

CRYPTOCURRENCY

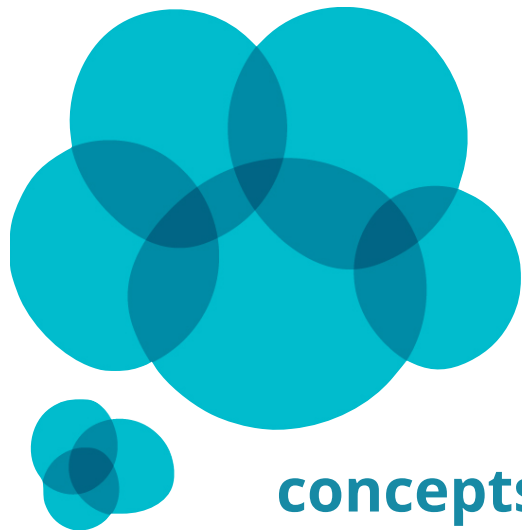
How It Works & Why It Matters

ThoughtWorks®

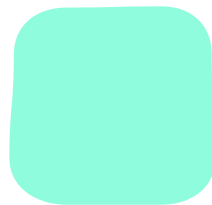
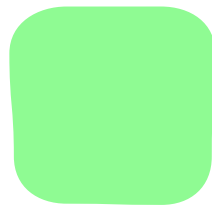
NEAL FORD

Director / Software Architect / Meme Wrangler

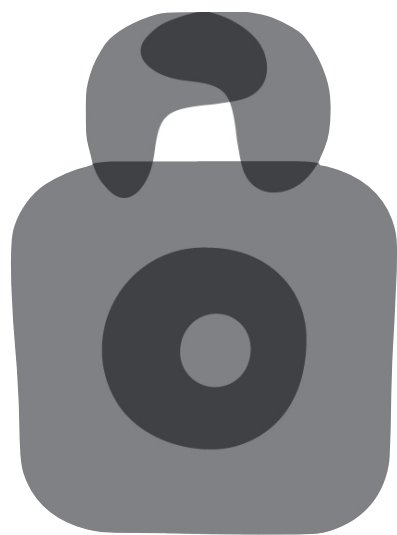
Agenda



concepts

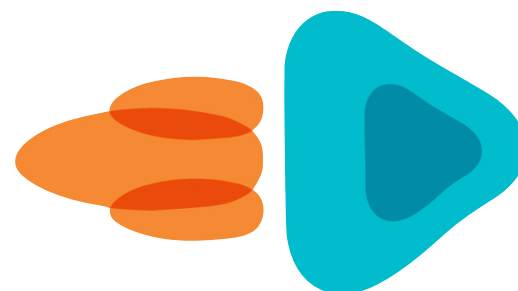


blockchain



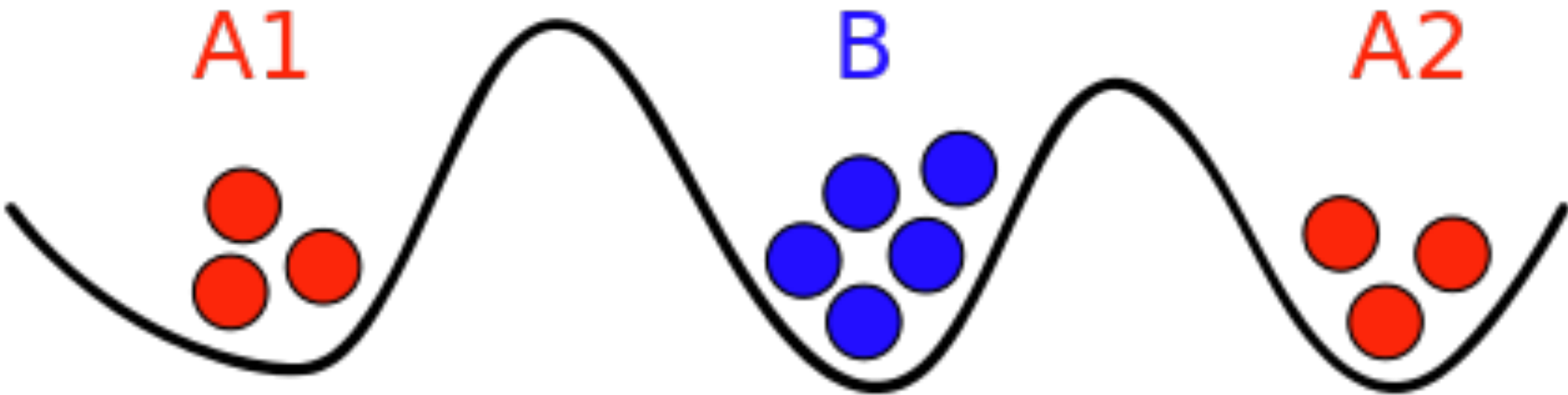
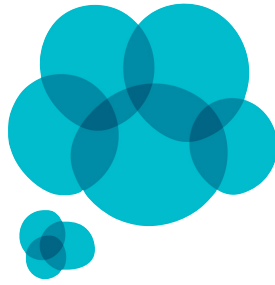
security

transactions



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

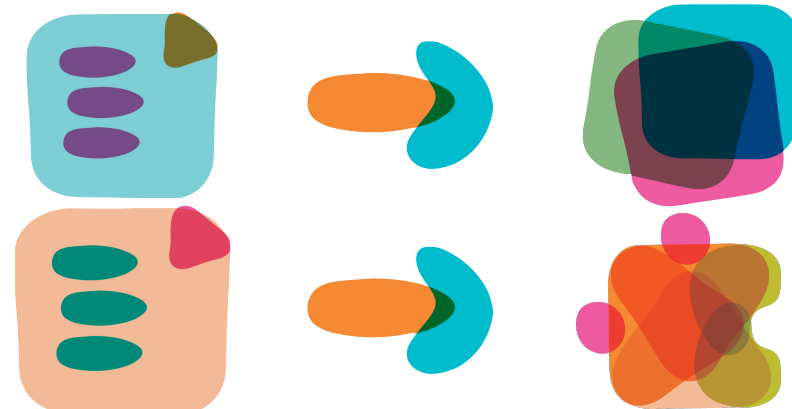


infeasible to generate a
message from its hash

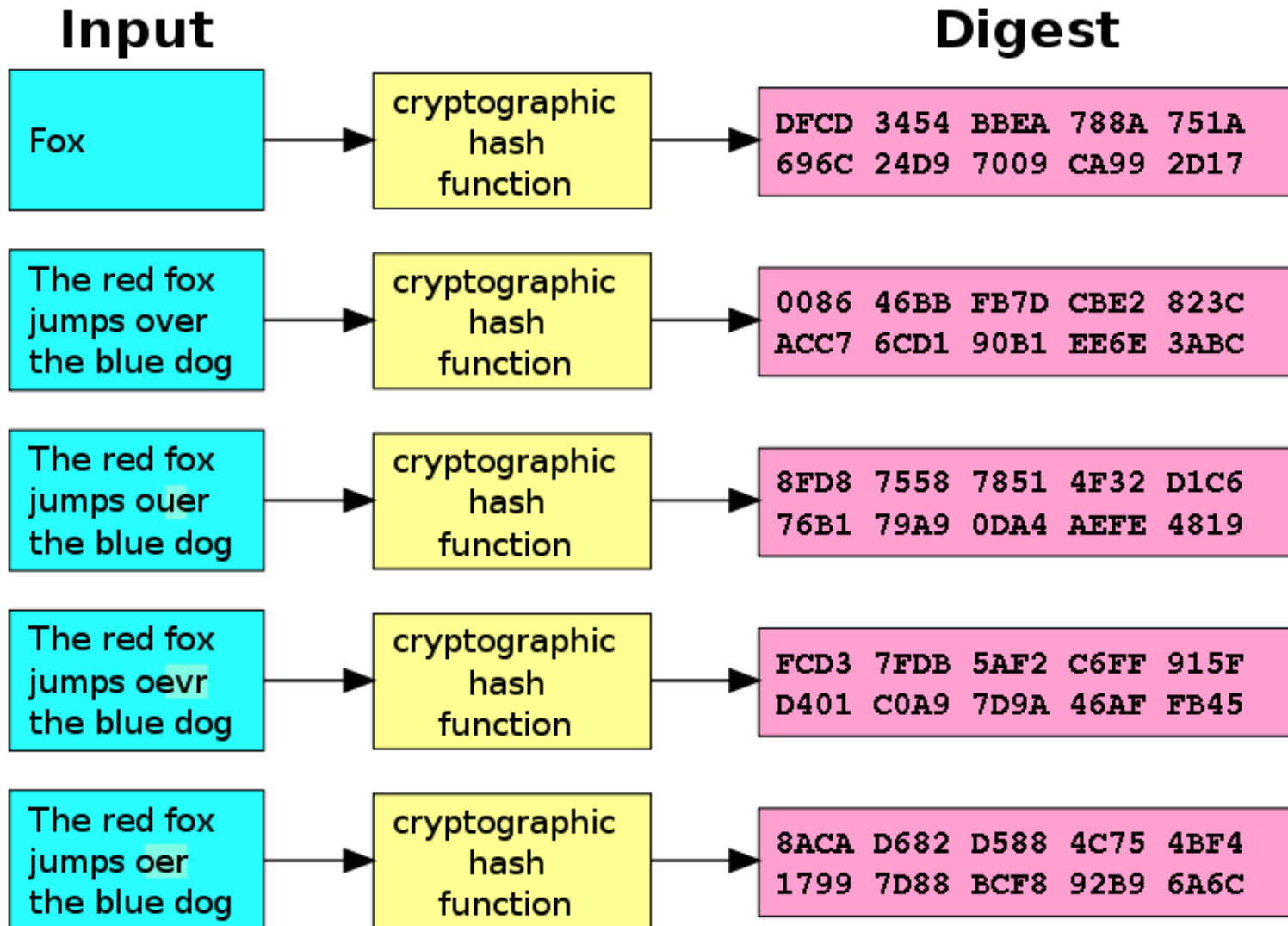
infeasible to modify a message
without changing the hash



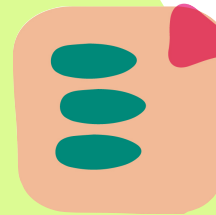
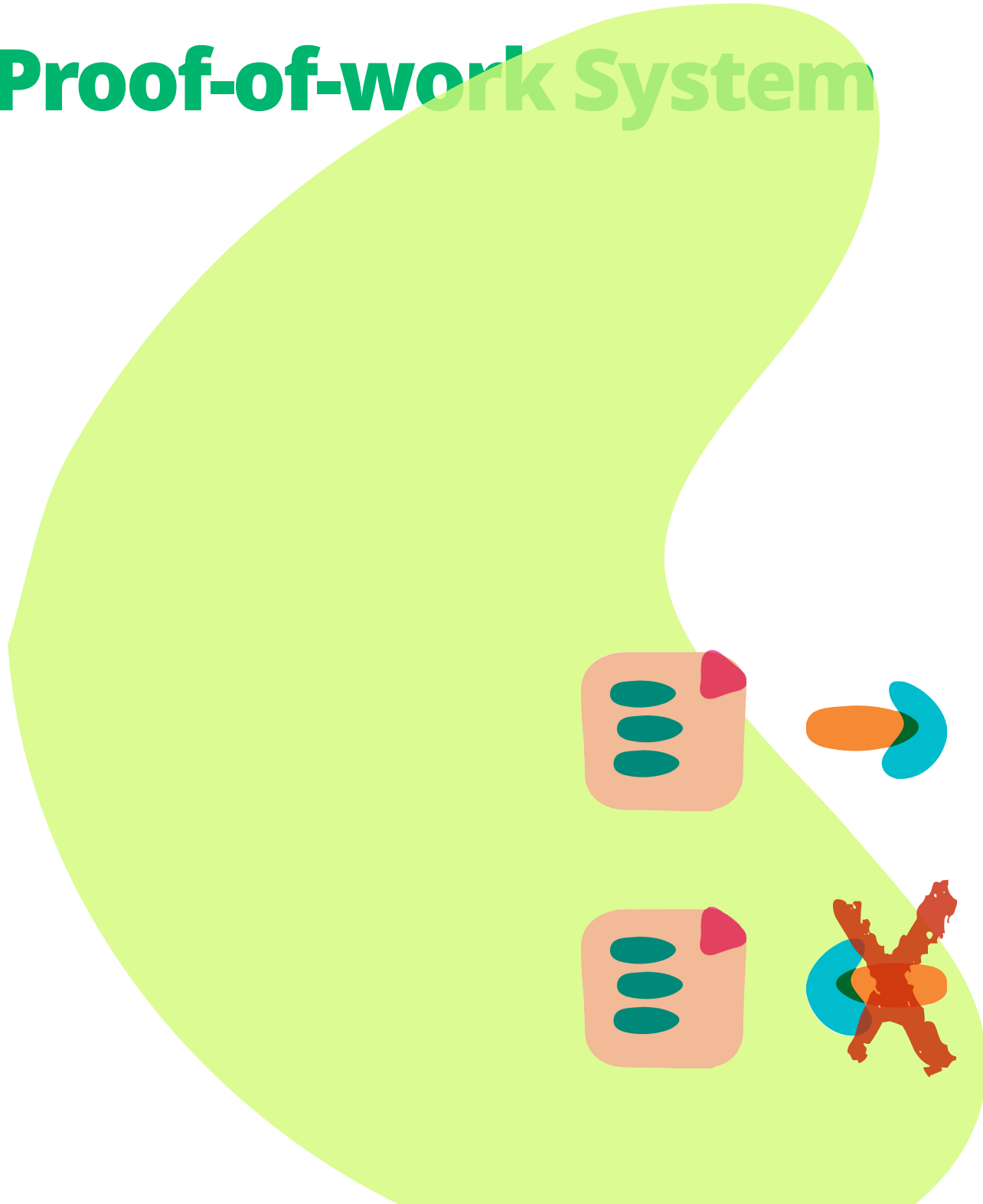
infeasible to find two different
messages with the same hash



SHA-1 at Work



Proof-of-work System



Proof of work

require 'digest'

s = Digest::SHA1.new

s << "Satoshi Nakamoto"

puts s.hexdigest

nonce = 0

loop do

 s << nonce.to_s

 puts s.hexdigest

 break if s.hexdigest[0] == '0'

 nonce = nonce + 1

end

puts nonce

```
a0dc65ffca799873cbea0ac274015b9526505daaaed385155425f7337704883e
a8e6cfb0a4ddca931ed69eba4b22c161765bfe557b77e0c28ca697dac2bc9f25
7a61d466a1b78536610ebd946d4ad2661256e860ac530197d7ce239d0020225c
d1e8686864db9931ccd9c3e6f15326c25000fa0b8c902a383baa8ec6b4848d36
4b1508aa6bfa2f045cdf4eeca864b875639fb94ec04a6d139309729ae315190d
94a872ccbc276a9be9a8d836929e3f40a49c66352d1eadd10ba0f753f6b641b1
f6ea160208ad0c738e252092448b4d625b2591d960b2b9c32aa4d59bf44716ec
44ea80ff3cbe229c436b2474ceac312af3af080cc588a2ed1fc04eccd6ed4274
fa6e151c69032b0f7b7d4bd6de1f36452d2bbc566703be4c48472d986205418d
563cc13aa52be6a8bba3eaaa0fc780e4164578fa6c3cb9be76f4fd1929e6449b
9e36fd9fb39392fd38f5fbabba822699a872e76ea77834f9ee50410f1f7a7f22
9102b0eaf4a7cd3672d81c62f1b0d6756d05ca53eb42aa07514ded6175c3f532
8cf8a465e0ba7d9672a190297edcfdb83df9d440e0bc3c4653556218d7a971c2
7a75a48c1511f32eb3bbc7313cc8ac62c11542e381785803be40aac0288d03af
fe595e3267dea562aeaa51522d61a266b000f29c4e235c009d5e8073b27d8d5e
50372ab66581561b38c213b318ddb9a8c83945e0fa269a6e81d37c6b0fb6615b
f0a73c72883744e1c41913af1f7cf064e14ed8e01e61519b8716d7492f8c77fa
8552c4d79b8dabaf41c5f1e089eb353885788caa5a1c33fe5141891c56992cab
c92e3f7f85187006dc9dab408cc667359bcff82b588d1fc22948f0b7407c8892
7241e8deb28ef142df42e048ab482dbb1a91a80658da8fe6c1e346dd900dafeb
7dc3ad5a16632e669d0e0bc882d139efa9f86e053f7a685d1dc0581d4583b9f0
77b54e3a280d4ba07c522ee3096a604840f13250e2afae48624c023d95eaeaaf
1749b3fc76a0e32e881075db1d771d0df0dead66c127fd69e26f122ad7589a37
0406b42df850c37fdb251b682a453611b701843b47db045880f530f4132dc958
```

22

Adding Word

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 =~

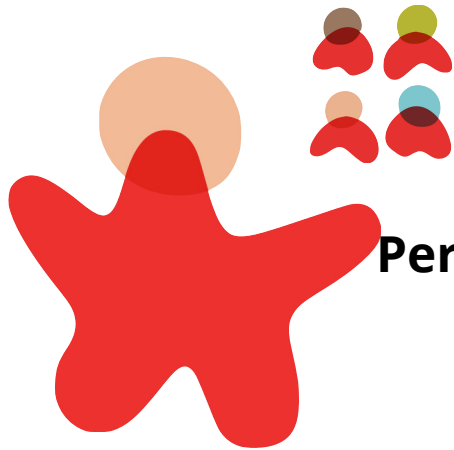
nonce = nonce + 1

end

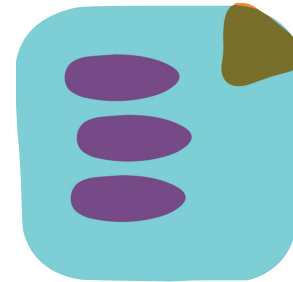
puts nonce

5100d734486fa5626af428d138c8429b63151eac9780a6f2800f335d155b34
38e530c02c37594e474bd3b01d3915a07160df0f6c40f1ba71101f0e2ddf426
deb0669954407f94f6bd879002dc54433e99f9d0b2611c0a3beab16c8c9b03cd
e795ac9f8892a6462df310d67fb1ab47f06f536dd1a2e780733d9c44bb39d74
865a0ebb5dde38dd9f8c0637a1c85a6ec2b6b7555f97fb4a2303127420652d4c
f6b77864b96ca1191dfa871b0d79b190de4c833112c241a5359a04e79e28b74
5fe2c7bdc6f7453e9943524678be88a54efc67297e0d55378dbbd72934dd033
7962d3a2ad921fab47e1e0a5e04ac9c964ef3252272d9c6f25964bcd4696a1
4a29d3a074648295446af7ea8f2cf4ab9da999ef220cbbbe1c3864790918fab
f9239207d1bb31d884a0f9ec95aabb278ad2f80f4cc3fbee121ac8b9ced29735
95b598a28a3a1f64d253119baf955daf2f19b13a136c86dae749a4be784fdb81
4627f54073dbb559e72587f2958788492c4f6c95a18db0ebd349119dc24171b
91cc025ccc0f43b00dbc63cb2bb6edd0bb3bd4230192374608194405dfa0fe62
58e327b8b72a2bee25209534a3eaf73648c9374732ce4140d561193a8e3c633
abe9e519b7a35bdb8e963a1f0af9f1a62fac682c2ce129365b52e34acc9140
bd67b6371038898d4ad3140fbf7b7d0677700a1aad5f8bde425c9e8a07cf448
89ad516e8299467b7fd2ff9c362b4457182fc675b5f40cf27a65e372216c3d6
6a80f6409dc7ed1c60a66d548bdee6edf69d97b62ef001f99b97ff60606b591
d0571bec1caff94fec76c6a2b01e459ed225ac910b85d4693022a77235c3003c
4771889850e2936ce409018f59d1a2de308ff2327b4b872d95084bd0f6f0b6c
1c07509c2842ad852f1f48542782c6f35ffb8484de5bcfbada926178c8ff9b6
73be28da1f95c92b2cc6e0b022b01300d8f1892c4d243ff6744cd0db6eb21a
9a39cee0f2ce9f3e3a35d0a254a07c9b056e7f1c8ed545618a7ac00c57c42cc2
f950c7945c82a2a01c0c89c29c1cb5441a2c31fa48674fbd6789d638d6c88cab
fa123e934e1e4a893115be702c30436f328b74eadd2cbf4d867f093a63c29ade
59fb9792b422be43f13ee3adc83996ede45098ad279e2f8183f075050ca0bf4
012d70553cf397c9be4b2ba5649ce31b609e2a716c82ca9087e7f14155ad55f
07e88489be05ce4d0b015587f7bde91134b6fd389728f77a63e68e41f10ad3
5685cd74d74340c916930c53f4d89141d4e0e08f5e165d9a5c2f70b51280c5f
a93c562b134c290a823ea1af2a78d7a2143eda27c09c770f52545021578e494
31d318a5a35d5a053ab797dc687f84e246aa1c6485ccf45e2db39a5e8e472f70
126f1d683af99e41500e5d3ea6303913649575c432f8fd2a289aae87ee8d488d
a7c95f200cd0e58699d52c7b5e593020e5ef610f44859c28a69e0c0fd1ac33b8
ee92bdfa77f3e7cf2d8301ef35a9b9649882a9500c4900f50e871b717f4546cf
04915fccc9f4464a9b2bd4bf4675c14fea4951f8ce28732f0346651517237969
b340ef491c2d40b29eae077058d6ba995e657cd66ec689b0cce79aa6155a363
59ccf7729b022a1d7d7f3b5160aae80647d6d047d71e1589a16ebfe30cd498e
160f4764bc336a0ac756b56eb4d38aea2aa2368dce738fbc5c7e90d203f2a
52897e090e4bc7d93420ee134c82b5066e8f4794dd14d8314bd432095d958e4
f08b4e601a41f4c07d6787ad84bef9194073d88b846b305e6d802136e3232a
a0d26ba77b9d0db1baafec0e67621826f334fdb805881a2440eb5190dc8e0171
478dfab89aa0261b3ad2aacc7e7eab2c5253dba5fbfd0f973681fe963478855b
72658c1873ad966b8c5c92ef8f89f91a013c67688e29667e1fca40116e8904
d3fa5dbd67e59c5272a3d788a4340ce2f950e1f511e1531cbb024827ba280f
b68e4916302ce8902b36545a32569dd4bfc3fce08ba450284212998a2ef78f7
147acca79bf1d42299412694641e999c43c514bc81739d70a202d59aaebde92
3eb48be5e529319390b1a12e4716f1db57ad9eb4af10d20b425dc6ffa2b84f7
254b81efc805a94329c9ab785af2260964b147ecfc629d7fd11f88d8ab411b6d
2bb2d9cb456e37c75faea2c8fa3b2bfcd5ce0c4ba732ade511d4593cd336d9
9c3b45c9b560130f495de0554653cefa8d218bbca6553cf1c311d8cf4cc662a6
6873a66edc79f4cf421526ce18d684cad720a5c44e7cfb6511135c0e67412390
b7818efc920daa4c0e4e67f6ee4a08946376ceaadcdcfdb6b74da6ecf369aef3
16aaacecf279dfb956df3c51768a047aba9878266d03e5f8298bf9dc5ca36b
751dc65e82247f5044207136dfb7ccb23239f78086a18488b1158d6ff36fa69b
458059b32b0c6aa145d65868ee51758b43b3a8dc6b95a9a2810cd85e15f950e3
1ca1b2ae59a4e44f2410bd76baf09b26e7d86cd300cc93c6f6b86cf09852c80e
eb2d5d8a7c3459a1dcf92294291dc1747f69ac50652d7bd10cb6954af0f8f006
3e2b65b196a0a961d6150885a639201e7b7503e7df71ac3b2fb102febe7375d2
ad4740cb6f501ba72f4036241cf2785823bfd0287d604372474dc62da9313a0
97b9bbfa8b41118f09bab635707d9c336d8eaa579049a6593e4c0e0d49231674
57302f16b39286ebd21385e2c1245e6822ffb498228b9650a0772f0163e7a649
4c72d41f09b78fa774feb37fa96f414282fa1d77bed9f7fb5b97becf9481b1c
93b7cc031693d3db677430a5ce63982d2ecbec9509aa3660213c39ce8a0adcf
c74eff9822b9bb16aa60f171c055ad357f3c59b5511dd601fb1cae753304a2
941a8cc1d72dfd59c2f0f94b74c9f634320b47e601607108e1f56e3dad66d0fd
47f9f19bc16b67d3018614a1c188d2c0ff1c887af614e1a7d7632d74e9fa8b5
d9c324475eda5c6c661346bde5fe8bf73bb18176010e4d0acd3eed6041b042
b123283aa09532de962dd52c6abf7caeb21cb13b172e891802b580677a42bd8b
baa02822df57eed5c99ee0460207d9468bd0db4f19cct525e9fda54e75aa27
5dae26f6ee1dccc407bbe288d289282b77671785dd45794862022a2faa0264b29
e3b3839a7eeab6d29aba2e6b8418332cc50f91eb46a0c7f057ec6916448f09f
9d4b3561a4b9223fba31ed7b6a899efc8b04769139c9c71be7c5f67b95725f7
7a2912ff0ba1981d0e6a2a50a33ae16e7b6f6e634dabdbd1266c19b4c7a4af61
e787b3b0526beeff5ff0368bb478e6f6c8132bea155fbfa7ee4be61a4ae33b
e0831c7b8439a00cc7f3fbbd98e80fbc135c1b4fe7bcd71e61860e90de24cd
1e4c7ae9215d04c6dbcc8d7f21a7dbb25a890b1620c983202f4495ee167de659
ddc728187d55bd3ea07980266a5e0b9d3e69bc26b0c1d88c41c4806e3263ce08
0d3c72a4c50c4a29dd1adfb9bcb32f5720dd970c28910e0326fb22507b72f833
200b02bbe2742daaed9df7cb7b7b62918bc61f103bc62e369f1faf5829b3abf
7e8bb89fc073b8aa56ae343c6fa1abca48ff6e0533f4e2b0060fee064c96f65
006c9d780c49828f0dddc881580faf621cab99e1261266bb17b1dabf4107ea2

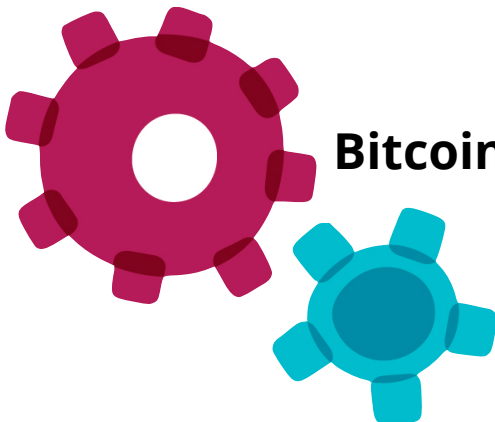
Satoshi Nakamoto



Person (or people)



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



Bitcoin software in 2009.

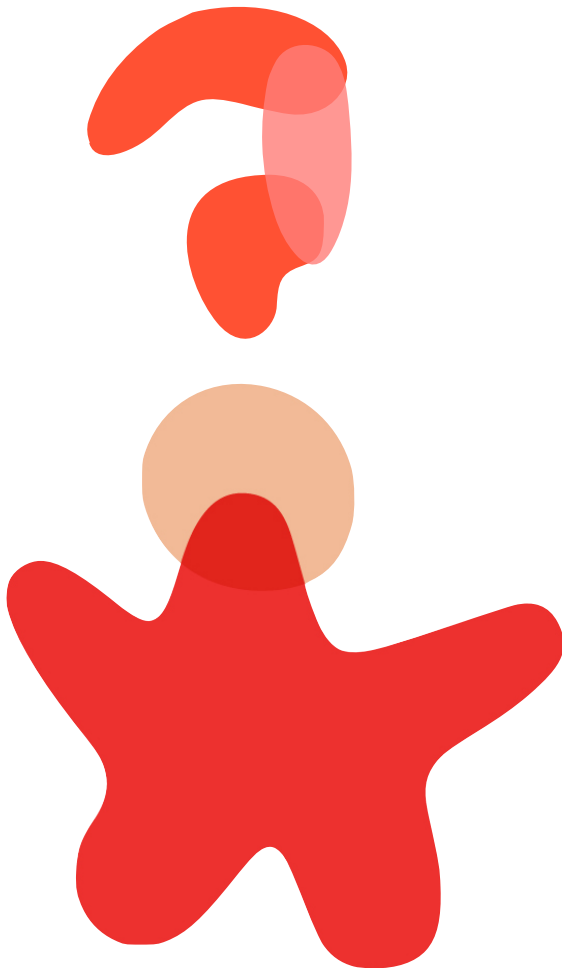


Anonymity ?

Cryptocurrency is disruptive!

Banned by several governments

Foundation for other *distributed trust* applications



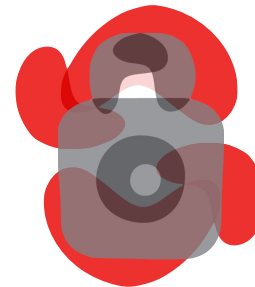
Implementation over Commodity



currency/commodity



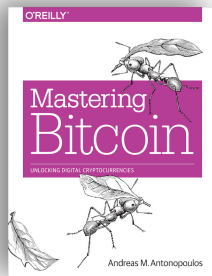
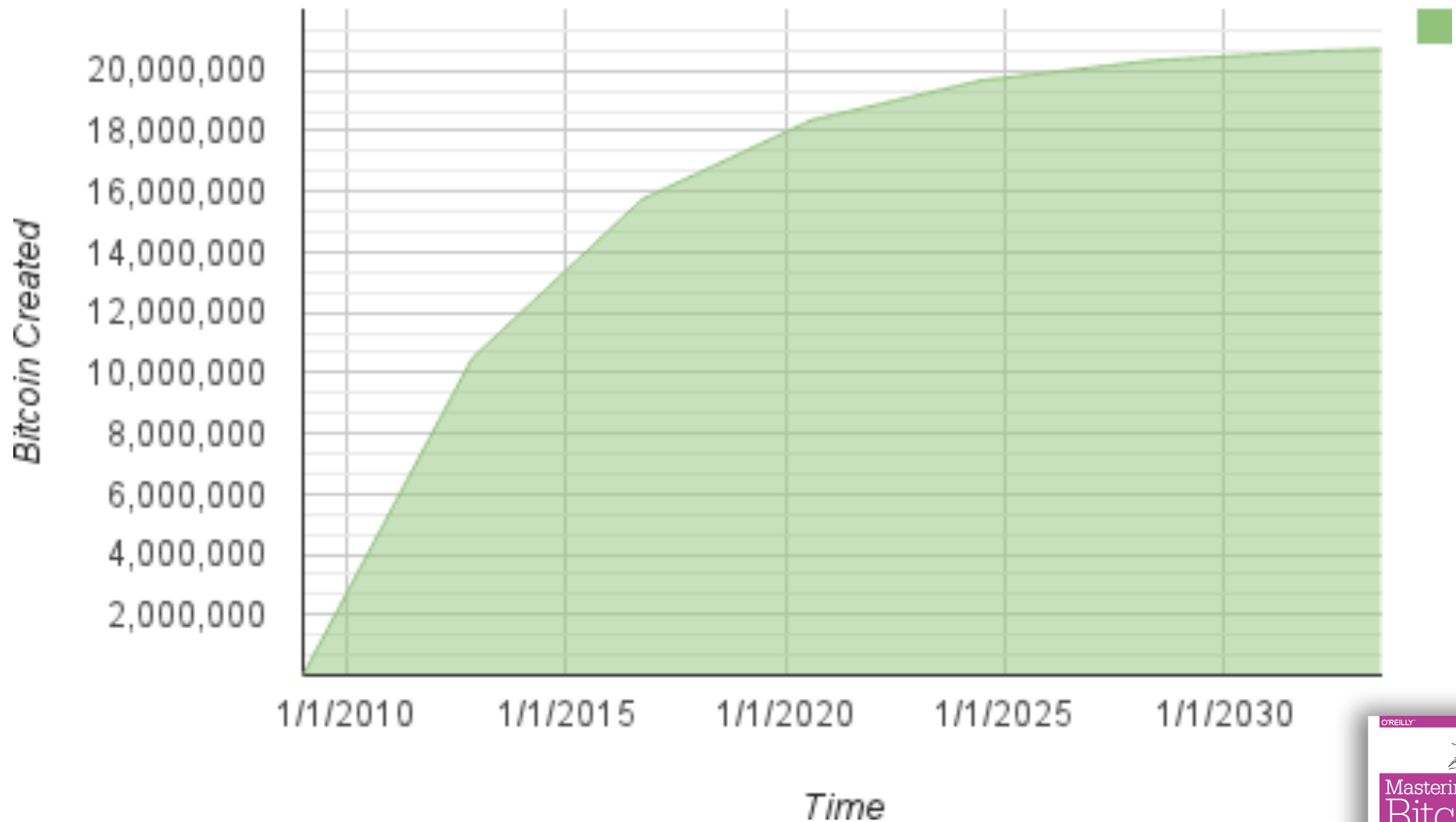
digital bearer instrument



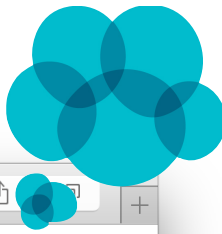
distributed trust

Deflationary Currency

Bitcoin Money Supply



Variations





WIKIPEDIA
The Free Encyclopedia

[Main page](#)
[Contents](#)
[Featured content](#)
[Current events](#)
[Random article](#)
[Donate to Wikipedia](#)
[Wikipedia store](#)

Interaction
[Help](#)
[About Wikipedia](#)
[Community portal](#)
[Recent changes](#)
[Contact page](#)

Tools
[What links here](#)
[Related changes](#)
[Upload file](#)
[Special pages](#)
[Permanent link](#)
[Page information](#)
[Wikidata item](#)
[Cite this page](#)

Print/export
[Create a book](#)
[Download as PDF](#)
[Printable version](#)

Languages
[中文](#)
[Edit links](#)

Article [Talk](#)

[Read](#) [Edit](#) [View history](#)

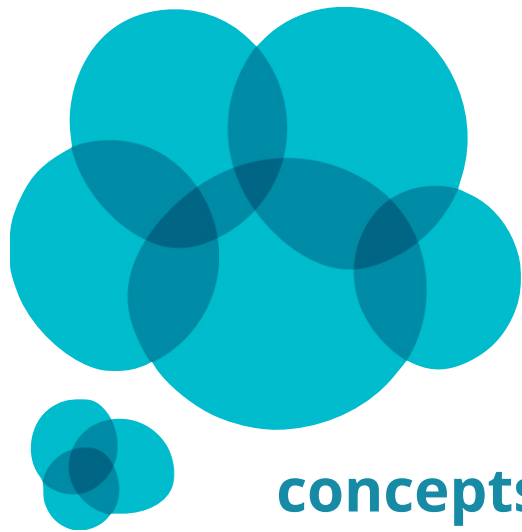
List of cryptocurrencies

From Wikipedia, the free encyclopedia

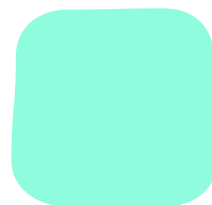
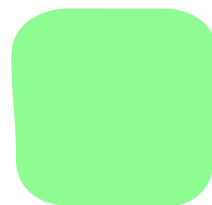
This is a list of notable [cryptocurrencies](#). There were more than 530 cryptocurrencies available for trade in online markets as of 5 January 2015 and more than 740 in total^[1] but only 10 of them had market capitalizations over \$10 million.^[2]

Release ↕	Active ↕	Currency ↕	Symbol ↕	Founder ↕	Hash Algorithm ↕	Timestamping ↕	Notes ↕
2014	Active	Auroracoin	AUR	Baldur Odinson (pseudonym) ^[3]	Script	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)	Script	POS	BlackCoin secures its network through a process called minting.
2014	Inactive	Coinye	KOI, COYE		Script	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]	Script ^[12]	POW	Based on an internet meme .
2011 ^[7]	Active	Litecoin	LTC	Charles Lee ^[13]	Script ^[7]	POW	First successful script 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 Quota Initiative	SHA-256d	POW	The underlying software for MazaCoin is derived from that of another

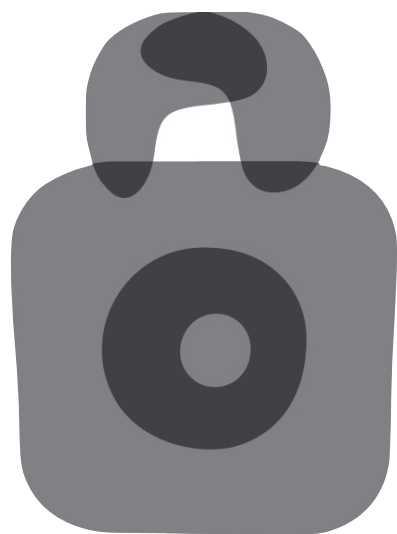
Agenda



concepts

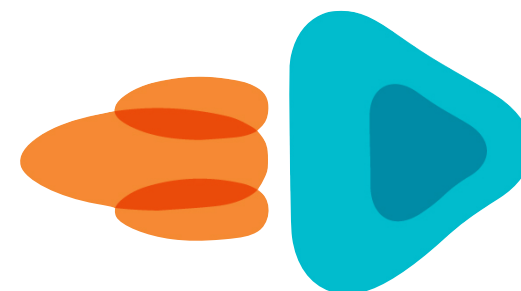


blockchain



security

transactions



implications

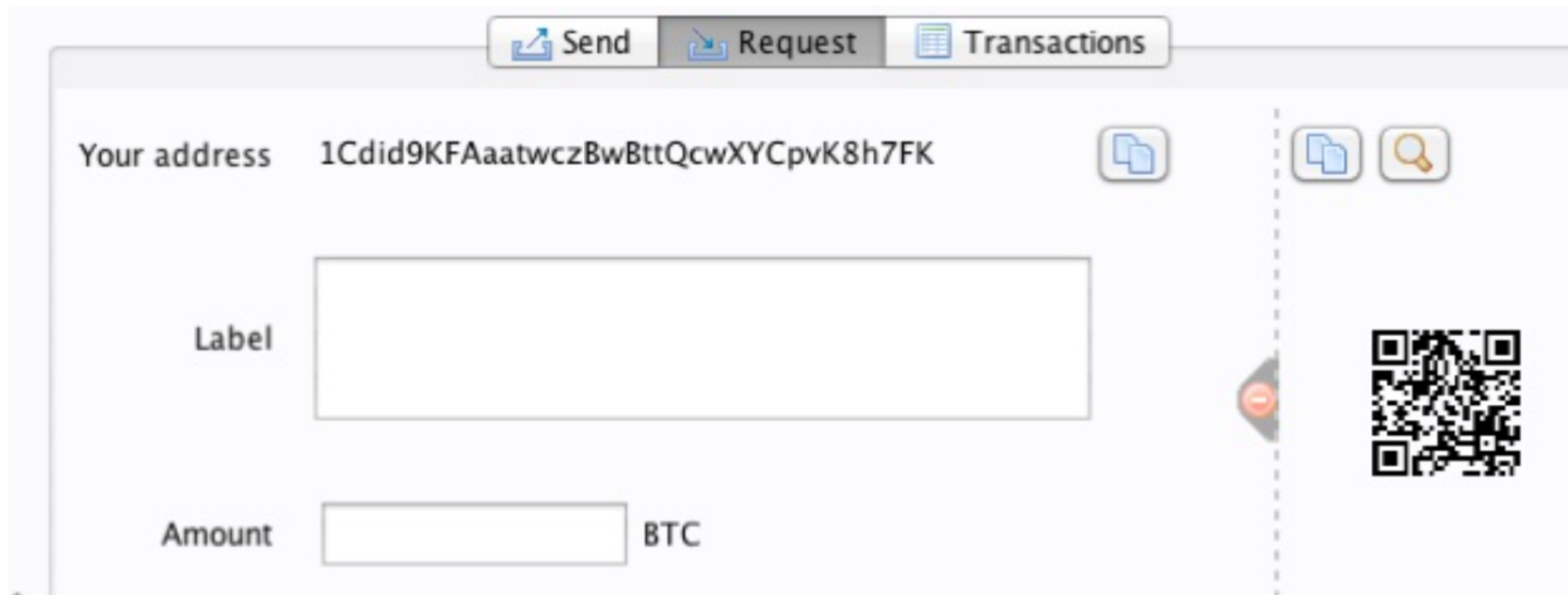


BitCoin Wallet



bitcoin.org

Bitcoin Address



Send Request Transactions

Your address 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

Label

Amount BTC

like email...



people can send stuff

UN-like email...



as many as you want



a wallet is a collection of addresses

Sending Bitcoin

 Custom Send 

From address

Any Address 

Pay to

bitcoin address 

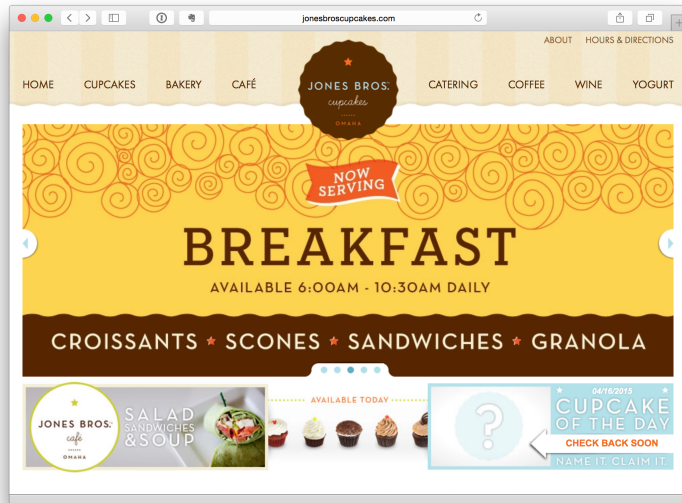
Amount to pay

BTC 0.00 

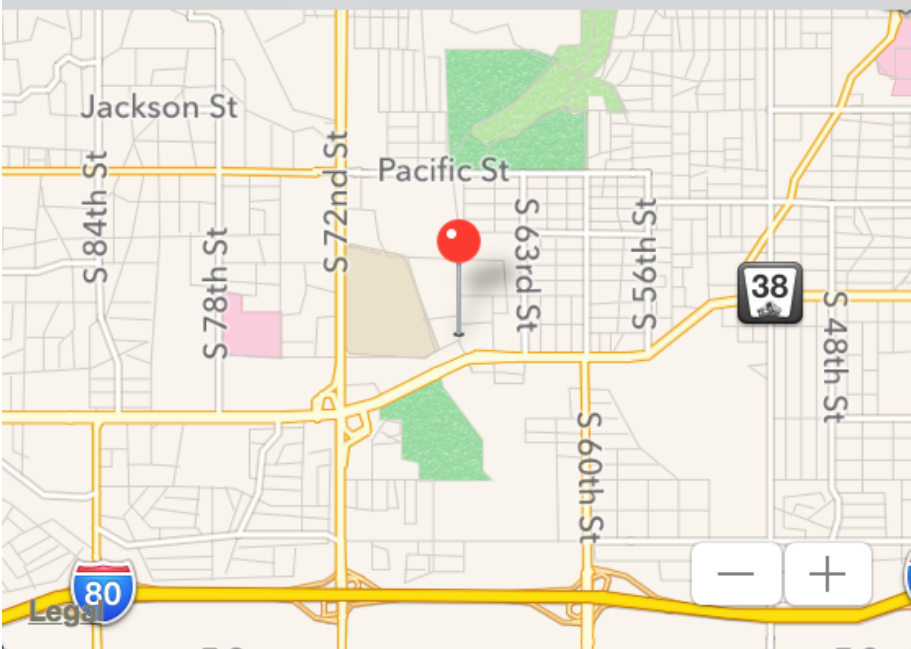
Fee (optional)

BTC 0.0005 

Bitcoin ATM



Omaha, Nebraska, United States



Buy a Cup of Coffee



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

Transaction Chain

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From
From (previous transactions Joe has received):
Joe 0.1005 BTC

OUTPUTS To
Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0005 BTC

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

INPUTS From
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice 0.1000 BTC

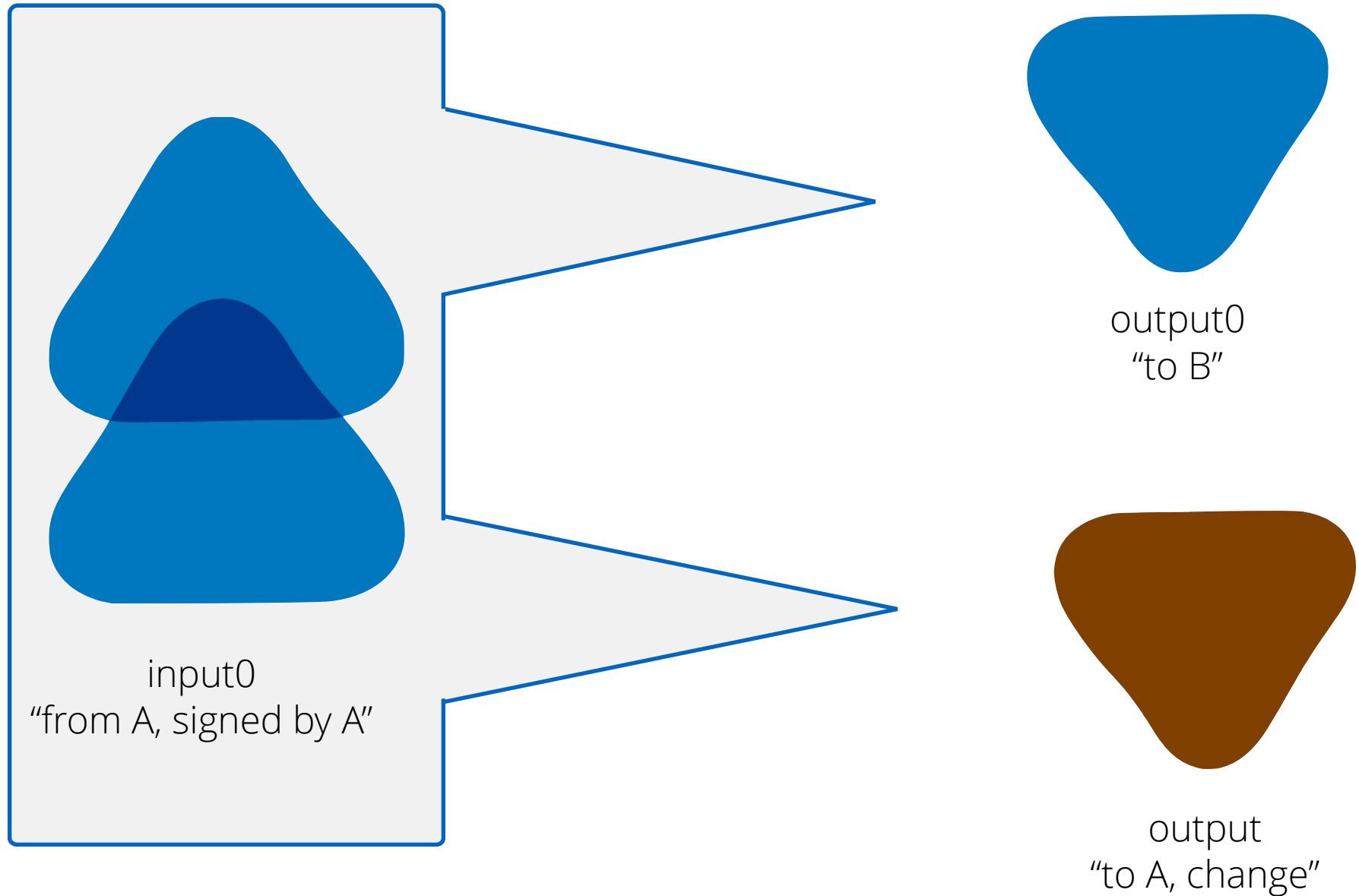
OUTPUTS To
Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

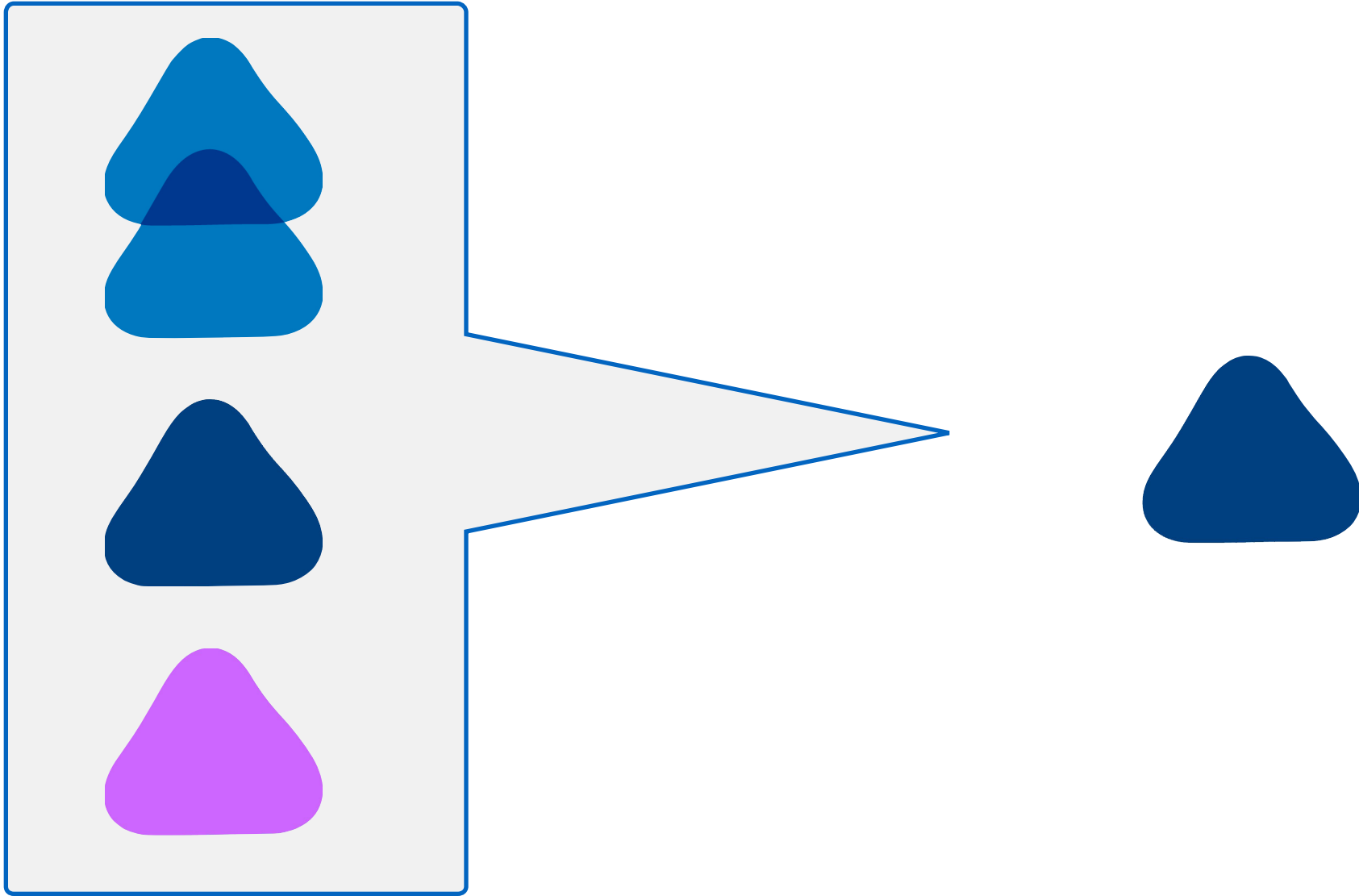
INPUTS From
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC

OUTPUTS To
Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

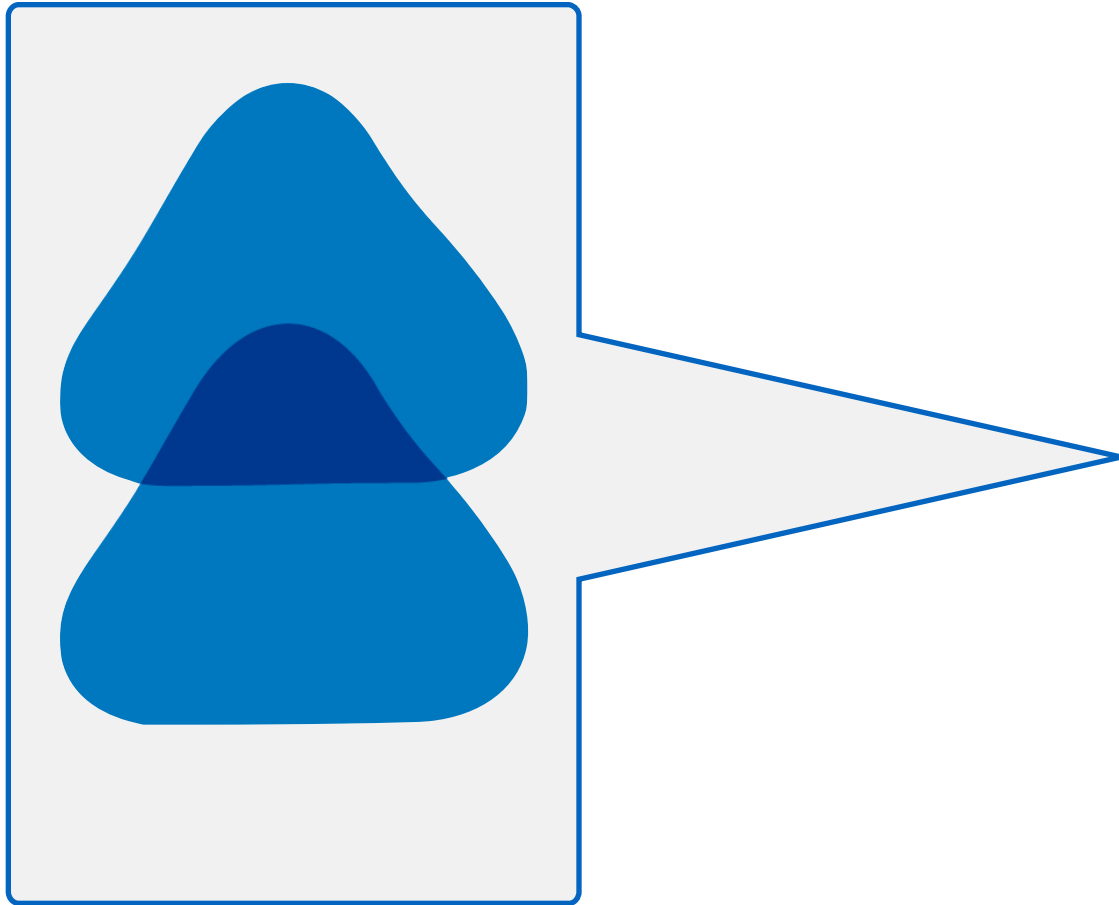
Common Transaction



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

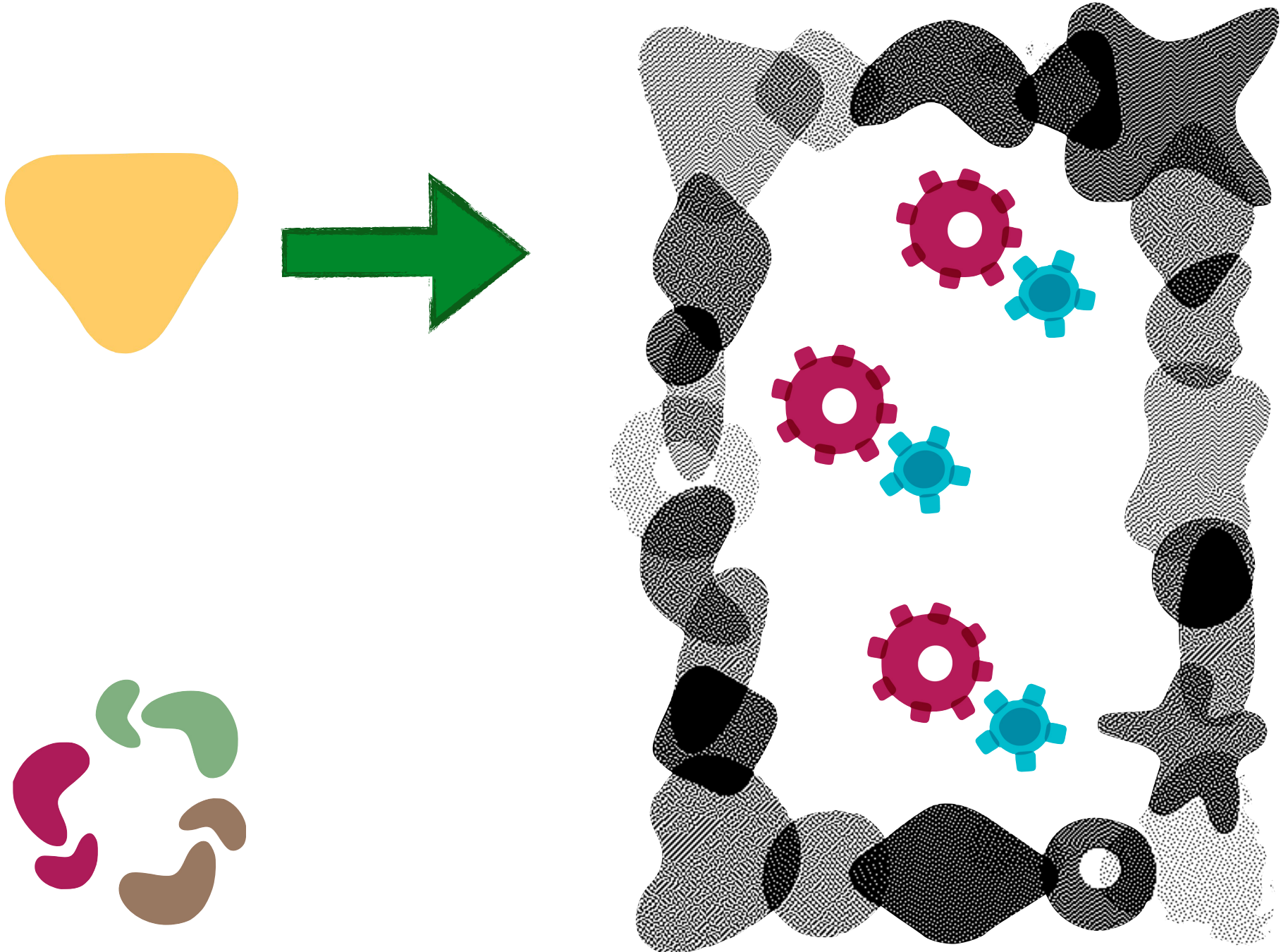
Summary

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

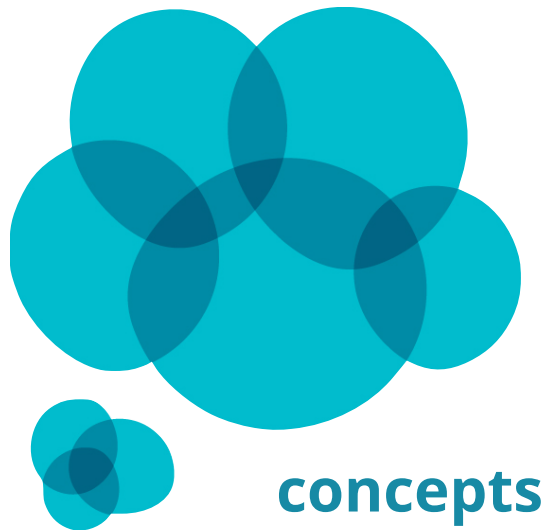
Inputs and Outputs

Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

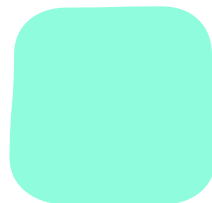
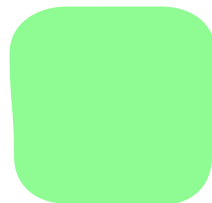
Add a Transaction to the Ledger



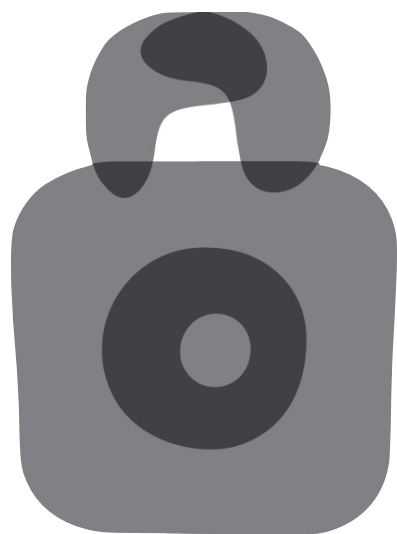
Agenda



concepts



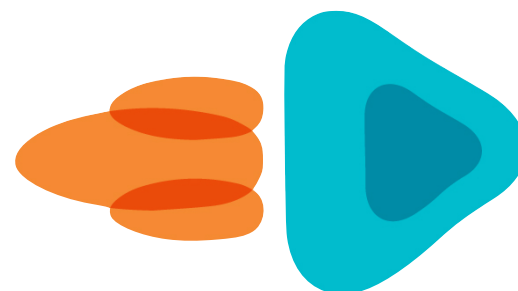
blockchain



security



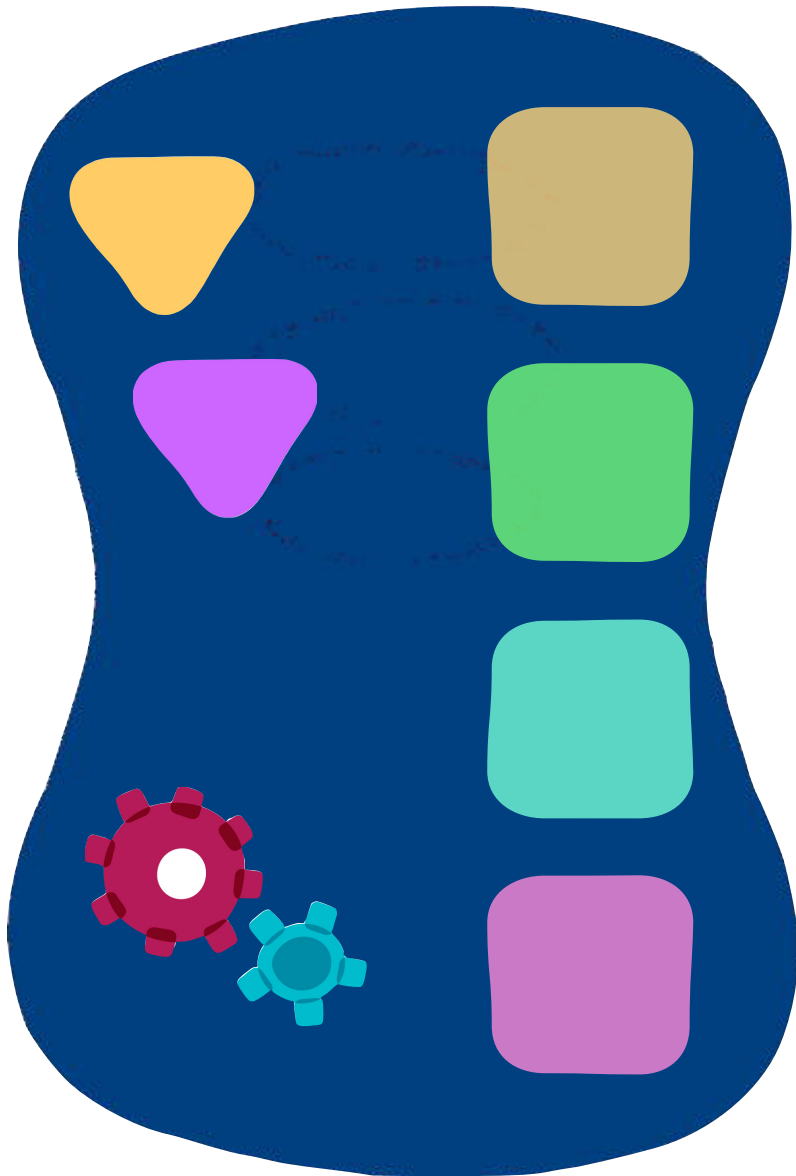
transactions



implications

Mining

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

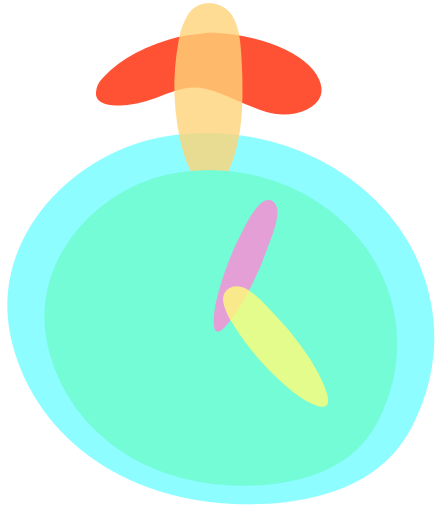


new bitcoin



transaction fee

Difficulty Targeting & Retargeting



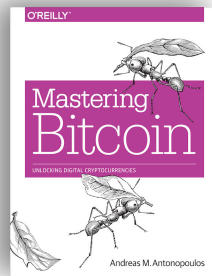
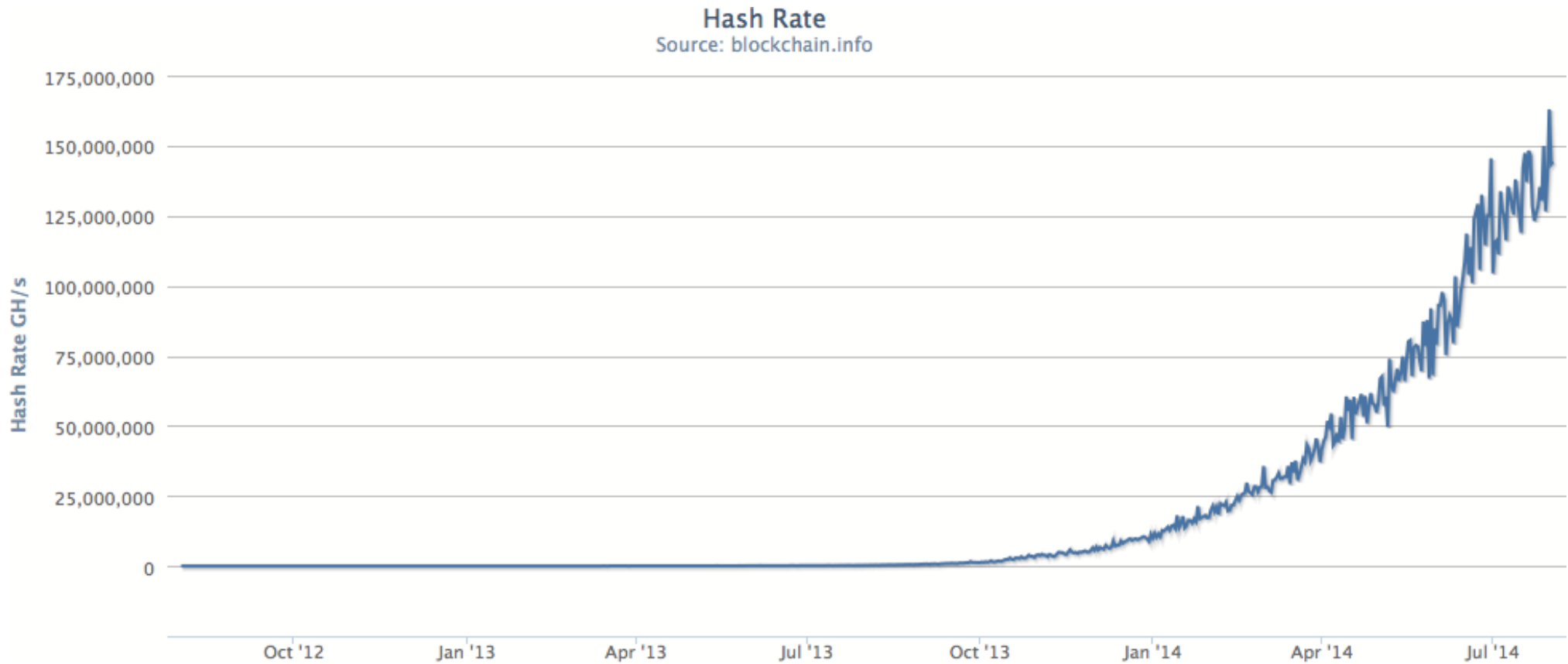
BitCoin blocks are generated every 10 minutes (on average)

expanded to accommodate increasing computing power

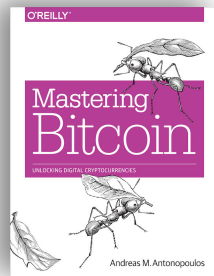
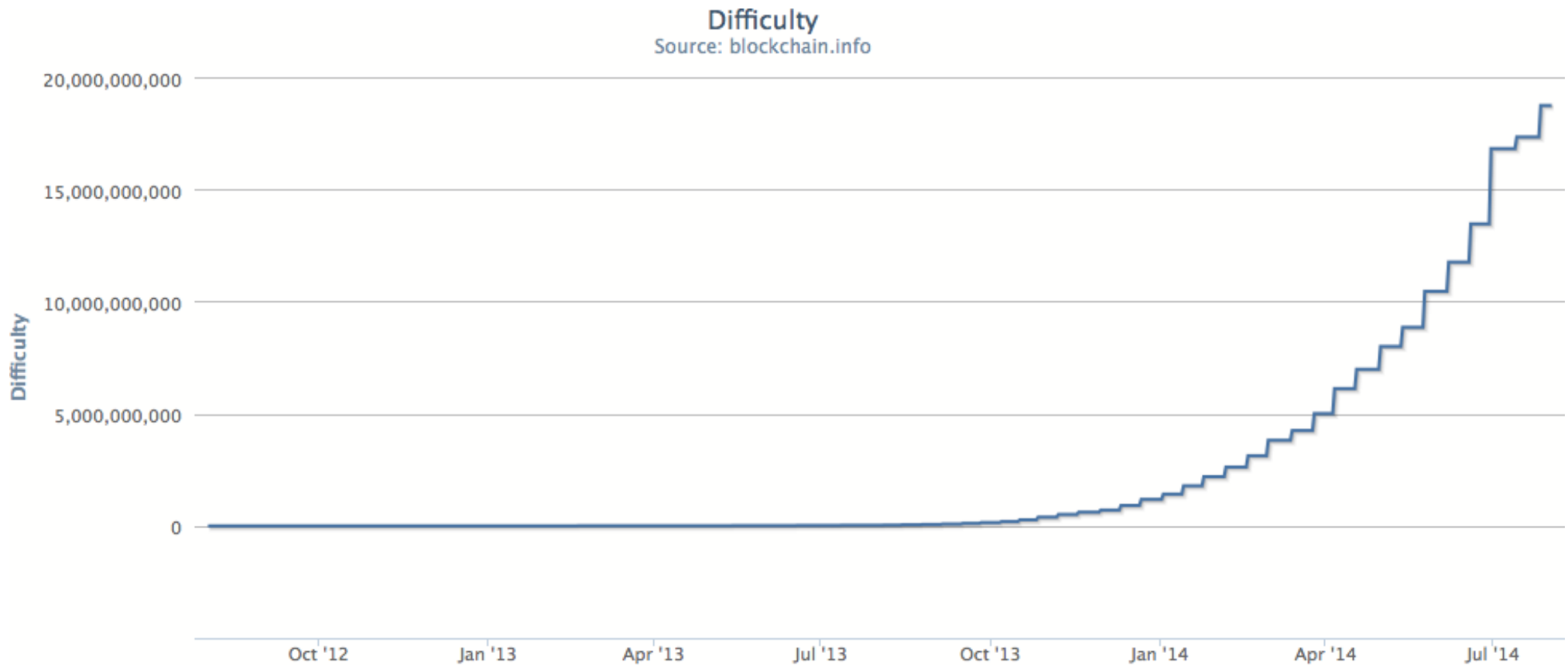
$$\text{New Difficulty} = \text{Old Difficulty} * (\text{Actual Time of Last 2016 Blocks} / 20160 \text{ minutes})$$

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

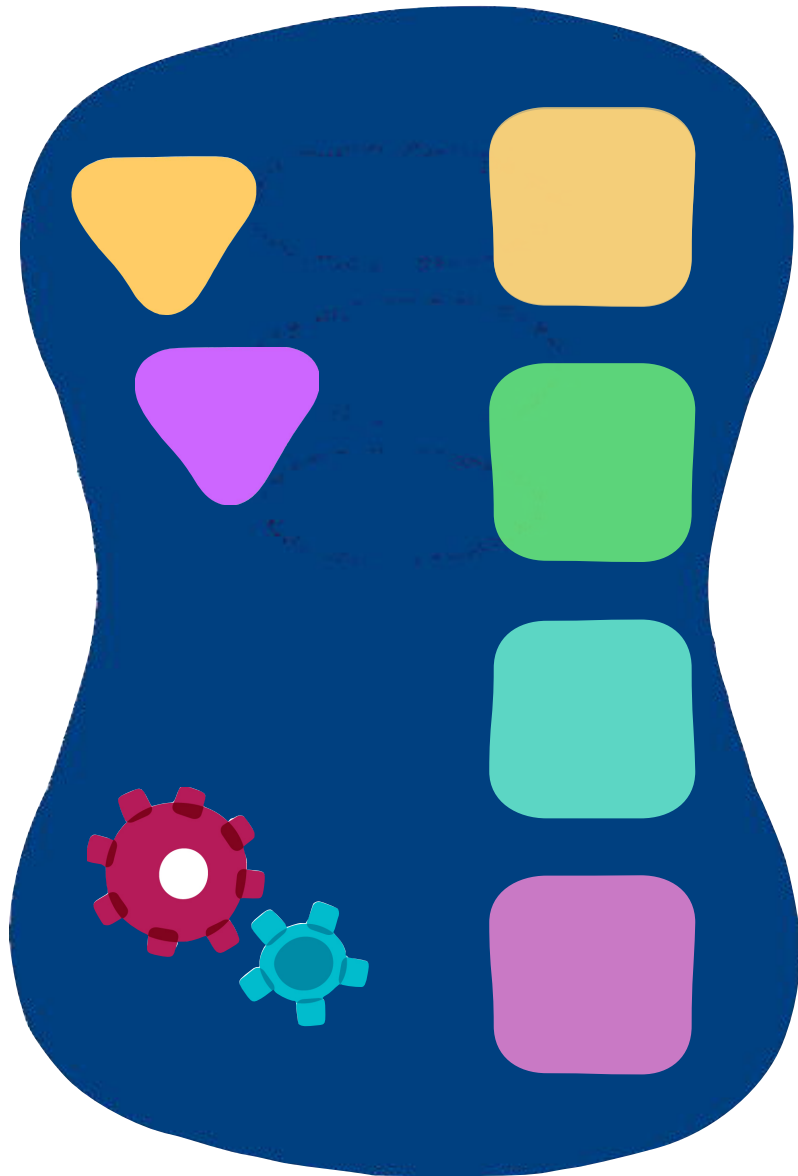
Mining Trends



Escalating Difficulty



Mining

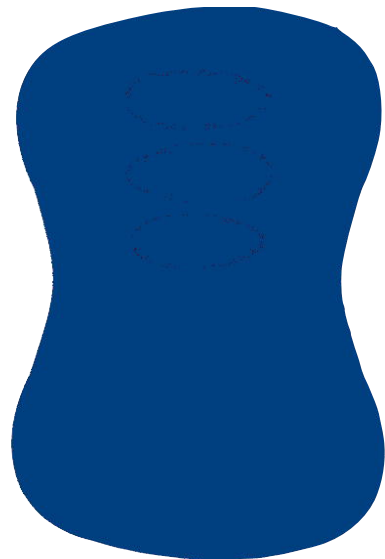


Mining

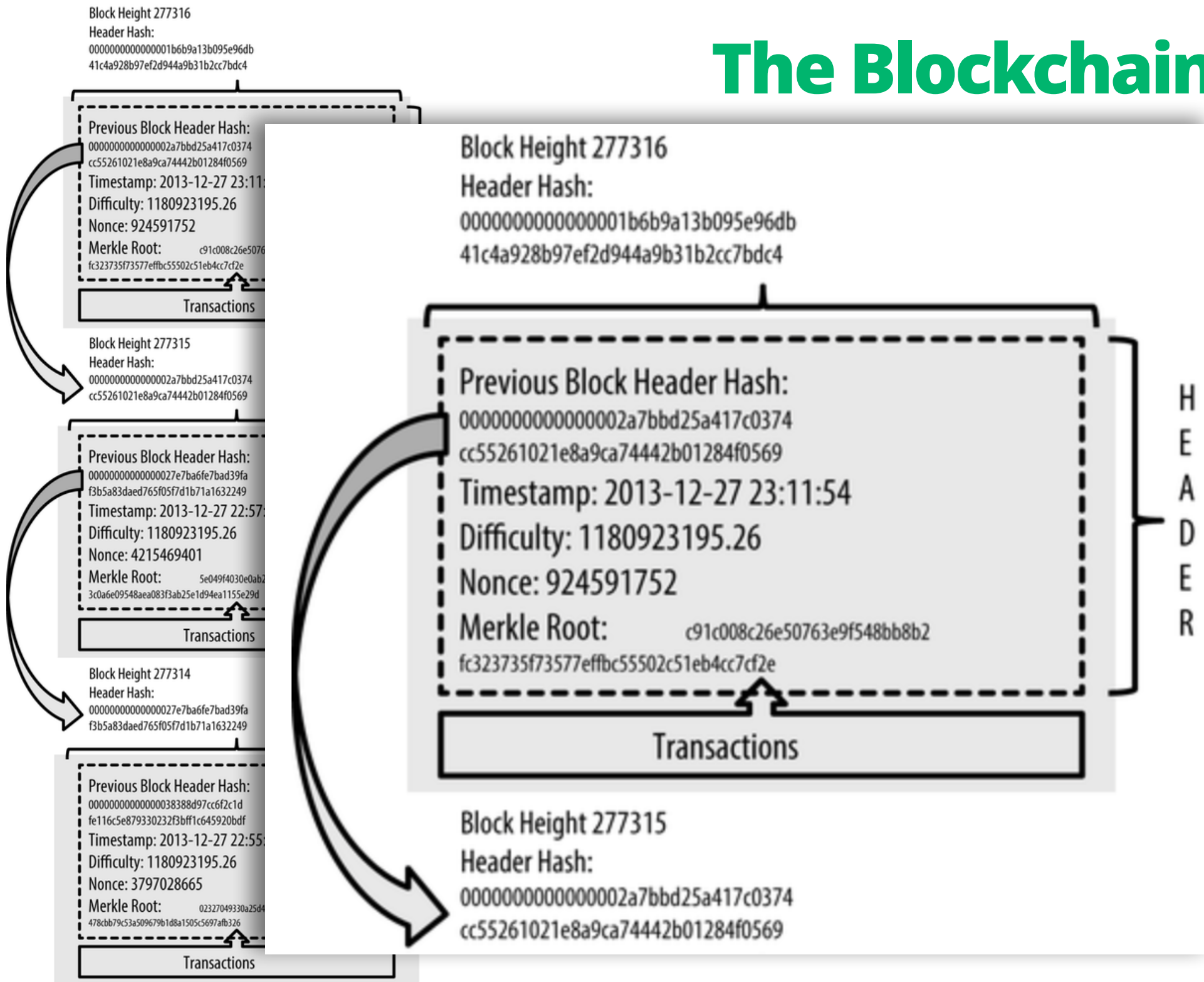
Priority =

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

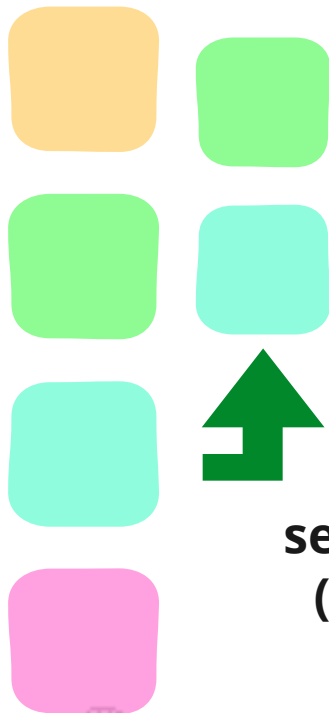
Transaction Size



The Blockchain



Assembling the Blockchain



main chain

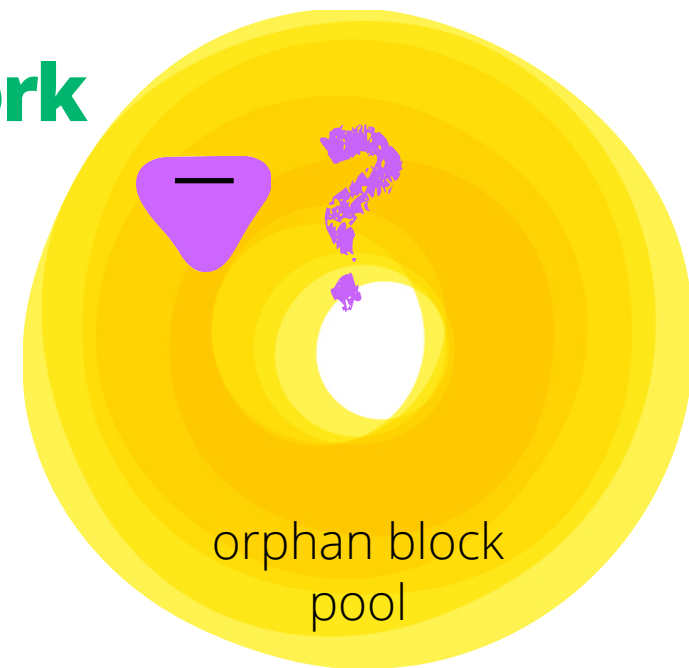
secondary chains
(forked blocks)

orphans

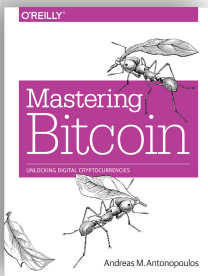
Adding to the Blockchain



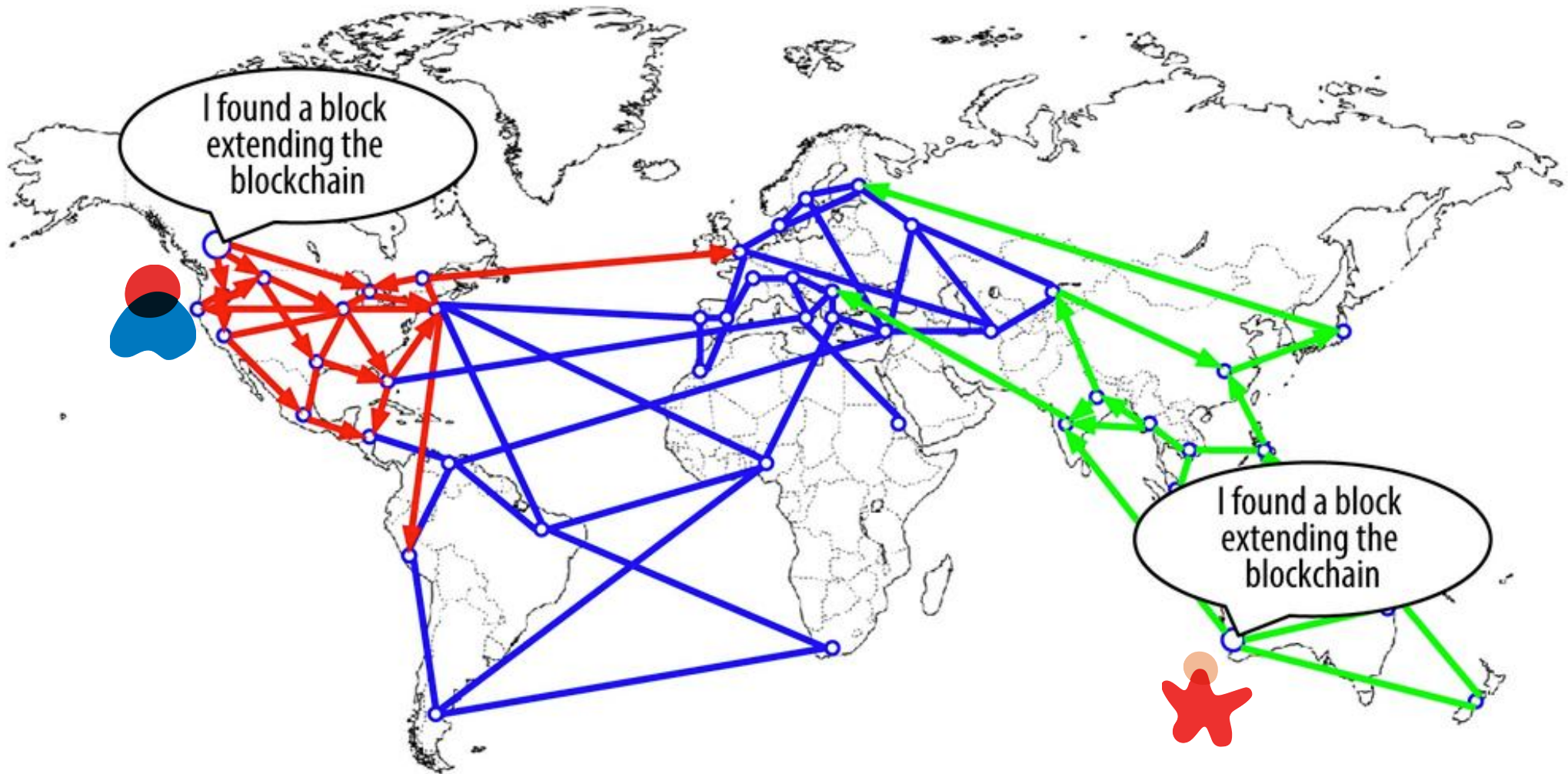
Blockchain Fork



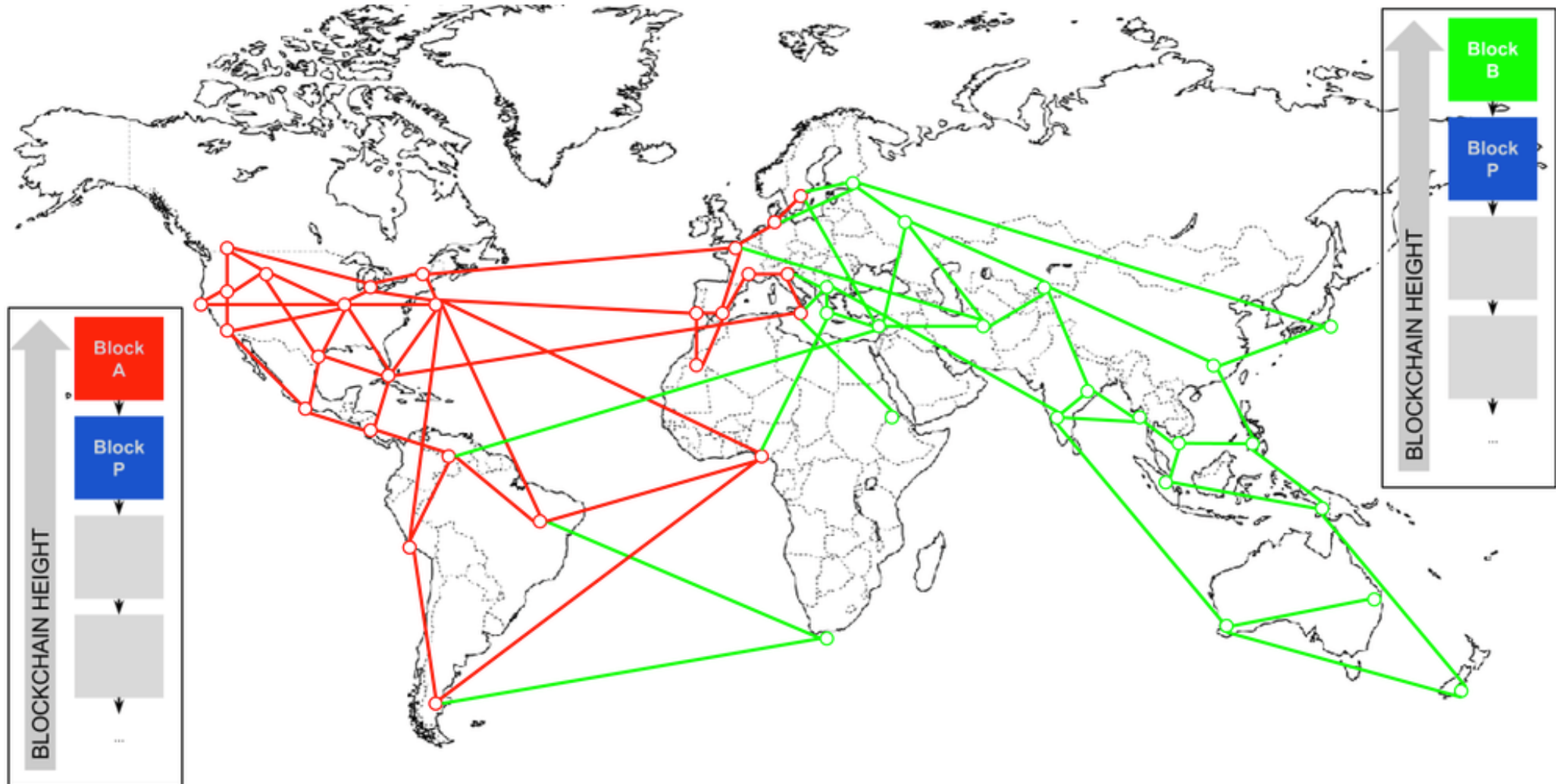
Blockchain Fork



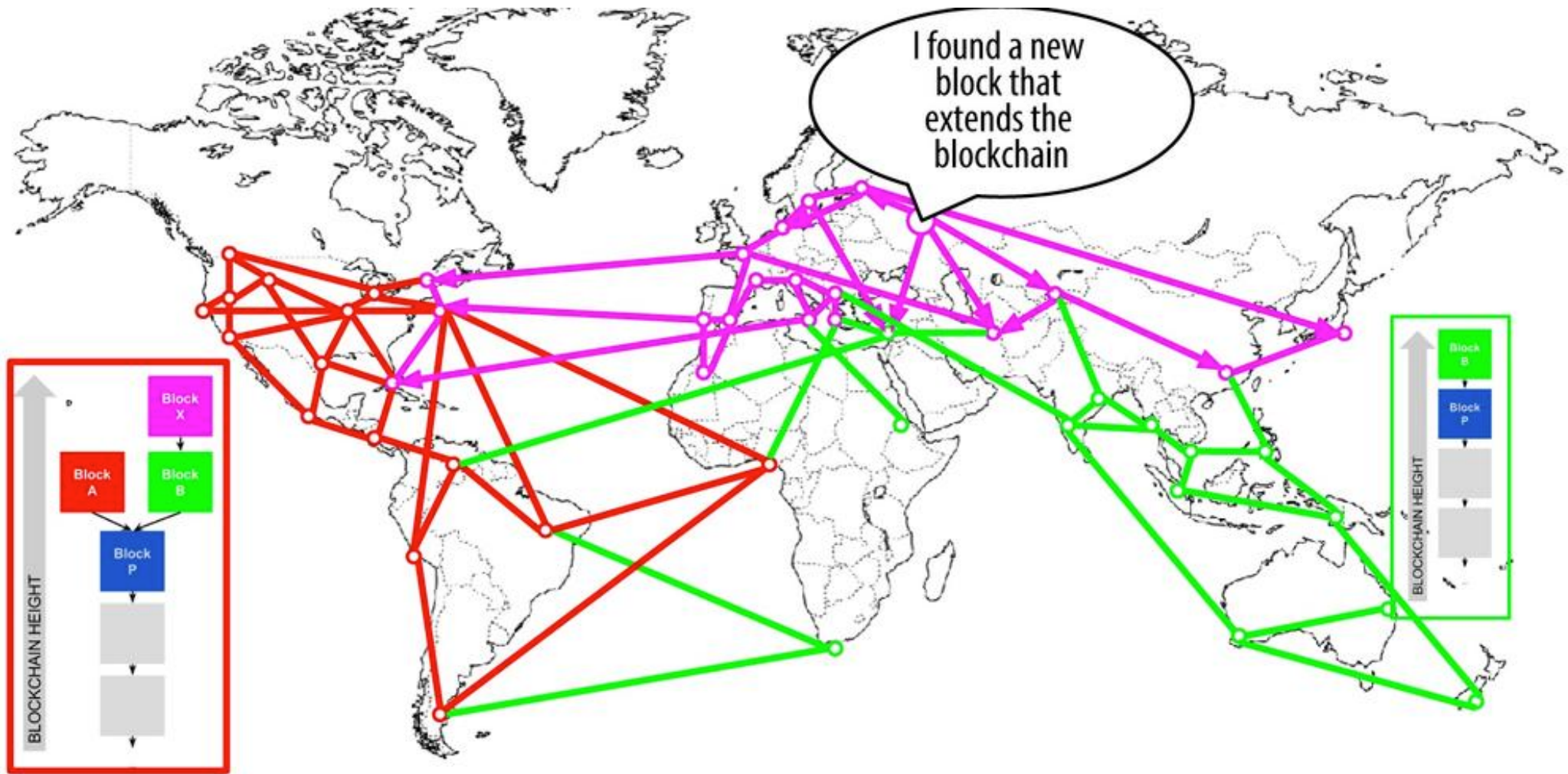
Blockchain Fork



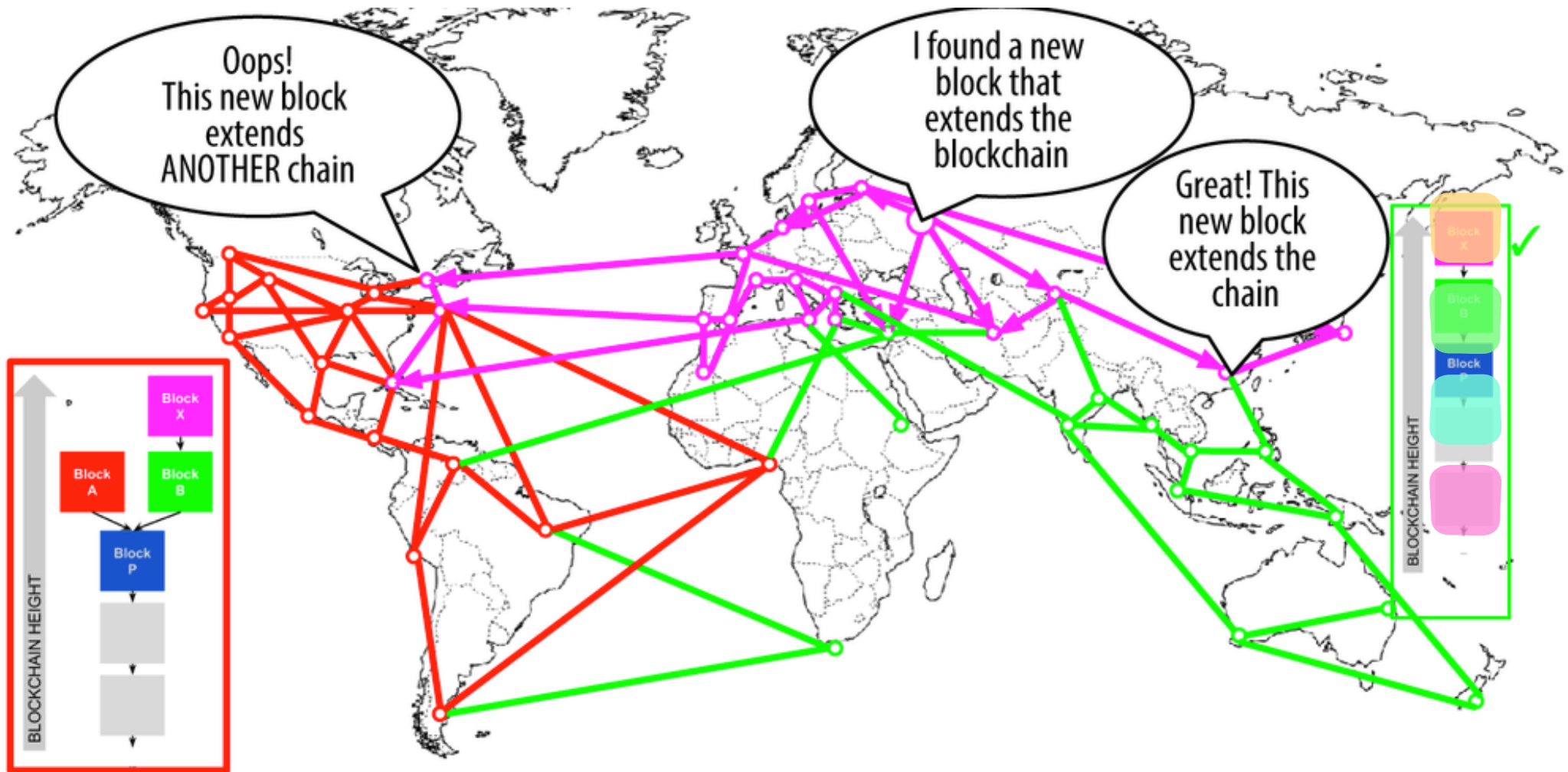
Blockchain Fork



Blockchain Fork

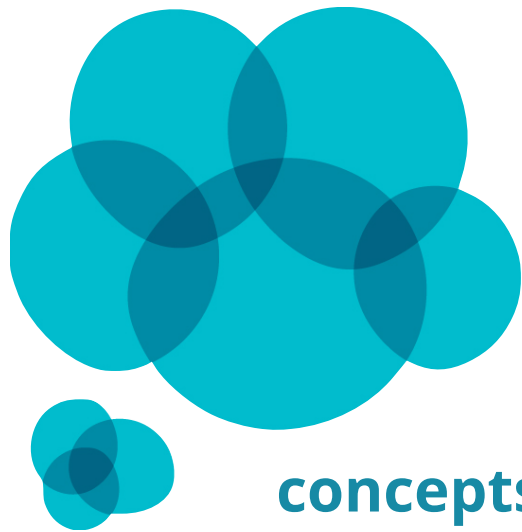


Blockchain Fork

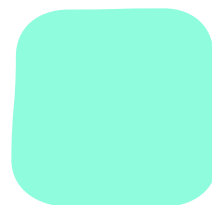
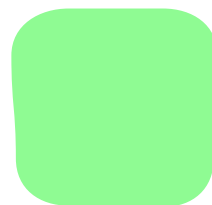


When in doubt, look for the most work

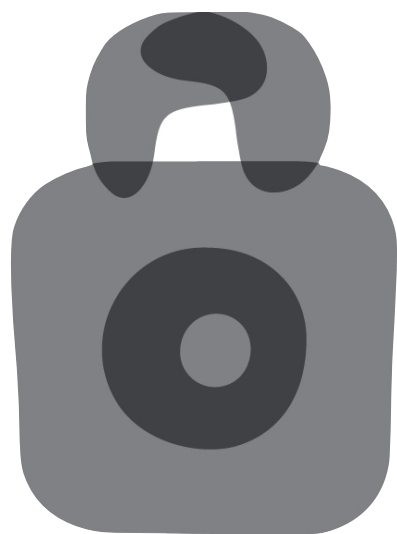
Agenda



concepts

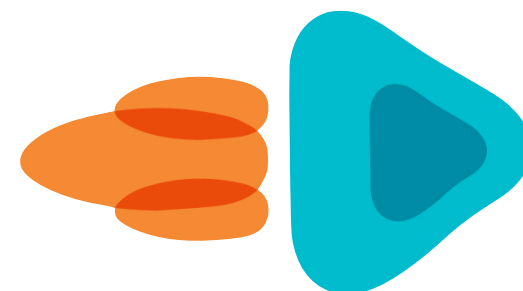


blockchain

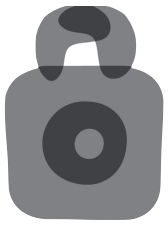


security

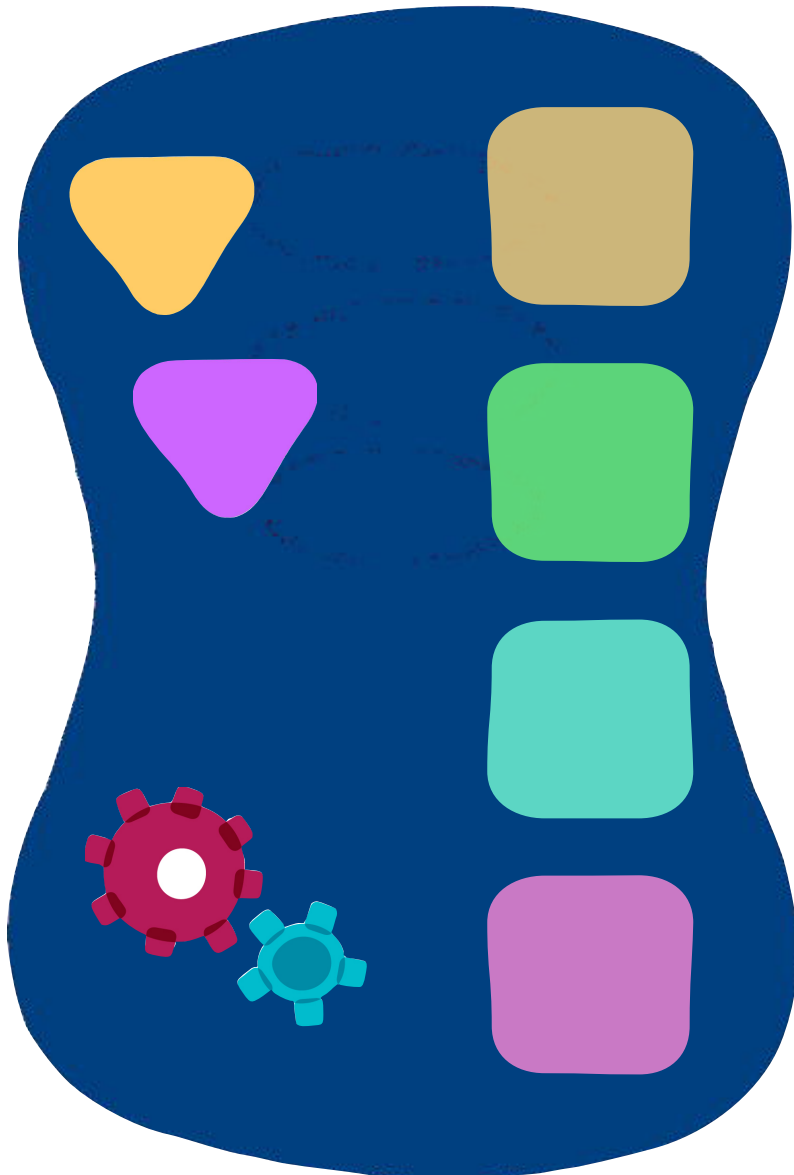
transactions



implications

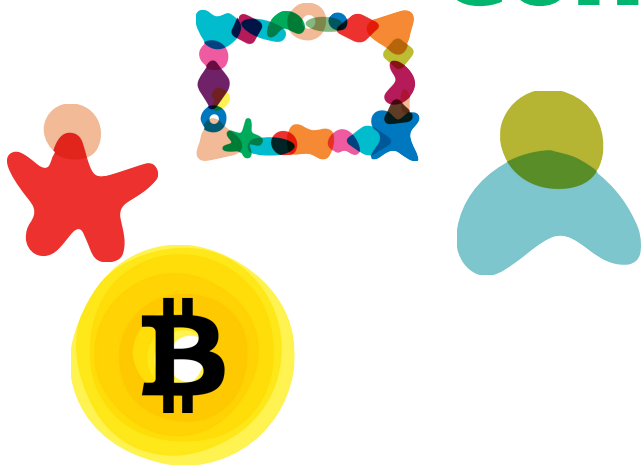


Validating a Block



- ▶ 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

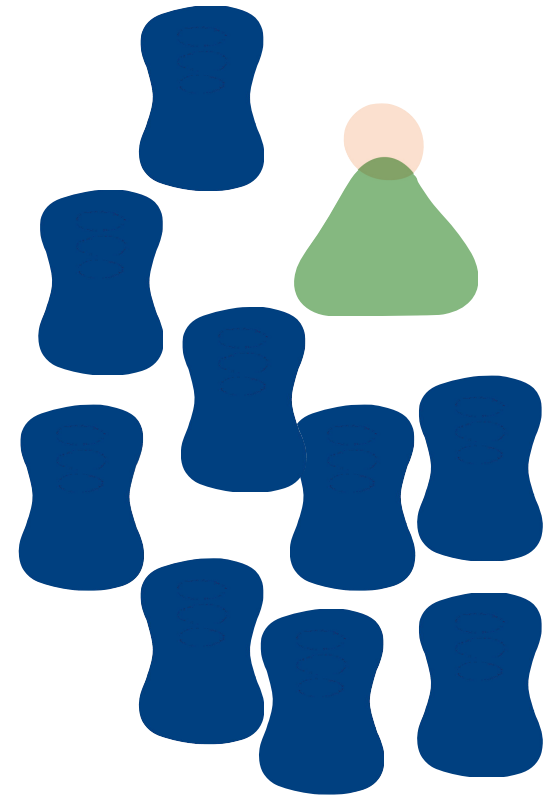
Consensus Attacks



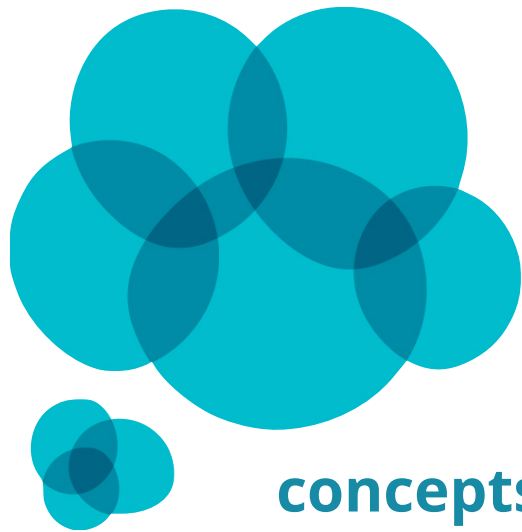
"51 %" attack

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

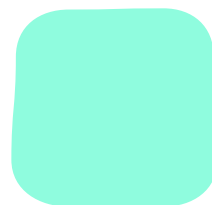
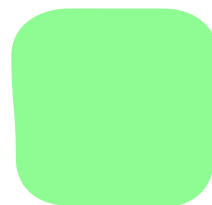
the older the transaction,
the more immutable it is



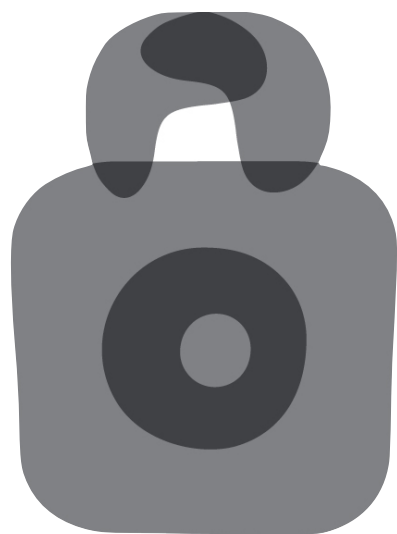
Agenda



concepts

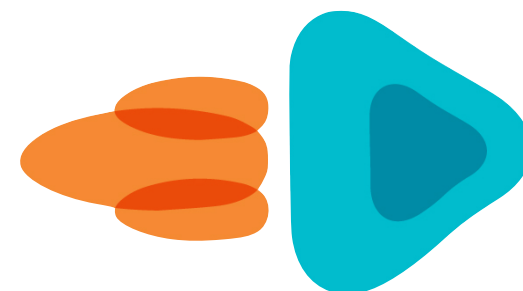


blockchain

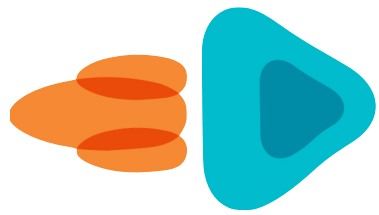


security

transactions



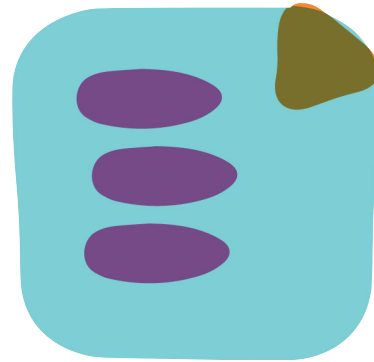
implications



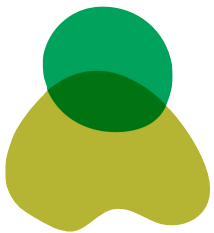
Implications



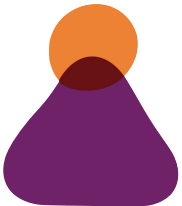
currency



contracts



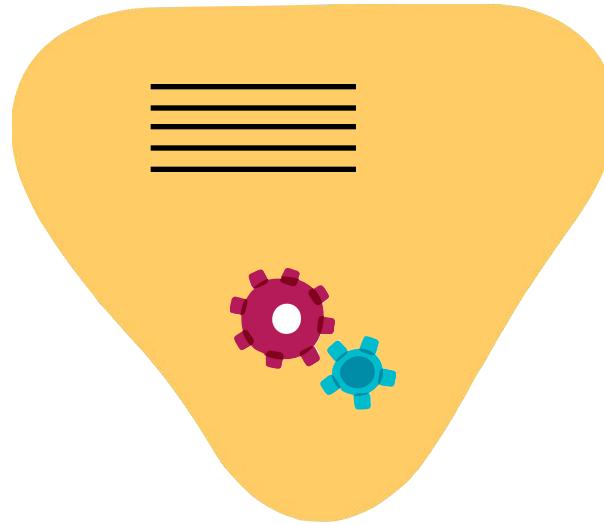
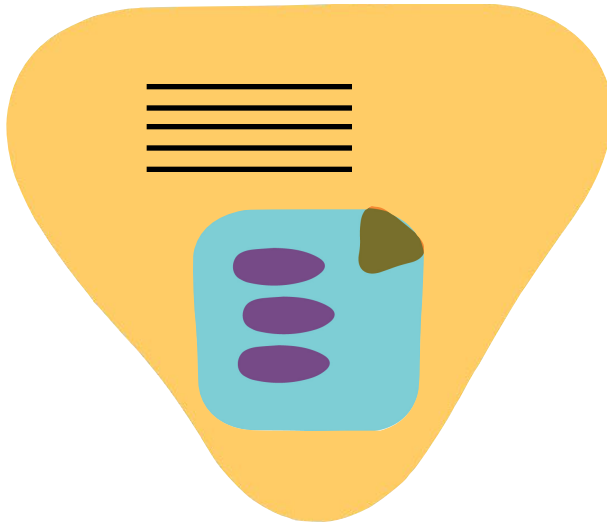
voting



reputation
index

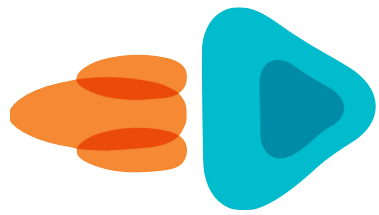


Content Binding



Transaction fees include size

Bigger payload == bigger fee



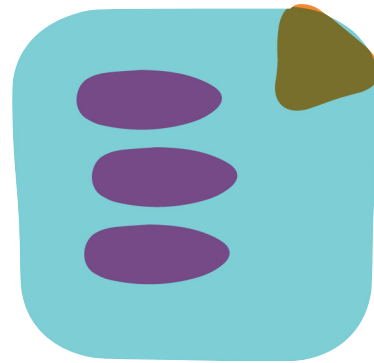
Implications



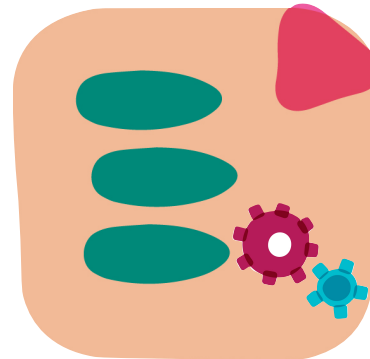
reputation
index



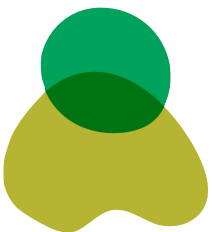
currency



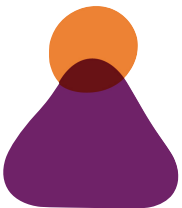
contracts



contracts
w/
conditions



voting



blockchain

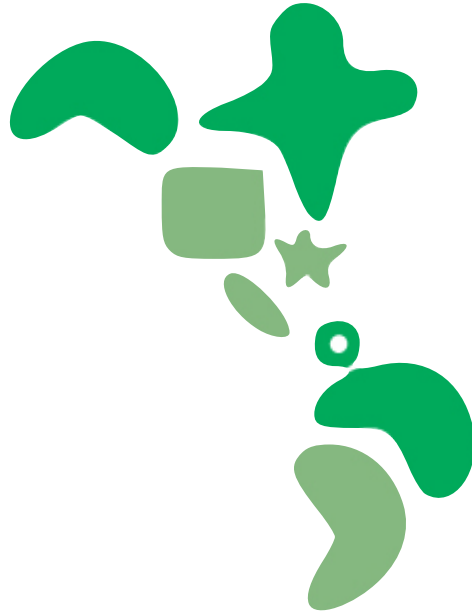
Positive Feedback Loop



Benefits



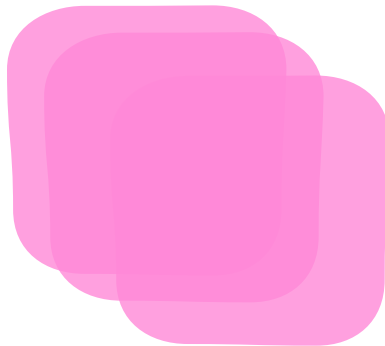
international
remittance
(w/ little or no fees)



international currency



micropayments



fight spam



public payments



Immutable == Forever

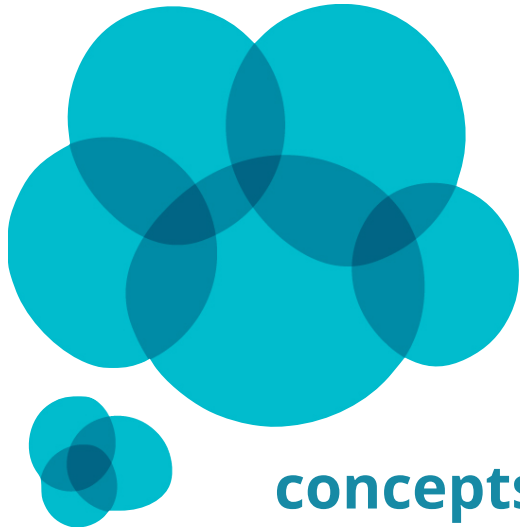
Permanent ledger

Distributed globally

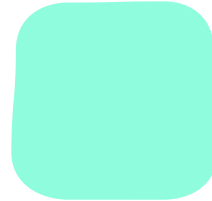
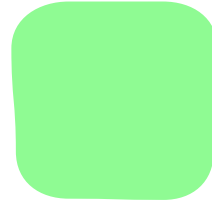
The older it is, the more immutable
it is

Be careful !

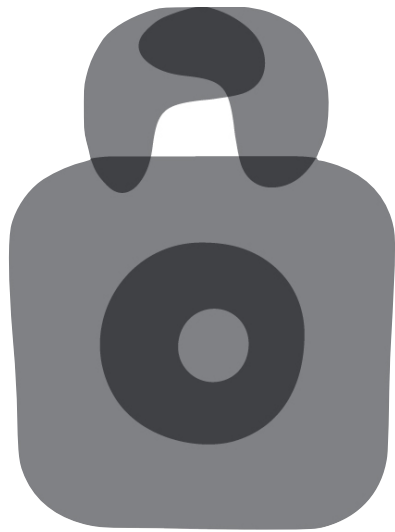
Summary



concepts

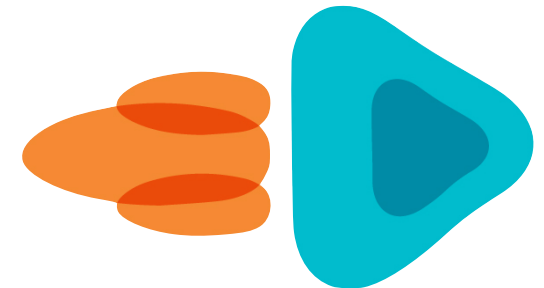


blockchain



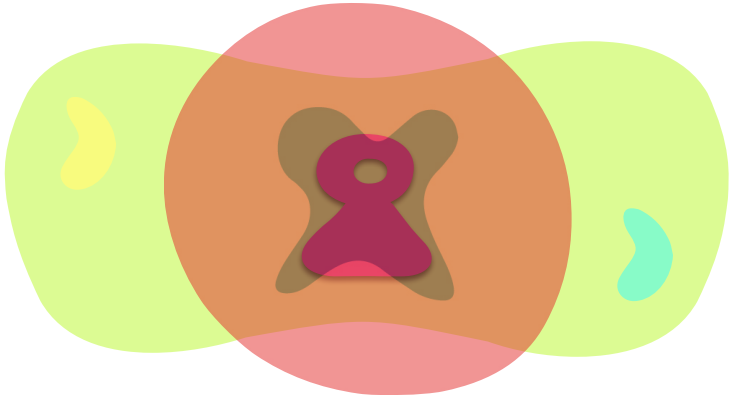
security

transactions

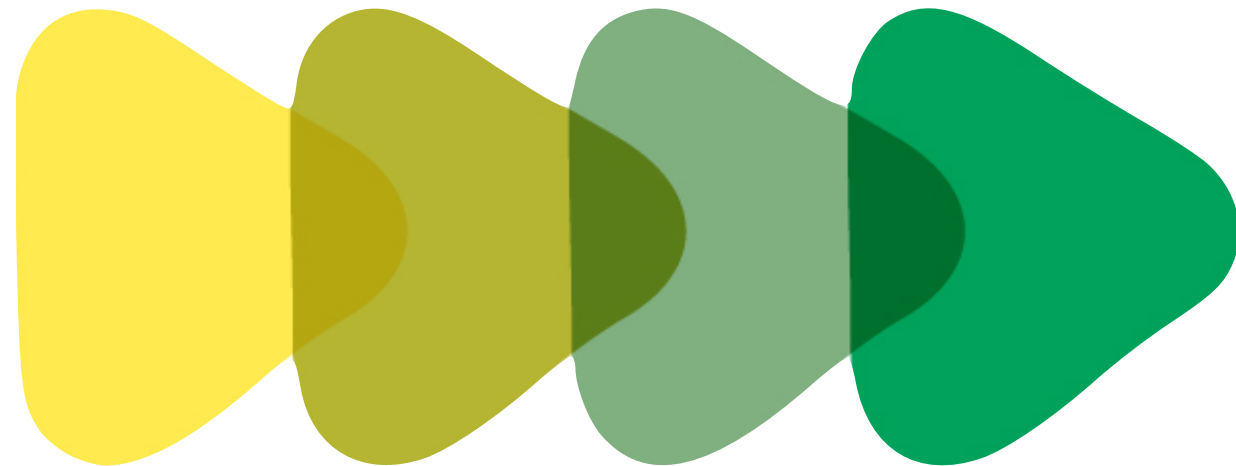


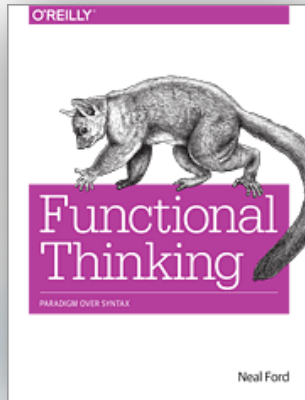
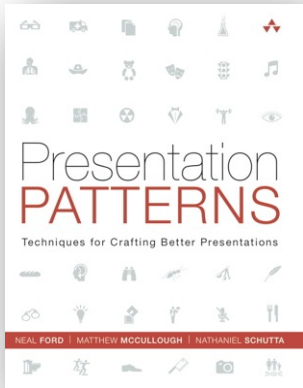
implications

Distributed Trust



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





nealford.com



@neal4d

ThoughtWorks®

NEAL FORD

Director / Software Architect / Meme Wrangler

