Introduction to Blockchains and crypto-thingamajigs*

*crypto-thingamajigs: used to refer to or address a person or thing whose name one has forgotten, does not know, or does not wish to mention.

In this case, crypto-currencies, crypto-assets, crypto-tokens, crypto-securities, etc.

March 19th, 2018

Boston College Law School / ILS

www.hugobenedetti.com

@Prof_Cryptoken

Key objectives

- Introduce blockchains and crypto-assets
- Describe the current crypto-things ecosystem

Why should we even talk about this?

- Crypto-market size $500 billion as of Feb 2018
  - Bitcoin $200 billion, 150 worth over $100 million
  - Over 4,000 cryptos actively traded
- Daily trading volume $25 billion (100+ exchanges)
- Crypto-assets raised over $4 billion in 2017 through Initial coin offerings (ICO)… the “new crowdfunding”
  - Only 7% of them could be considered securities (semi-equity), the rest are rewards/presale of products.
- Research initiatives led by Central banks, Financial Institutions Consortia, Philanthropic foundations, payment processors (Visa, Mastercard and AMEX), etc.

A Blockchain is just a way to structure data

- The novelty provided by blockchains is not the structuring of the data, but its role within a protocol that describes how data can be decentralized and made publicly available while maintaining security without requiring trust among agents.

- Blockchain is not Bitcoin.
  - Bitcoin is one protocol that uses a blockchain to register data. There are many others (more than 2,000) crypto-things similar to Bitcoin.

- But, as Bitcoin is the most famous, I will use it as a basic example and then generalize to blockchains.

What is Bitcoin?

- Evolution of several cryptocurrency proposals dating back to 1976[1]. Satoshi Nakamoto (pseudonym) distributed a whitepaper of his protocol on 2008 and shared the code in January 3rd, 2009.

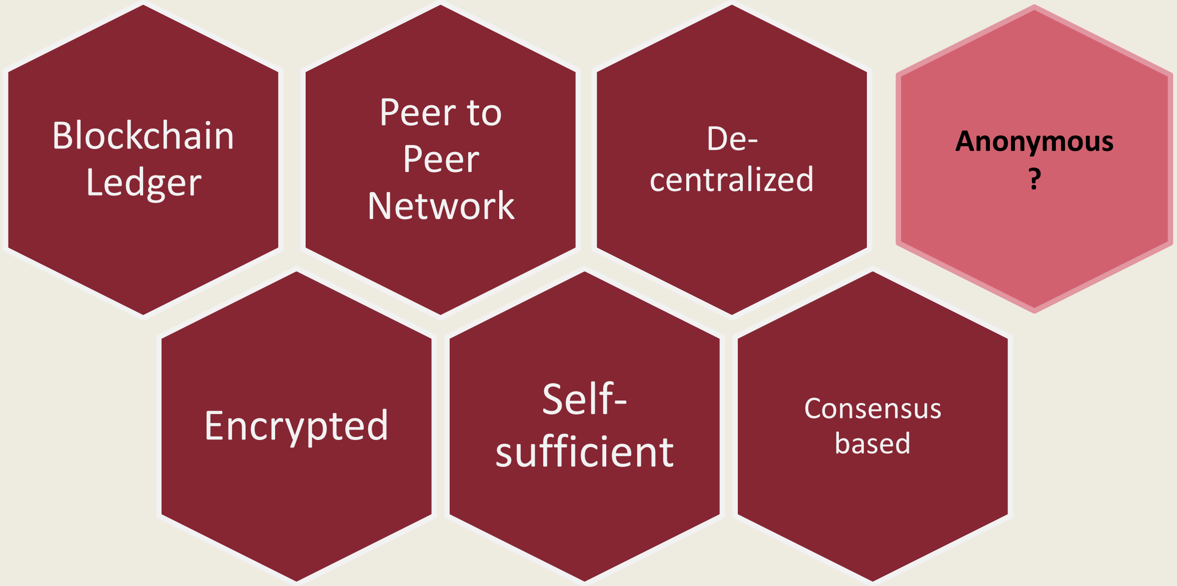
- Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen [2].

- Self-sufficient, peer-to-peer payment network, based on cryptographic proofs and blockchain accounting (rather than trust between participants or institutions).

[1] Cypherpunk mailing list

[2] www.bitcoin.org

Key elements of Bitcoin



Blockchain Ledger

Peer to Peer Network

De-centralized

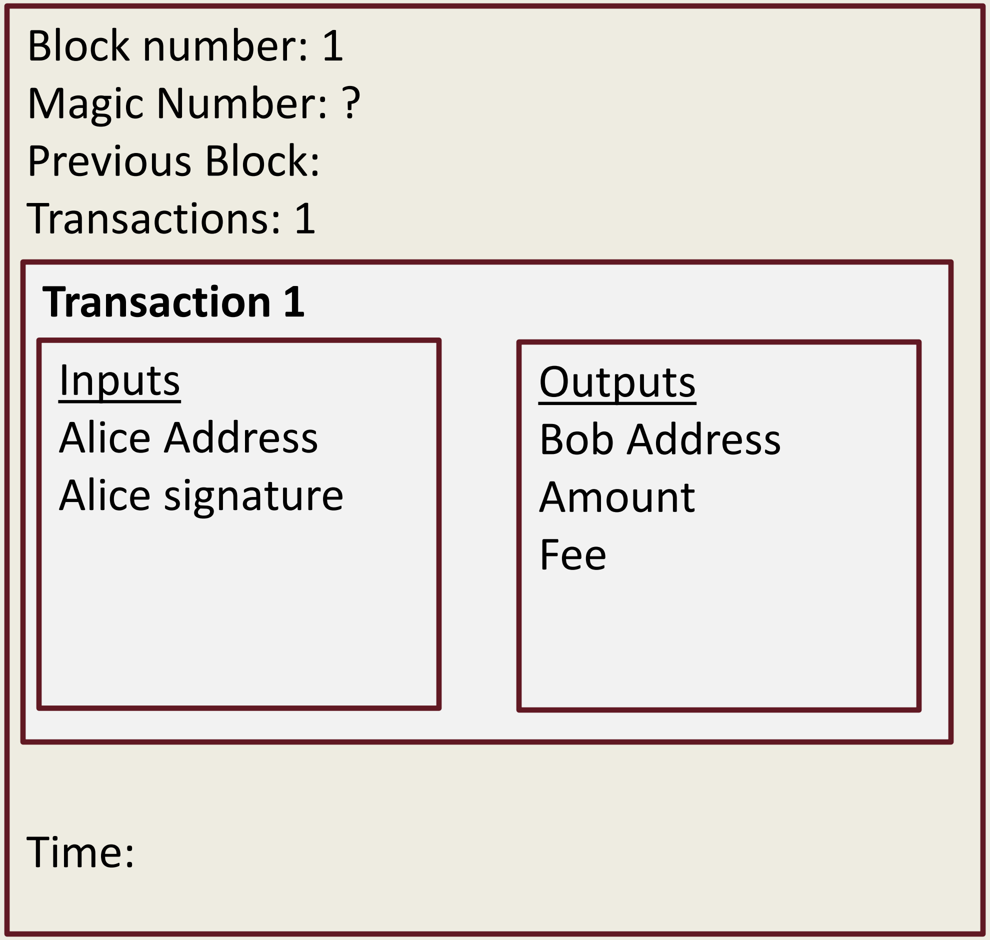
Anonymous ?

Encrypted

Self-sufficient

Consensus based

Blockchain: Chain of blocks!



Block number: 1

Magic Number: ?

Previous Block:

Transactions: 1

Transaction 1

Inputs

Alice Address

Alice signature

Outputs

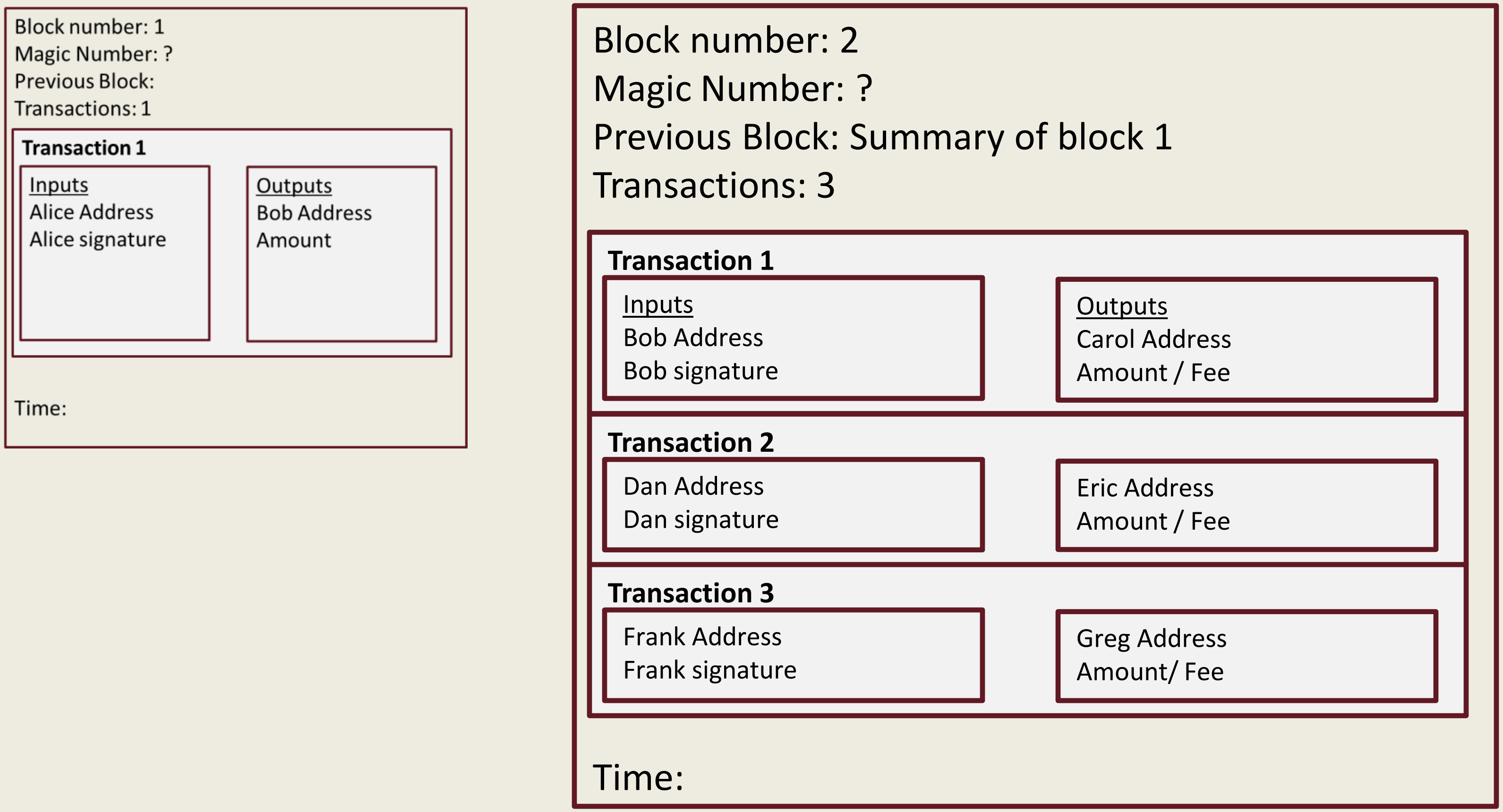
Bob Address

Amount

Fee

Time:

Blockchain: Chain of blocks!



Block number: 1
Magic Number: ?
Previous Block:
Transactions: 1

Transaction 1

Inputs
Alice Address
Alice signature

Outputs
Bob Address
Amount

Time:

Block number: 2
Magic Number: ?
Previous Block: Summary of block 1
Transactions: 3

Transaction 1

Inputs
Bob Address
Bob signature

Outputs
Carol Address
Amount / Fee

Transaction 2

Dan Address
Dan signature

Eric Address
Amount / Fee

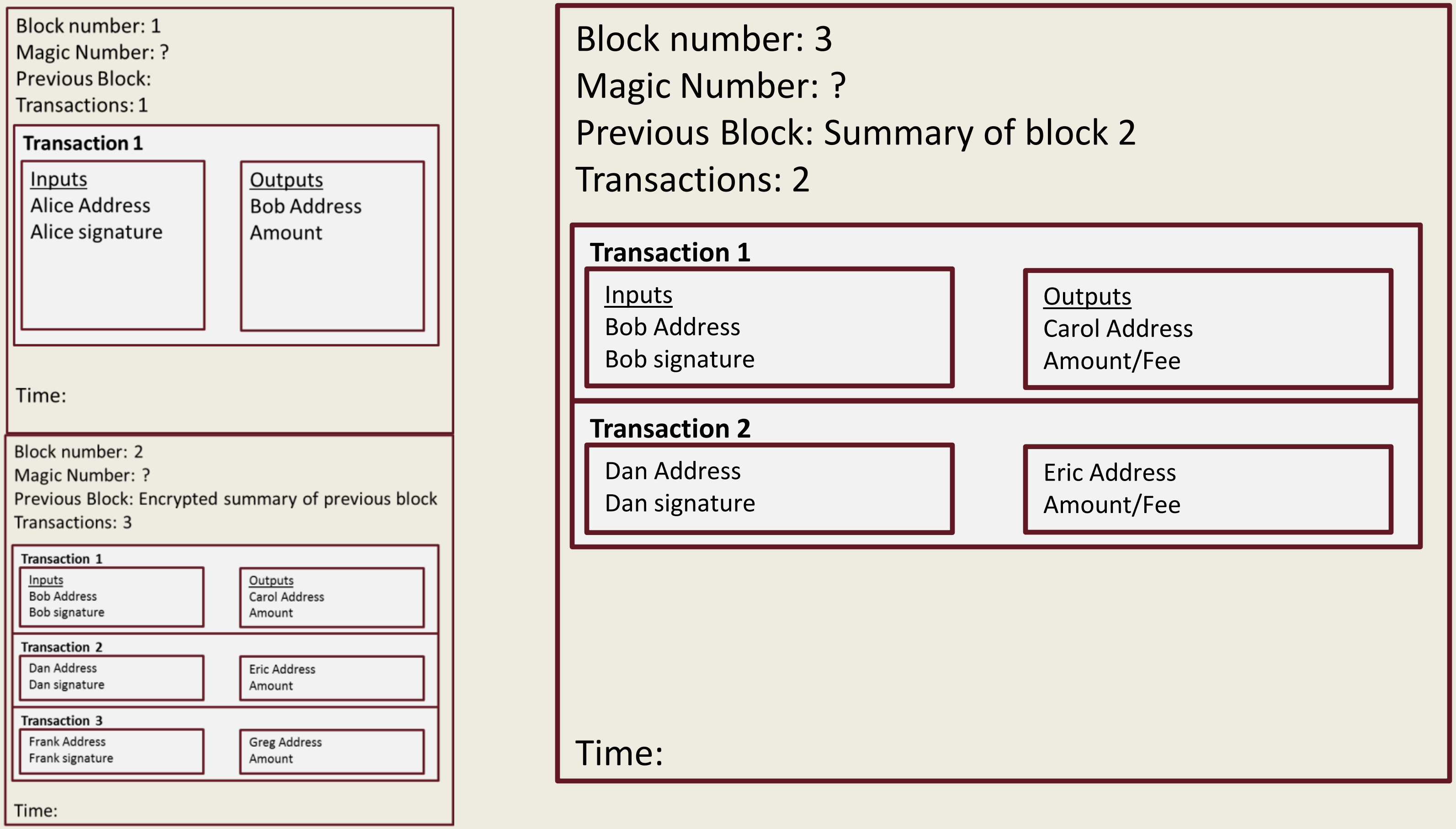
Transaction 3

Frank Address
Frank signature

Greg Address
Amount/ Fee

Time:

Blockchain: Chain of blocks!



Block number: 1
Magic Number: ?
Previous Block:
Transactions: 1

Transaction 1

Inputs
Alice Address
Alice signature

Outputs
Bob Address
Amount

Time:

Block number: 2
Magic Number: ?
Previous Block: Encrypted summary of previous block
Transactions: 3

Transaction 1

Inputs
Bob Address
Bob signature

Outputs
Carol Address
Amount

Transaction 2

Dan Address
Dan signature

Eric Address
Amount

Transaction 3

Frank Address
Frank signature

Greg Address
Amount

Time:

Block number: 3
Magic Number: ?
Previous Block: Summary of block 2
Transactions: 2

Transaction 1

Inputs
Bob Address
Bob signature

Outputs
Carol Address
Amount/Fee

Transaction 2

Dan Address
Dan signature

Eric Address
Amount/Fee

Time:

Anyone can join, listen, talk and validate

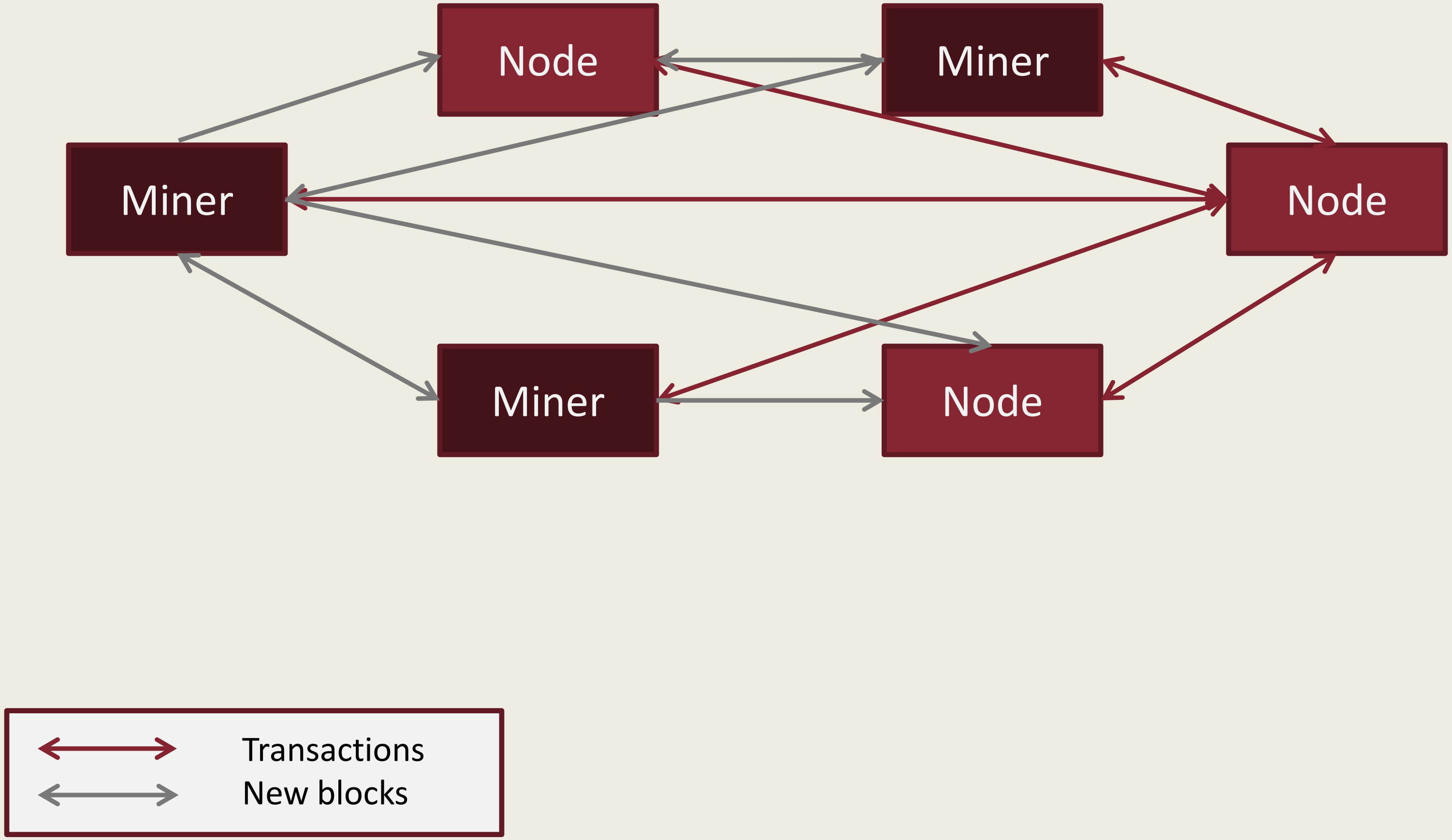
- As a peer to peer network, anyone can download the Bitcoin core software and get access to all the history of transactions.

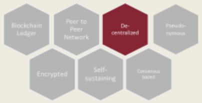
- The software allows for the transfer of 2 sets of information:
  - Peer to peer (P2P) network of transactions (“mempool”). Think of a blog of uncleared transactions.
  - P2P network of validated blocks. Each block is a list of transactions that have been validated.

- Computers connected to the network are called “nodes”. Computers that also try to validate blocks are called “miners”.

- To post a transaction, you have to go through a node that will relay the information to all other nodes (enters in the mempool). A miner will take your transaction and try to write it in a block (transaction leaves the mempool and is recorded on the blockchain).

Anyone can join, listen, talk and validate





Decentralized means no central authority

- Anyone can download the software and connect.
  - There is no way to block a person.
  - Anyone connected can create addresses, private keys (passwords) and public keys (validators). Large enough availability to be considered infinite.
- The code is open source, so anyone can use it and modify it.
  - Users can propose changes to the community, and if a large portion of the community agrees, the change is implemented.
  - If a minority of users want changes but the community doesn’t agree, the minority can launch an alternate cryptocurrency based on Bitcoin.
- The only way to block Bitcoin, is to disconnect all nodes, erase all copies of the blockchain, all copies of the code, and all copies of the new versions of the code.

Encryption ties each transaction, each block and the reward process

Encryption plays 3 roles:

- Secures each transaction, so only the holder of a valid private key (password) can create transactions, that can be verified by anyone using a public signature.

- Secures each block. A record of the previous block is attached to the current block. If someone tries to change block 1, it has to change block 2, block 3 until reaching the current block.

- Assigns rewards to the validators of the network.

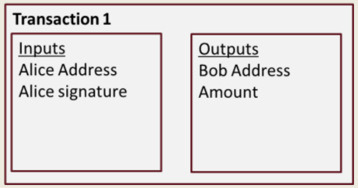
It’s all about the “hash”

- Hash functions are just functions that take input values to create an output deterministic on the input.

- Bitcoin uses the hash function SHA256. This translates any text (of any length) to a 256 bit code, equivalent to 64 alphanumeric characters.
  - Not a 1 to 1 mapping (not necessary anyway)
  - Not decrypted (yet)
  - Small changes in input lead to very different output

Signed, sealed and delivered

- The originator of a transaction (Alice) fills the data for a transaction:



Transaction 1

Inputs
Alice Address
Alice signature

Outputs
Bob Address
Amount

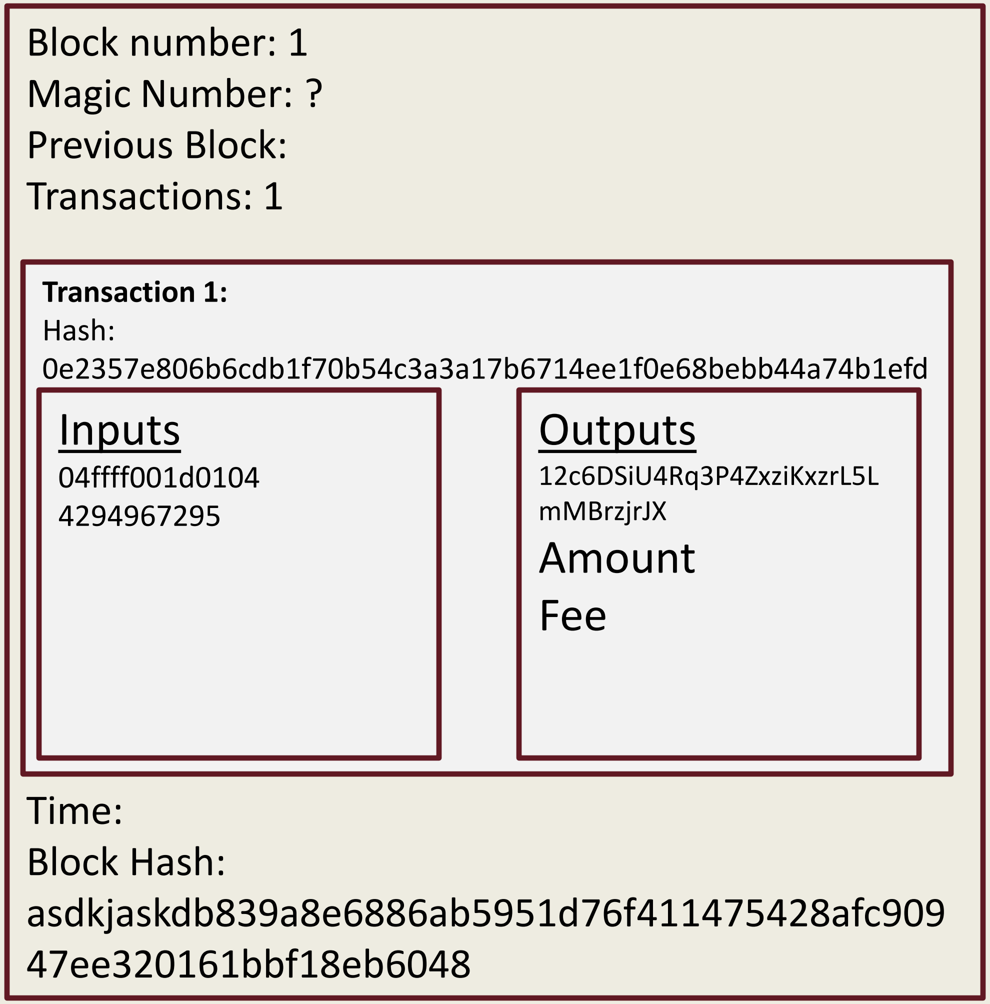
- This transaction will then be hashed (transformed into 64 alphanumeric characters) and digitally signed.

- The digital signature requires 2 keys. A private key (password) and a public key. The private key can "create" encrypted messages and the public key can "open" encrypted messages, but cannot create them.

- Alice signs by applying a transformation function to the hash of the transaction and her private password.

- Bob or anyone can use the public key to verify that the transaction was originated by Alice. Bob can't use the public key to generate a signature, so he can't change the transaction nor create new ones.

Block gets the hash of the hashes



Block number: 1
Magic Number: ?
Previous Block:
Transactions: 1

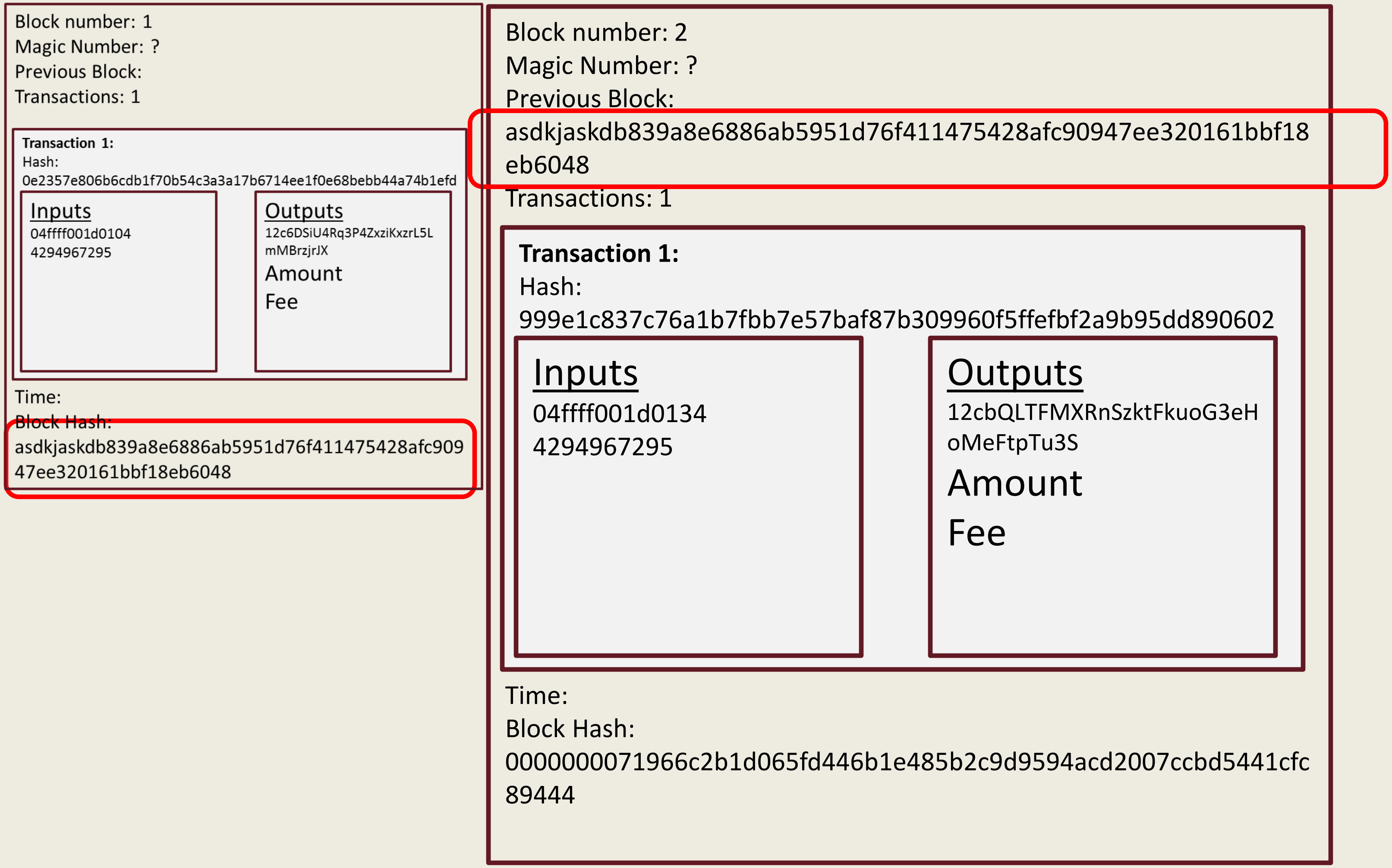
Transaction 1:
Hash:
0e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd

Inputs
04ffff001d0104
4294967295

Outputs
12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX
Amount
Fee

Time:
Block Hash:
asdkjaskdb839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

The hash of the previous block is included in the current block



Block number: 1
Magic Number: ?
Previous Block:
Transactions: 1

Transaction 1:
Hash:
0e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd

Inputs
04ffff001d0104
4294967295

Outputs
12c6DSiU4Rq3P4ZxziKxzrL5L
mMBrzjrJX
Amount
Fee

Time:
Block Hash:
asdkjaskdb839a8e6886ab5951d76f411475428afc909
47ee320161bbf18eb6048

Block number: 2
Magic Number: ?
Previous Block:
asdkjaskdb839a8e6886ab5951d76f411475428afc90947ee320161bbf18
eb6048
Transactions: 1

Transaction 1:
Hash:
999e1c837c76a1b7fbb7e57baf87b309960f5ffefbf2a9b95dd890602

Inputs
04ffff001d0134
4294967295

Outputs
12cbQLTFMXRnSzktFkuoG3eH
oMeFtpTu3S
Amount
Fee

Time:
Block Hash:
0000000071966c2b1d065fd446b1e485b2c9d9594acd2007ccbd5441cfc
89444

Encryption pays

- Quick digression that will tie encryption with self-sustainability and rewards to miners [(3)]

- How could we assign pay to each node/miners?
  - Evenly
  - Proportional to their contribution to the network
  - Randomly
  - Randomly, with probabilities proportional to their contribution to the network

- In the Bitcoin network, miners are paid in new bitcoins, hence the system is self-sufficient in the sense it does not need to connect to the “real” monetary economy.

[(3)] Validators of transactions and log keepers

Enter the magic number, AKA Nonce

Block number: 1
Magic Number (Nonce)
Previous Block:
Transactions: 1

Transaction 1:
Hash:
0e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd

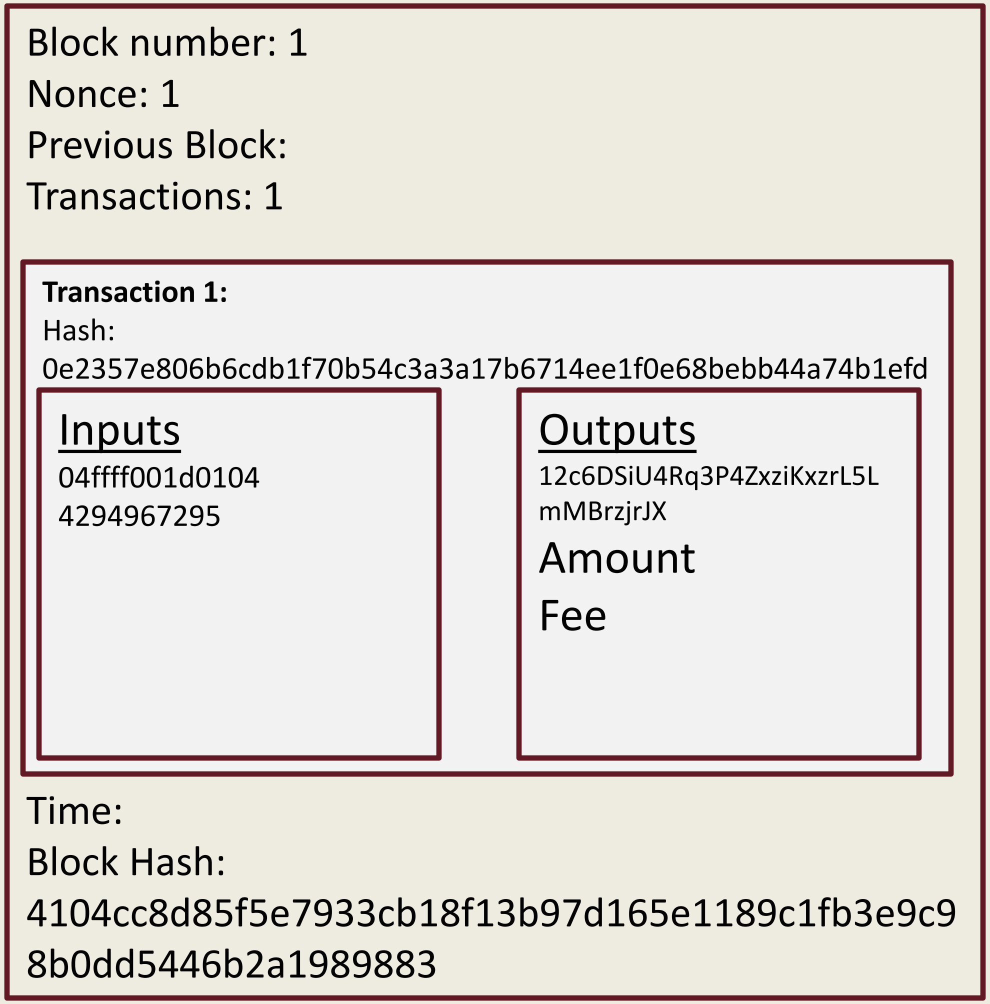
Inputs
04ffff001d0104
4294967295

Outputs
12c6DSiU4Rq3P4ZxziKxzrL5L
mMBrzjrJX
Amount
Fee

Time:
Block Hash:
a6f7f1c0dad0f2eb6b13c4f33de664b1b0e9f22efad599
4a6d5b6086d85e85e3

- Each miner receives transactions :
  - Check the input is valid
  - Check the signature is valid
  - Check the amount is valid
  - Very quick… nanoseconds per transaction
- Once a certain number of transactions are received, it calculates the hash of the block
- The goal is to get a hash that starts with certain number of zeros
- The miner will try different nonce until the hash is valid

Enter the magic number, AKA Nonce



Block number: 1
Nonce: 1
Previous Block:
Transactions: 1

Transaction 1:
Hash:
0e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd

Inputs
04ffff001d0104
4294967295

Outputs
12c6DSiU4Rq3P4ZxziKxzrL5L
mMBrzjrJX
Amount
Fee

Time:
Block Hash:
4104cc8d85f5e7933cb18f13b97d165e1189c1fb3e9c9
8b0dd5446b2a1989883

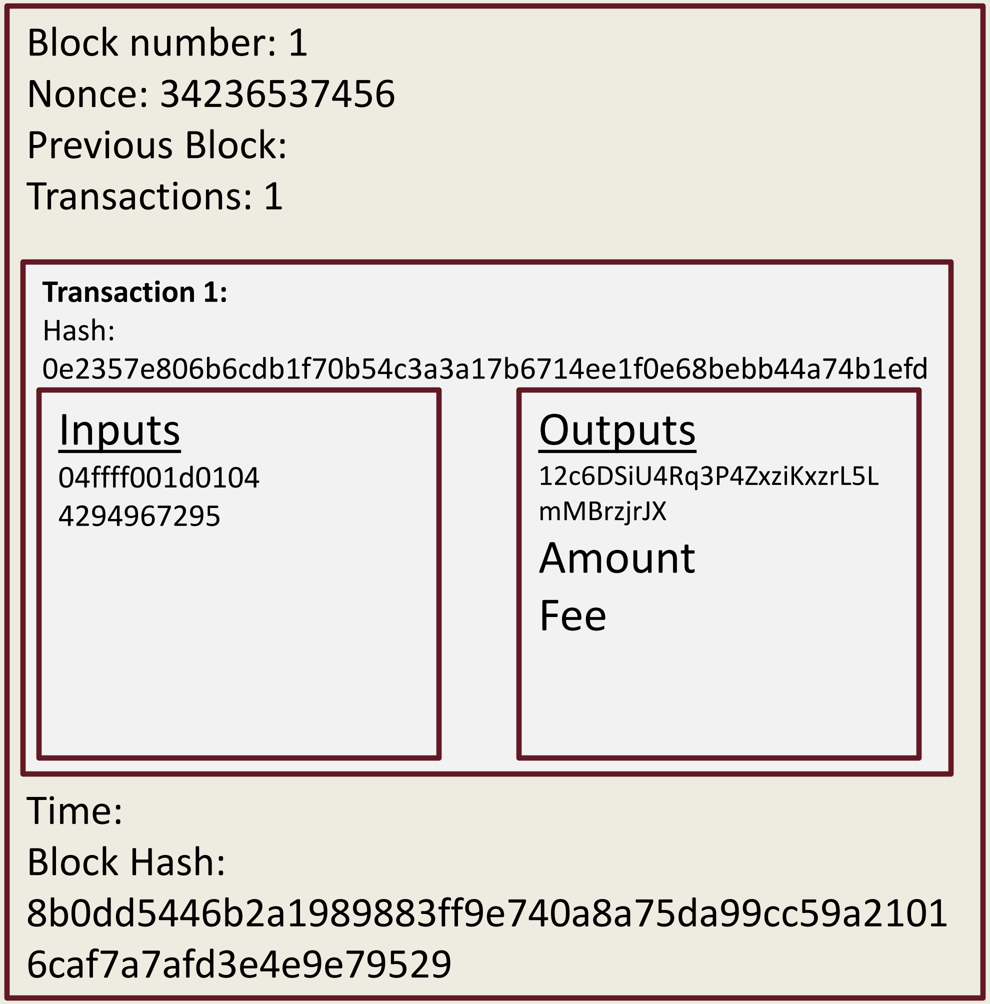
- Each miner receives transactions :
  - Check the input is valid
  - Check the signature is valid
  - Check the amount is valid
  - Very quick… nanoseconds per transaction

- Once a certain number of transactions are received, it calculates the hash of the block

- The goal is to get a hash that starts with certain number of zeros

- The miner will try different nonce until the hash is valid

Enter the magic number, AKA Nonce



Block number: 1
Nonce: 34236537456
Previous Block:
Transactions: 1

Transaction 1:
Hash:
0e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd

Inputs
04ffff001d0104
4294967295

Outputs
12c6DSiU4Rq3P4ZxziKxzrL5L
mMBrzjrJX
Amount
Fee

Time:
Block Hash:
8b0dd5446b2a1989883ff9e740a8a75da99cc59a2101
6caf7a7afd3e4e9e79529

- Each miner receives transactions :
  - Check the input is valid
  - Check the signature is valid
  - Check the amount is valid
  - Very quick… nanoseconds per transaction
- Once a certain number of transactions are received, it calculates the hash of the block
- The goal is to get a hash that starts with certain number of zeros
- The miner will try different nonce until the hash is valid

Enter the magic number, AKA Nonce

Block number: 1
Nonce: 456456
Previous Block:
Transactions: 1

Transaction 1:
Hash:
0e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd

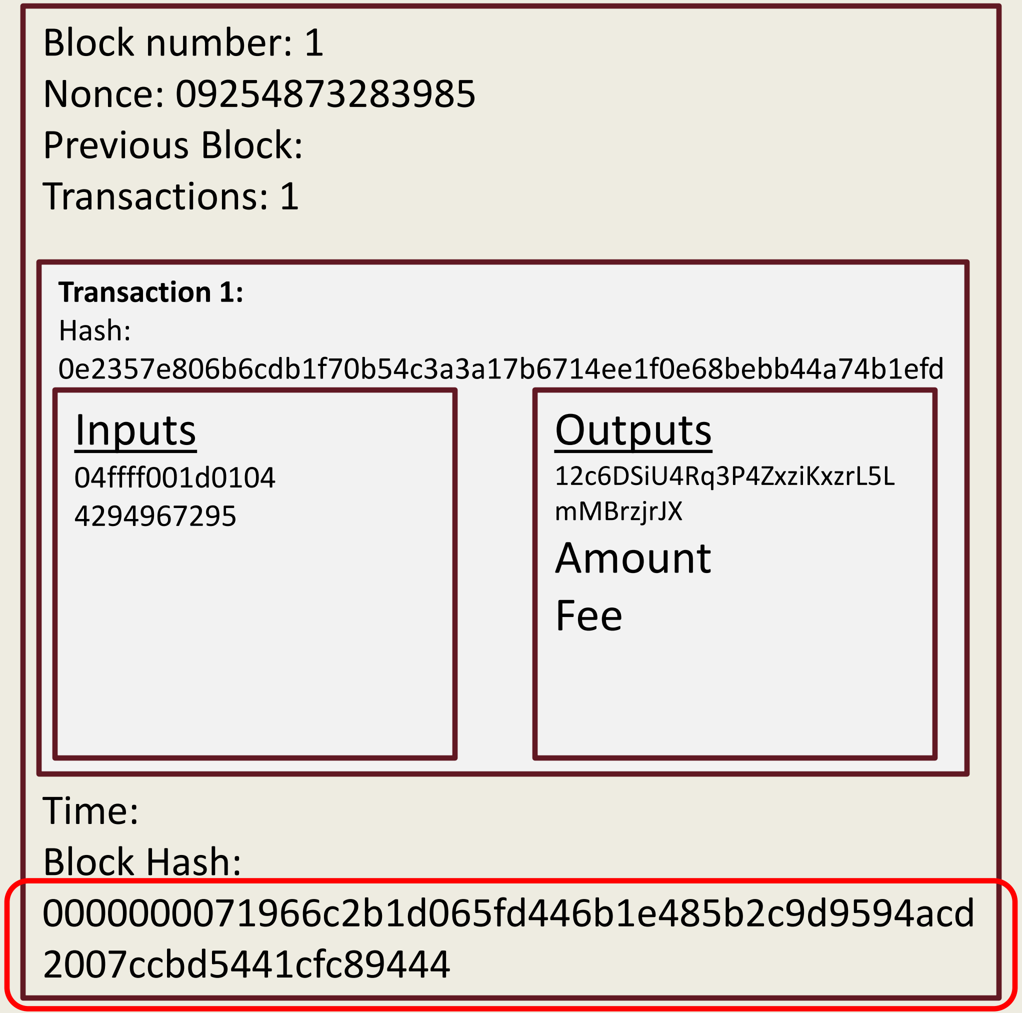
Inputs
04ffff001d0104
4294967295

Outputs
12c6DSiU4Rq3P4ZxziKxzrL5L
mMBrzjrJX
Amount
Fee

Time:
Block Hash:
049dd5446b2a1989883ff9e740a8a75da99cc59a2101
6caf7a7afd3e4e9e79529

- Each miner receives transactions :
  - Check the input is valid
  - Check the signature is valid
  - Check the amount is valid
  - Very quick… nanoseconds per transaction
- Once a certain number of transactions are received, it calculates the hash of the block
- The goal is to get a hash that starts with certain number of zeros
- The miner will try different nonce until the hash is valid

Enter the magic number, AKA Nonce



Block number: 1
Nonce: 09254873283985
Previous Block:
Transactions: 1

Transaction 1:
Hash:
0e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd

Inputs
04ffff001d0104
4294967295

Outputs
12c6DSiU4Rq3P4ZxziKxzrL5L
mMBrzjrJX
Amount
Fee

Time:
Block Hash:
000000071966c2b1d065fd446b1e485b2c9d9594acd
2007ccbd5441cfc89444

- Each miner receives transactions :
  - Check the input is valid
  - Check the signature is valid
  - Check the amount is valid
  - Very quick… nanoseconds per transaction
- Once a certain number of transactions are received, it calculates the hash of the block
- The goal is to get a hash that starts with certain number of zeros
- The miner will try different nonce until the hash is valid
- This is called “Proof of Work”

Encryption pays

- The first miner that finds a valid hash, receives a mining reward and the transaction fees.
  - The miner gets to write a transaction directed to the address of his/her choosing, with a transaction value equal to the mining fee (currently 12.5 BTC plus all the transaction fees).

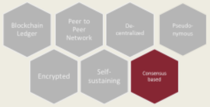
- As technology evolves, hashing becomes faster… Satoshi thought of this and included a calibrating mechanism. Difficulty is adjusted every 2 weeks to keep the time to block at an average of 10 minutes.

- Difficulty has increased exponentially[4] with large effects in the hardware market, industrial structure of mining, energy consumption and stability of the overall community.

[4] As of Nov 2017, 9 quadrillion hashes per second. A high-end PC would solve once every few million years, compared to 10 minutes in Jan 2009.

How does hashing make this safe?

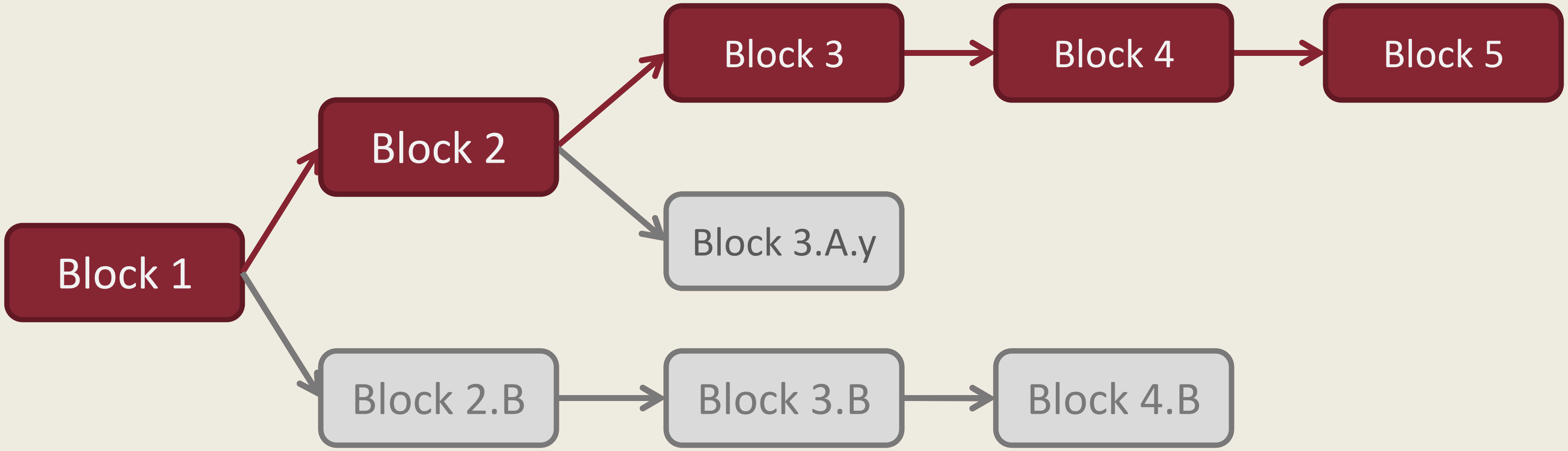
- Suppose we are currently in block 3. If someone wants to change something in block 1, it would have to:
  - Change a transaction (or delete)
  - Solve the new PoW of block 1
  - Link new PoW of block1 into block2
  - Check if transactions in block 2 are affected by the change in block 1, if they are, need to change them too
  - Solve the new PoW of block 2
  - Link new PoW of block 2 into block 3… before anyone creates block 4!
- It’s very difficult to “hack” a digital signature (no known hacks, ever), so a miner can only change his own transactions or not include certain transactions.



Reaching consensus

- Suppose 2 miners (A and B) solve the PoW relatively close in time.
  - Both distribute their block to the network. Some will get the block from A, other from B.
  - These blocks might have the same transactions or not.
  - One will have a mining reward to A, the other to B.
  - The miners will have to choose which block to use. They will check consistency of the block, if ok, start working on a new block, using either A or B as last valid block.
  - One or more miners will solve a new block and post it… the process repeats itself until one chain becomes sufficiently longer.

Only the longest survives



The left behind are… forgotten

- Even though the forgotten miners wrote transactions on the blockchain, those transactions are not recorded in the longest chain, hence are not valid anymore.

- The users transactions are not lost, they could have been already included in the parallel chains, and in the worst case, they will still be in the mempool and will be included soon.

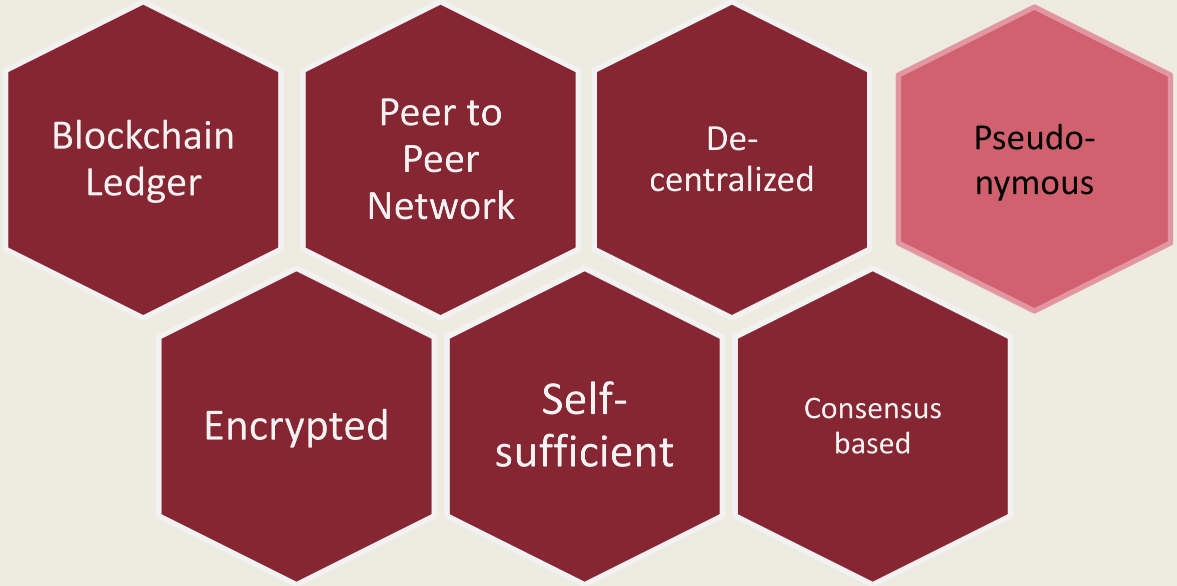
- This makes it difficult for someone to know if their transaction will remain valid.

- The rule of thumb, 6 blocks serve as confirmation (+- 1 hour)

Bitcoin is not anonymous…

- There are no names, just addresses… but since the address is known, it becomes a pseudonymous.
  - Since all the transactions are visible, anyone can trace back any and all the transactions of an address.
  - With one transaction identified, all transactions related to that address become compromised.
  - Several companies are dedicated to blockchain analysis (IRS, DEA, SEC, Interpol are their largest clients)
  - Bitcoin protocol only allows for the transfer of bitcoin. People use bitcoin to transfer fiat currency. If an exchange, a wallet, or a bank is used, then most likely the person will be identified.

Recap: Key elements of Bitcoin



Blockchain Ledger

Peer to Peer Network

De-centralized

Pseudo-nymous

Encrypted

Self-sufficient

Consensus based

What is Bitcoin?

- Self-sufficient, peer-to-peer payment network, based on cryptographic proofs and blockchain accounting (rather than trust between participants or institutions).

- The Bitcoin protocol allows to create payment services, without a central authority to validate transactions… fast settlement, no counter party risk, no counterfeit risk… on the digital side.

Some myths about bitcoin

Myth

1. Anonymous, untraceable
   - Mixers and tumblers
2. Safe, un-hackable
3. No transaction fee
4. No need for banks
5. No need for middle men

Truth

1. Already discussed
   - Already hacked
2. Private keys are so far un-hackable, but human error and social engineering are still in the picture
3. Around 1% just for network access
4. Bitcoin only handles storage and bitcoin payments… banks do more
5. Exchanges, wallets, banks and payment services are unregulated, provide no transparency nor guarantee

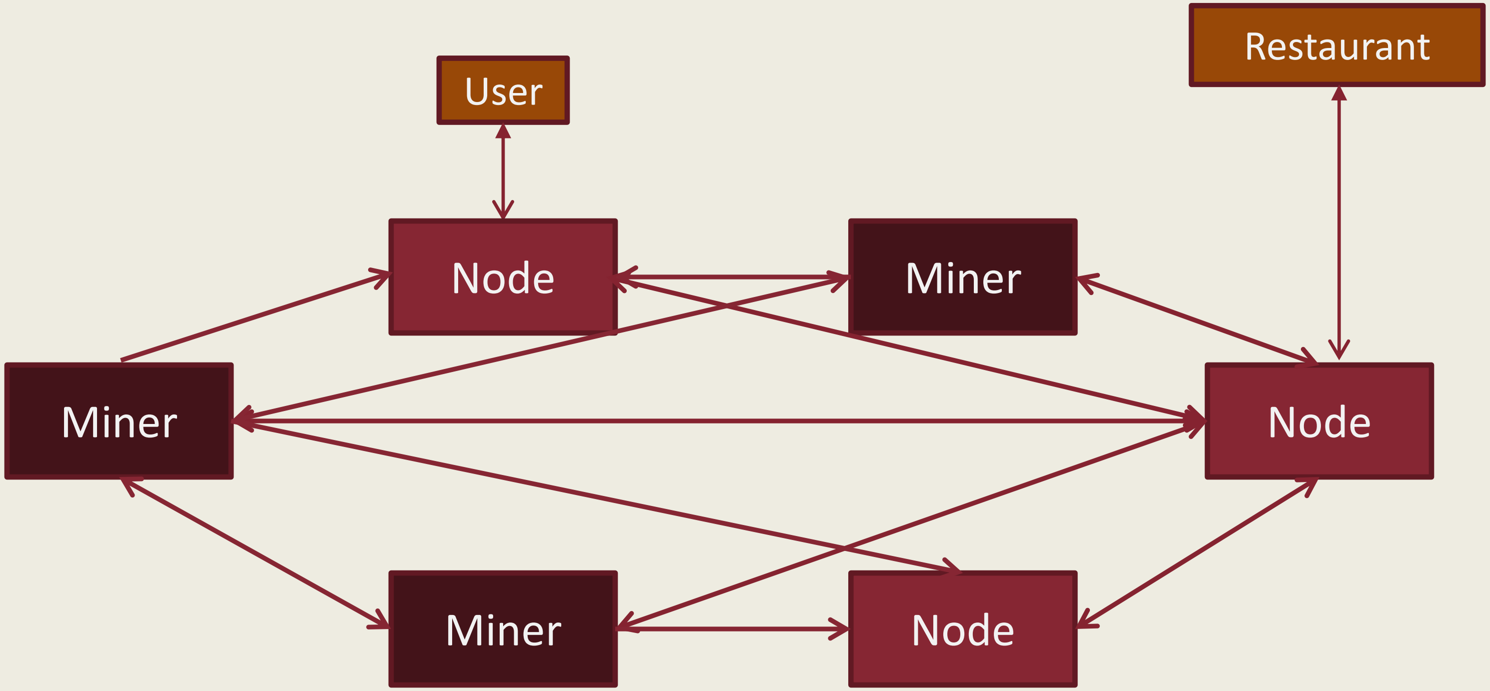
Main Current Concerns

- Concentration of miners: 4 pools (groups of ASICs) control 55%-60% of the blocks. Less than 20 addresses per day.
  - Security risk.
  - Opportunistic behavior/cartels (switch blockchain, exit network)

- As there are more transactions, the mempool is growing, so people are willing to pay higher fees to get miners to write their transactions in the current block.
  - Solution: Increase block size/ decrease the size of each transaction => more transactions per block, lower wait time and lower fees. Miners oppose.

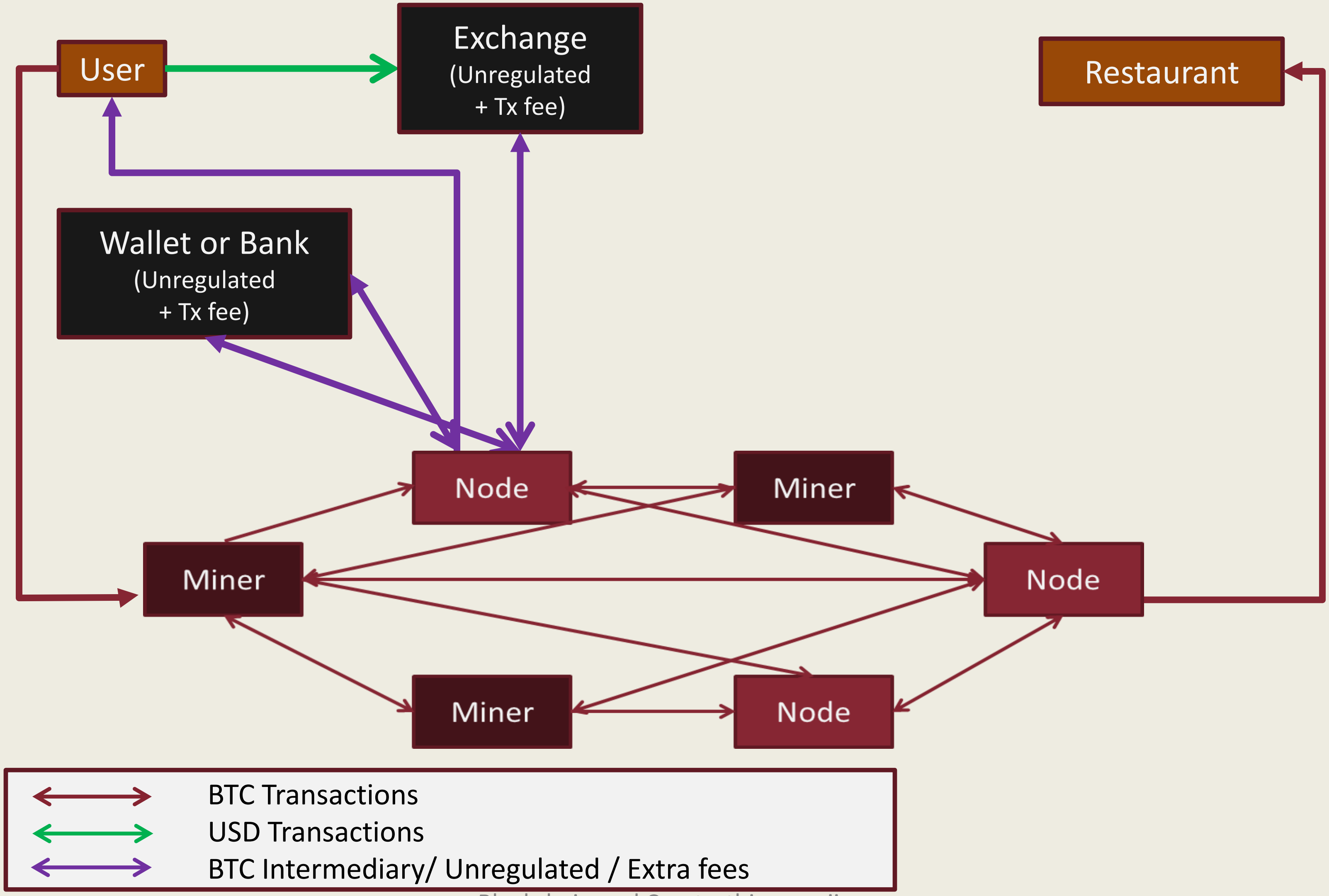
- Power consumption of the PoW equivalent to Denmark… for no other purpose than to randomly assign payments. (and to provide the most secure network to date)

Satoshi’s Ecosystem



⟷ BTC Transactions

Current Ecosystem



User

Exchange
(Unregulated
+ Tx fee)

Restaurant

Wallet or Bank
(Unregulated
+ Tx fee)

Node

Miner

Miner

Node

Miner

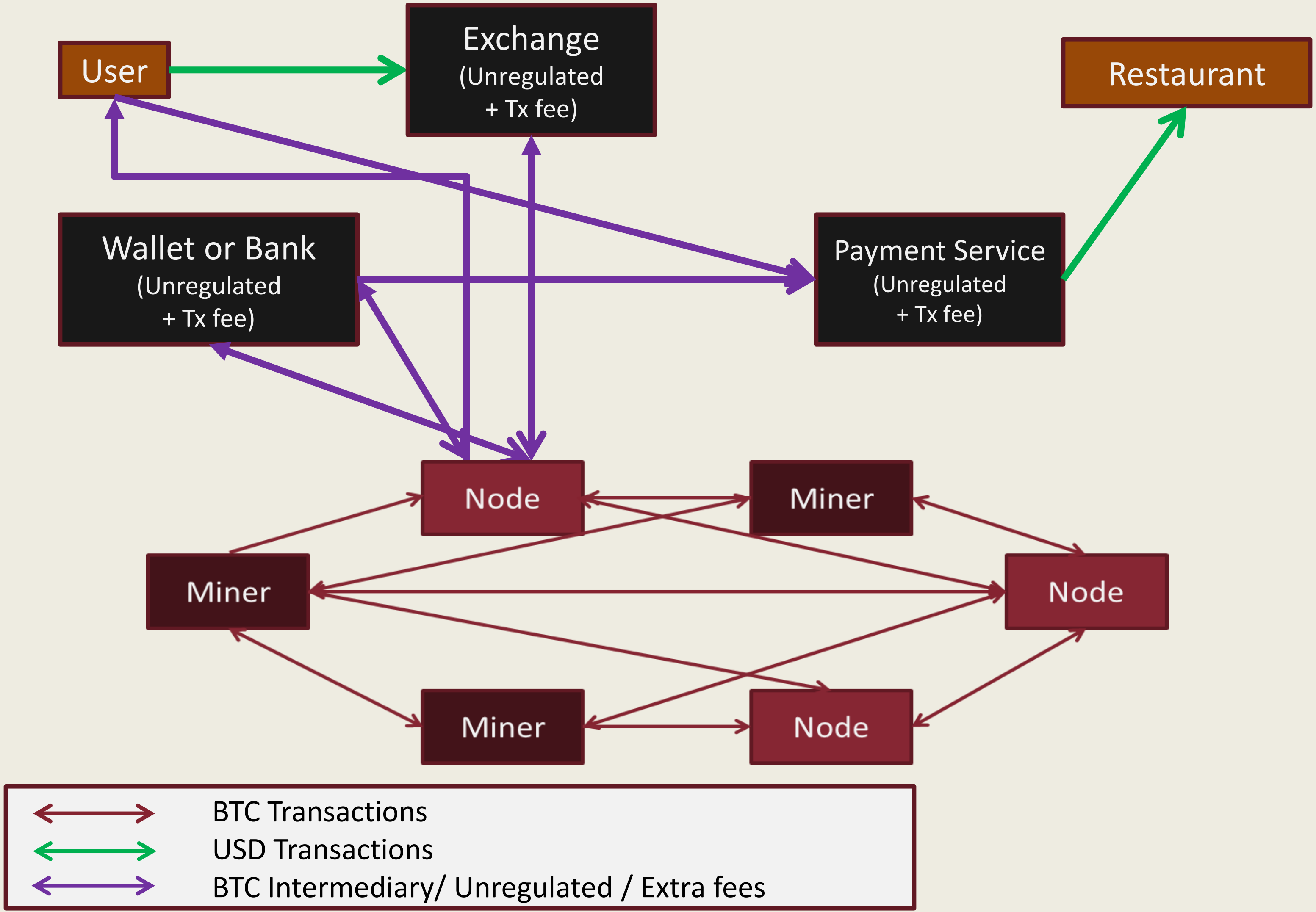
Node

⟷ BTC Transactions

⟷ USD Transactions

⟷ BTC Intermediary/ Unregulated / Extra fees

Current Ecosystem



User

Exchange
(Unregulated
+ Tx fee)

Restaurant

Wallet or Bank
(Unregulated
+ Tx fee)

Payment Service
(Unregulated
+ Tx fee)

Node

Miner

Miner

Node

Miner

Node

↔ BTC Transactions

↔ USD Transactions

↔ BTC Intermediary/ Unregulated / Extra fees

Other Crypto-assets

- Creating a crypto-thing involves highly advanced technical knowledge of cutting edge computer science protocols:
  - google (crypto currency creator)

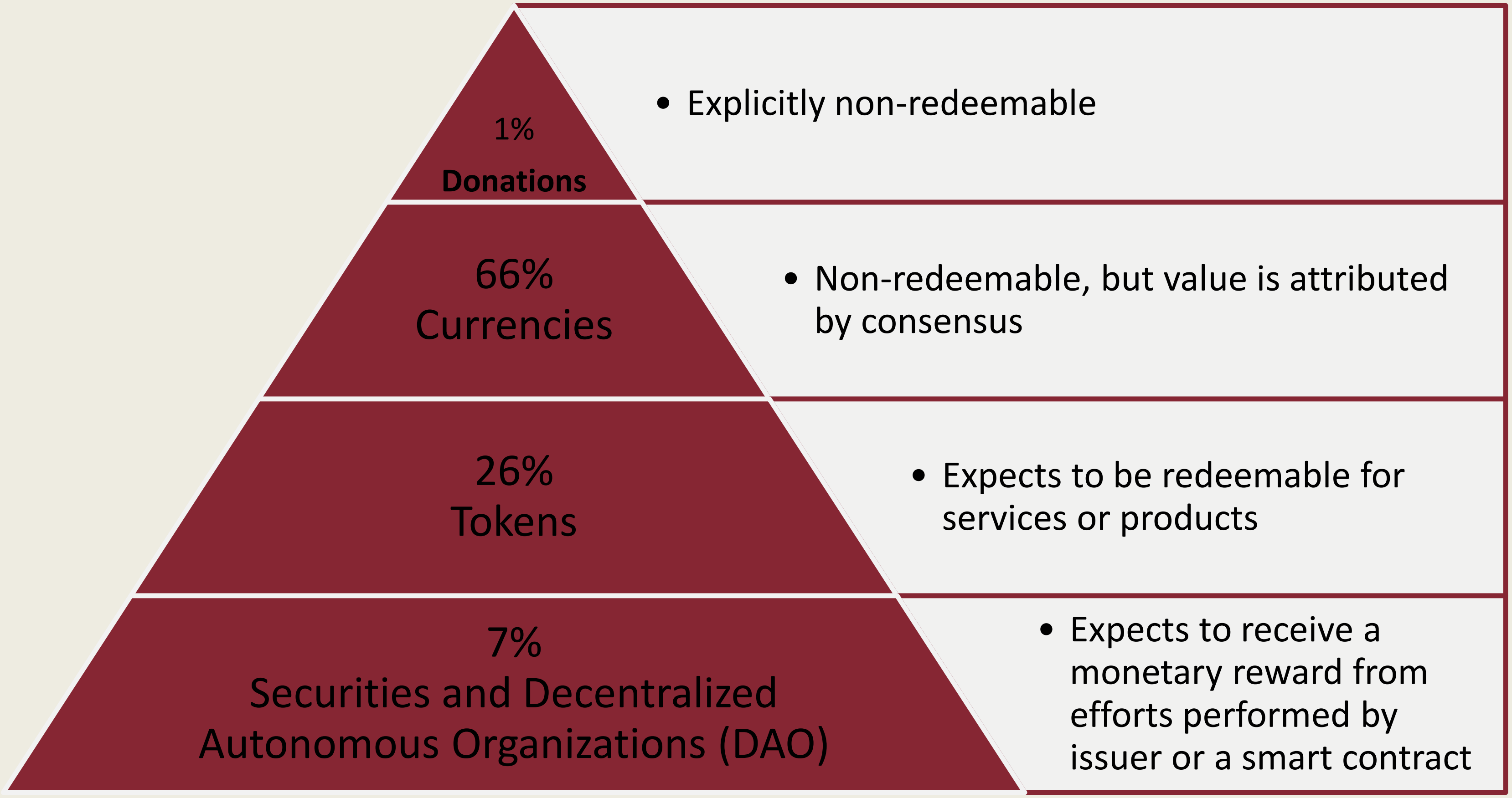
- Not completely accurate, but many crypto-things were, are and will be created this way.

- Over 4,000 crypto-things

- What makes them different?
  - Name
  - Block s
  - Laten
  - Mini
  - Distri
  - Cons
  - Hash
  - Diffic

We have over 3,000 “tries”, we should know what works and what doesn’t…

Spectrum of 1,400 crypto-things



1%
Donations

- Explicitly non-redeemable

66%
Currencies

- Non-redeemable, but value is attributed by consensus

26%
Tokens

- Expects to be redeemable for services or products

7%
Securities and Decentralized Autonomous Organizations (DAO)

- Expects to receive a monetary reward from efforts performed by issuer or a smart contract

Crypto Types

- Donations:
  - BioBar is a Proof of Work/Proof of Stake cryptocurrency created to make donations reach Registered Organizations once the Community agrees on which ones will have the use of Donated Funds.
  - Boats and Bitches is a Proof of Stake cryptocurrency based on the X11 algorithm. Fed up with all the lies and scams found in the ICO world, the coin devs decided to throw an honest ICO in which the purpose of the funding campaign is to pay for a boat party.

- Currencies:
  - BitTokens is a cryptocurrency that aims to be an improved version of Bitcoin, with faster blocktimes and higher transaction capabilities. BitTokens use the Sha256d hashing algortihm and has a 3 minute block time.

Crypto Types

- Tokens:
  - Aeternity is a scalable blockchain platform that enables high bandwidth transacting, purely-functional smart contracts, and decentralized oracles. The use of the blockchain is not free, and requires that the user spends a token called Aeon. Aeons are used as payment for any resources one consumes on the platform, as well as the basis for financial applications implemented on the platform. All system fees get paid with aeon, all smart contracts settle in aeon.

- Securities/ Decentralized Autonomous Organizations:
  - Adelphoi is a cryptocurrency community with its own economic ecosystem which can be interacted with through the use of the ADL token. The Adephoil community focuses on creating, developing and implementing usecases that involve blockchain technology in multiple industries. Projects are chosen by the community and successful ventures are either re-invested for further growth or issued as rewards to stakeholders.
  - The Blockchain Index is a product that allows investors from the traditional market to participate into a curated index of cryptocurrencies. The BLX token represents a stake in the fund and can be withdrawn from the Iconomi platform. Blockchain Index is not accessible to US citizens.

So… what comes next for you?

Fall down the crypto rabbit hole

- Suggestions for BC Law:
  - Discuss on how should we classify these thingamajics, follow up on the diverse opinions from SEC, CFTC, IRS, etc.
  - ICOS (initial coins offerings, Token generation events, etc).
  - Discuss on smart contracts
  - Coding for lawyers? (checkout WulfKaal.com)
  - See what other Law Schools are doing. Cardozo has amazing working groups on Blockchain-crypto.
  - Get involved!!! Boston crypto-community is HUGE and very welcoming
  - Reach out to me, I'll love to help.

www.hugobenedetti.com

@Prof_Cryptoken