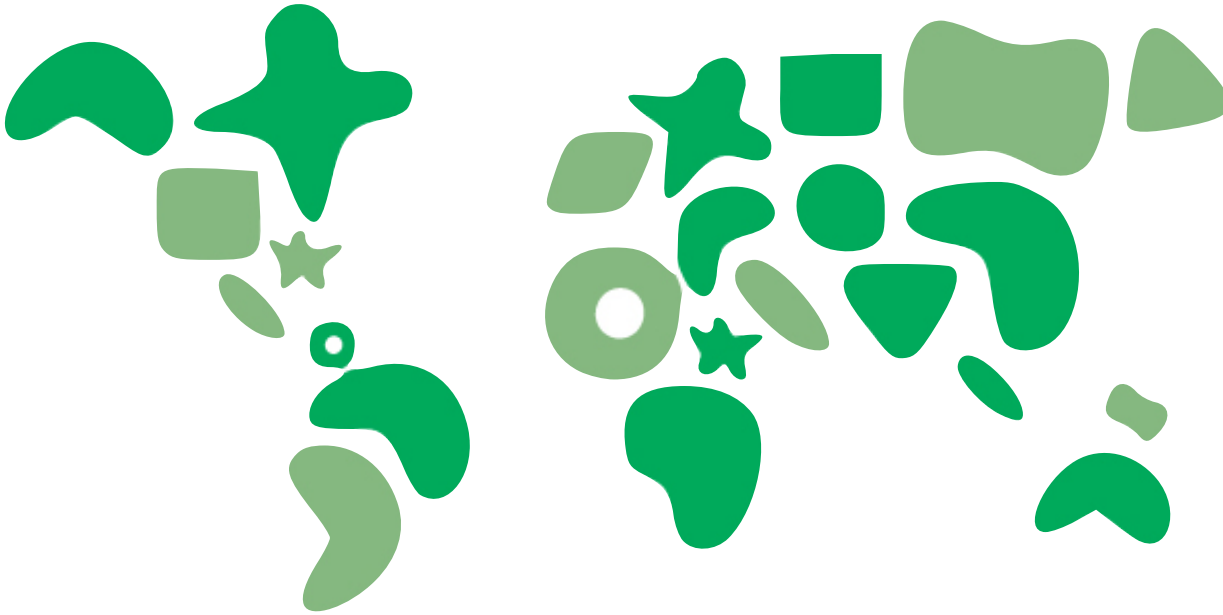


blockchain

Positive Feedback Loop

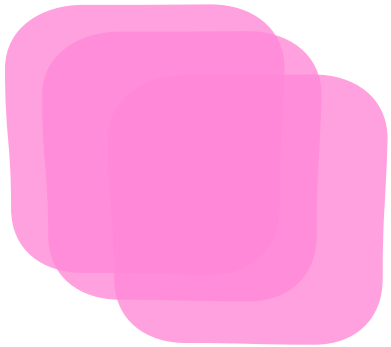
Benefits

international remittance (w/ little or no fees)



international currency

micropayments



fight spam

public payments

Immutable == Forever

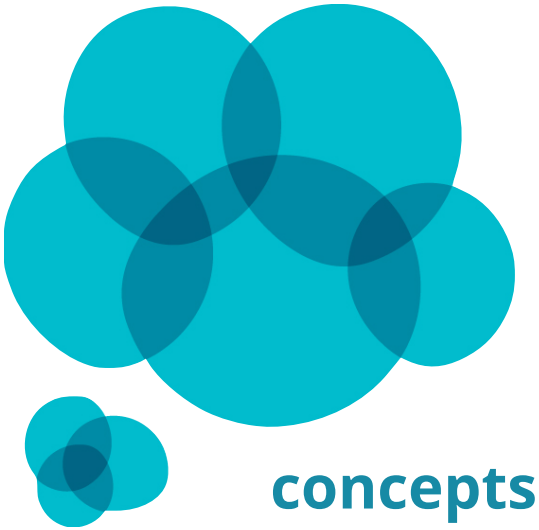
Permanent ledger

Distributed globally

The older it is, the more immutable it is

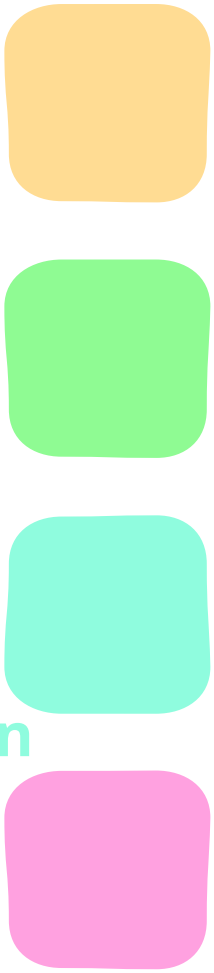
Be careful !

Summary

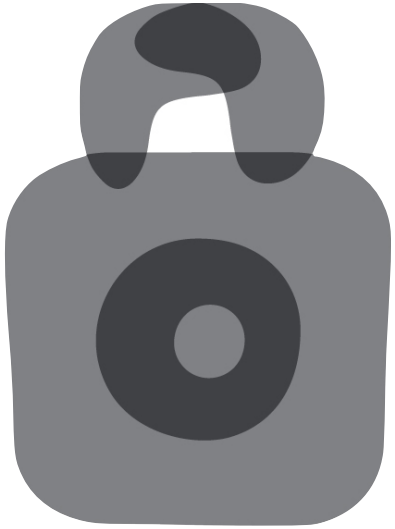


concepts

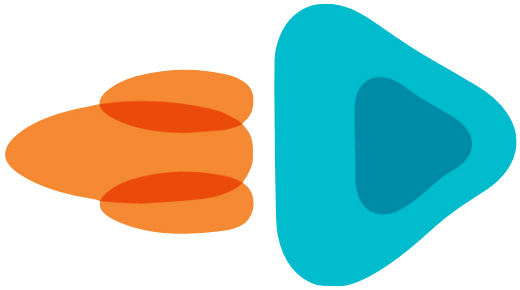
transactions



blockchain

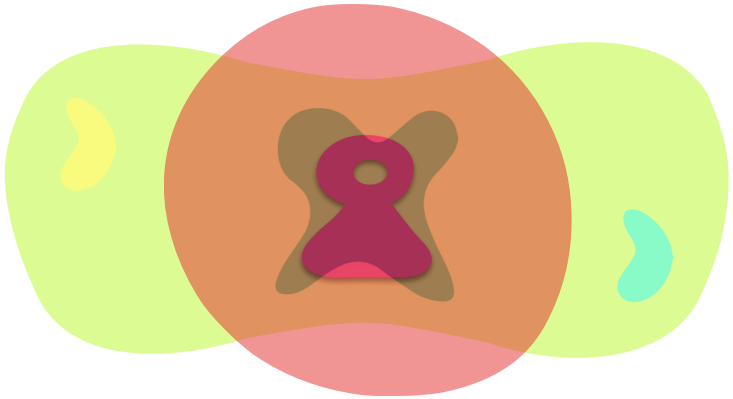


security

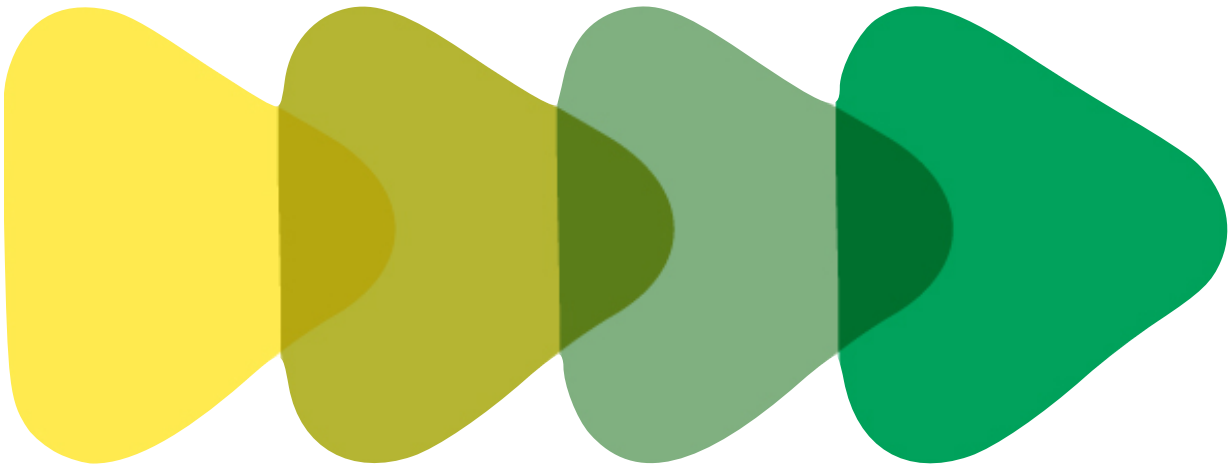


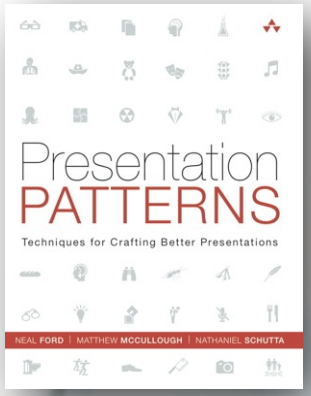
implications

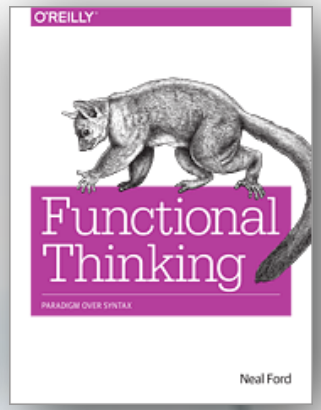
Distributed Trust



“...the most important Internet protocol since email.”







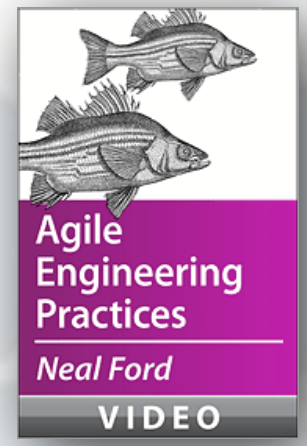
nealford.com

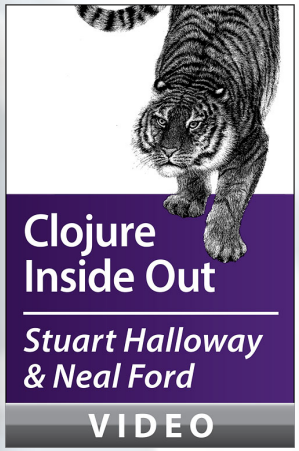
@neal4d

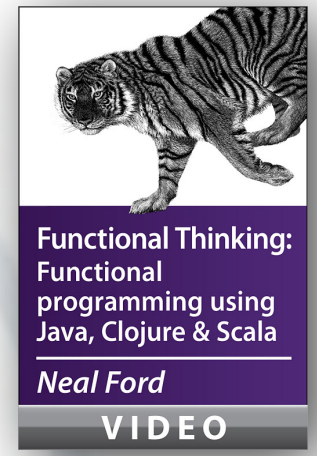
ThoughtWorks®

NEAL FORD

Director / Software Architect / Meme Wrangler







O'REILLY®

SOFTWARE ARCHITECTURE SERIES