Masterclass on Bitcoin, Ethereum & CryptoAssets

Thiyagarajan M (Rajan), twitter.com/mtrajan
Belavadi Prahlad, belavadi.com

October 2017

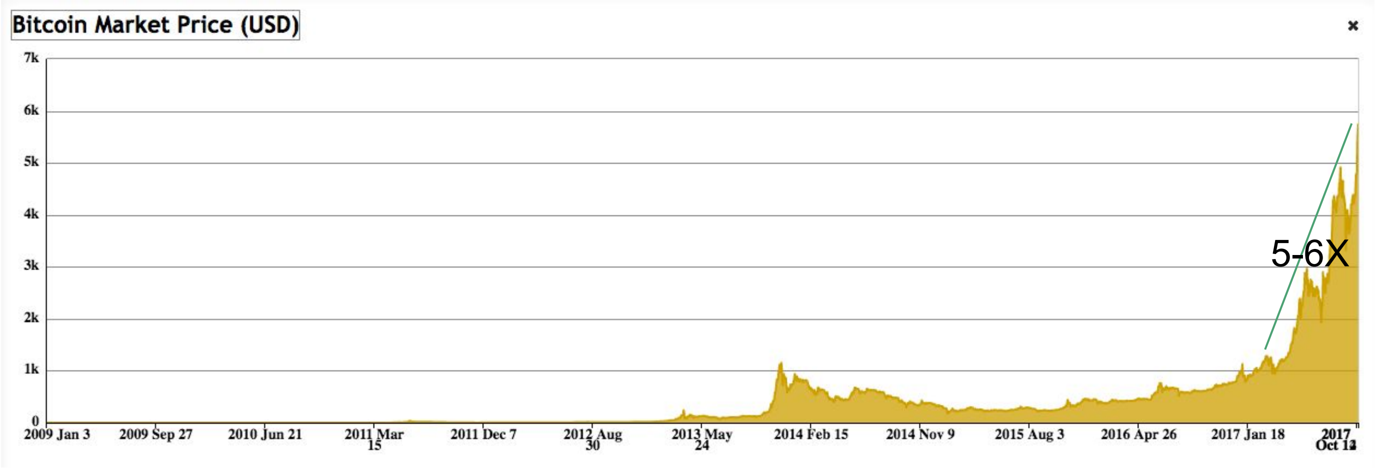
What would you like to see covered ?

Agenda

- Why blockchain & why now ?
- Module 1 - Blockchain, Bitcoin & Ethereum Basics
- Module 2 - Under the hood - Bitcoin, Ethereum
- Module 3 - Valuation for Crypto Assets
- Module 4 - ICO

Why should you care about blockchain now ?

$100 in 2009 in bitcoin will be $500 million in 2017

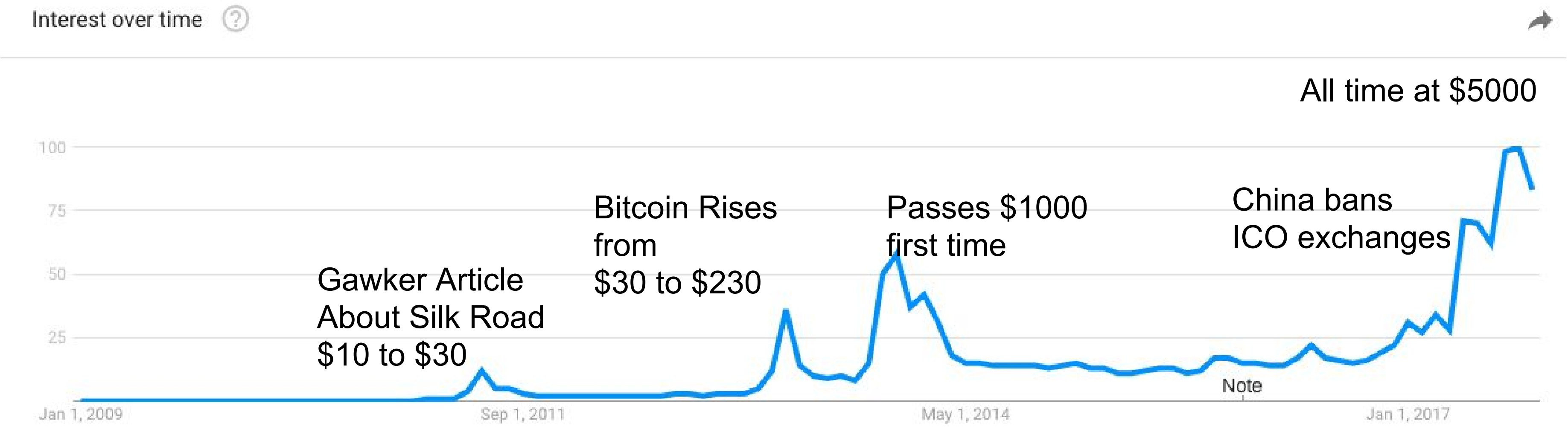


As 20 Oct 2017

7% of 1 cent (1/100 $) in 2009 to $5000 on Oct 15 2017

Fastest growth of anything known to humans

Google Search Trends - Bitcoin



Gawker Article About Silk Road $10 to $30

Bitcoin Rises from $30 to $230

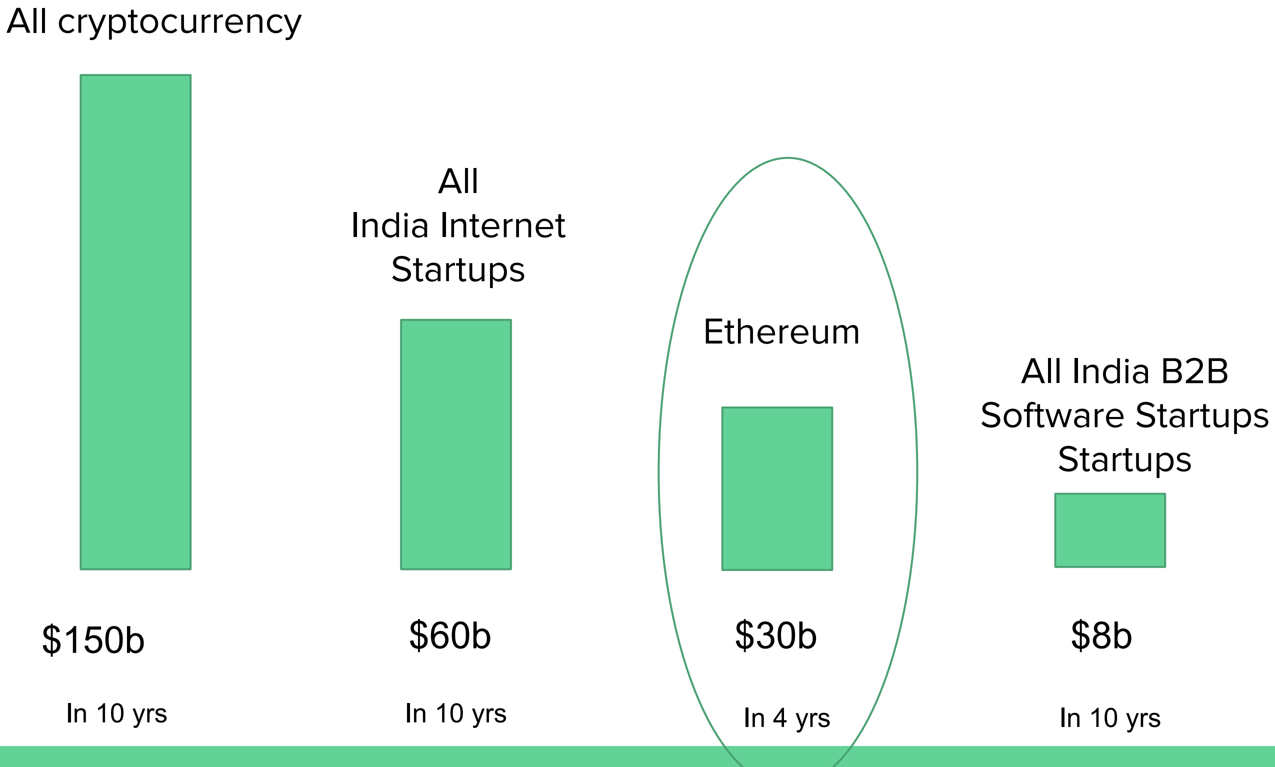
Passes $1000 first time

China bans ICO exchanges

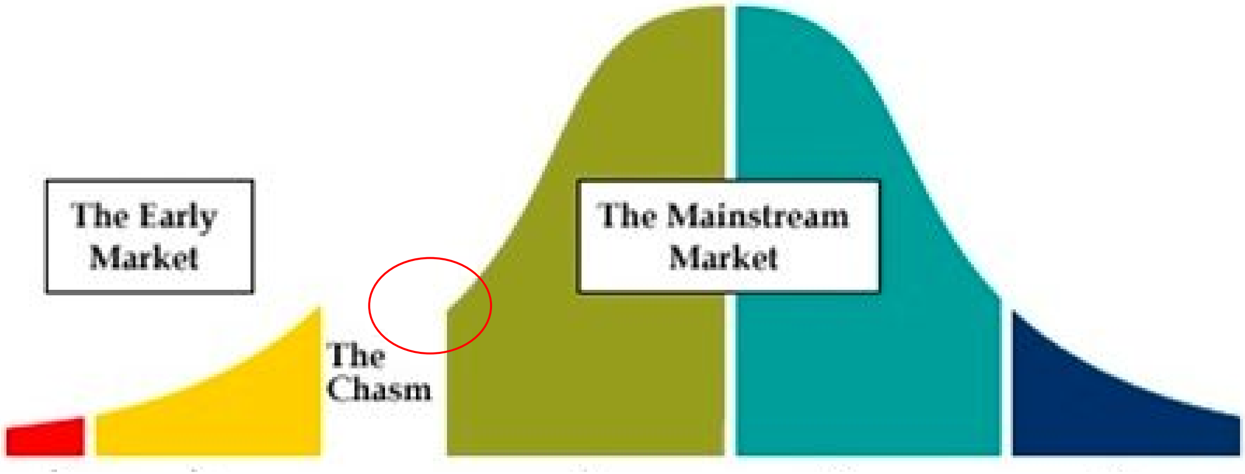
All time at $5000

https://trends.google.com/trends/explore?date=2009-01-01%202017-10-15&q=bitcoin

Ethereum is the new Java



In 3rd Stage, hitting escape velocity



Prototype Stage

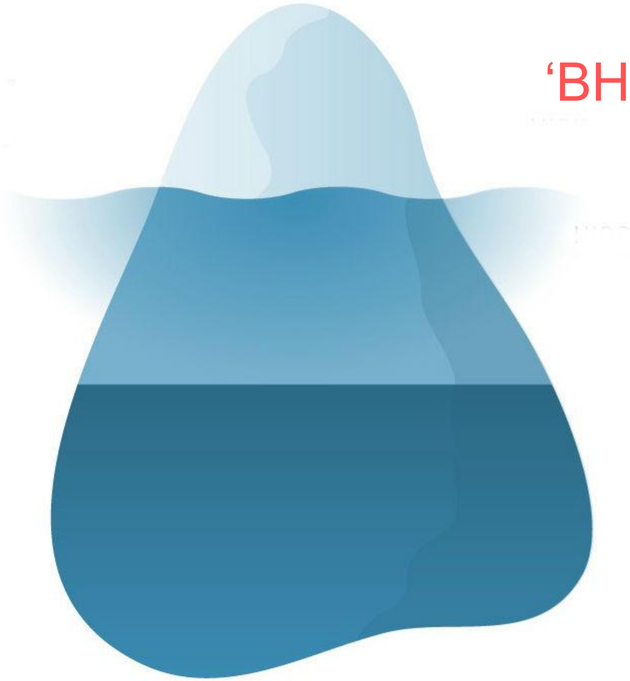
Sin Enterprise
(Gambling, Black Markets)

Legitimate Enterprise

The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships -
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808762

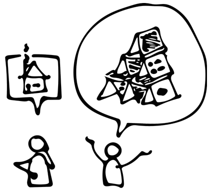
Module 1 - Blockchain, Bitcoin & Ethereum Basics

Understanding - Bhajan, Gita & Veda Level



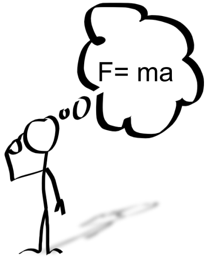
‘BHAJAN’ LEVEL

*‘Repeatable **Metaphors’***



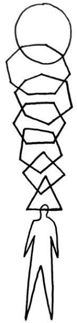
‘GITA’ LEVEL

*‘Simple Formula/ **Mental Models’***

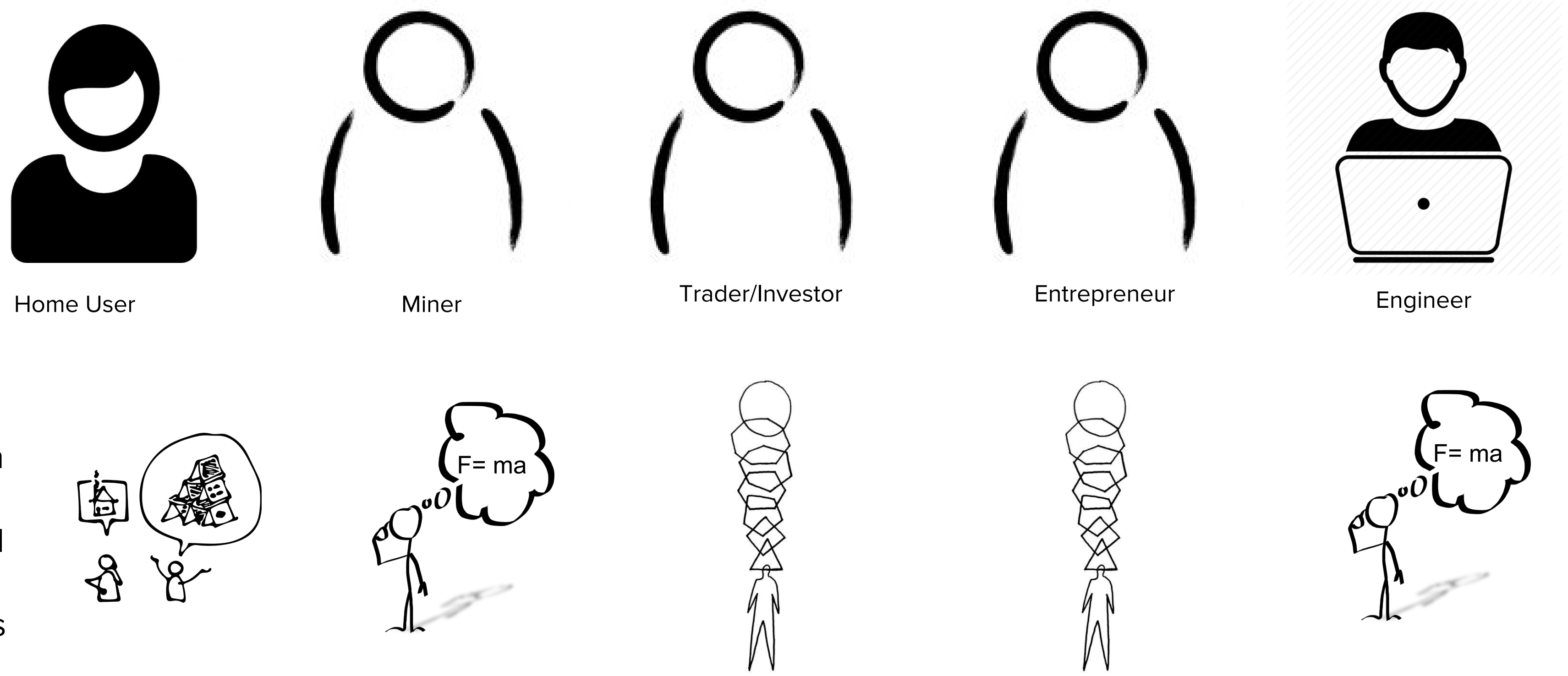


‘VEDA’ LEVEL

***‘First Principle** Thinking’*



Level of understanding per user type



Home User

Miner

Trader/Investor

Entrepreneur

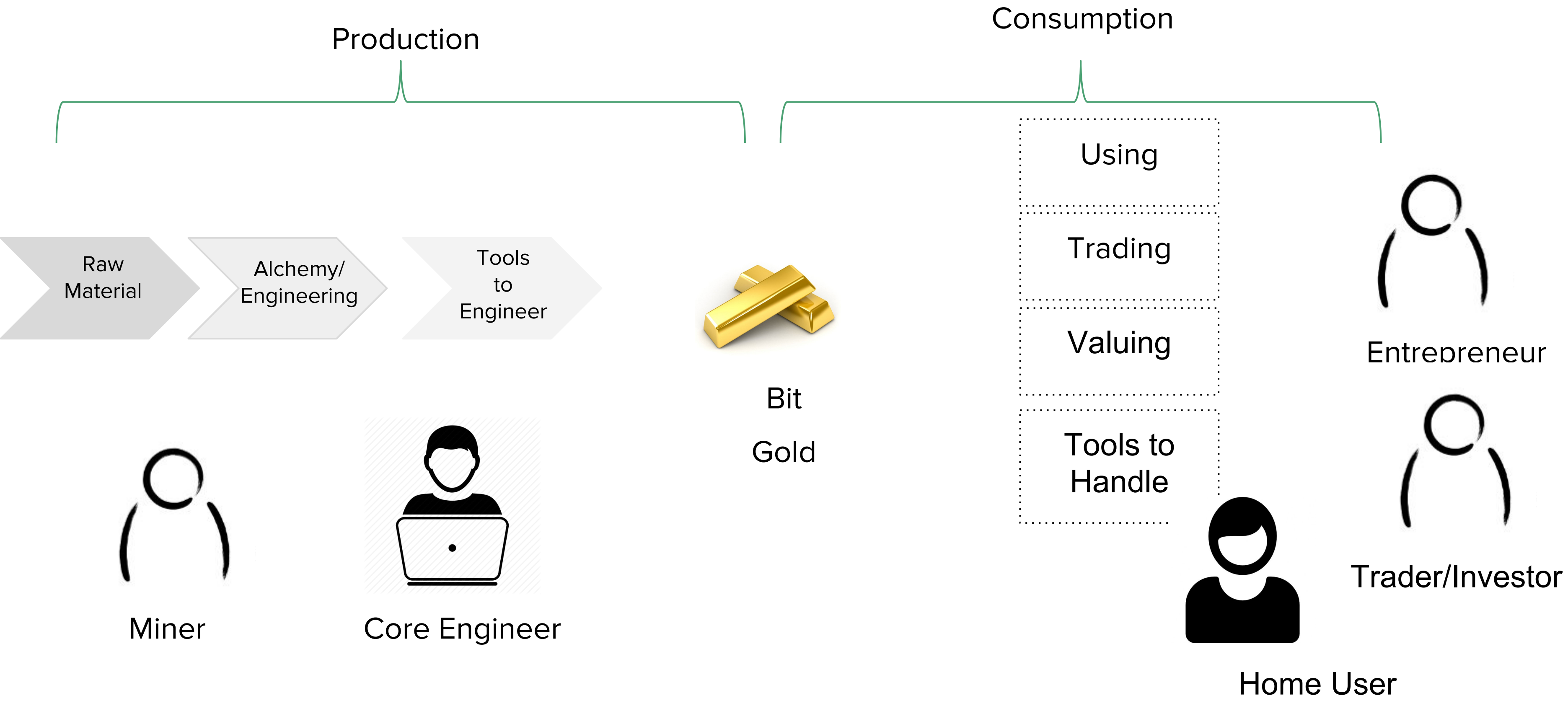
Engineer

Tech

Legal

Business

Position in Value Chain



Production

Raw Material

Alchemy/ Engineering

Tools to Engineer

Miner

Core Engineer

Bit

Gold

Consumption

Using

Trading

Valuing

Tools to Handle

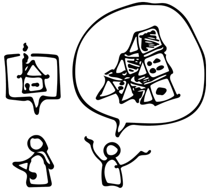
Entrepreneur

Trader/Investor

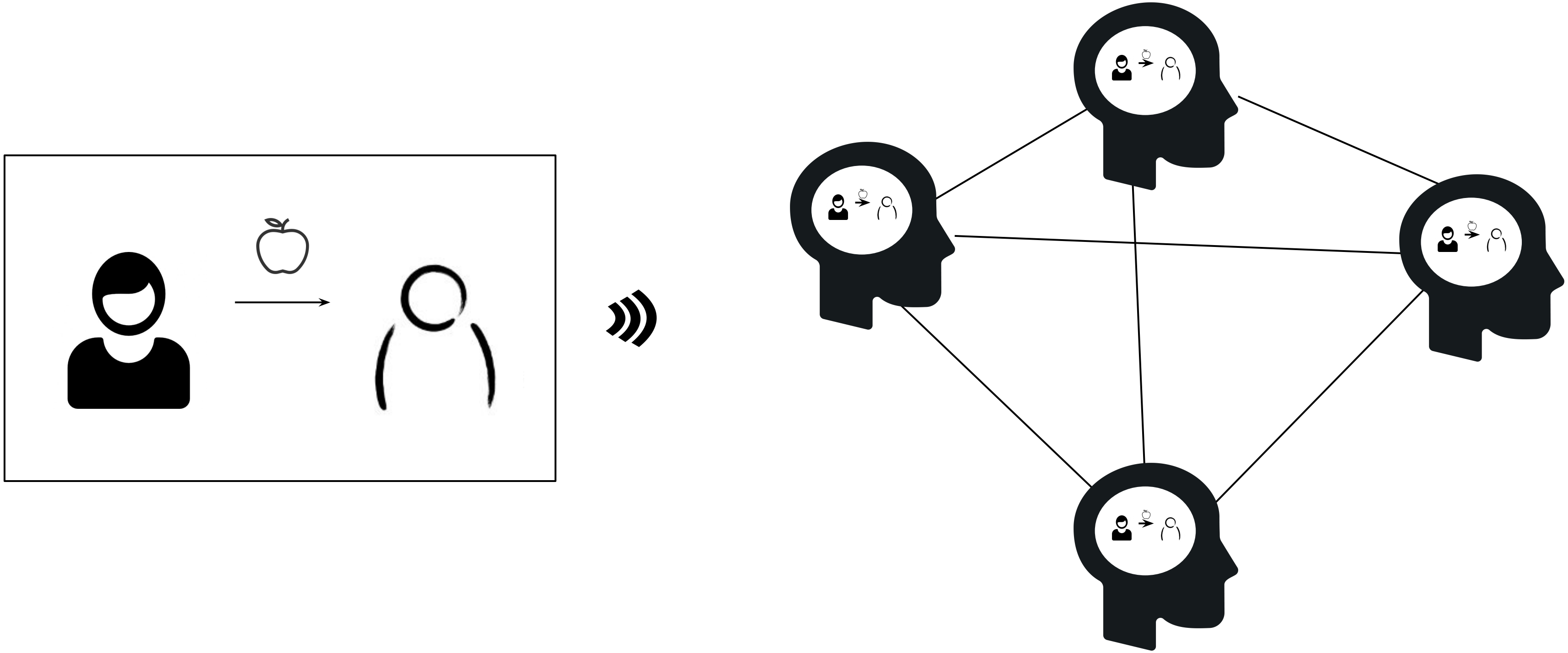
Home User

BLOCKCHAIN

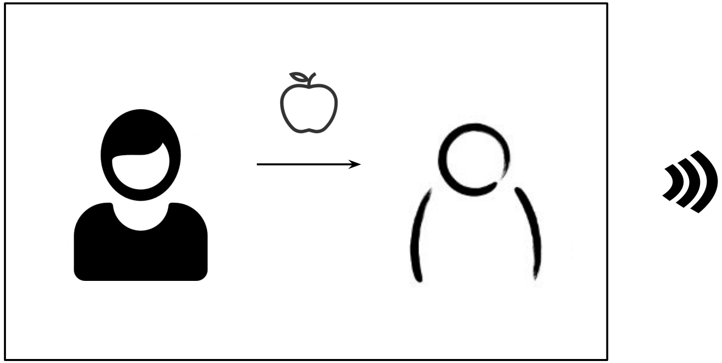
Home User

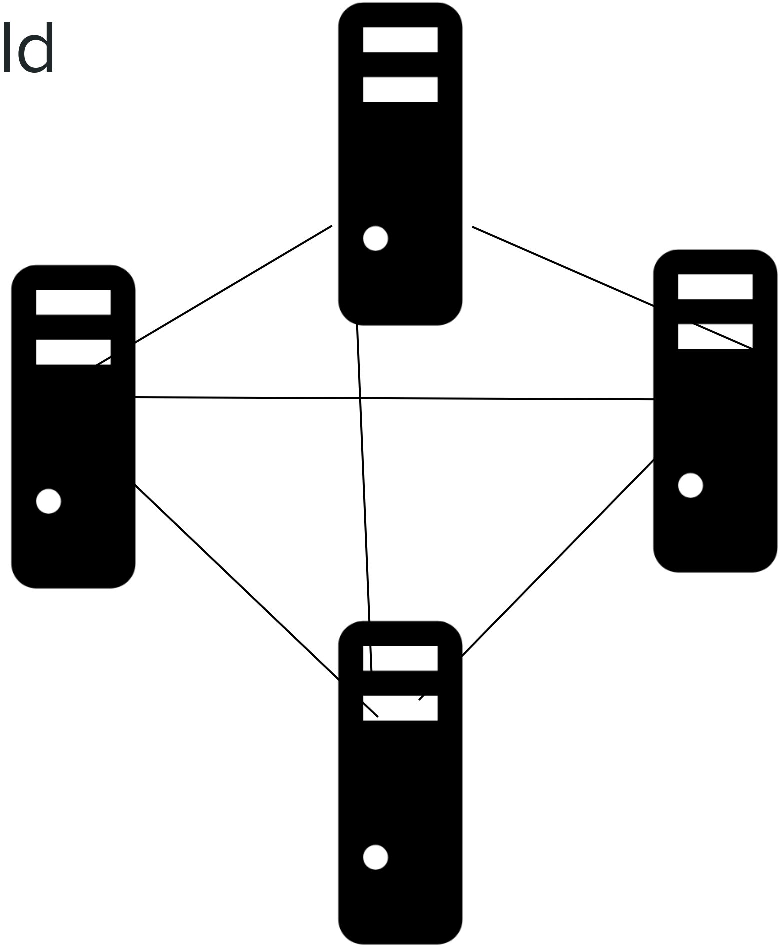


Transaction recorded

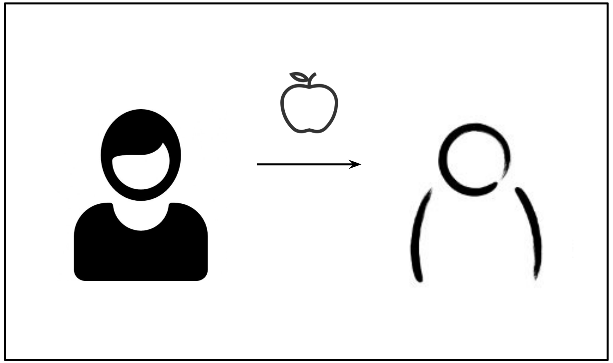


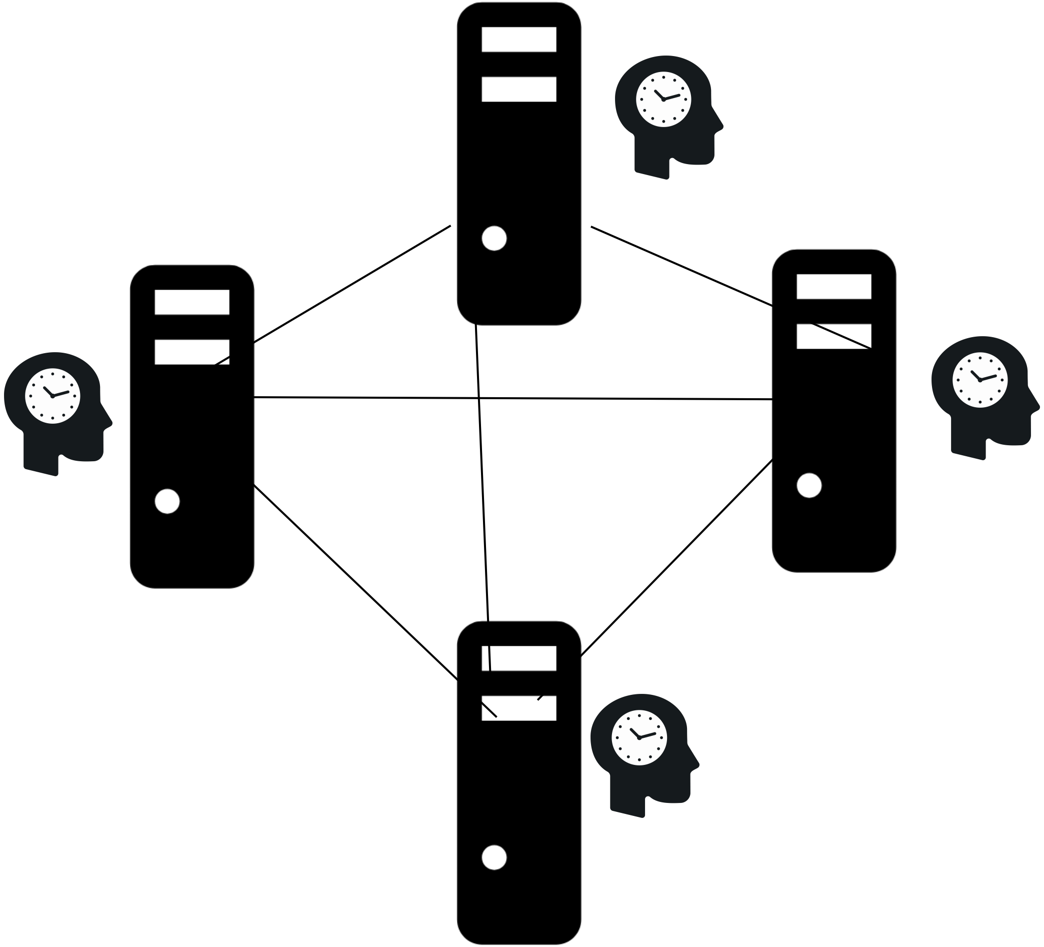
Distributed across the world





Never forgotten





Blockchain

bitcoin

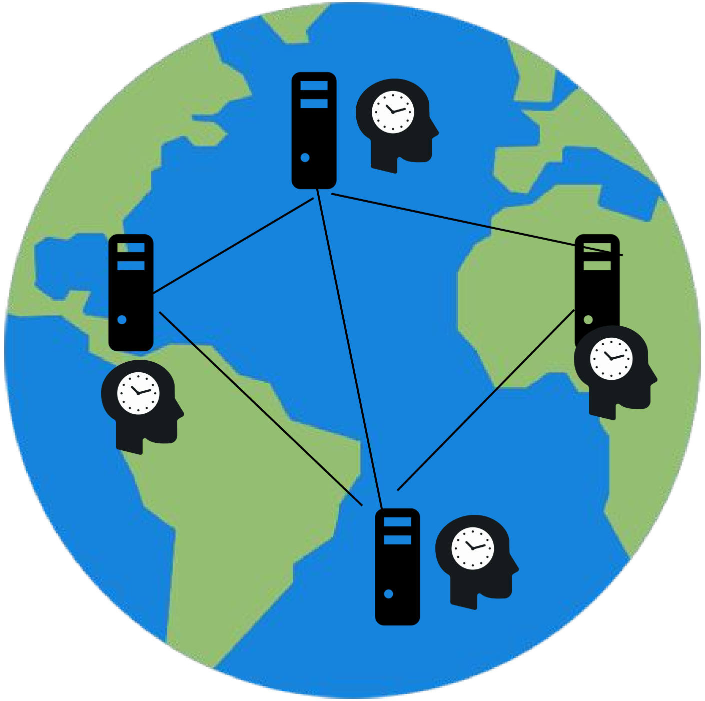
Cryptographically Secure

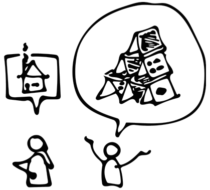
Unforgettable

Global — Linked to Internet

Database

Process storage





Bitcoin was the first blockchain

WIKILEAKS

SATOSHI NAKOMOTO

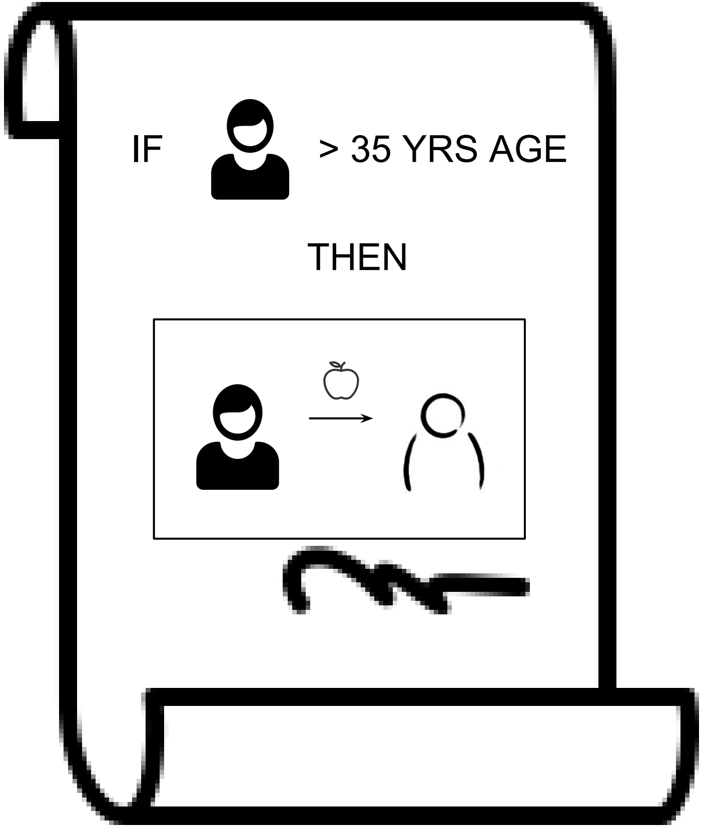
2008 CRISIS

MTGOX
SILK ROAD

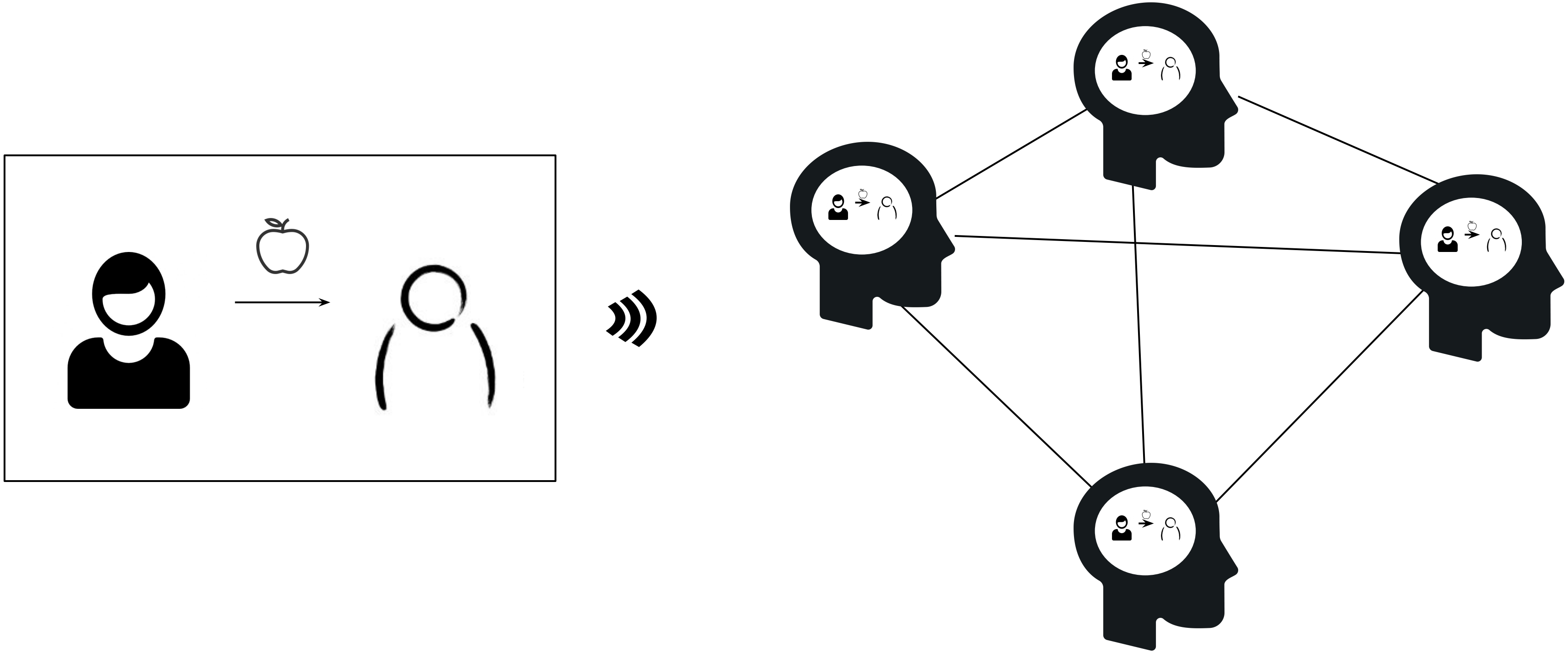
WHITEPAPER 2009

10000 BTC
PIZZA

Under a condition



Record the transaction



Blockchain

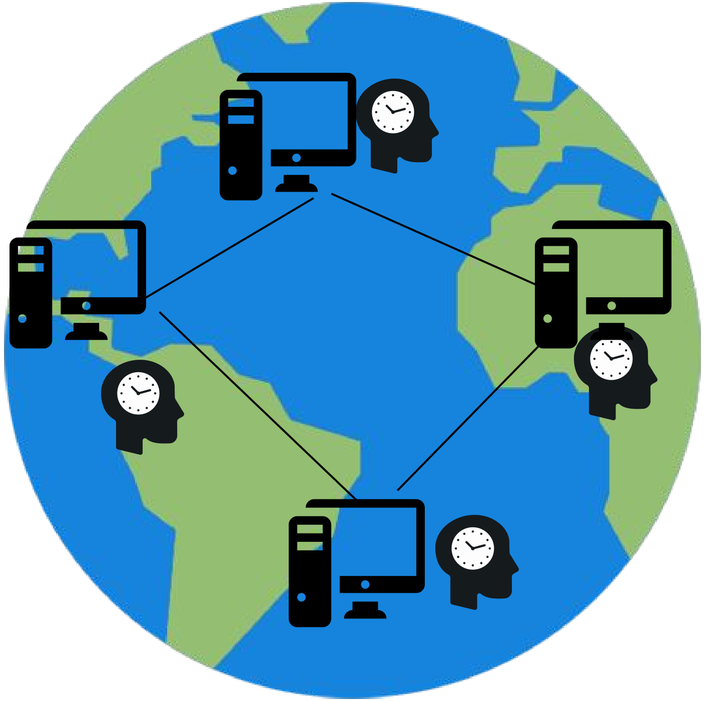
Cryptographically Secure

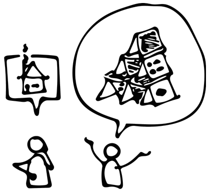
Unforgettable

Global — Linked to Internet

Computer

Process storage & code





A programmable type blockchain is ETHEREUM

VITALIK BUTERIN

MASTERCOIN

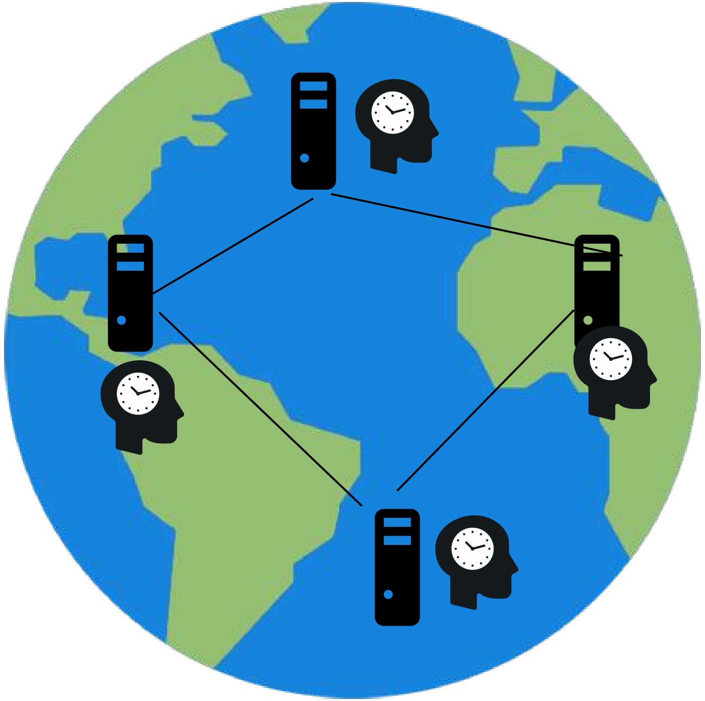
BETA RELEASE
2015

18M CROWDSALE

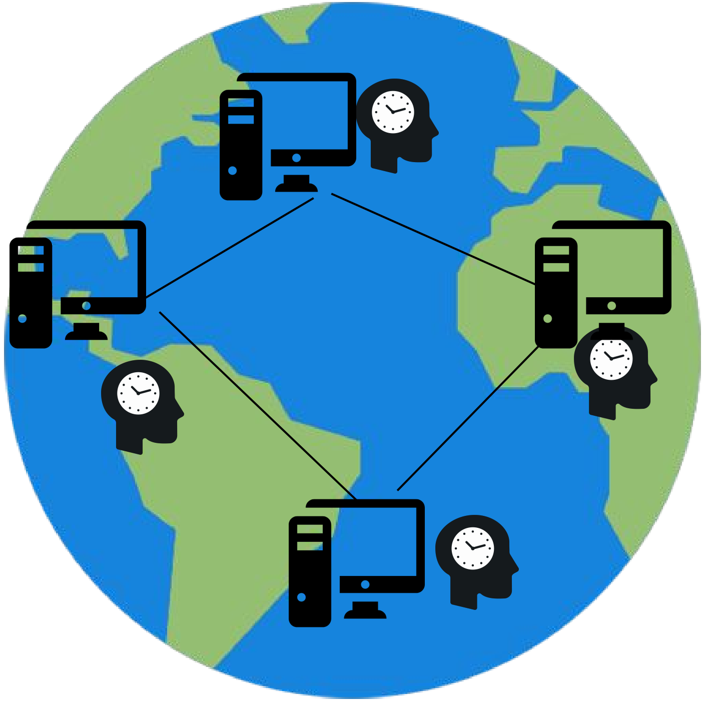
WHITEPAPER 2013

STABLE RELEASE
PI DAY

Bitcoin & Ethereum

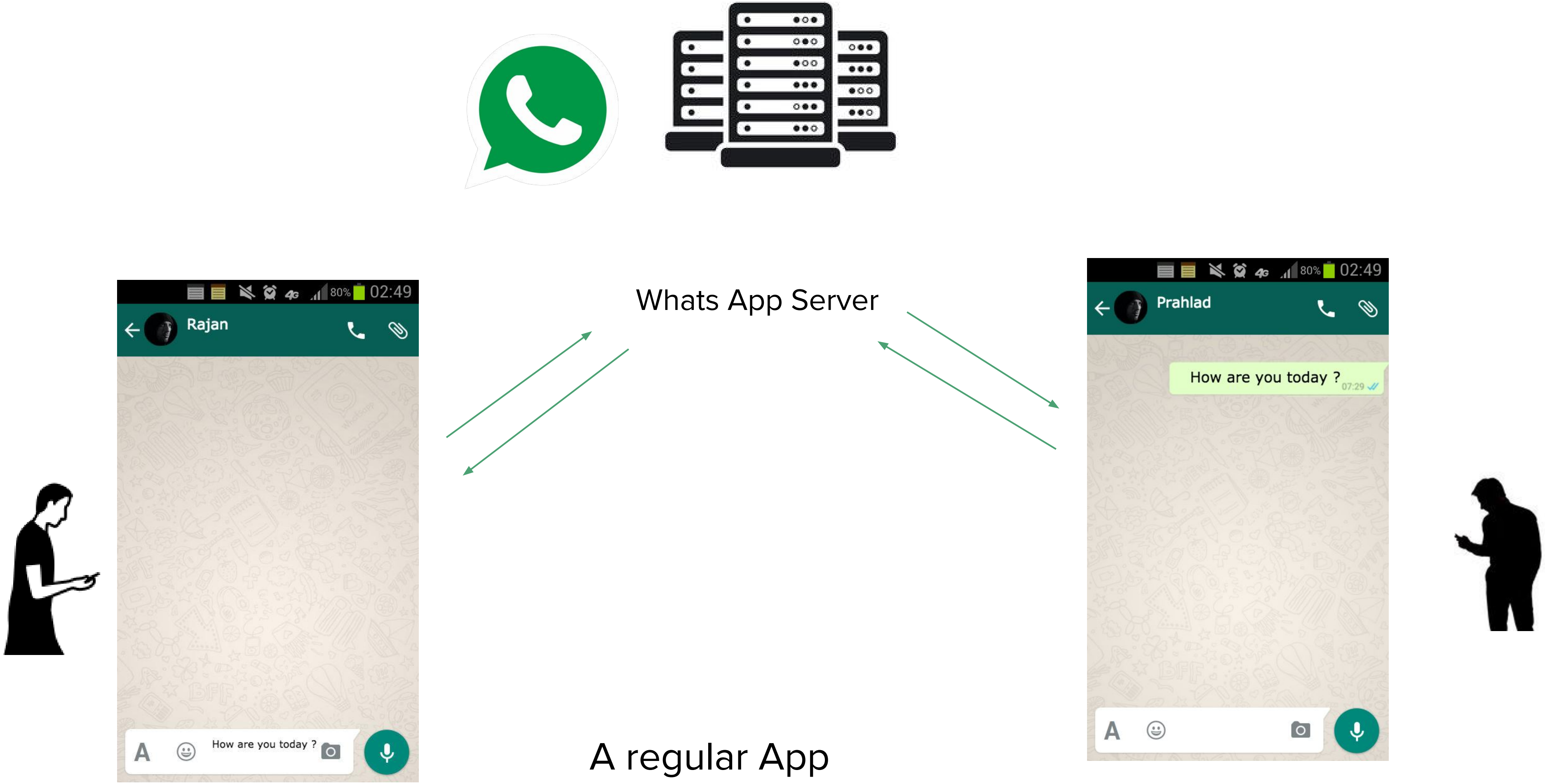


Unforgettable Global Database
(Bitcoin)



Unforgettable Global Computer
(Ethereum)

DApp

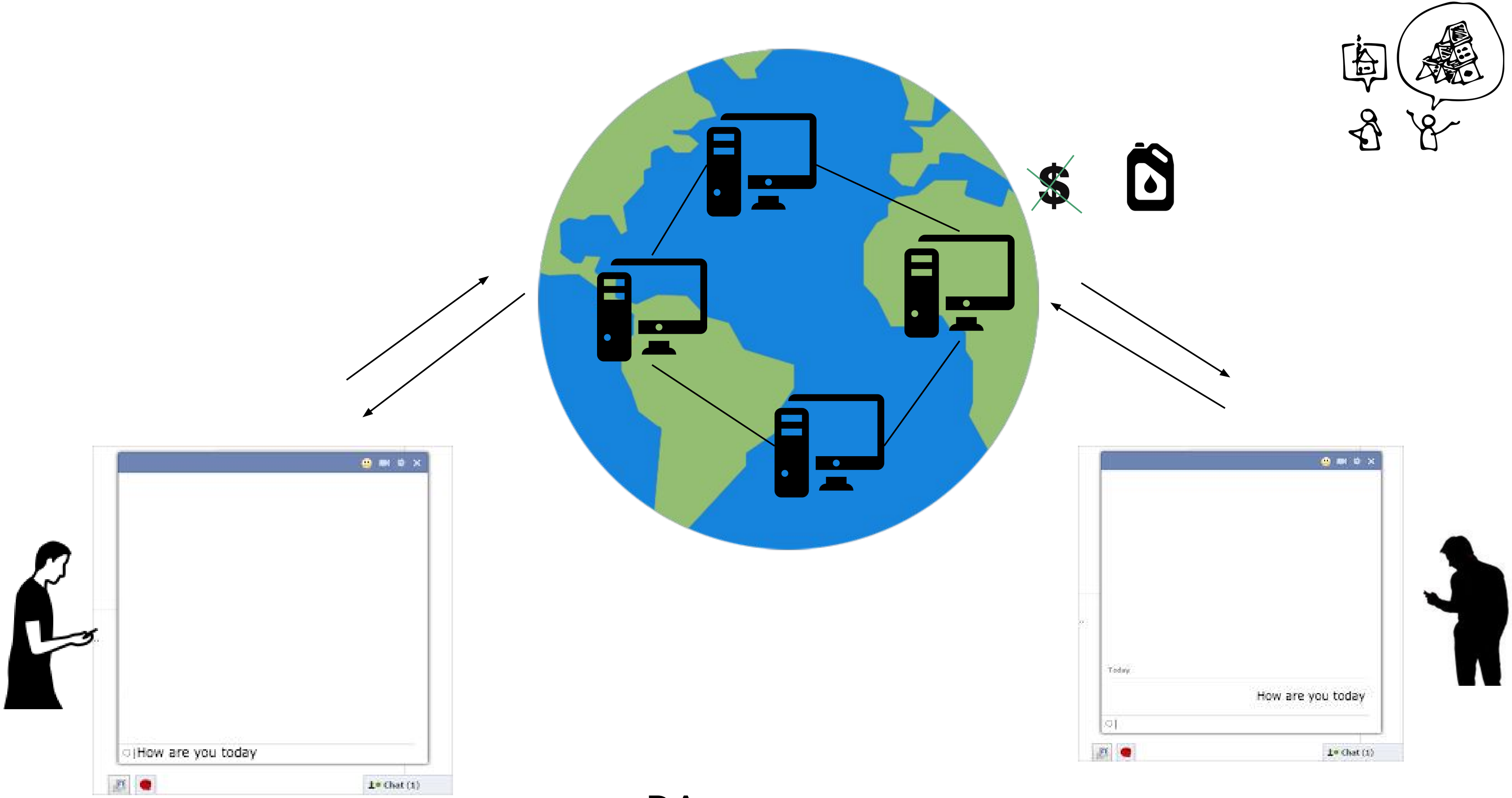


How are you today ?

How are you today ? 07:29

Whats App Server

A regular App



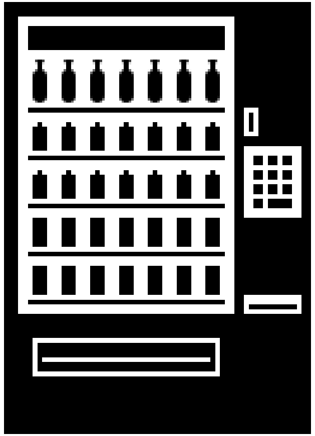
How are you today

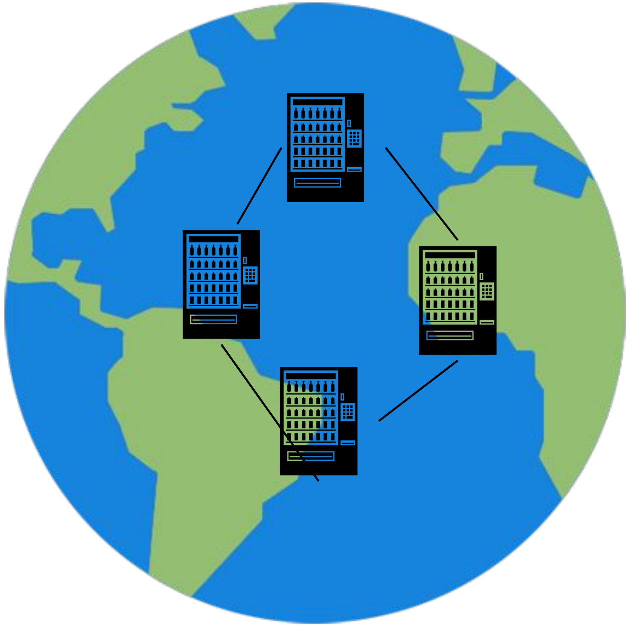
How are you today

DApp

Smart Contracts

A smart contract is like a vending machine





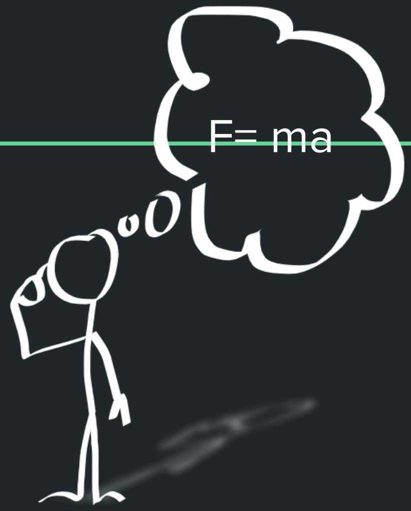
“If you put in $2.50, and press this button, you will get a Diet Coke.”

Website is to HTML, Smartcontract is to DApp

Many many more that use the blockchain concept

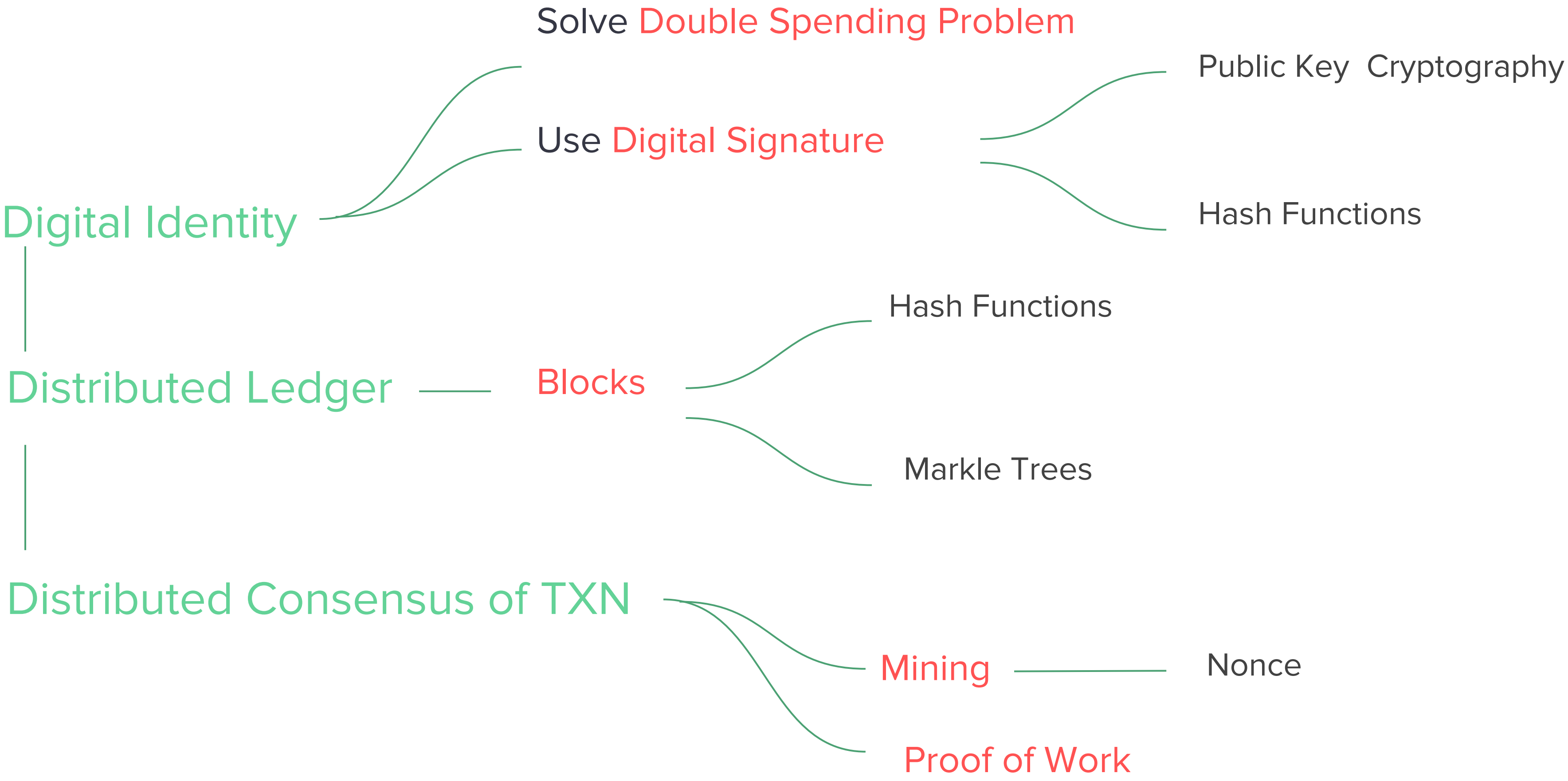
bitcoin
namecoin
litecoin
ripple
Đ
CASH
DASH
MONERO
ETHEREUM

Module 2 - Under the hood



Bitcoin is an alternate money system

Identification	Digital Identity
+	+
Ledger	Distributed Ledger
+	+
Consensus of TXN	Distributed Consensus of TXN
Money & Banking System	Cryptocurrency



Solve Double Spending Problem

Use Digital Signature

Public Key Cryptography

Hash Functions

Digital Identity

Hash Functions

Distributed Ledger

Blocks

Markle Trees

Distributed Consensus of TXN

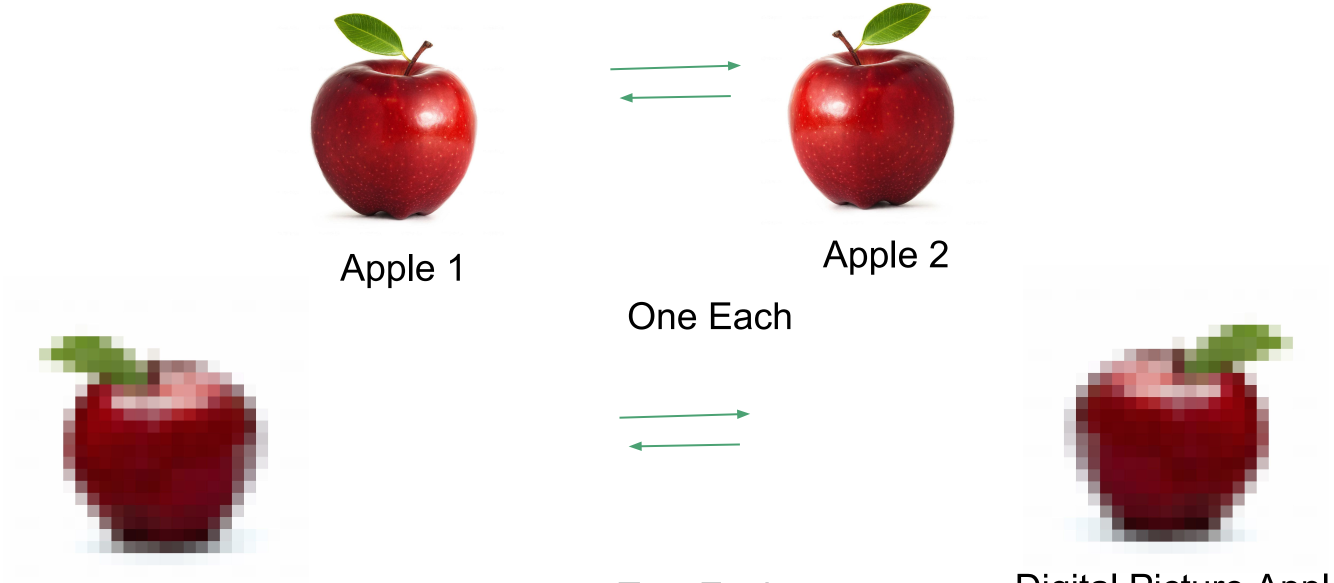
Mining

Nonce

Proof of Work

Digital Identity

Double spending problem



Apple 1

Apple 2

One Each

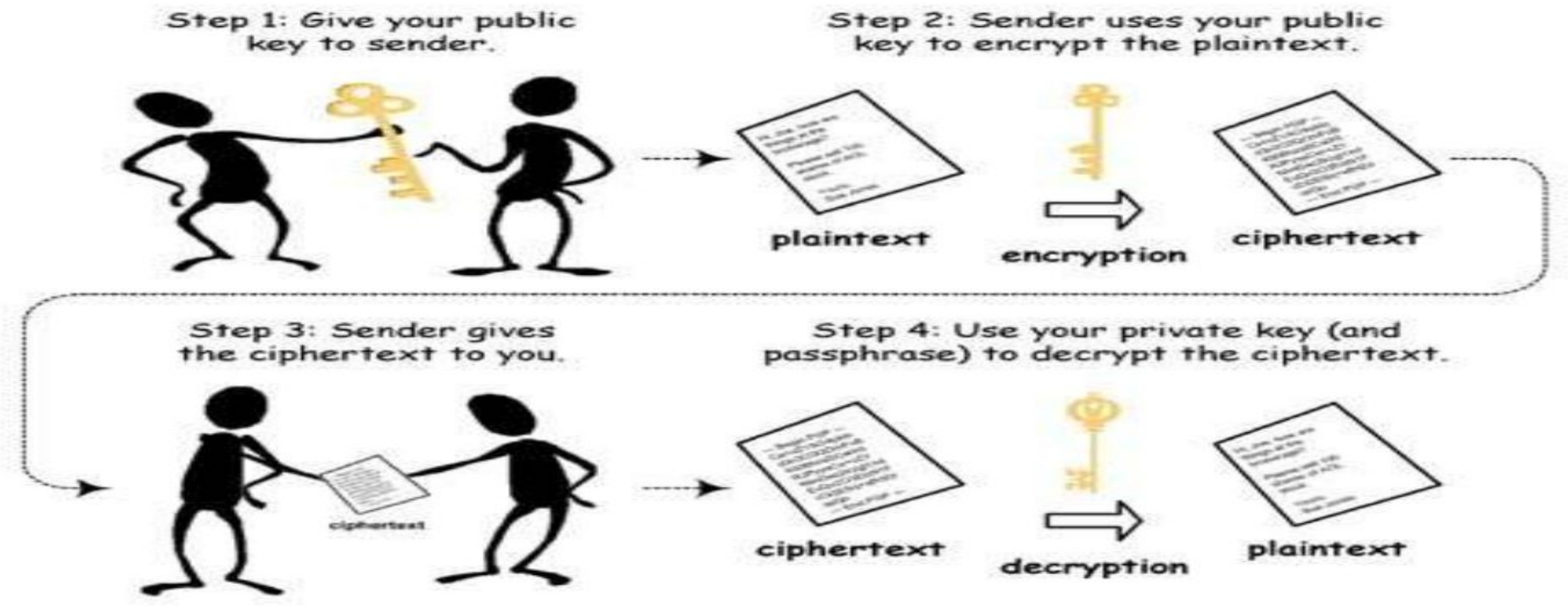
Digital Picture Apple 1

Two Each

Digital Picture Apple 2

A digital currency solution must solve double spending in addition to establishment of trust to be used widespread.

Public key cryptography used for establishing identity



Step 1: Give your public key to sender.

Step 2: Sender uses your public key to encrypt the plaintext.

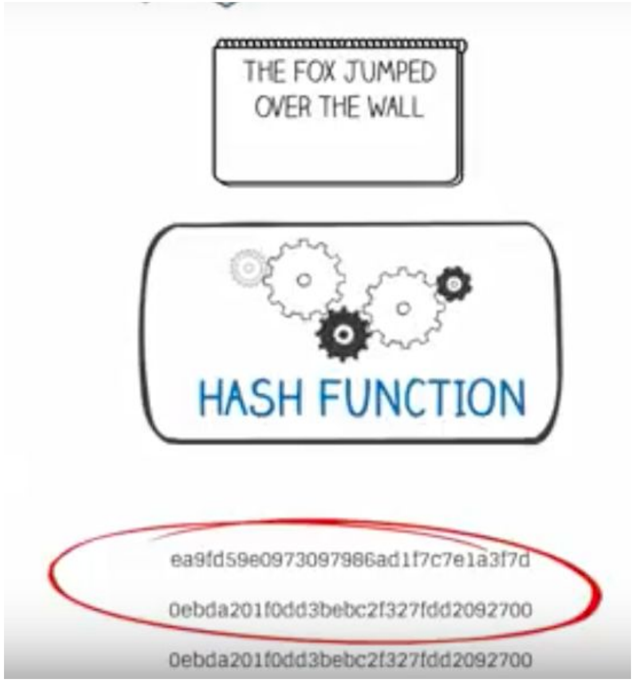
Step 3: Sender gives the ciphertext to you.

Step 4: Use your private key (and passphrase) to decrypt the ciphertext.

Example - RSA

Source - https://www.slideshare.net/sangavisankar/cryptography-25681251

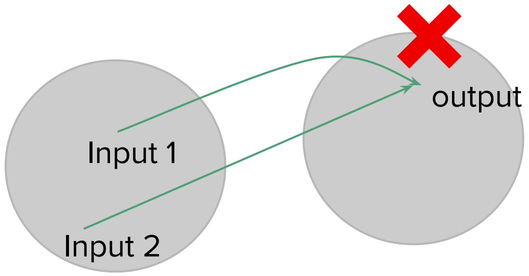
Hash function a process that create a fixed length output


THE FOX JUMPED
OVER THE WALL
HASH FUNCTION
ea9fd59e0973097986ad1f7c7e1a3f7d
0ebda201f0dd3bebc2f327fdd2092700
0ebda201f0dd3bebc2f327fdd2092700

Example SHA 256, MD5

https://www.youtube.com/watch?v=qZ9q5eVotm0

Important things about a Hash function

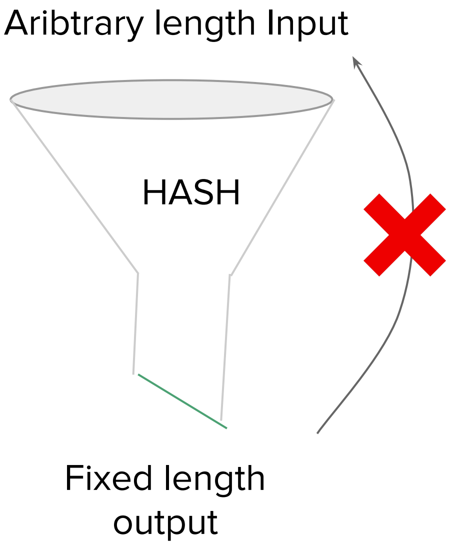


output

Input 1

Input 2

Collision Free

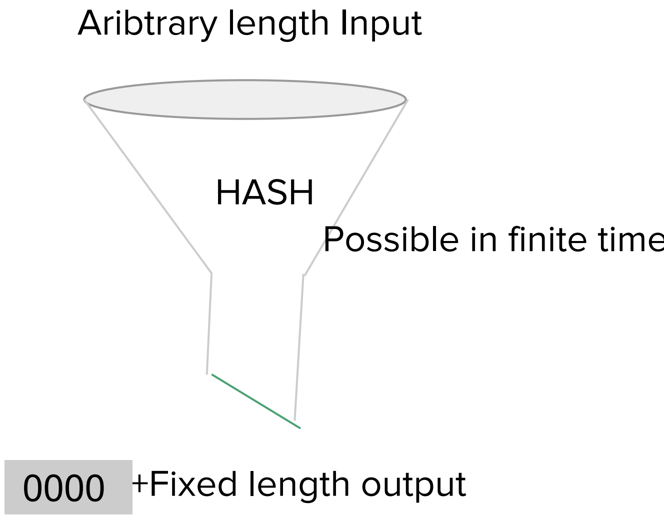


Aribtrary length Input

HASH

Fixed length output

HIding



Aribtrary length Input

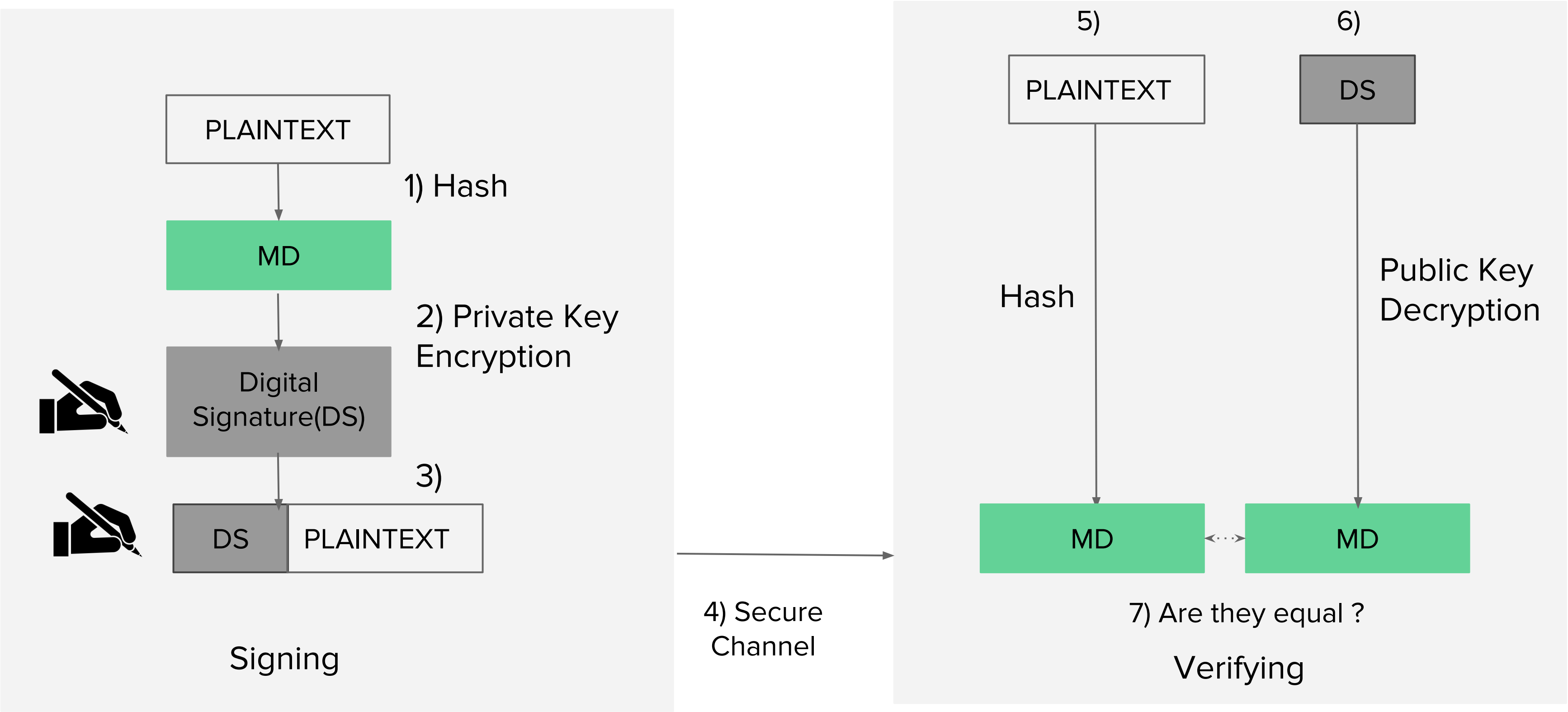
HASH

Possible in finite time

0000 +Fixed length output

Puzzle Friendliness

Digital Signature



PLAINTEXT

1) Hash

MD

2) Private Key Encryption

Digital Signature(DS)

3)

DS PLAINTEXT

Signing

4) Secure Channel

5)

PLAINTEXT

Hash

MD

6)

DS

Public Key Decryption

MD

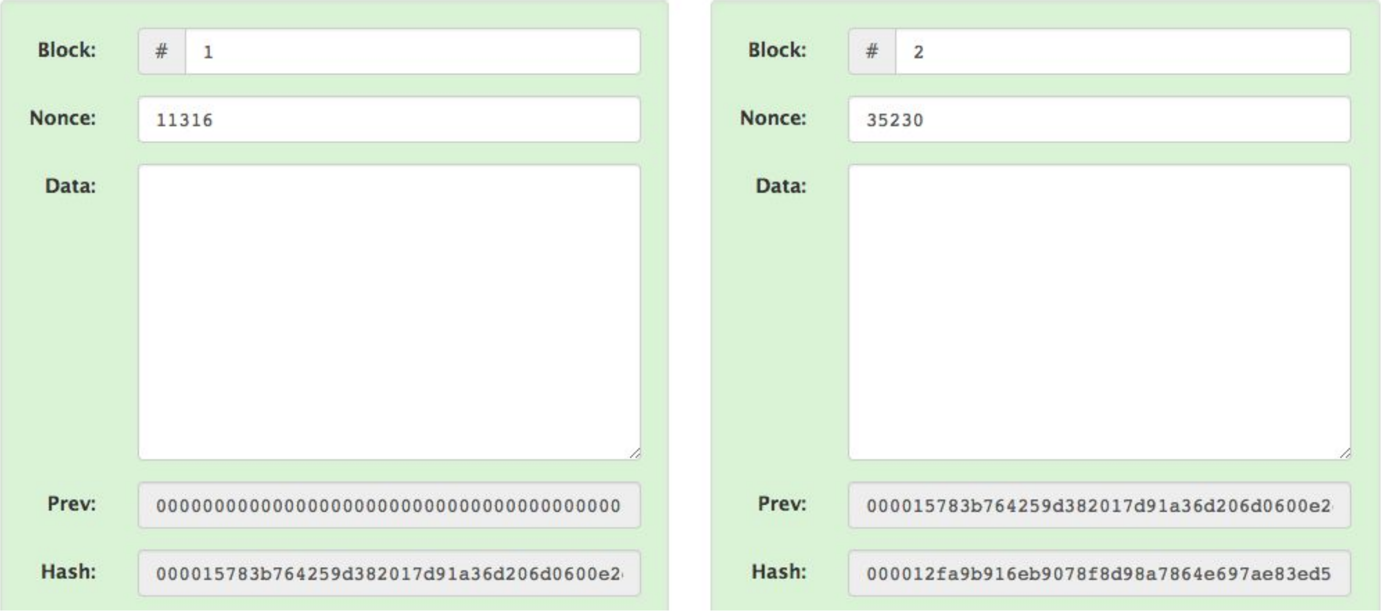
7) Are they equal ?

Verifying

Distributed Ledger

Blocks & Nonce

https://anders.com/blockchain/block.html



Block: # 1

Nonce: 11316

Data:

Prev: 0000000000000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d206d0600e2

Block: # 2

Nonce: 35230

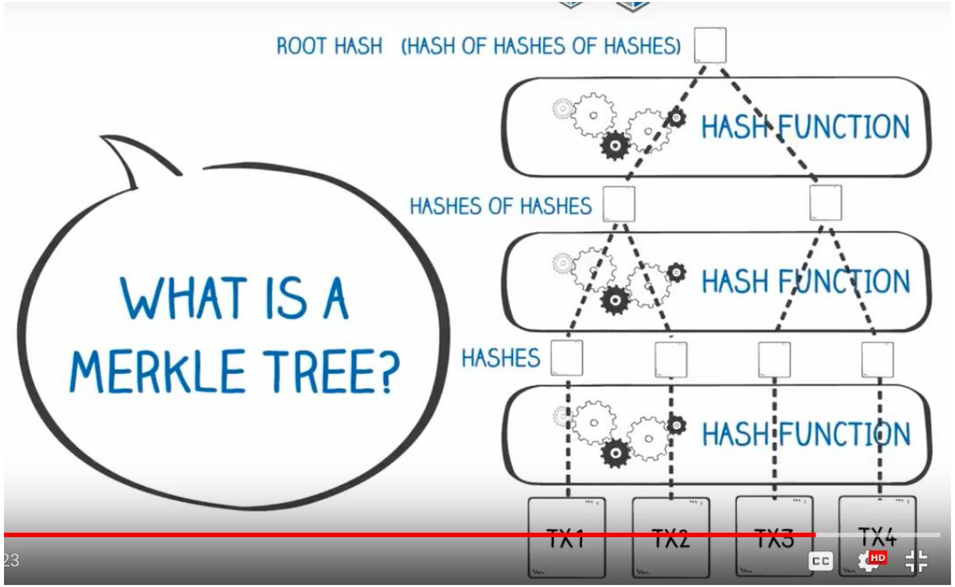
Data:

Prev: 000015783b764259d382017d91a36d206d0600e2

Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed5

https://www.youtube.com/watch?v=_160oMzblY8

Merkle Trees



https://youtu.be/lik9aaFIsl4?t=1m59s

Distributed Consensus

Proof of Work

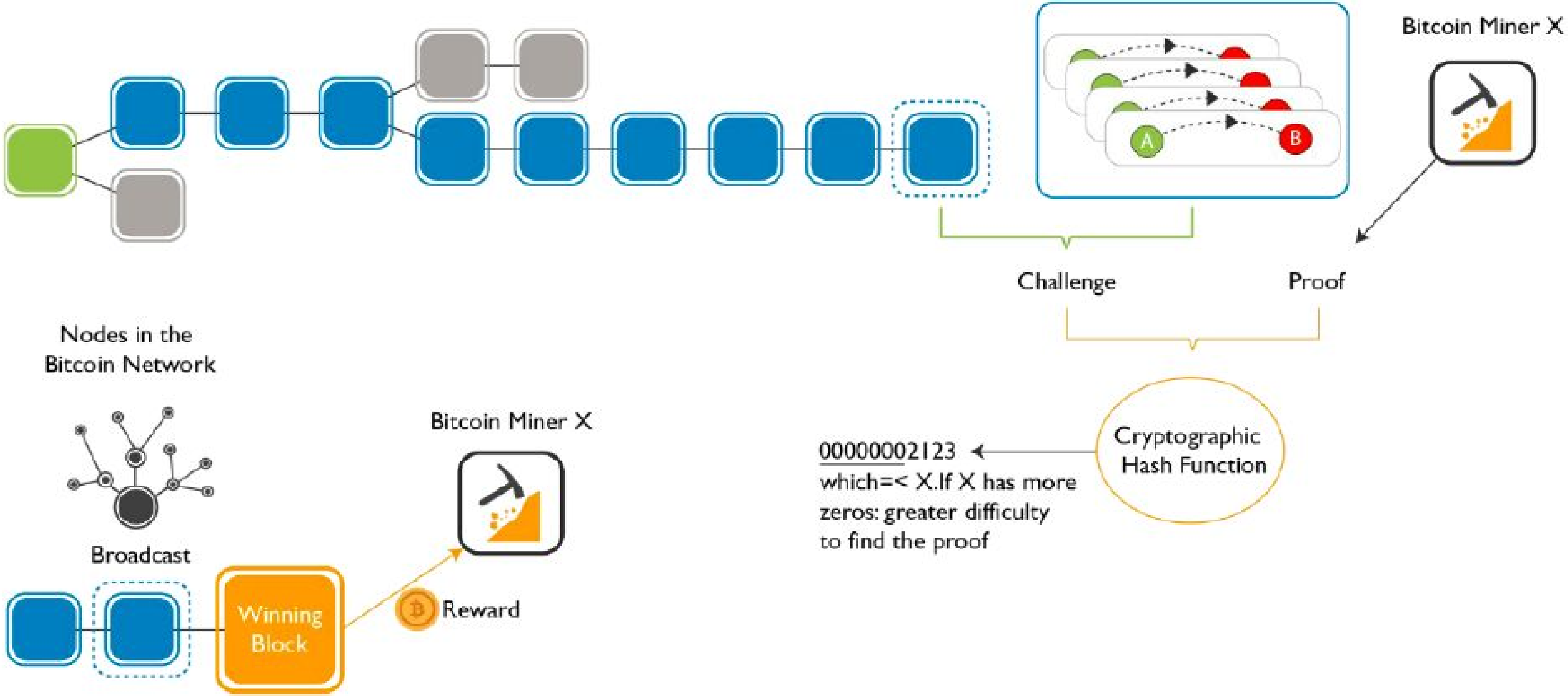
? + = 8

A guessing game

https://www.youtube.com/watch?v=fxjqKXCxWzk

Another - https://www.youtube.com/watch?v=jXni0KDQNsc

Proof of Work in Blockchain


Bitcoin Miner X
A
B
Challenge
Proof
Nodes in the Bitcoin Network
Bitcoin Miner X
Cryptographic Hash Function
00000002123 which=< X.If X has more zeros: greater difficulty to find the proof
Broadcast
Winning Block
Reward

Bitcoin Mining

https://www.youtube.com/watch?v=TD09UhjleK8

Putting it all together, Bitcoin in 5 mins

https://www.youtube.com/watch?v=l9jOJk30eQs&t=65s

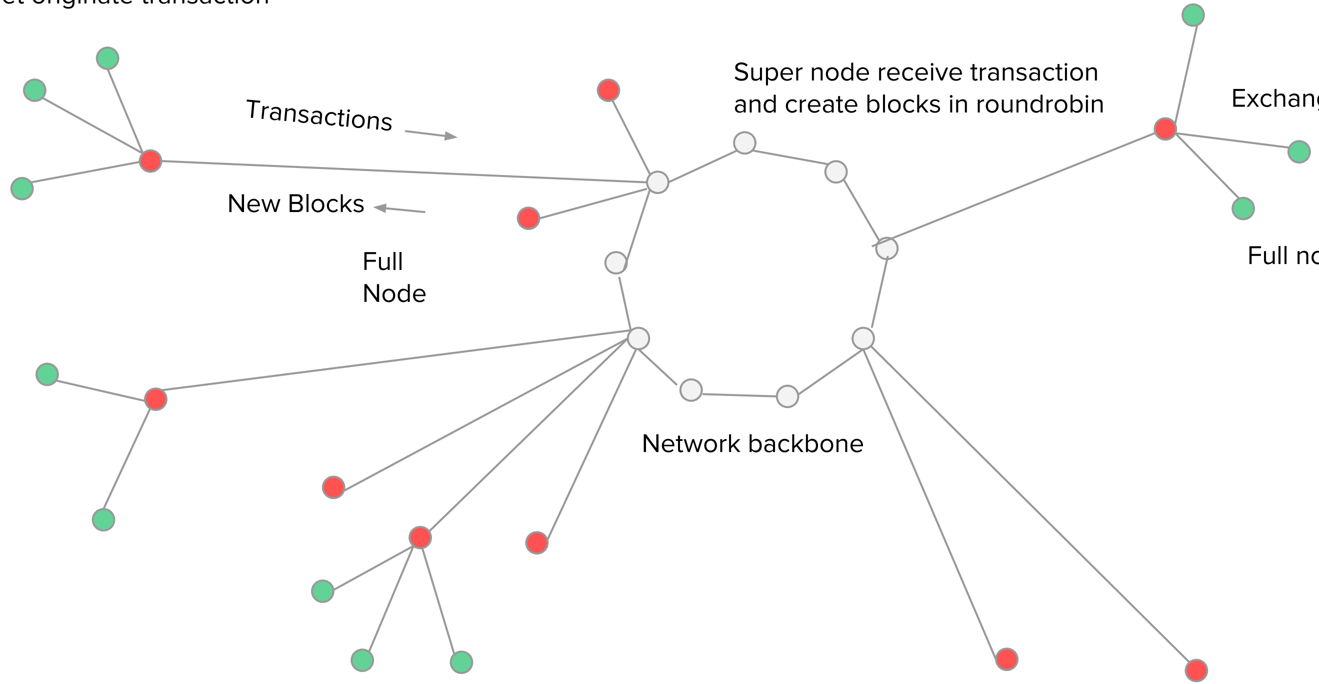
More In depth, Bitcoin in 22 mins

https://www.youtube.com/watch?v=Lx9zgZCMqXE&t=956s

Exercise 1

- Visit Blockchain.info
- Dissect transaction on blockchain
- Understand what a transaction composes of
- Visit bitaddress.org to generate a bitcoin address
- Understand the relation between public, private key and bitcoin address

Bitcoin node in the network is client running bitcoin software



Payment Processor

Wallet originate transaction

Transactions

New Blocks

Full
Node

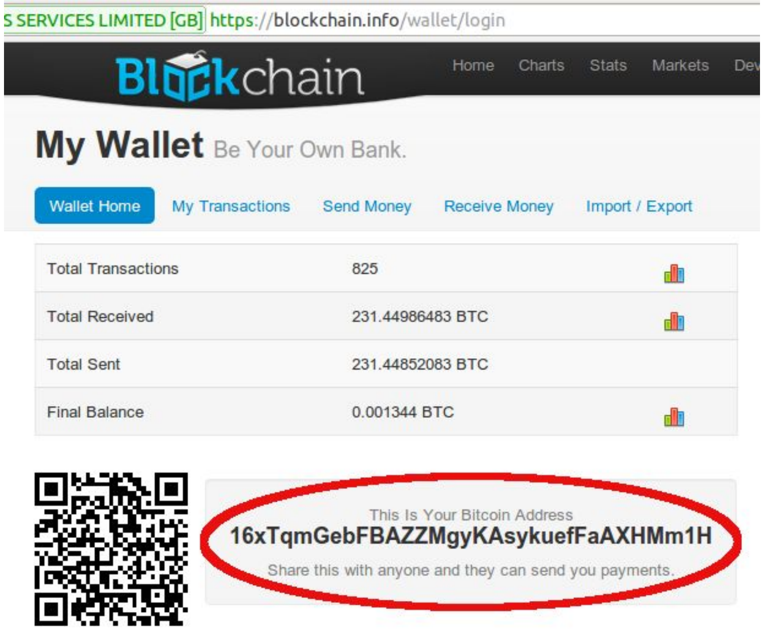
Super node receive transaction
and create blocks in roundrobin

Exchange

Full node

Network backbone

Bitcoin Address - an entity that can own bitcoin, generated through private key

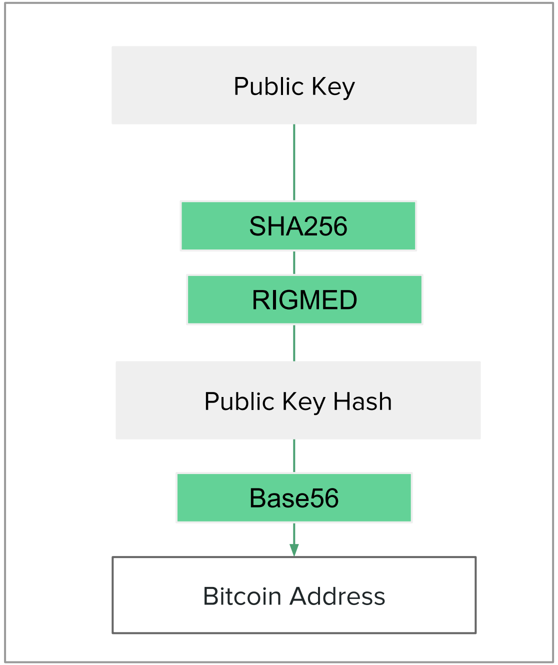


S SERVICES LIMITED [GB] https://blockchain.info/wallet/login

My Wallet Be Your Own Bank.

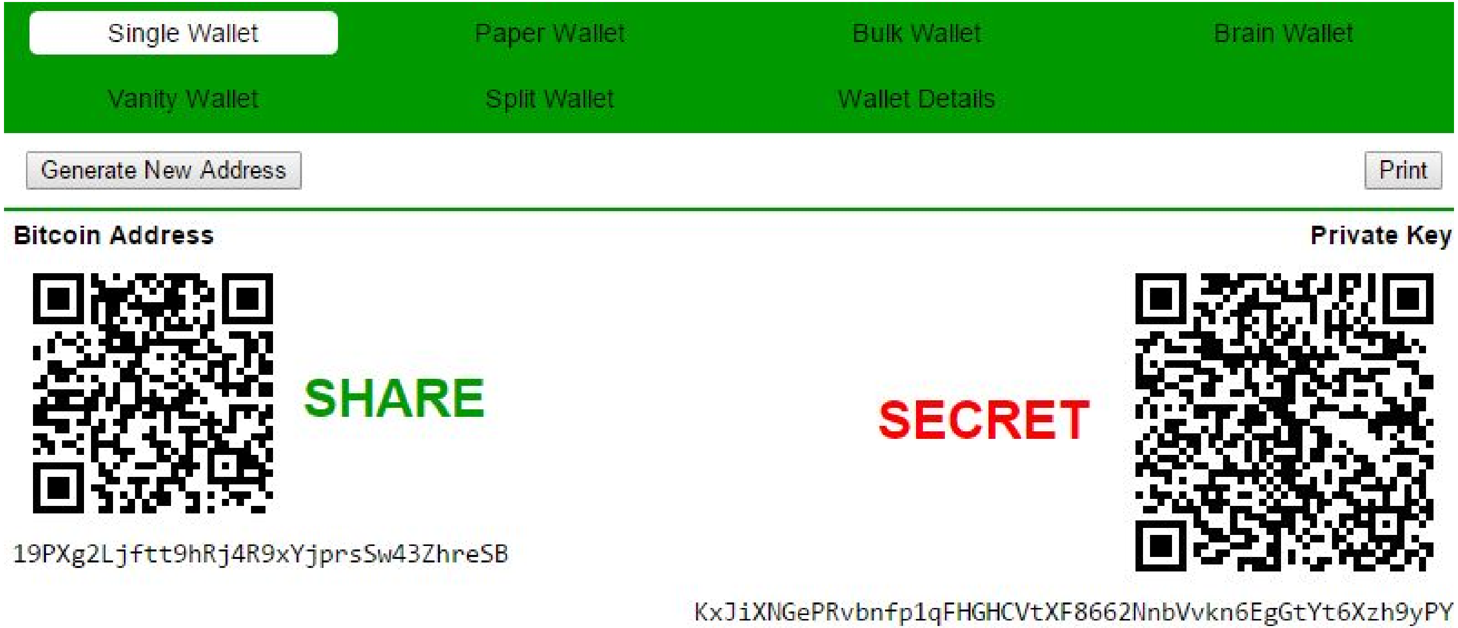
Total Transactions	825
Total Received	231.44986483 BTC
Total Sent	231.44852083 BTC
Final Balance	0.001344 BTC

This Is Your Bitcoin Address
16xTqmGebFBAZZMgyKAsykuefFaAXHMm1H
Share this with anyone and they can send you payments.



BItcoin Wallet

A Bitcoin wallet is as simple as a single pairing of a Bitcoin address with its corresponding Bitcoin private key



Bitcoin Address

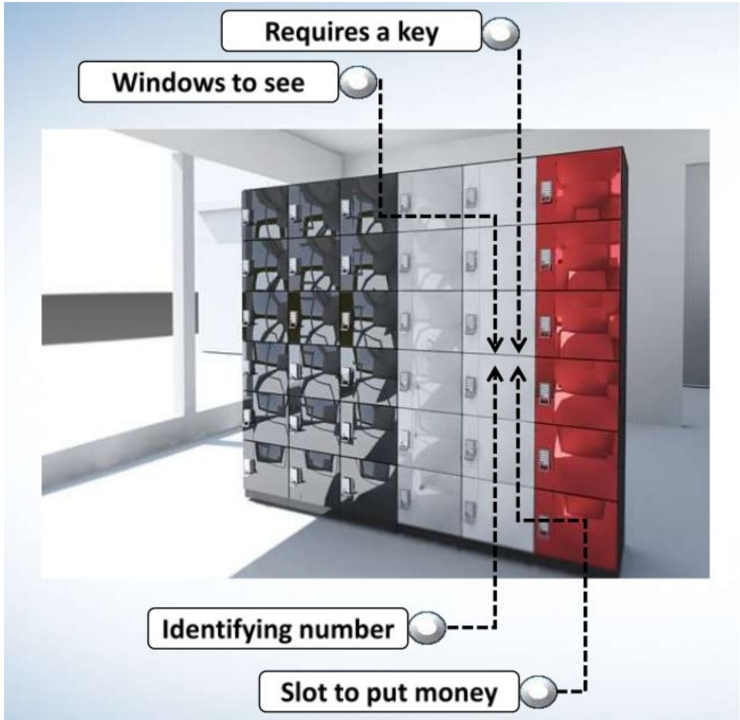
19PXg2Ljftt9hRj4R9xYjprsSw43ZhreSB

Private Key

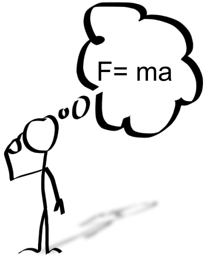
KxJiXNGePRvbnfp1qFHGHCVtXF8662NnbVvkn6EgGtYt6Xzh9yPY

Discussion

Blockchain



- Group of lockers in a public space
- Has a window that anyone can view
- Public key to put money
- Uses a wallet to keep track of all locker key



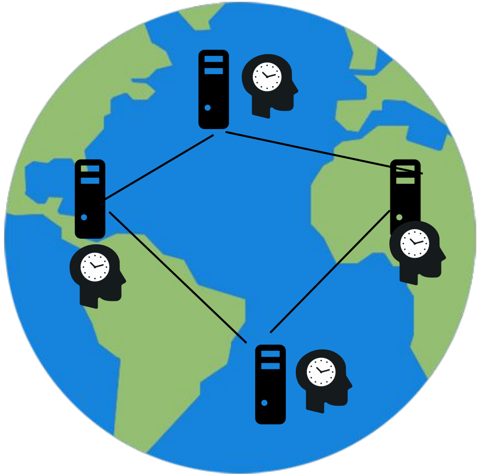
Source - https://www.slideshare.net/opusconsulting/blockchain-technology-a-primer

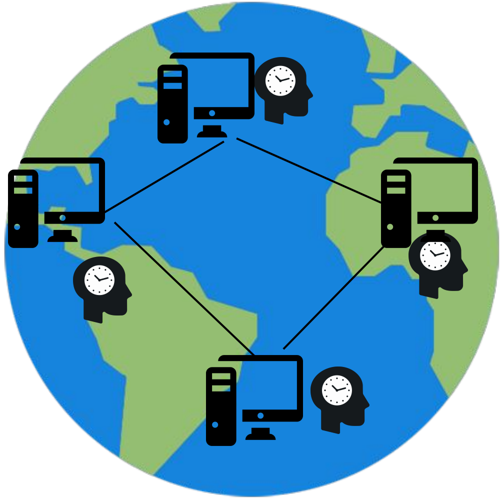
Bitcoin - Technical definition

Bitcoin combines the idea of using computational puzzles to regulate the creation of new currency units with the idea of secure timestamping to record a ledger of transactions and prevent double spending

Ethereum

From distributed database to distributed computer





Bitcoin

Ethereum

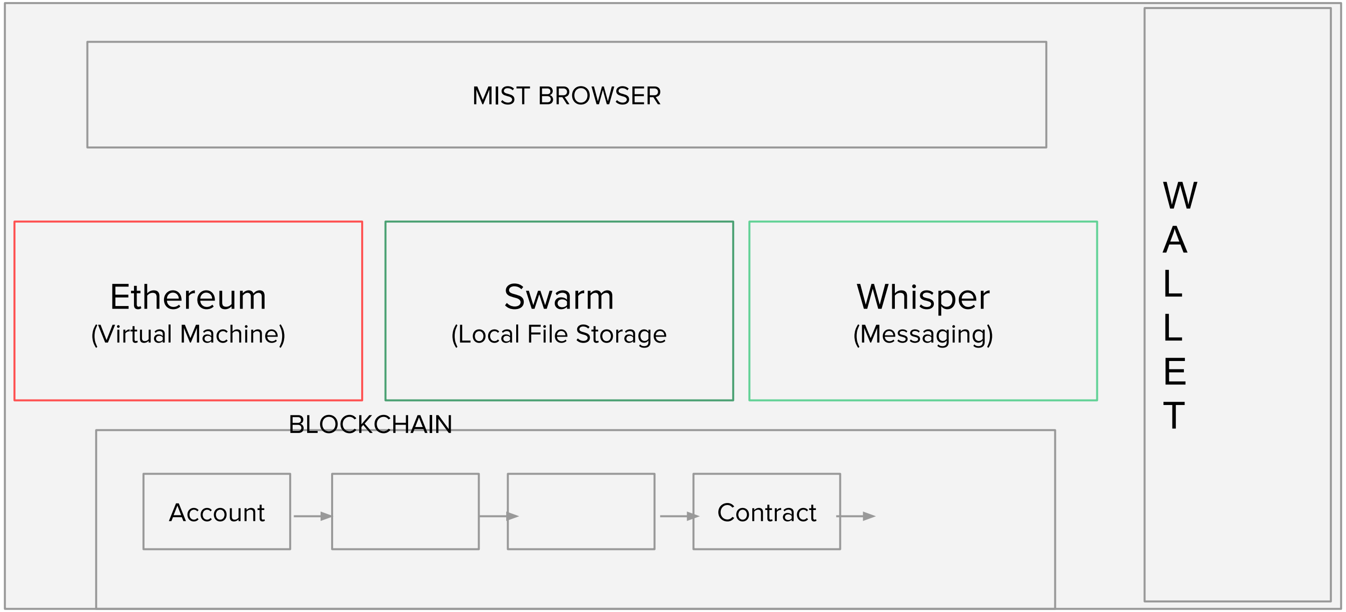
Other significant changes from Bitcoin

- Two node type - Account & Contract
- Rent for using blockchain - Gas
  - Transaction originator pays
- Is it a turing complete machine
- Name of the currency is Ether
- Different hashing algorithm (Ethash)
- Network of Networks

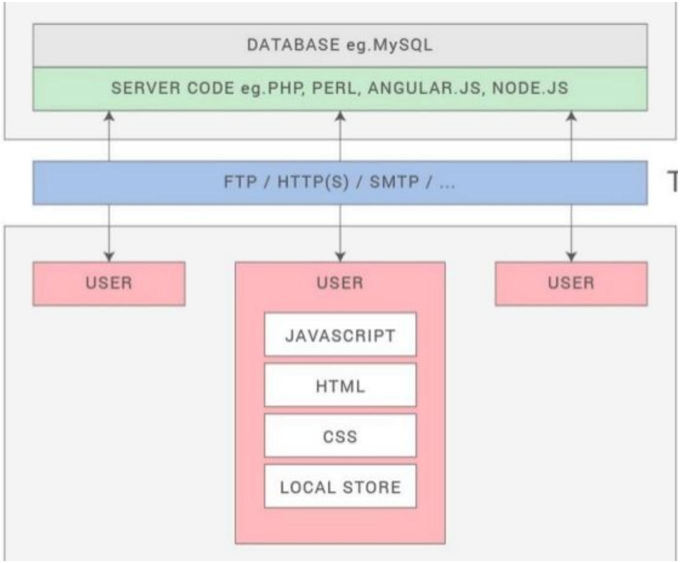
Exercise 2 Ethereum

- Download Ethereum Client (& MIST Browser)
- Create an account My Ether Wallet

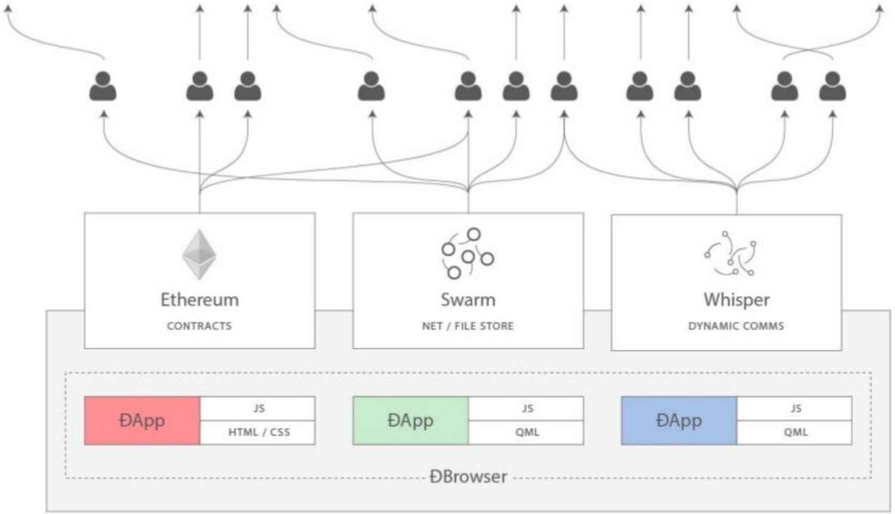
Ethereum client is a node in the blockchain



Client Server Apps vs DApps

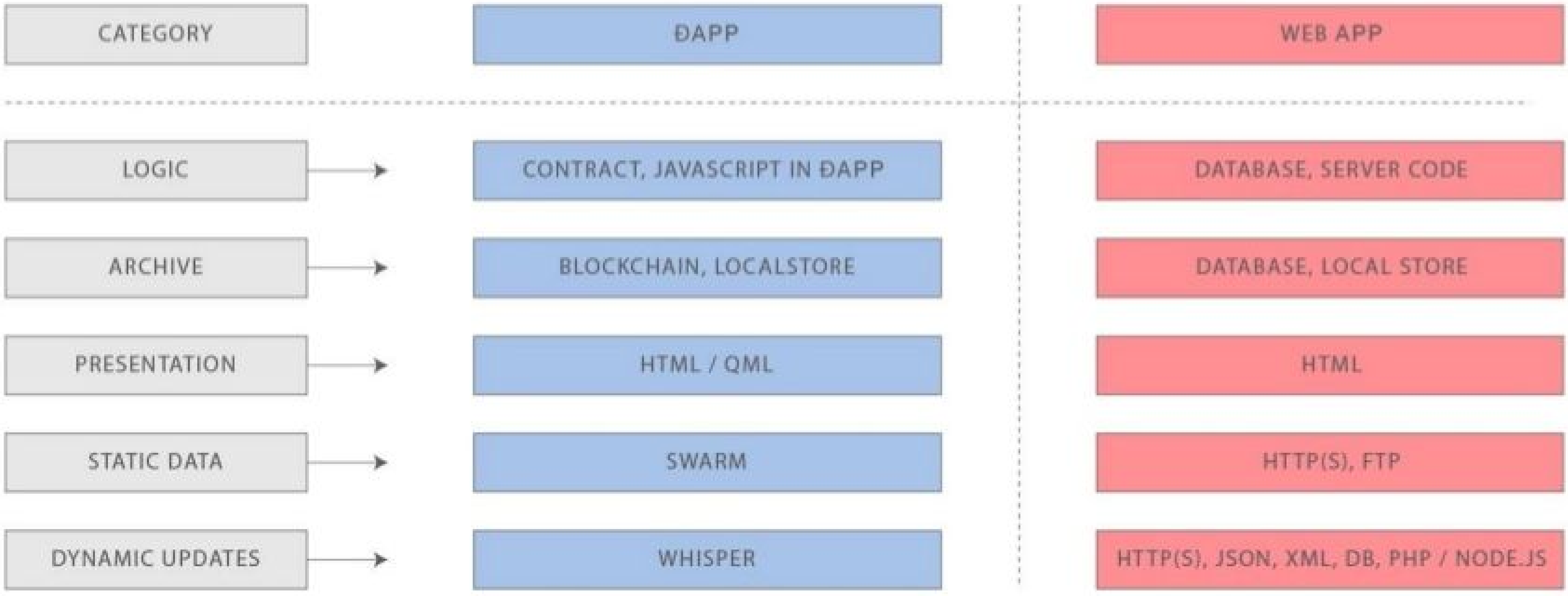

DATABASE eg.MySQL
SERVER CODE eg.PHP, PERL, ANGULAR.JS, NODE.JS
FTP / HTTP(S) / SMTP / ...
USER
USER
USER
JAVASCRIPT
HTML
CSS
LOCAL STORE

Web 2.0



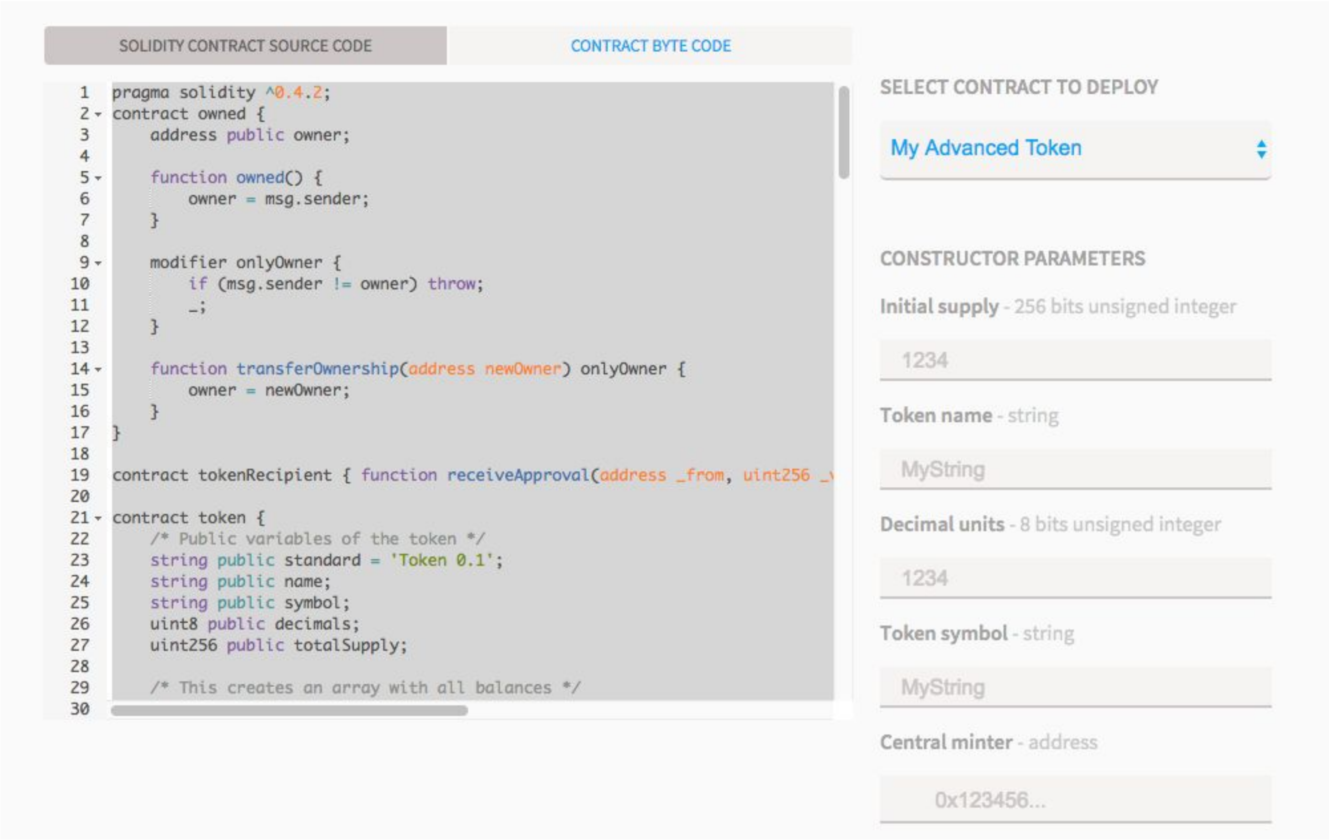
Web 3.0

Web without any server



CATEGORY	ĐAPP	WEB APP
LOGIC	CONTRACT, JAVASCRIPT IN ĐAPP	DATABASE, SERVER CODE
ARCHIVE	BLOCKCHAIN, LOCALSTORE	DATABASE, LOCAL STORE
PRESENTATION	HTML / QML	HTML
STATIC DATA	SWARM	HTTP(S), FTP
DYNAMIC UPDATES	WHISPER	HTTP(S), JSON, XML, DB, PHP / NODE.JS

Solidity & Token - Quick Intro



```
pragma solidity ^0.4.2;
contract owned {
    address public owner;

    function owned() {
        owner = msg.sender;
    }

    modifier onlyOwner {
        if (msg.sender != owner) throw;
        _;
    }

    function transferOwnership(address newOwner) onlyOwner {
        owner = newOwner;
    }
}

contract tokenRecipient { function receiveApproval(address _from, uint256 _

contract token {
    /* Public variables of the token */
    string public standard = 'Token 0.1';
    string public name;
    string public symbol;
    uint8 public decimals;
    uint256 public totalSupply;

    /* This creates an array with all balances */
```

SELECT CONTRACT TO DEPLOY

My Advanced Token

CONSTRUCTOR PARAMETERS

Initial supply - 256 bits unsigned integer

1234

Token name - string

MyString

Decimal units - 8 bits unsigned integer

1234

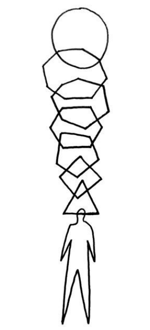
Token symbol - string

MyString

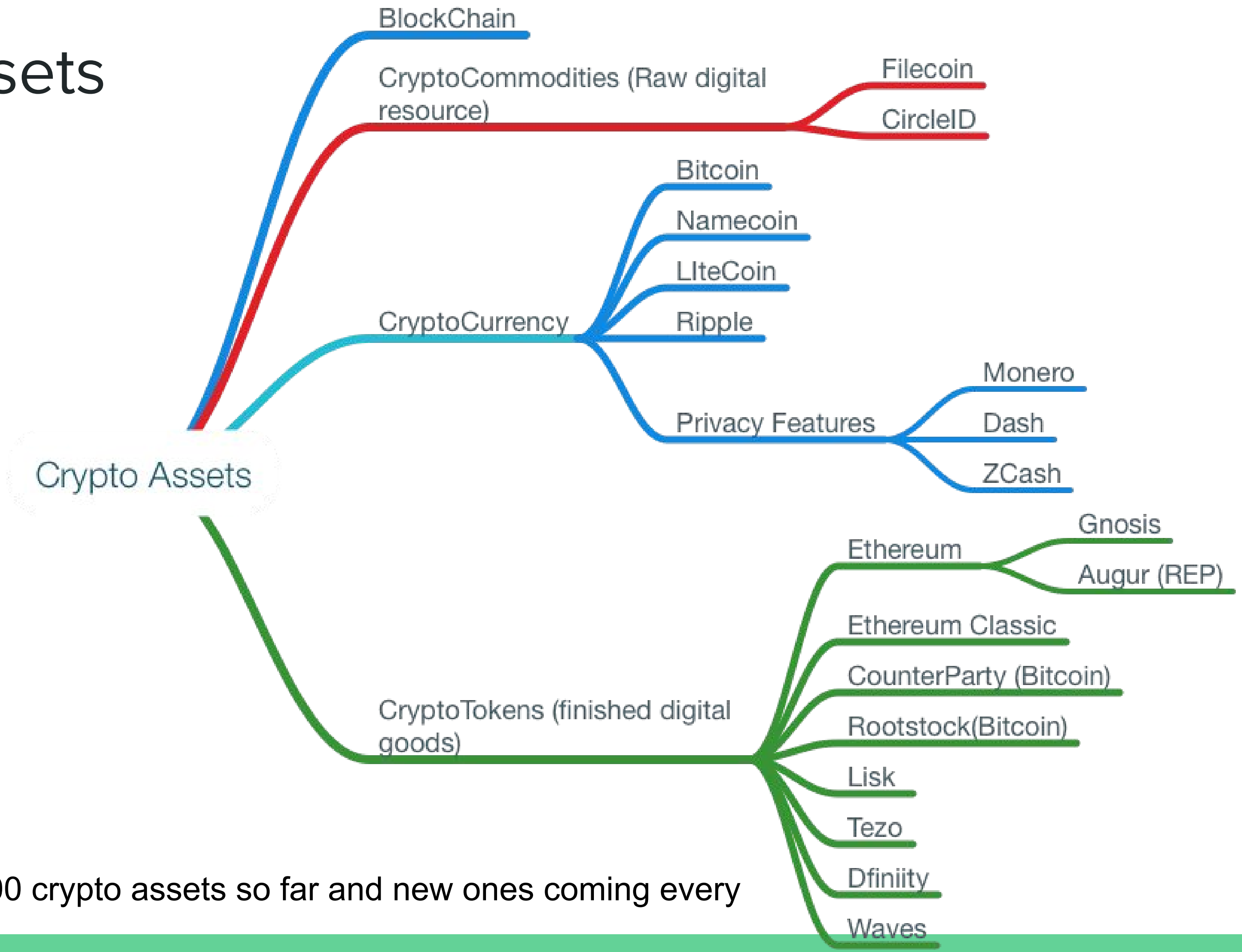
Central minter - address

0x123456...

Module 3 - CryptoAssets & Valuation



Crypto Assets



There are about 800 crypto assets so far and new ones coming every month

Should bitcoin be valued like $ or gold or other other commodity ?

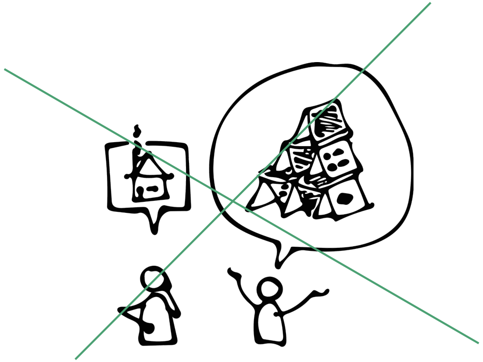
If bitcoin does not serve the payment use case as anticipated, why is it trading at $6000 ?

Should an ICO token be valued like IPO stock or startup angel investment ?

Bitcoin like money, ICO like IPO is only a metaphor

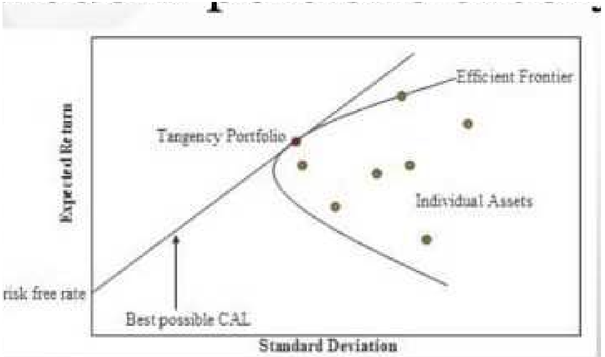
“All models are wrong, some are useful but some dangerous ” - NN Taleb

“It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so.” - Mark Twain

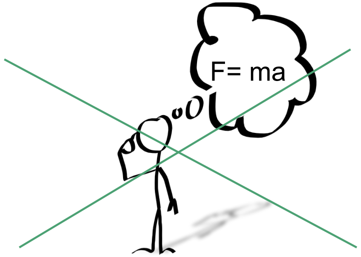


“Never confuse brains with a bull market” - Warren Buffett

Popular mental models break down



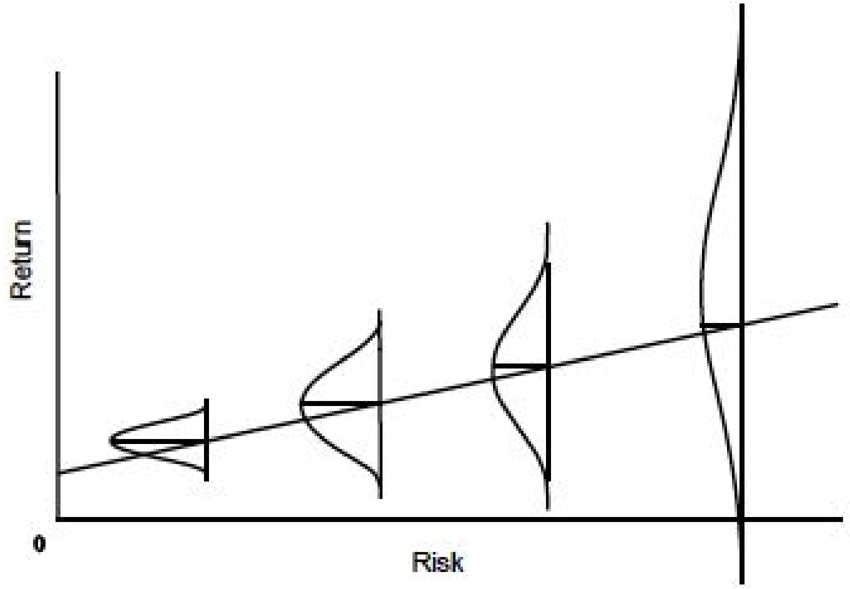
Modern Portfolio Theory (Standard Deviation, Sharpe Ratio, Correlation) have several limitation already

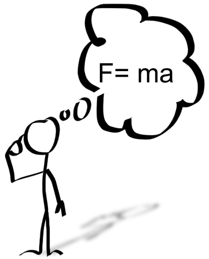


"Never forget the six-foot tall man who drowned crossing the stream that was five feet deep on average."- Charlie Munger

Many mental models are creaky

Volatility is not risk



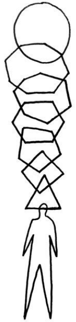


Source - Howard Marks, Oaktree Capital

What is value ?

Marx Talks about

Use Value, Exchange Value, Symbol Value, Store Value

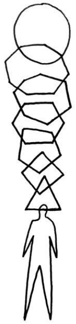


Value arises from imagination of future

Fear and Hunger

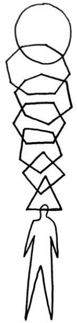
Money is story with highest belief coefficient

that help in survival against both fear and hunger in the future



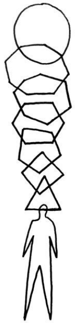
Belief/trust on Nation state as custodian of the money story is broken

Alternates ? Gold, Distributed Consensus ?



“Bitcoin will be a store of value when everyone believes it is. The price is the current probability. Fundamental analysis is impossible. “

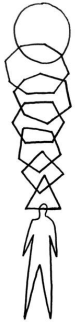
@naval



What is valuation ?

Estimating / forecasting the future

”We have two classes of forecasters: Those who don’t know – and those who don’t know they don’t know. ” - Kenneth Galbraith



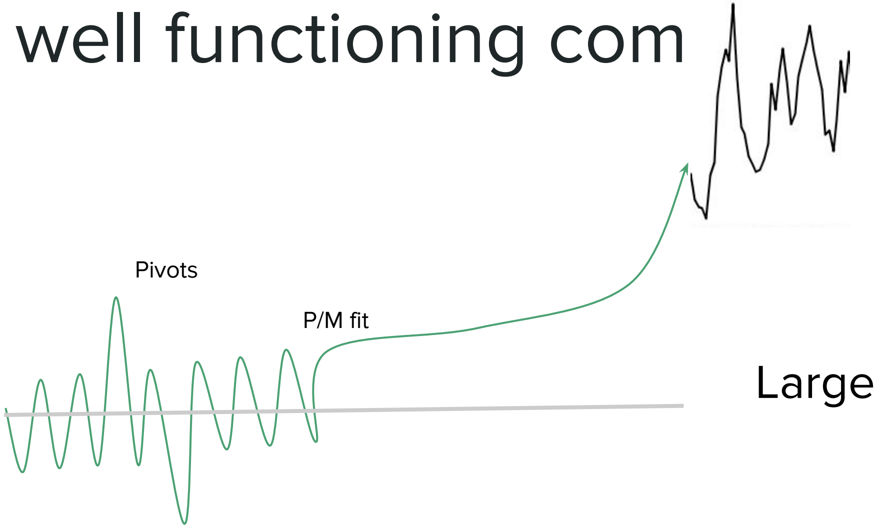
Startrek Journey

Startup valuations are 80% story, 20% data

Public company valuations are 20% story, 80% data

Innovation Accounting tracks journev of a startup to well functioning com

Idea/Startup



Large Company

Takes 7-11 year journey

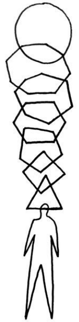
Power law, 1 in 10,000 succeed

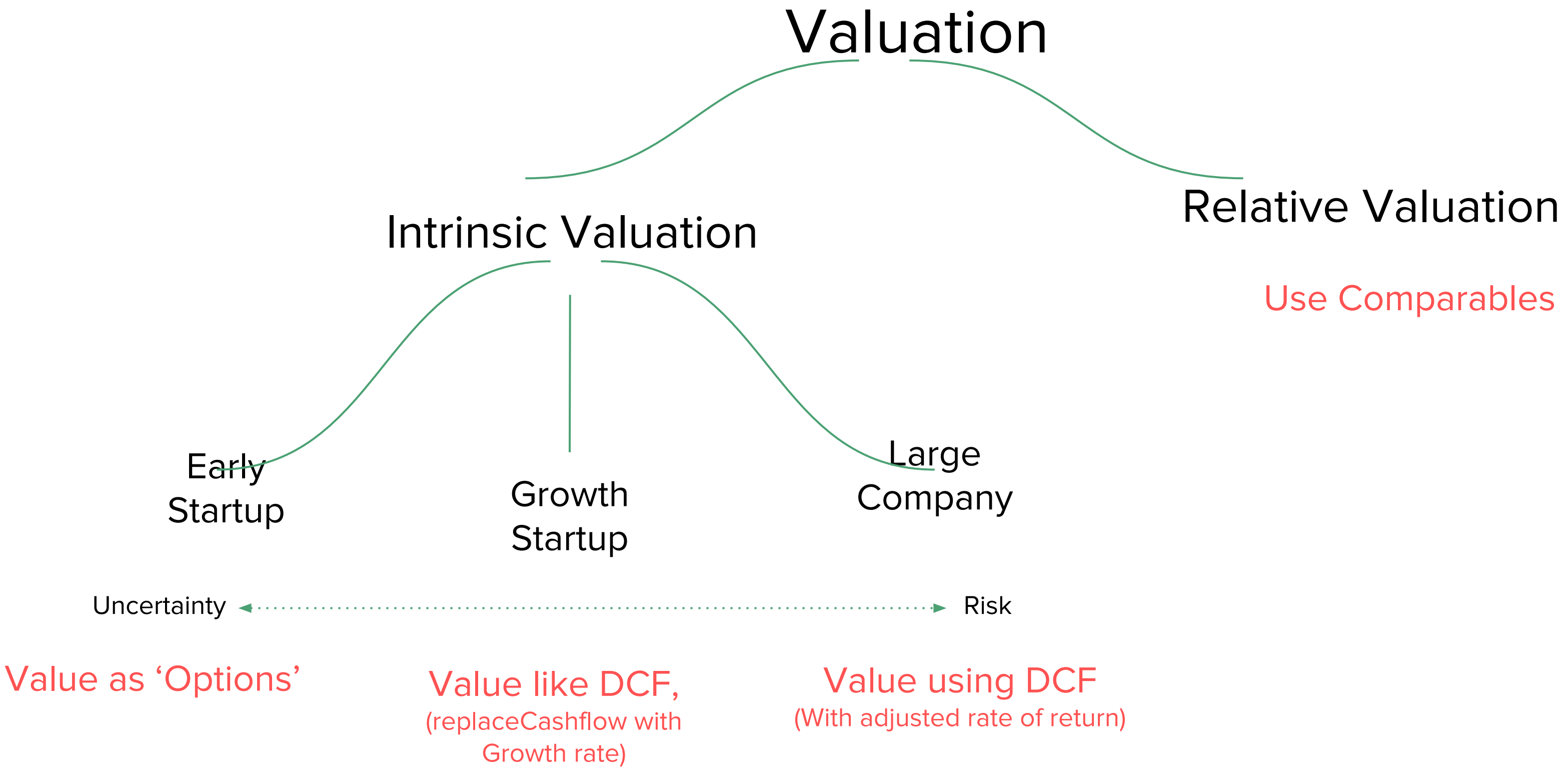
Uncertain & Non repeatable Value

Probability distribution Unknown

Certain & Repeated Value

Probability distribution Known





Valuation

Intrinsic Valuation

Early Startup

Growth Startup

Large Company

Uncertainty

Risk

Value as ‘Options’

Value like DCF, (replaceCashflow with Growth rate)

Value using DCF (With adjusted rate of return)

Relative Valuation

Use Comparables

DCF - Discounted Cash Flow

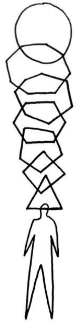
Source - Aswath Damodaran

About Price (aka Relative Valuation)

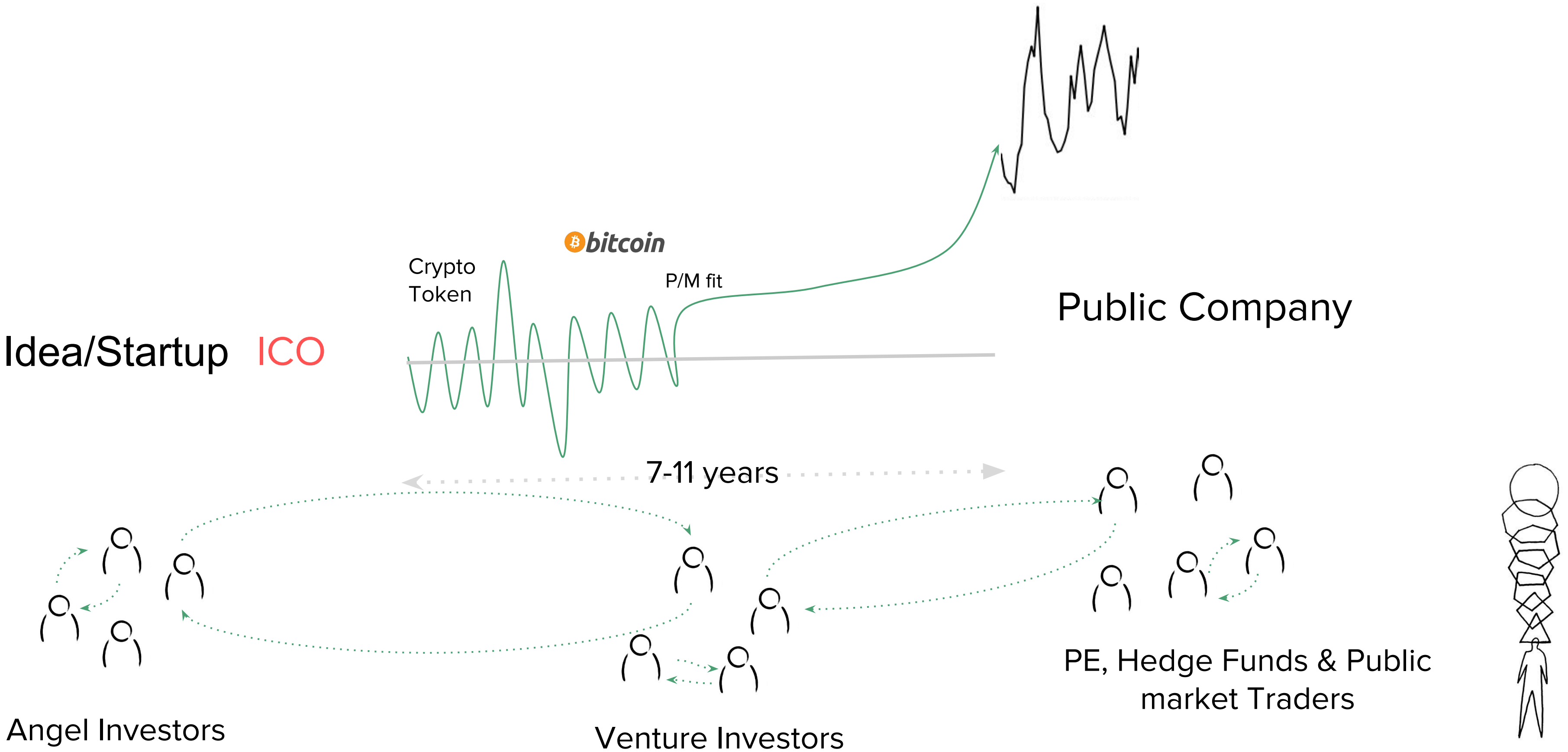
“Can’t estimate or predict the outcome of the collective based on individual action, markets are emergent” - NN Taleb

“Markets can remain irrational longer than you can remain solvent”

- John Maynard Keynes



Relative Valuation is arbitrage or pyramid scheme ?



Idea/Startup ICO

Crypto Token

bitcoin

P/M fit

Public Company

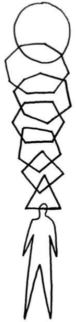
7-11 years

Angel Investors

Venture Investors

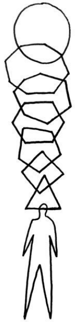
PE, Hedge Funds & Public market Traders

ICOs possibly best treated like angel investments



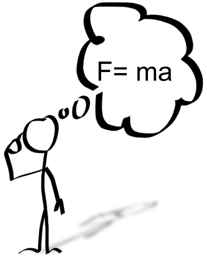
Error in your mental model is my opportunity - Value investing

Value is different from Price, Picking mispriced, Invest out of cycle



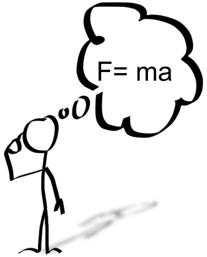
Arriving at an intrinsic value still need lot of assumptions

For a given supply & velocity of token, what is the GDP (measured in $) of the use case need to be supported



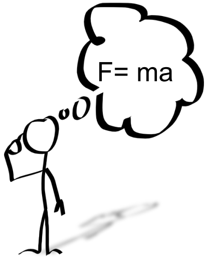
$MV = PQ$

M = size of the asset base, V = velocity of the asset , P = price of the digital resource being provisioned, Q = quantity of the digital resource being provisioned



INET Valuation, Example from Chris Burniske

https://docs.google.com/spreadsheets/d/1ng4vv3TUE0DoB12diyc8nRfZuAN13k3aRR30gmuKM2Y/edit#gid=1912132017



New Markets in early stage, must watch out for

Speculation of Crowds , Bubbles, Ponzi Scheme & Scams, Cornering , Pumping & Dumping.

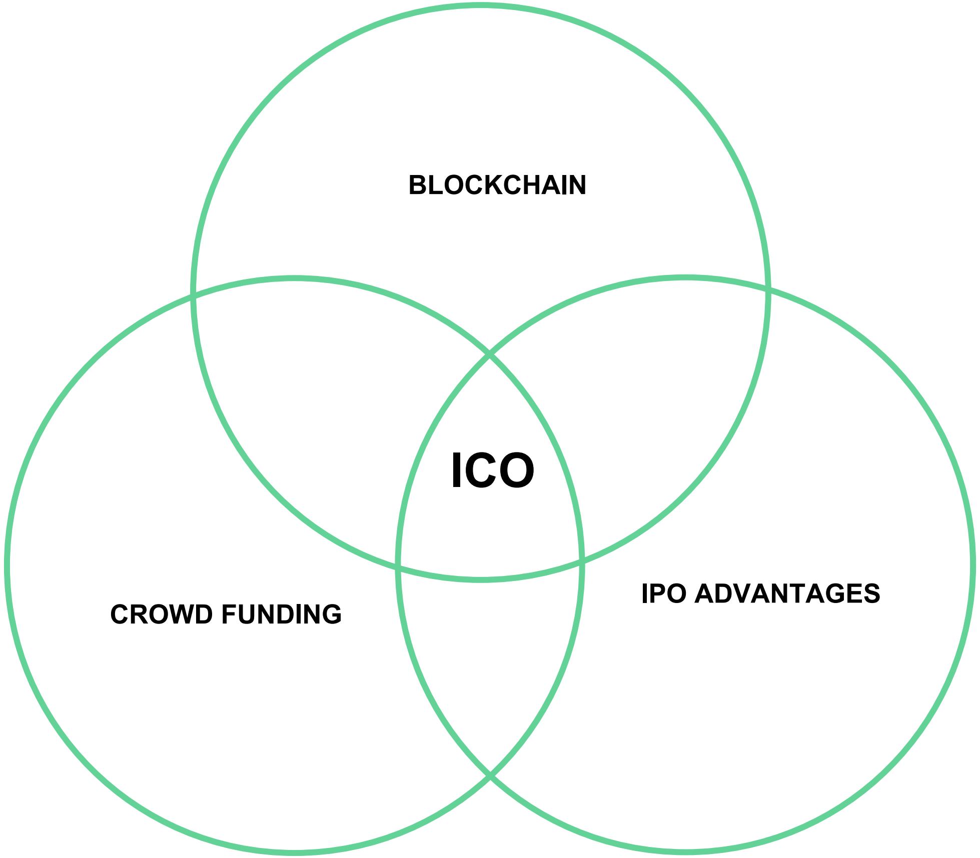
Exercise 3

Visit coinmarketcap.com

List the price of one Ethereum based toke, bitoon based tokens and write their $ values.

Module 4 - ICO

ICO is like an IPO for early stage startups

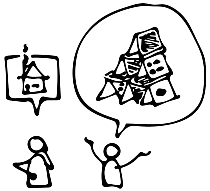


BLOCKCHAIN

ICO

CROWD FUNDING

IPO ADVANTAGES



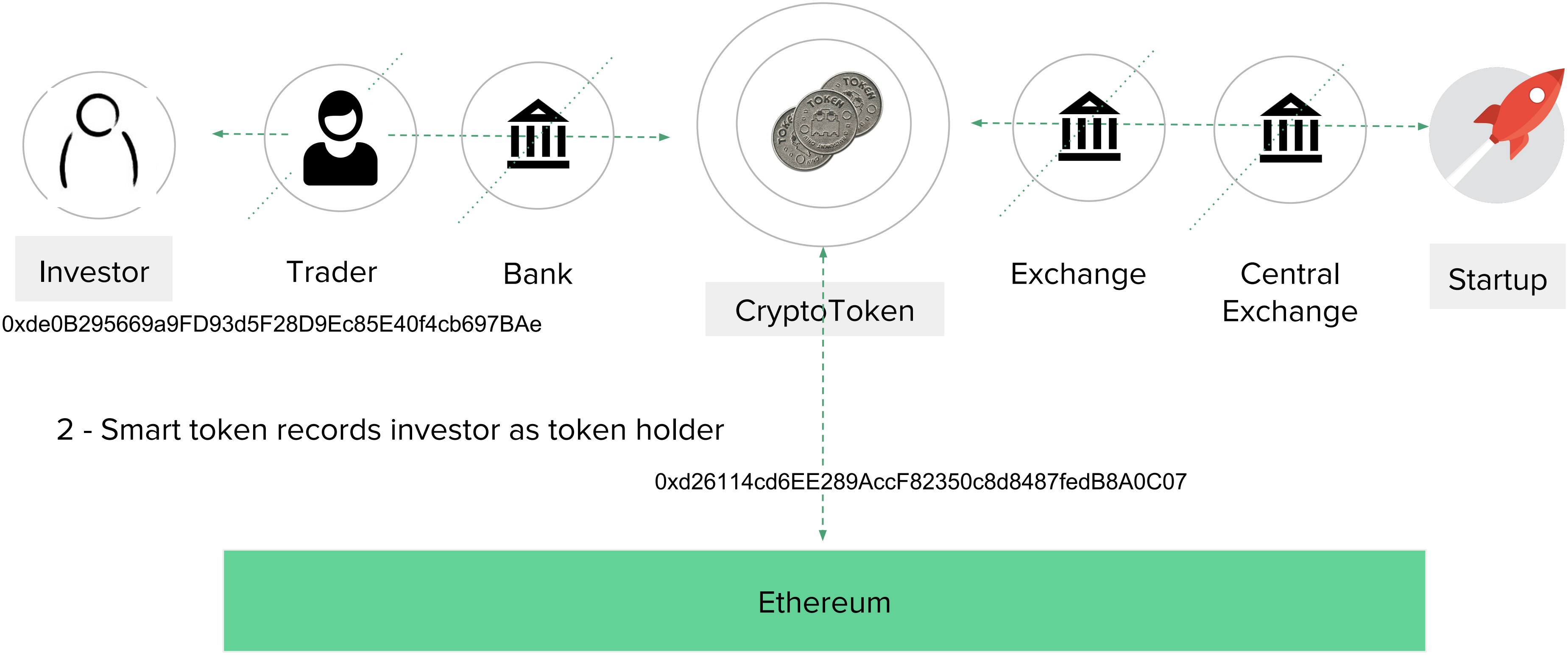
Initial coin offering (ICO) is an unregulated and controversial means of crowdfunding via use of cryptocurrency, which can be a source of capital for startup companies

The coin (aka Token) in an ICO is a symbol of ownership interest in an enterprise—a digital stock certificate

via Wikipedia

1 - Investor sends cryptocurrency gain a smart token

3 - Company accompanies the cryptocurrency held in token



Investor

Trader

Bank

CryptoToken

Exchange

Central Exchange

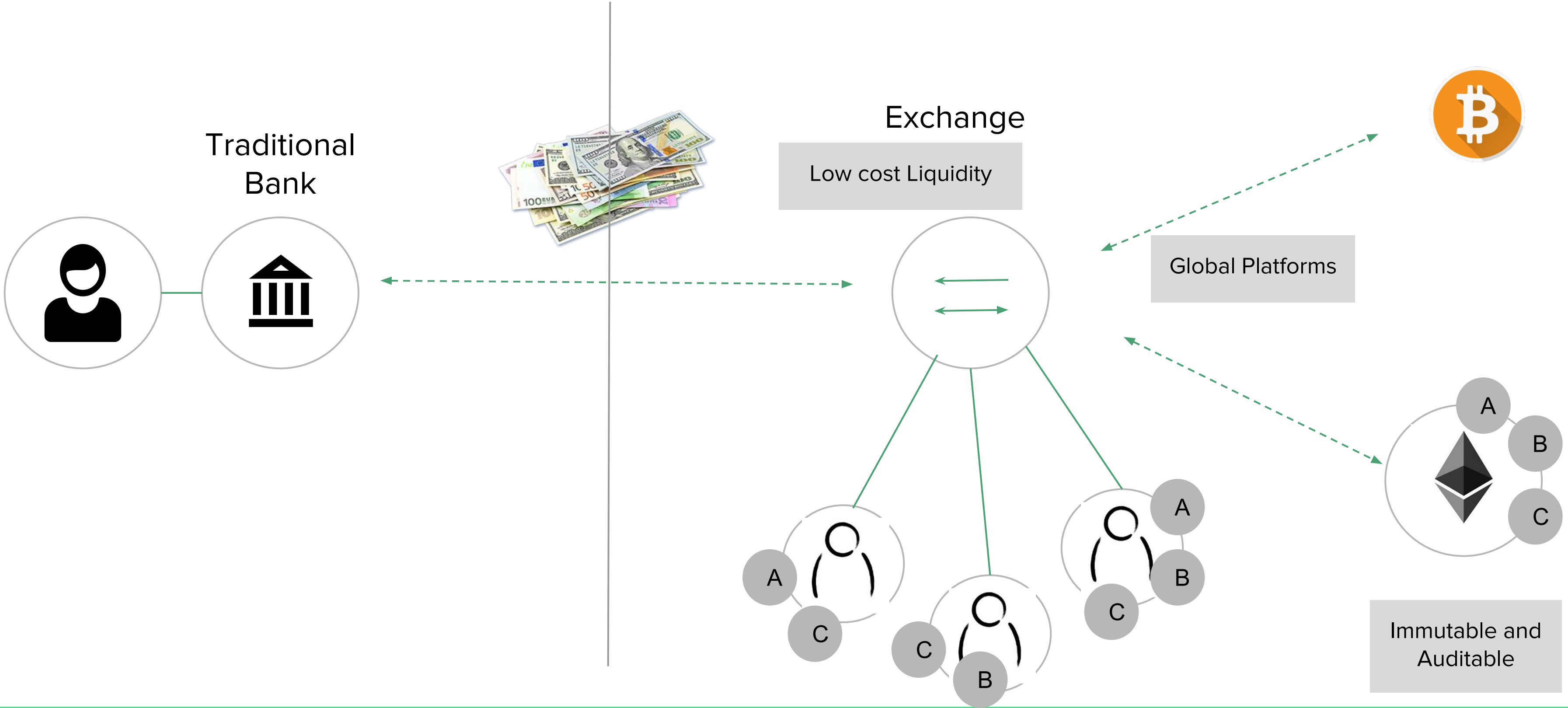
Startup

0xde0B295669a9FD93d5F28D9Ec85E40f4cb697BAe

2 - Smart token records investor as token holder

0xd26114cd6EE289AccF82350c8d8487fedB8A0C07

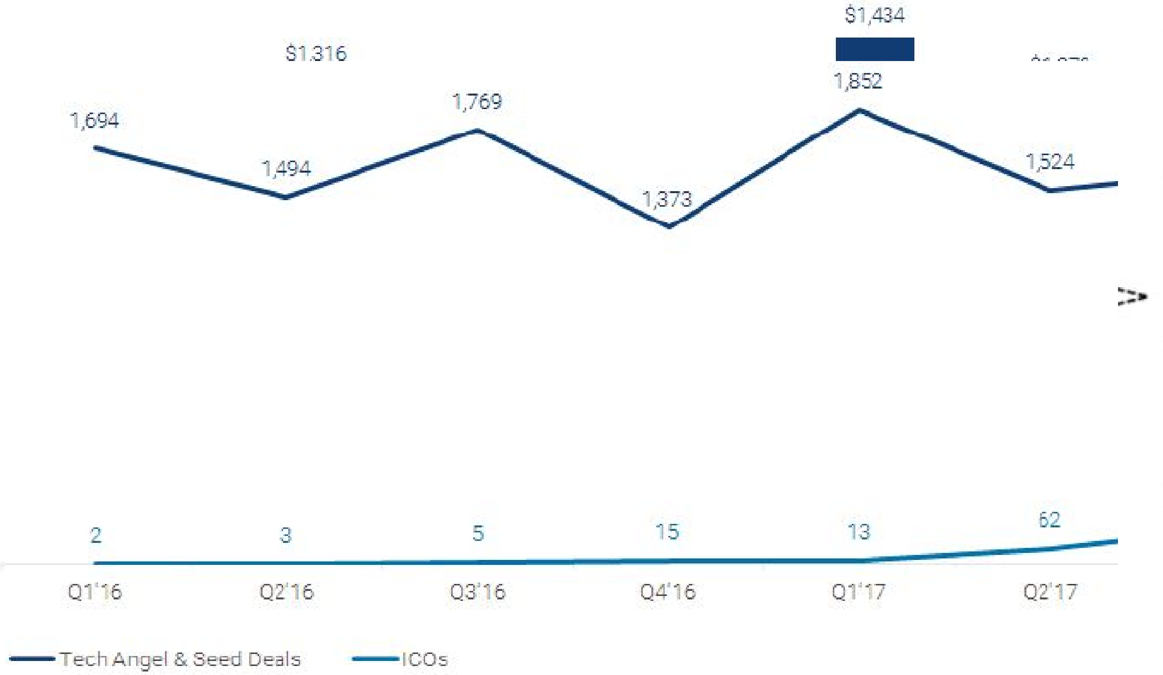
Ethereum


Traditional Bank
Exchange
Low cost Liquidity
Global Platforms
A
B
C
A
C
C
B
A
B
C
Immutable and Auditable

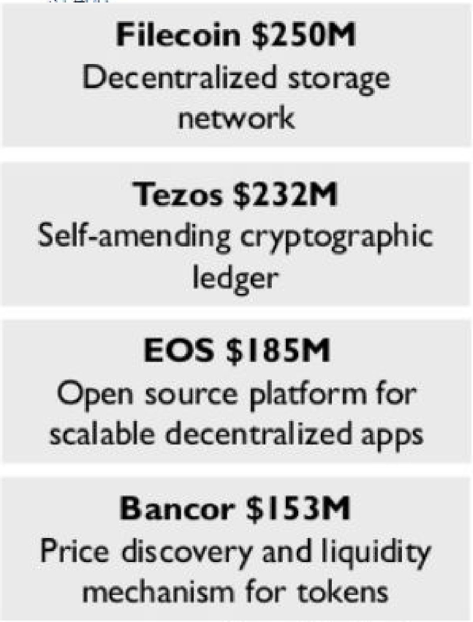
Comparison with other fundraising methods

	ICO	Equity Crowdfunding	Reward Crowdfunding	VC	IPO
Startup stage	Prototype	Prototype	Prototype	Prototype - Midstage	Latestage
Equity	No	Yes	No	Yes	Yes
Requirements	White paper (optional) - Desired Amount - Project milestones - Team - Types of tokens - Exchange rates	Education materials - Investment - Description - Types of securities - Investment limits	Education materials - Project description - Marketing deck - Types of research	Pitch Deck - Business model - Use of funds - Management	Prospectus - Company - Description - Types of securities - Management - 3 year profitability
Investors	Blockchain Enthusiasts	Angel Investors	Early Adopters	Limited Partners	Public
Period	3-4 months	1-3 months	1-3 months	3-12 months	> 1 year
Fundraising cost	Low	Medium	Low	High	High
Channel	Online	Online	Online	Offline	Offline
Liquidity	Low-Medium	Low	Low	Low	Medium
Investor Downside risks	Fraud, Project Fails	Bankrupt	Project Fails	Devalue, Bankrupt	Price Drop

ICO > VC & ICO ~= Angel in Q3 2017



Sources: CB Insights, TokenData, CoinSchedule.



Filecoin $250M
Decentralized storage network

Tezos $232M
Self-amending cryptographic ledger

EOS $185M
Open source platform for scalable decentralized apps

Bancor $153M
Price discovery and liquidity mechanism for tokens

Source: CB Insights, Fortune

Pros and Cons of getting involved in an ICO

Pros

- Some people are getting rich.
- Transcends global boundaries
- Speed and cost of fund raising massive reduced down to 3-4 months

Cons

- You may not be one of the people becoming rich
- Unregulated - Potential of fraud such as pyramid schemes, scams
- No straight forward way to pick winners
- Overfunding, capital inefficiency likelihood

Crypto token looks like ‘securities(equity/share)’, feels like ‘securities’, quack like an ‘securities’ object.

Is it securities and be regulated as such ?

CryptoAssets classified like following for regulation

	Purpose	Velocity	At Scale
Cryptocurrency	Multi purpose	Low	Rivals gold and national currency
Crypto (Utility) Tokens	Single purpose	High	Value depends on duration for which token of dapp need to be held
CryptoSecurities	Single purpose	Low	Value depends on increasing liquidity of assets fundamental value

Regulators can take several approach

- Laissez - faire - Crack only on wrong projects
- Choke Liquidity - Control or crackdown the alternate assets digital exchange
- Fire & Brimstone - Declare all ICOs (Cryptotokens) illegal

Regulators of different countries

Country	Regulator	Key points
US	SEC	Application of the Howey Test (investment of money in a common enterprise with an expectation of profit predominantly from the effort of others) to ICOs to determine if a particular token should be classified as a security falling under securities law
Singapore	MAS	No definitive regulation but have viewed cryptocurrencies with a light touch MAS has launched a tokenized version of the SGC via Project Ulsin
Switzerland	FINM	No regulation, cryptocurrency are treated as assets
UK	FCA	ICO is treated as an investment with subjective interpretation
China	People Bank of China	Issued a ban on ICO on Sep4. Concerns over fraud and pyramid schemes
India	RBI/SEBI	Have been very conservative in past, (mobile payments, Fintech) Will soon announce

Japan,Australia are favourable countries

Self Regulatory Framework

In absence of regulatory framework the bitcoin and ethereum community has taken upon itself to explore self policing

Difficulties for a regulator

So much divergence for existing mental model & definition- securities

Transcends geography and are funded by crypto which does not have a central backing

Pseudoanonymous - While identity can be found but difficult

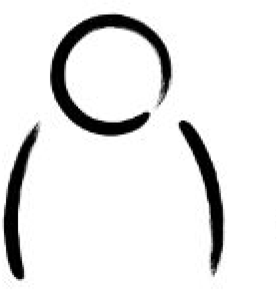
Self Regulatory Framework

SAFT - Simple Agreement of Future Tokens
Based on SAFE (equity) an agreement for raising money for equity in return without having to issue debt note.
SAFE is only offered to “accredited investors”

Crowdfunding - Guidance on which digital assets are deemed securities whether firms selling it must register.
Can use a regulatory sandbox

Other mechanisms - Escrow Accounts (3rd party release based on milestone completion.
Use KYC ; Setting up minimum investment amount

How to do an ICO



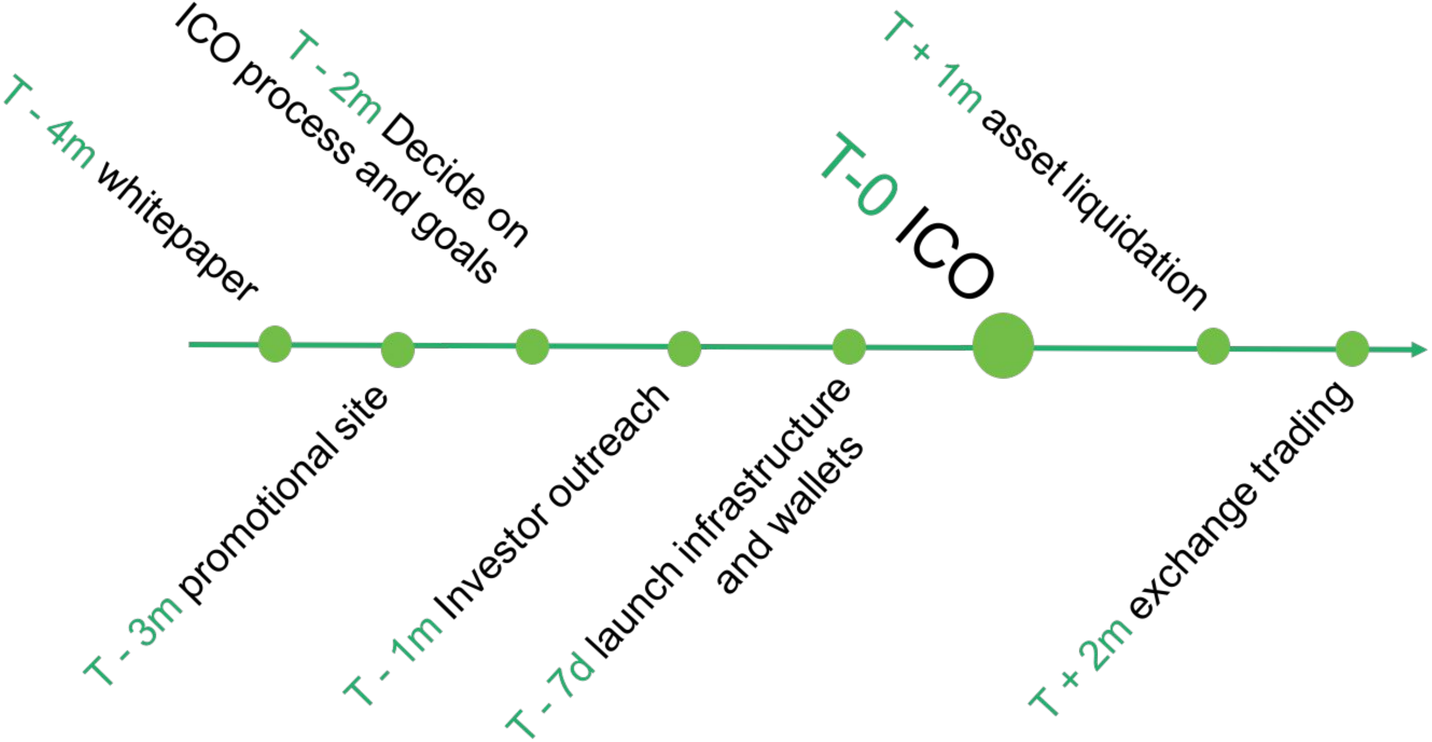
Entrepreneur

Steps

Fundraising in ICO is similar to IPO however raising tokens are faster and costs a fraction

		ICO	IPO
1	Initiate	Write a summary, announce to crypto community to gather interest and feedback	HIre an investment banker to underwrite an IPO
2	Documentation	Whitepaper and website	Filings with SEC (US), SEBI(India) Registration statement Prospectus
3	Marketing	PR Campaign Crypto Forums Slack Telegram	Roadshow Pre Sale IPO Set Pricing
4	Sales Process	Buyer send cryptocurrencies to a digital address; smart contracts issue tokens according to exchange ratio	Allocate shares according to book building
5	Listing	Tokens listed on a crypto exchange	Shared listed on an exchange

Timeline


T - 4m whitepaper
T - 3m promotional site
T - 2m Decide on ICO process and goals
T - 1m Investor outreach
T - 7d launch infrastructure and wallets
T-0 ICO
T + 1m asset liquidation
T + 2m exchange trading

Sample Whitepaper

Examples of ICO Whitepapers:

- Ethereum
- Tezos
- Bancor
- Basic Attention Token on Brave Browser

Solidity Sample Code

Example: pCoin

- pCoin.sol
- pCoinCrowdsale.sol
- DeployContract.sol

- Readthedocs
- Reading List
- Solidity Tutorials

~~Home User~~

Trader

How to Invest in an ICO

What to do before investing in ICOs ?

- Browse an ICO list website like https://icobench.com/ or http://tokenfilings.com/
- Create and operate your valuation process checklist (based on valuation lessons learnt before)
- Run your due diligence
- Acquire your cryptocurrencies & wallets

Where to trade

- Poloniex
- Kraken
- Token Market
- Airswap
- Coinbase

How to spot a scam ICO ?

- Lack of Public team profiles
- Compromised or missing escrow
- No technical details in the whitepaper
- Unrealistic goal
- Missing code repository on Github
- Vague Promises
- Illegitimate affiliations
- Too good to be true Incentives

Appendix