Course Outline

- ❑ Introduction
- ❑ Money and token economy
- ❑ Cryptography
- ❑ Blockchain data structure
- ❑ Mining and PoW
- ❑ Consensus algorithms / Filecoin
- ❑ Bitcoin as a platform
- ❑ Ethereum and smart contracts
- ❑ Distributed applications & enterprise DLT
- ❑ Security
- ❑ Scalability
- ❑ Privacy

Course Schedule & Logistics

❑ Time – Friday 7:30-10:20pm, Zoom

- ❖ Feb: 5, 19, 26 - Project & team formation
- ❖ Mar: 5, 12, 19, 26
- ❖ Apr: 9, 16, 23, 30
- ❖ May: 7

❑ Course Evaluation

- ❖ Class participation: 20%
- ❖ Homework: 30%
- ❖ Course Project: 50%

Last Time (Review)

Blockchain from ICT point of view – data, computation, intelligence

- ❑ **Why – a ledger system maters**
- ❑ **Database versus enabling technologies for ICT**
- ❑ **Data perspective**
- ❑ **From ledger to "distributed computing" – smart contract**
- ❑ **Intelligence perspective**

Today

Money, token, history, and eco-system

- ❑ Money, currency, token – macro economics
- ❑ Blockchain economics
- ❑ Key concepts and technology developments
- ❑ ICO, STO, Stable Coins
- ❑ Crypto projects

Blockchain Economics

Classical Case — Prisoner's Dilemma

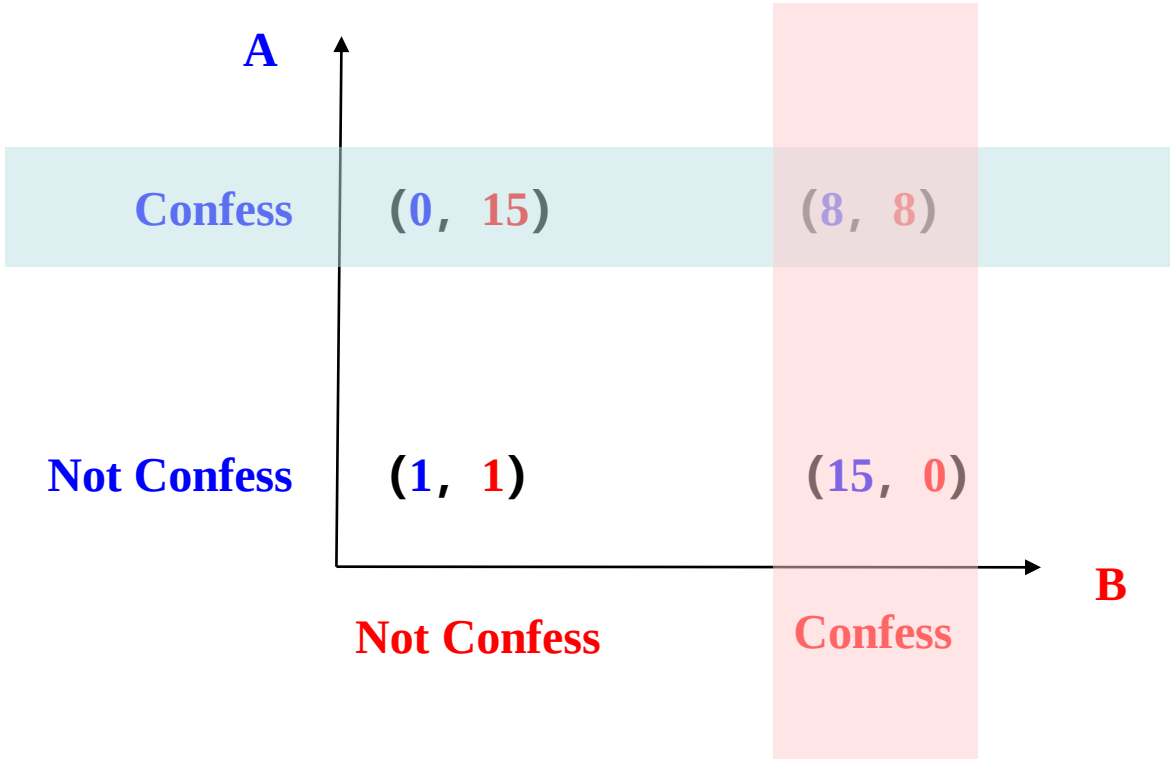
In 1950， to describe the game process, Tucker created this model

Two prisoners were caught and being trialed seperately

- **If both confess, 8-year sentence for each**
- **If one confess and another not, the one confessed is free and the other 15-year sentence**
- **If both do not confess, 1-year sentence for each**

Will they confess (choose not to cooperate) or not confess (choose to cooperate)?

Classical Case — Prisoner's Dilemma



Nash Equilibrium

- Based on his own best interests, both will confess and get 8-year sentence, even if the cooperation (not confess) will have a global optimum (1 year).
- According to game theory, (8, 8) is the Nash Equilibria. Anyone chooses to change (move away from this point), will end up worse off. This point is **Nash Equilibrium**
- Nash Equilibrium may not be the global optimum point

Nash Equilibrium – How to find the equilibrium strategy?

- Rock-Scissor-Cloth: 1/3-1/3-1/3 is NE strategy
- How about the complex problem?
- Game theory says it exists, but not how to find it

- If your laptop cannot find it, neither can market - Kamal Jain, eBay
- Math -> Truth
- Computer Science -> Complexity
- Game Theory -> Algorithmic Game Theory

Algorithmic Game Theory

- Quantize the cost of non-cooperation – **Price of Anarchy**, measures gap between cooperation (centralization) and competition (distribution, de-centralization, independently maximize self interests)
- In Prisoner Dilemma, Price of Anarchy is unlimited
- Need centralization/coordination
- How about other situations
  - Network，bitcoin，social group

Algorithmic Game Theory – Network Problem

- Network problems：networking, traffic
- Packets/drivers “selfish routing” result in overcrowding pathways and creating congestion?
- T. Roughgarden & E. Tardos (2002) proved that “selfish routing” has a price of anarchy of 4/3

- Distributed routing is only 33% worse than centralization/top-down coordination

- Internet works well without any central authority

Blockchain Economic Model

Blockchain Economic Model

Token Economy

Virtual Economy

- **Blockchain Value Ledger - Measurement**
- **Blockchain Smart Contract – auto execution, computation (intelligence)**
- **Blockchain Value Net – Programmable society, community/operation (logic/code/process)**

Goal is to maximize the resource utilization

- Physical society resource
  - Time （T）
  - Space （S）
  - Value/Energy （V/E）
- Virtual/cyber eco-system resource
  - bandwidth （b）： related to time (T)
  - storage （s）： space in the virtual world (S)
  - computation （c）： generate value, consume energy (V/E)
- Under the resource constraints, optimize (V/E)

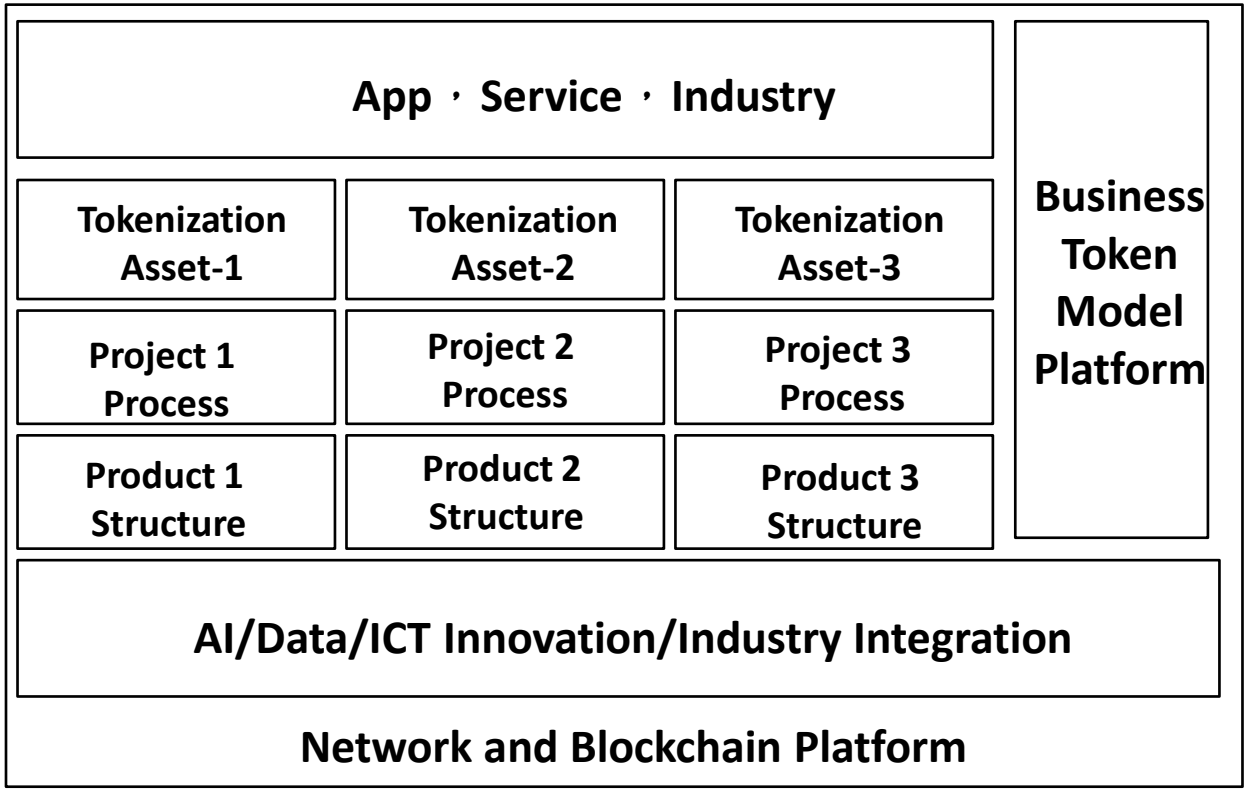
Blockchain Community Eco-System

- V -> s -> V
  - Token: Bitcoin
- V -> c, s -> V
  - Token: Ethereum Ether/Gas
- V -> c, s -> V
  - Token: Crypto Exchange, trade volume (trans-fee mining)
- T -> c, s -> V
  - Blockchain Virtual Education

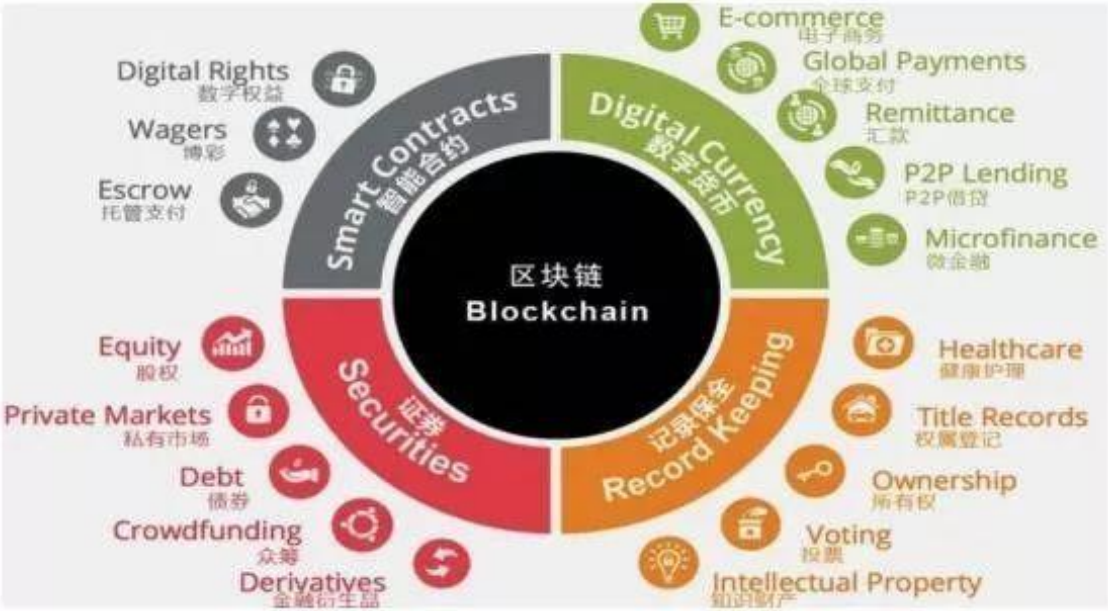
Build blockchain virtual community & economy

deflation, inflation, adjustable

Business – Decentralization/Tokenization

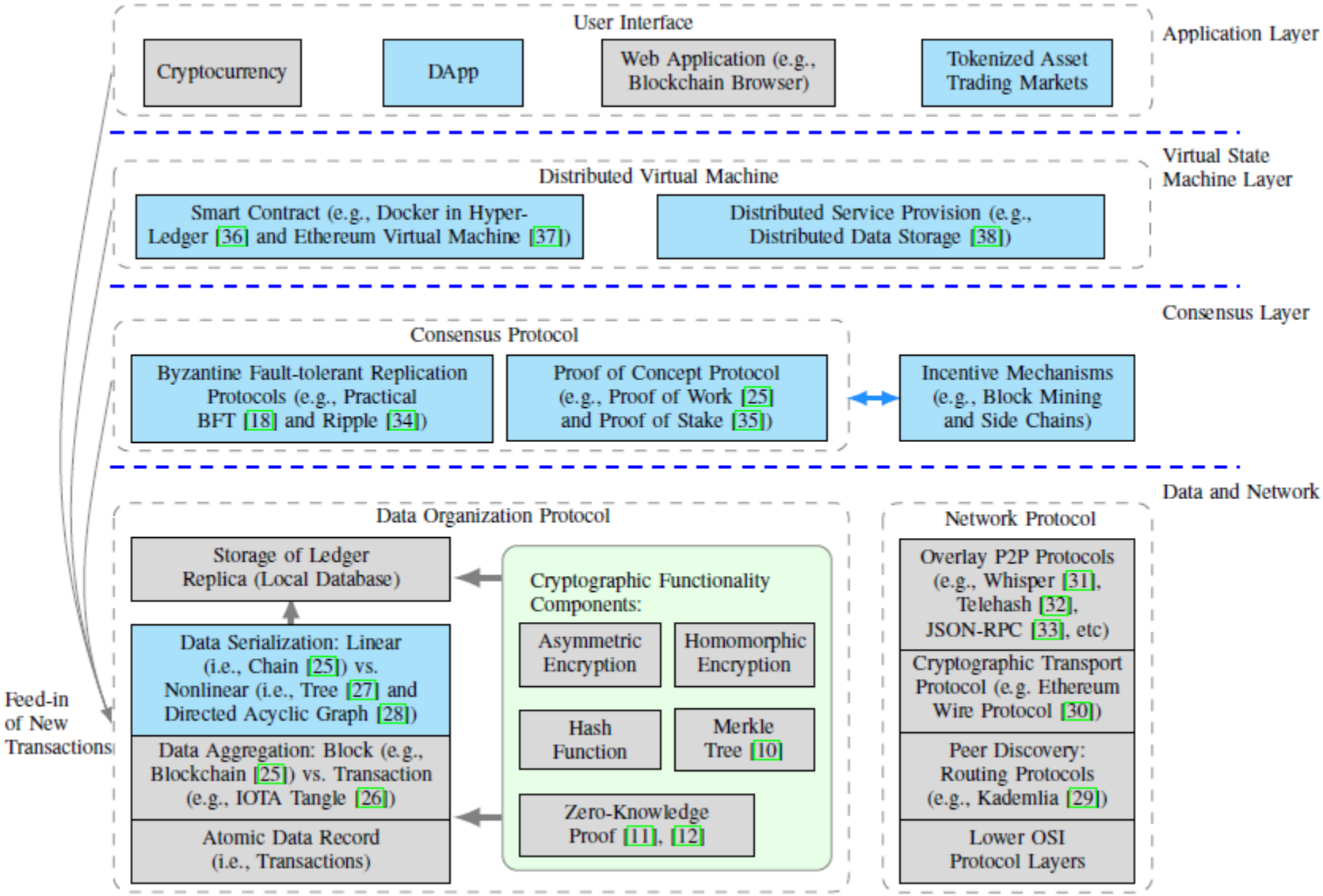


Generations of Blockchains



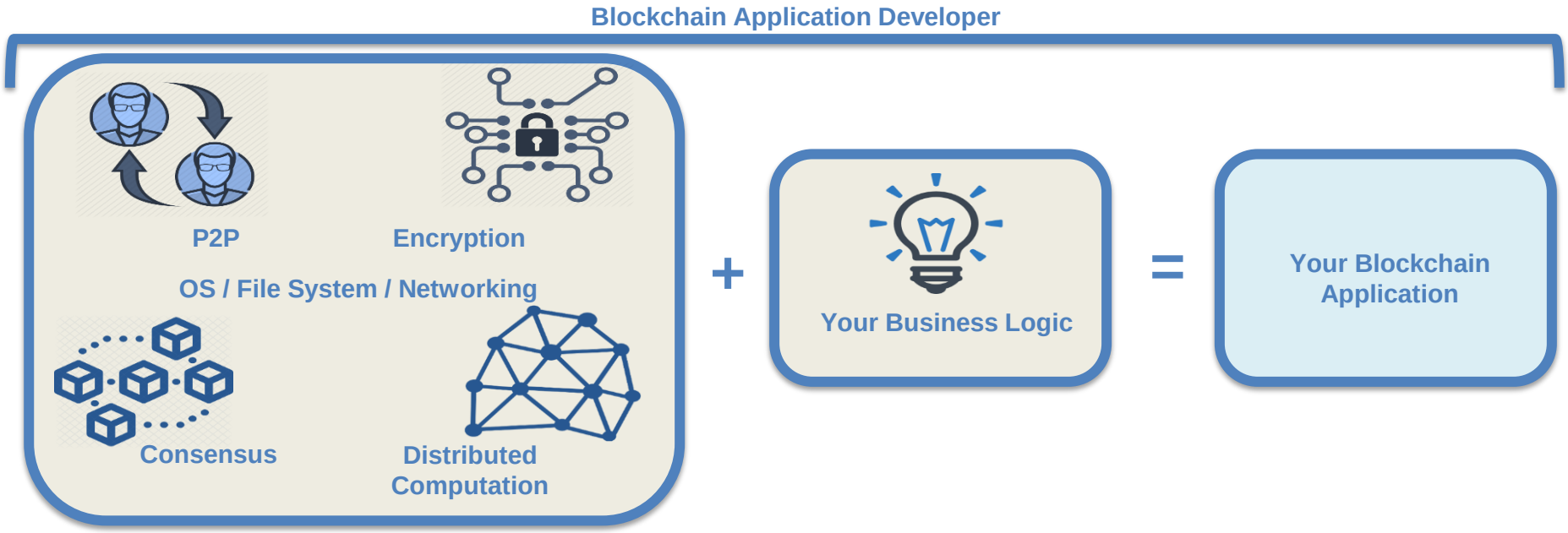
- **Blockchain 1.0: programmable money – carrier currency -> Ledger Record**
  - Ledger record is both the means and ends (method and purpose)
- **Blockchain 2.0: programmable finance – smart contract (code execute contracts for people)**
  - Value Record, shares/debts/rights registration, transfer, securities/contracts/betting exchange
- **Blockchain 3.0: programmable society**
  - Value Internet – info/data with value, can record rights, quantify, and store
  - Record everything valuable – code represents logical things – most of society (minus moods, sensation etc.)

Blockchain Network Implementation Stacks

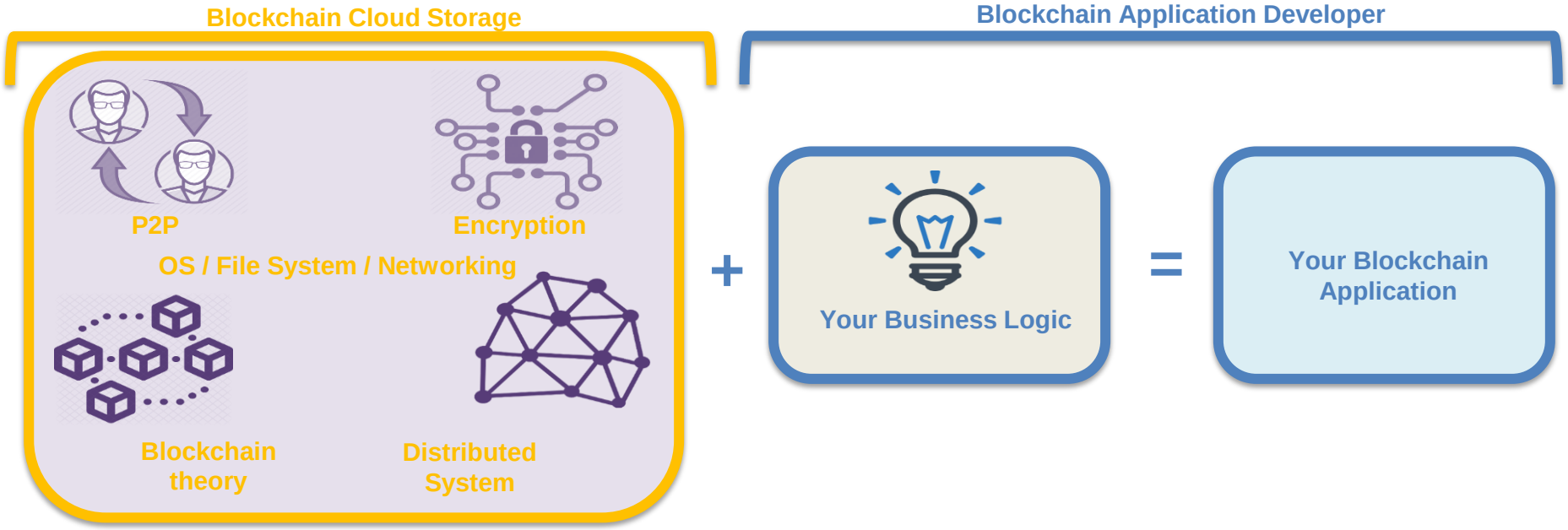


From “A survey on consensus mechanisms and mining management in blockchain networks” by Wang and Hoang

To Develop an blockchain application (General)



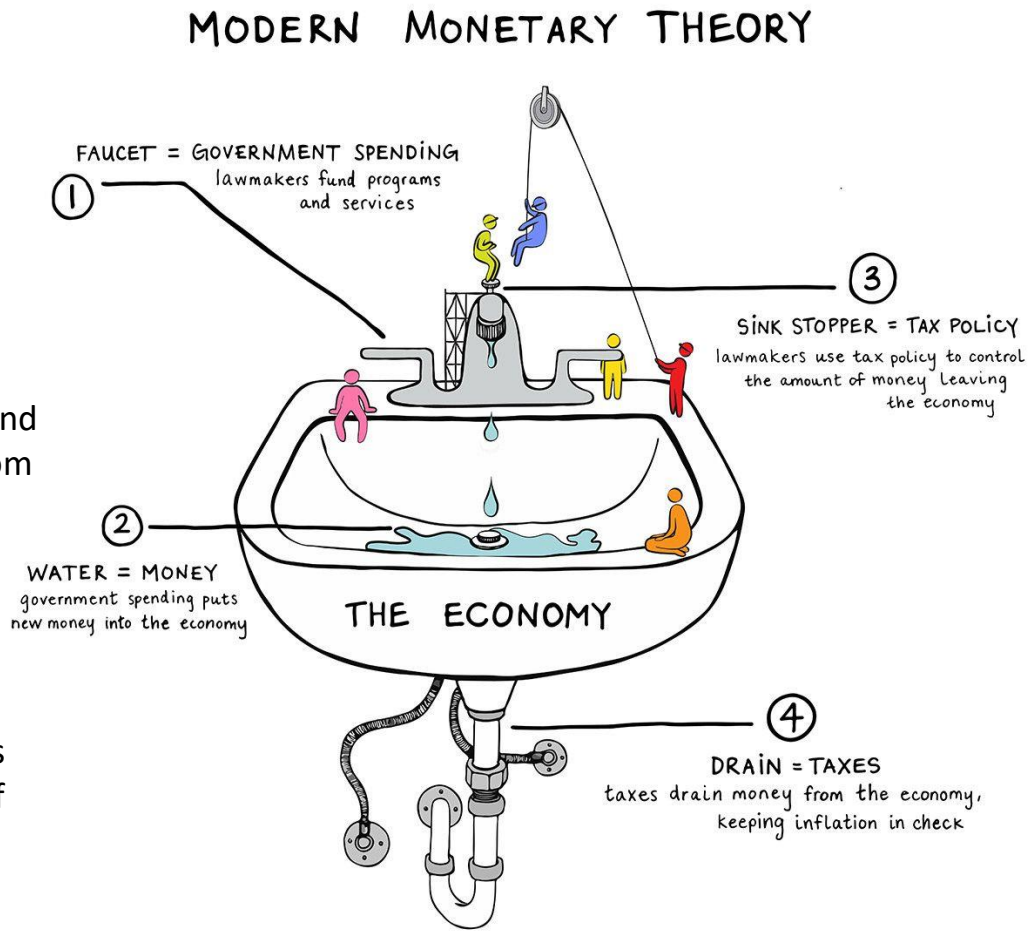
To Develop an blockchain application



Money / Currency

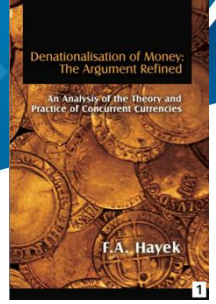
Modern Monetary Theory

- **Mainstream economics view: government spending is funded by taxes and debt issuance**
- **MMT describes currency as a public monopoly for government, which**
  - Can pay for anything without collecting money with taxes or debt issuance in advance
  - Cannot default on debt denominated in its own currency
  - Is only limited in its money creation and purchases by inflation, which accelerates once real resources are utilized at full employment
  - Can control demand-pull inflation by taxation and bond issuance, which remove excess money from circulation
  - Impact of government deficits on interest rates



"US can pay any debt it has because we can always print money to do that. There is zero probability of default." - Alan Greenspan

De-nationalization of Money



- Instead of government issuing currency in monopoly and force by legal tender laws
- Private businesses should be allowed to issue their money competing for acceptance
- Stability in value is presumed to be the decisive factor for acceptance
- Competition favors currencies with the greatest stability in value since a devalued currency hurts creditors, and an upward-revalued currency hurts debtors
- An extensive basket of commodities may form the ideal monetary base
- Institutions issue and regulate their currency primarily through loan-making, and secondarily through currency buying and selling activities
- Press reports info on whether currencies are within defined tolerance

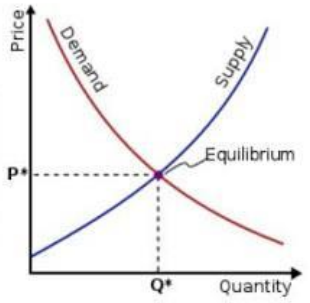
Criticisms

- By design, government currency or Hayek's design?
- Existing monetary institutions evolved to meet real economic needs
- Competitive moneys may result in new monopoly
- Real costs and inefficiencies of competing monies
- Most stable currencies win market acceptance?

Theoretical roots for Bitcoin

Adam Smith's : "Invisible Hand"

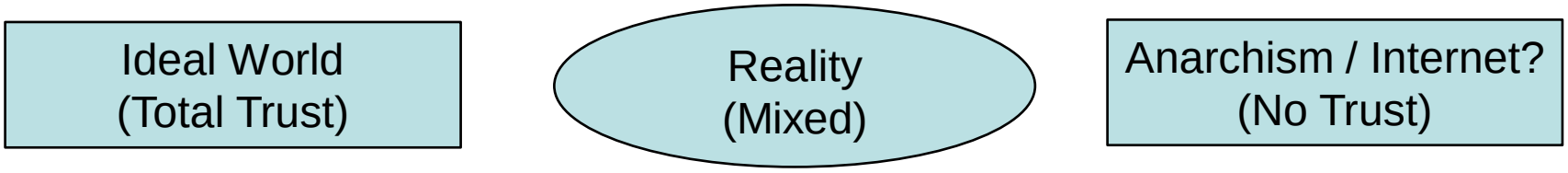
"The sole purpose of all production is to provide the best possible goods to the consumer at the lowest possible price. Society should assist producers of goods and services only to the extent that assisting them benefits the consumer…he intends his own gain; and he is in this, as in many other causes, **led by an invisible hand** to promote an end which was no part of his intention…By pursuing his own interest, he frequently promotes that of society."



Historical Review on Bitcoin and Cryptocurrency

Cryptocurrency – High Level View

- **Who are you?**
- **What have you?**
  - Earned (sweat)
  - Exchange
  - Given by someone
- **What's on the record?**
  - Who writes what on the ledger?



What is Bitcoin?

❑Cryptocurrency

- ❖A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank
- ❖Built upon computer science, cryptography, and economics

❑Bitcoin is a cryptocurrency

- ❖"Bitcoin" can refer to:
  - ✓Bitcoin (uppercase) - the protocol, software, and community
  - ✓bitcoins (conventionally lowercase) - the unit

❑Bitcoin exists as software

- ❖To use Bitcoin by downloading a Bitcoin client, which generates a digital wallet for you
- ❖Bitcoin client generates a Bitcoin address, which you give to people so that they can send you bitcoins

Bitcoin – The Innovation

- Cyptocurrencies have been around since the 1980s
- The early ones, Digicash and Ecash failed because they did not provide a solution to the "double spend" problem - the same digital key you could spend twice or more
- Bitcoin solves the double spend problem

Notable electronic payment systems and proposals

ACC	CyberCents	iKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
CheckFree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone
ClickShare	FSTC Electronic Check	Mini-Pay	PayTrust	VisaCash
CommerceNet	Geldkarte	Minitix	PayWord	Wallie
CommercePOINT	Globe Left	MobileMoney	Peppercoin	Way2Pay
CommerceSTAGE	Hashcash	Mojo	PhoneTicks	WorldPay
Cybank	HINDE	Mollie	Playspan	X-Pay
CyberCash	iBill	Mondex	Polling	

Cryptocurrency History

Cryptocurrency/blockchain history has representative stages

- ❑ Pre Bitcoin: libertarian dreams and ideals
- ❑ Early Bitcoin: scandals, hacks, and illegal activity
- ❑ Scalability debates and Ethereum
- ❑ Token economy
- ❑ Boom and bust cycles

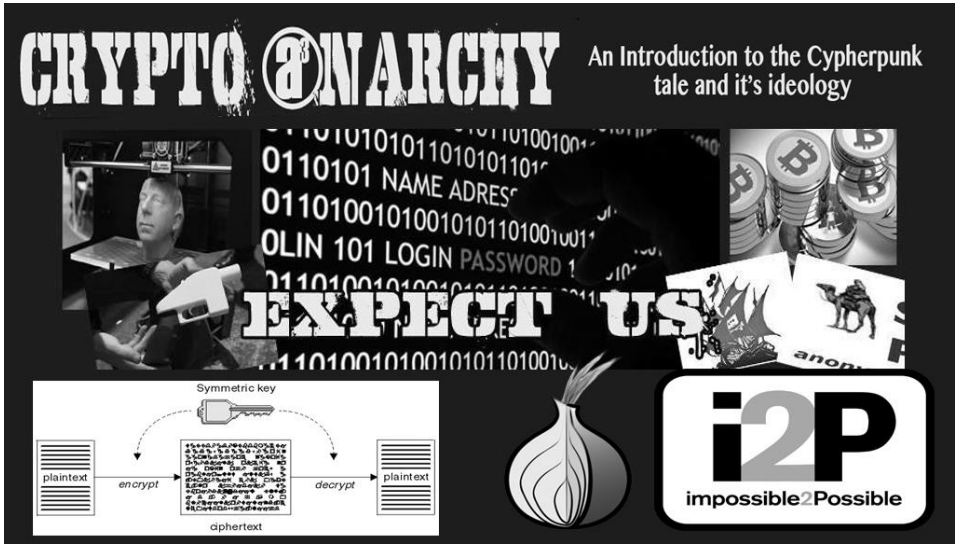
Pre Bitcoin-2009:
Libertarian Dreams and Ideals

Libertarian Dreams

- **With the advancement of technology in the 80s and 90s, the Cypherpunk movement came into being**
- **Roots in libertarianism and cryptography**
  - Libertarianism is a political ideology advocating the non-aggression principle and laissez faire government
  - Cryptography is the science of securing communication in the presence of third parties

A Cypherpunk's Manifesto

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world"

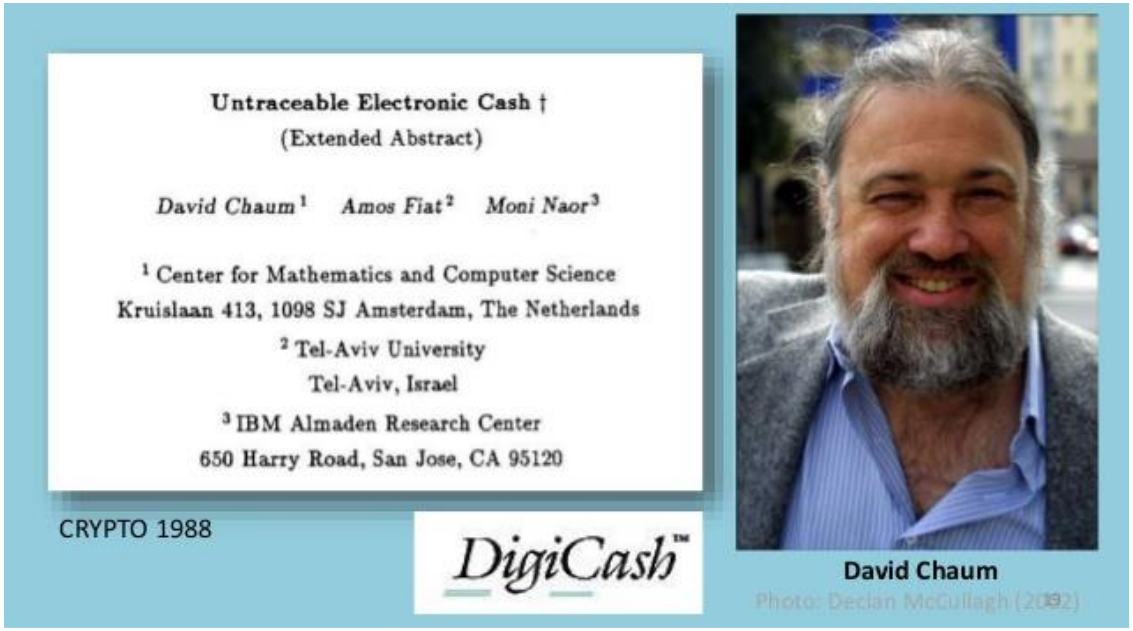


Changing Money

- **Existing financial system - threats to individual privacy**
  - Public key cryptography allowed people to have blind digital signatures, which gave people the ability to sign off on transactions without providing any identifying information
  - Future cryptocurrency creators learned from the mistake of centralization and tried to decentralize currency
- **DigiCash is the most famous example of the early cryptocurrencies**
- **DigiCash used public-key cryptography**

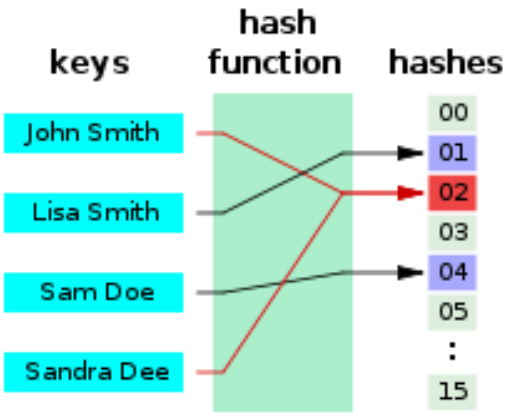
EARLY ATTEMPTS AT CRYPTOCURRENCY - DigiCash

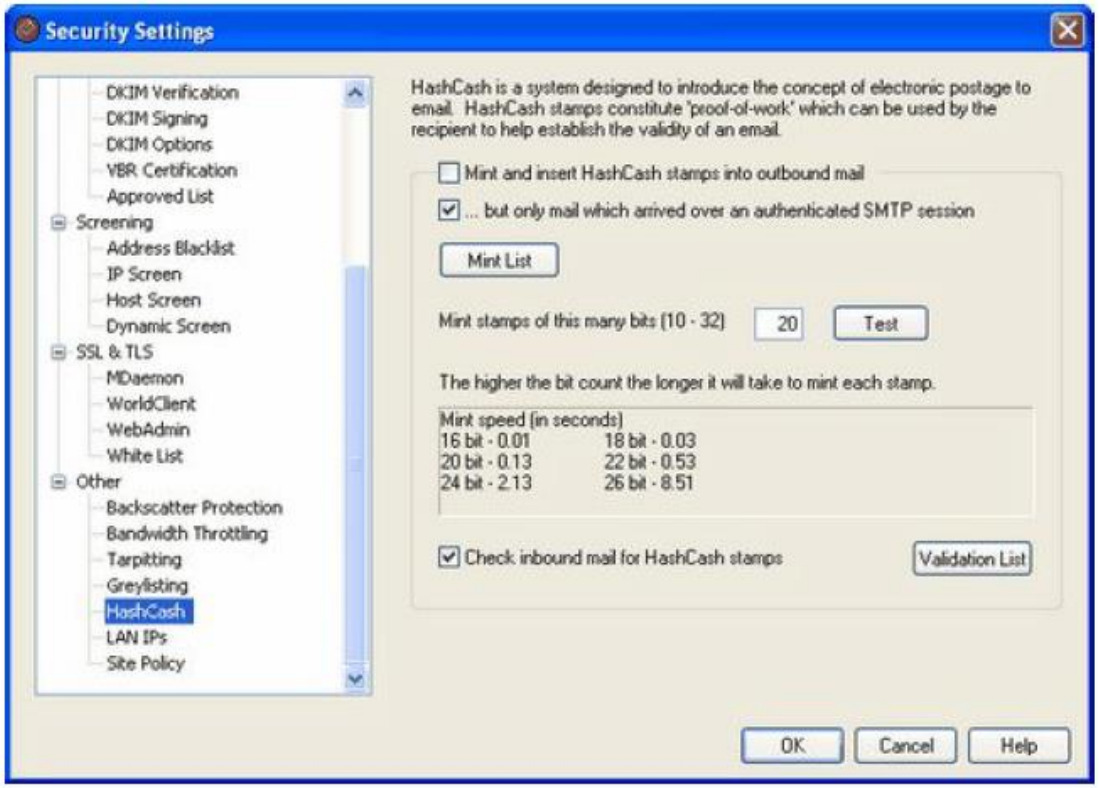
- **DigiCash**: "Blind signatures" public key cryptography
  - Allowed users to sign off on transactions without revealing anything about their identity
  - **Failed due to centralization** – David Chaum's company needs to confirm every digital signature.
  - Eventually, Chaum's company went bankrupt and DigiCash went down with it



EARLY ATTEMPTS AT CRYPTOCURRENCY - HashCash

- **A hash function is a math equation - easy to compute / hard to reverse**
- **HashCash: Coins minted by expending resources instead of by a central bank**
- In 1997 by Adam Back - computers solve hash functions to earn the currency - to ensure that the currency is scarce
- The process of solving functions (or puzzles) to earn something - “Proof-of-Work”
- Originally designed as a mechanism to limit **email spam**





EARLY ATTEMPTS AT CRYPTOCURRENCY – B-MONEY

- **In 1998, Wei Dai published "b-money - an anonymous, distributed electronic cash system" - money impossible to regulate**
- Requires a specified amount of computational work (aka Proof-of-Work)
- The work done verified by the community who update a collective ledger book
- The worker is awarded funds for their effort
- Exchange of funds is accomplished by collective bookkeeping and authenticated with cryptographic hashes.
- Contracts are enforced through the broadcast and signing of transactions with digital signatures

- Relationship with Satoshi Nakamoto
  - ✓ Wei Dai and Adam Back - first two people contacted by Satoshi Nakamoto as he was developing Bitcoin in 2008
  - ✓ b-money was referenced in Bitcoin whitepaper
  - ✓ The smallest unit of Ether (cryptocurrency of the Ethereum) is the **wei**

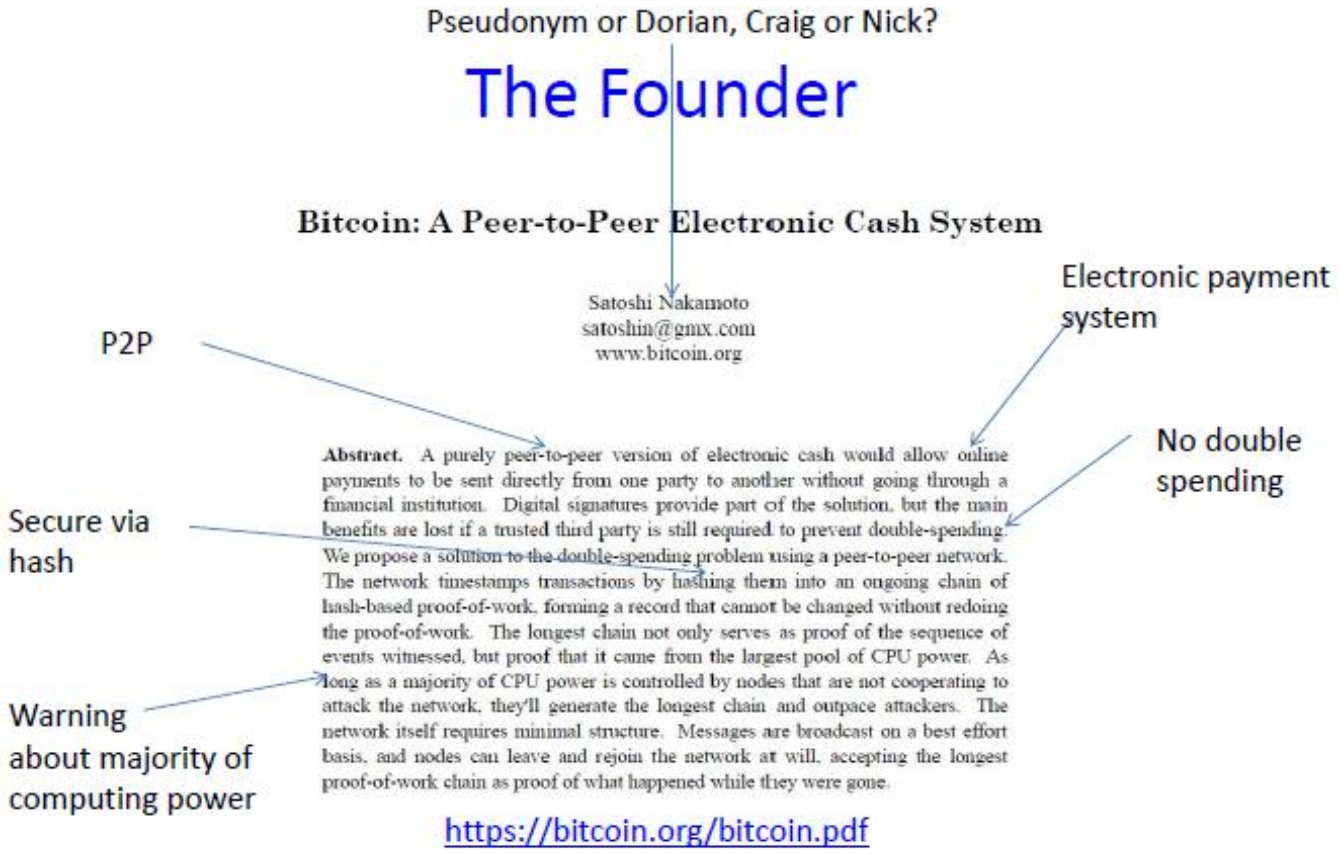
SATOSHI NAKAMOTO – 2008: BITCOIN WHITEPAPER

- Satoshi Nakamoto: anonymous creator of Bitcoin, wrote the white paper
- Do we need trust? - “electronic payment system based on cryptographic proof instead of trust”
- Solution to distributed consensus: Proof-of-Work, “one-CPU-one-vote”

2009-2010:
The early development of Bitcoin

SATOSHI NAKAMOTO – 2008: BITCOIN WHITEPAPER

- An Open Source Project, with developer mailing list and github repositories
- Satoshi remained a visible member until Dec. 2010 before disappearing
- The network was "started" January 3, 2009 with the Genesis Block
- Bitcoin v0.1 was released January 9, 2009



Bitcoin: The First Cryptocurrency

- Genesis block mined Jan 3, 2009
- The coinbase of the genesis block references a story in the Times of London newspaper involving the Chancellor bailing out banks, pointing to Bitcoin's libertarian, anti-financial establishment roots
- First bitcoin transaction on Jan 12, 2009 with Hal Finney

Block 0

Short link: http://blockexplorer.com/b/0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Time: 2009-01-03 18:15:05

Difficulty: 1 ("Bits": 1d00ffff)

Transactions: 1

Total BTC: 50

Size: 285 bytes

Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce: 2083236893

Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

Innovative Properties of Bitcoin

- **Open financial network + pseudonymous (no personal info)**
- **Borderless**
  - Remittances
- **Censorship-resistant and immutable**
  - Trust in math and code, not 3rd party
  - Irreversible payments – no charge back
- **Programmable money**
  - Good for machine to machine payments

Traits of Money	Gold	Fiat (US Dollar)	Crypto (Bitcoin)
Fungible *(Interchangeable)*	High	High	High
Non-Consumable	High	High	High
Portability	Moderate	High	High
Durable	High	Moderate	High
Highly Divisible	Moderate	Moderate	High
Secure *(Cannot be counterfeited)*	Moderate	Moderate	High
Easily Transactable	Low	High	High
Scarce *(Predictable Supply)*	Moderate	Low	High
Sovereign *(Government Issued)*	Low	High	Low
Decentralized	Low	Low	High
Smart *(Programmable)*	Low	Low	High

https://www.reddit.com/r/Bitcoin/comments/4b8ne0/rbitcoin_faq_newcomers_please_read/

The 500 Million Dollar Pizza

- Bitcoin gains value
- On May 22, 2010, Laszlo Hanyecz purchased $25 worth of pizza for 10,000 BTC
- World's first ever Bitcoin transaction for a tangible asset
- 10,000 BTC is now equivalent to $510,000,000
- **Bitcoin went from worthless internet money to something with real value**
- For most people, mining bitcoin was merely a hobby. This purchase validated the use of bitcoin for its original purpose as a cryptocurrency actually used for buying goods. So in a way, by trailblazing the currency's use, Laszlo is a hero to bitcoin enthusiasts.

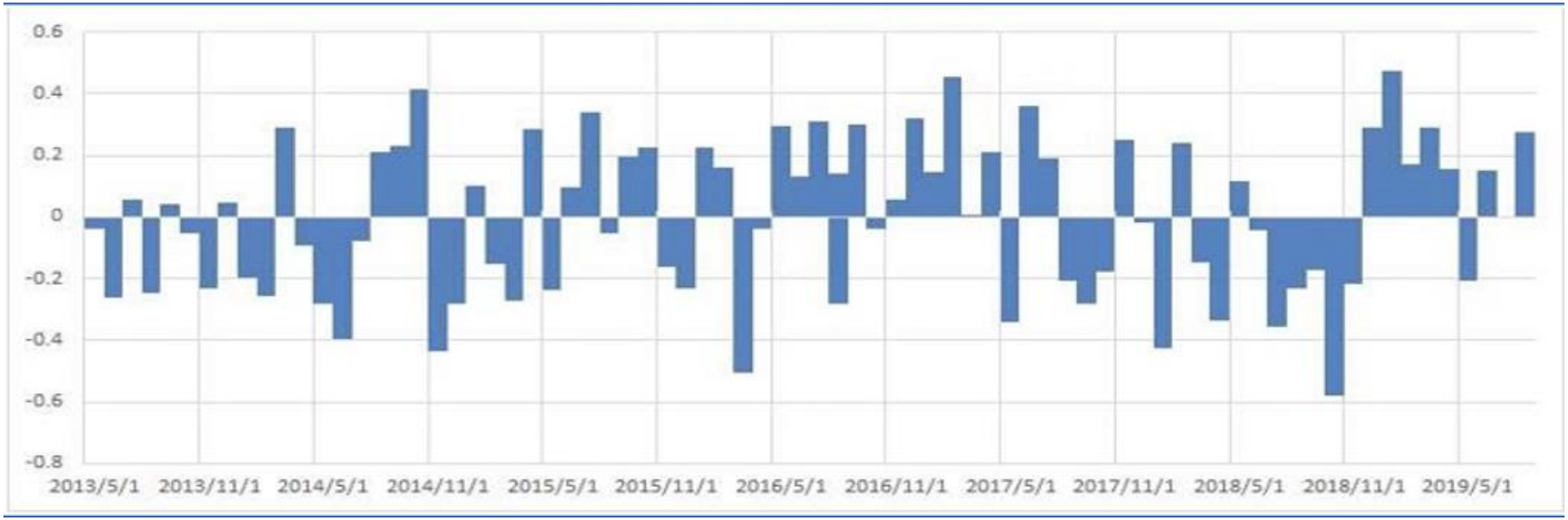
Use Cases of Bitcoin

https://cointelegraph.com/news/300-increase-in-bitcoin-buys-across-eu-as-greece-falls-into-arrears

- ❑ **Remittances: Sending money cheaply across borders**
  - Controversial
- ❑ **Digital goods: Irreversible trades**
  - Prevent chargeback for a good you can't recall
- ❑ **Machine to machine payments, IoT**
- ❑ **Currency for autonomous networks**
- ❑ **Micropayments: Ex. Pay per article**
- ❑ **Digital gold: Alternative store of value**

Is Bitcoin Digital Gold?

- Correlation between Gold & Bitcoin

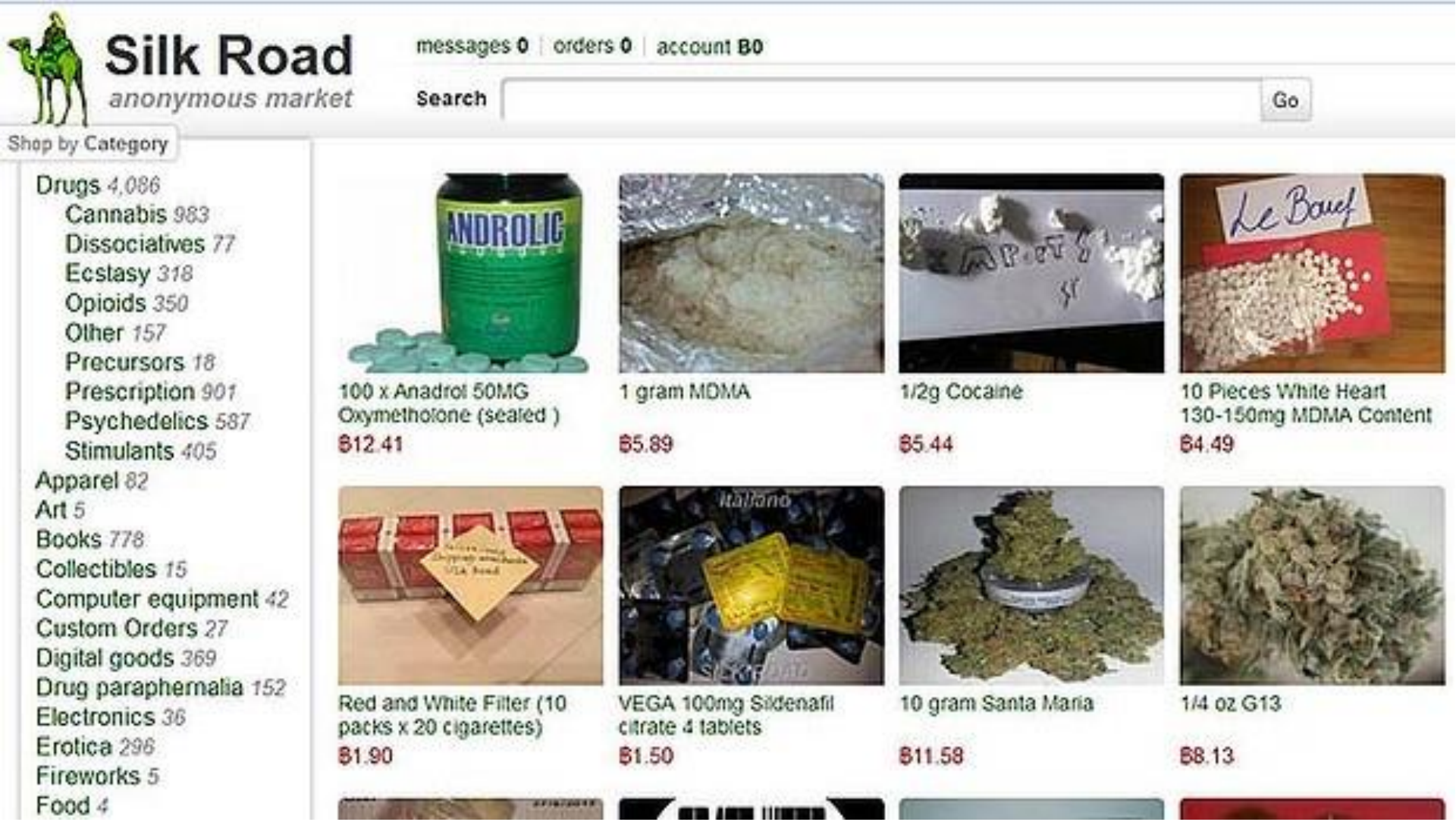


2010-2012: Early Bitcoin - Scandals, Hacks, Illegal activity

Bitcoin Theft - Mt. Gox

- 2010: Jed McCaleb creates Mt. Gox, the biggest online bitcoin exchange
- 2011: Mt. Gox suffered a significant breach of security that resulted in fraudulent trading - the site was shut down for 7 days
- The breach compromised the Mt. Gox database with a leak of the user table that contained user names, email addresses, and password hashes of 60,000 accounts
- 2014: Mt. Gox lost 744,408 bitcoins in a theft that went unnoticed for years
- 2014: Mt. Gox is handling 70% of transactions
- An admin account was accessed from which sell orders were issued for hundreds of thousands of Bitcoins, which forced the Mt. Gox price down from US$17.51 to US$0.01 per Bitcoin
- Eventually, Mt. Gox declared bankruptcy

Bitcoin Drug Scandal



Silk Road

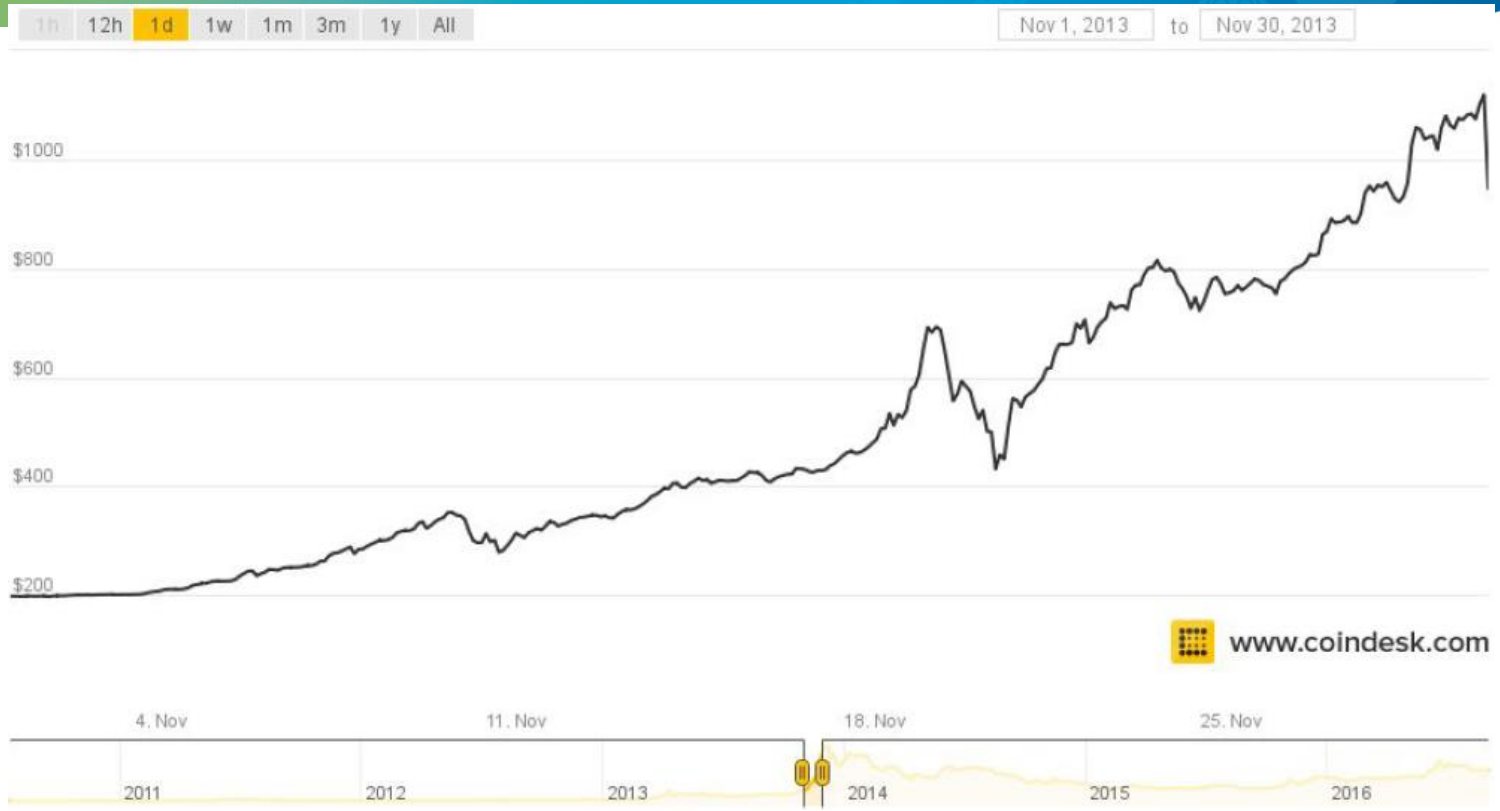
- February 2011: Silk Road opens as the anonymous “eBay of Drugs”, using Tor and Bitcoin.
- Drugs and black market goods become the use case for Bitcoin
- October 2013: FBI shut down Silk Road, seizing $3.6M dollars worth of bitcoin
- Ross Ulbricht, the founder of Silk Road, is serving a life sentence without possibility of parole

Recent Incident

- Quadrigacx: a Canadian cryptocurrency exchange
- Lost password to access the $136m worth of bitcoin, Litcoin and other cryptocurrencies from investors
- Mr. Gerald Cotton, who is in sole charge of handling deposits and payouts, died unexpectedly in India in Dec. 2018

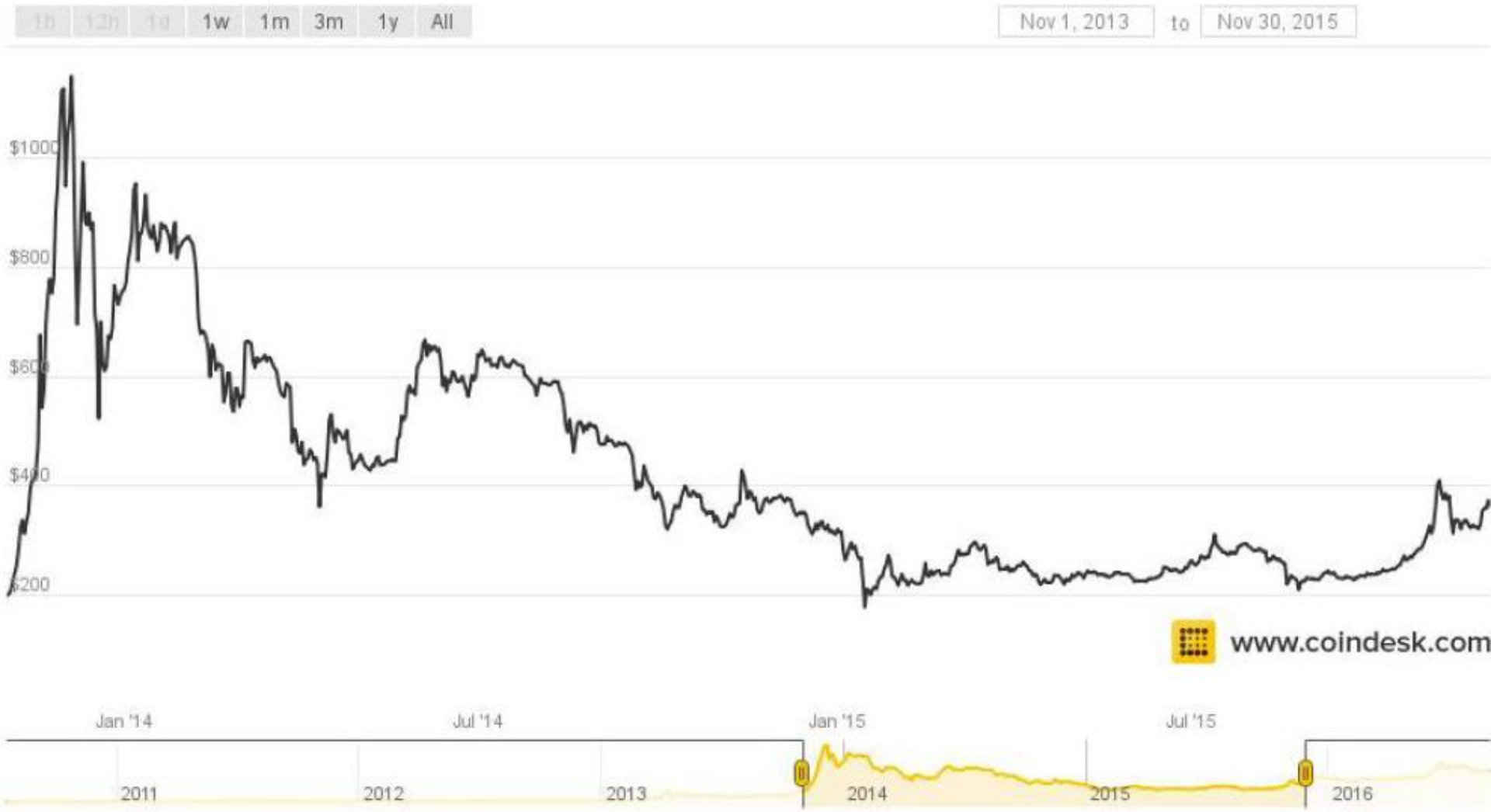
Boom & Bust Cycles

Hype



- ❑2014 Sep. Tim Draper: Bitcoin's Price Still Headed to $10k
- ❑Explosion of Altcoins: Litecoin, Zcash, Stellar, Peercoin, Dogecoin, DASH, Monero, Ripple
- ❑The Bitcoin Association would meet once a week, and so much news was happening that virtually every meeting was about the latest company that went bankrupt, the latest hack, the latest ponzi scheme

Bubble Burst




ICO
Initial Coin Offering

2013-2020:
Ethereum Rise Up

Ethereum Timeline

Ethereum is a Turing-complete protocol that uses its coin ether as “fuel”. Platform for decentralized applications + Smart Contracts.

History

- Late 2013: Ethereum described in whitepaper by Vitalik Buterin
- July and August 2014: Ethereum crowdsale
- July 30th 2015: Ethereum blockchain launched
- May 2016: Value of Ethereum tokens worth more than $1 billion

Huge potential for new governance models

- July 2016 : TheDAO rise and hack
- TheDAO - largest crowdfunded project built on Ethereum. Someone found an exploit in the DAO code to steal $120M worth of Ether
- Ethereum fork to a chain where the attacker didn't get funds

Ethereum Up and Down

- **Regulatory Circumstances:**
  - Securities and Exchange Commission would ruling on securities

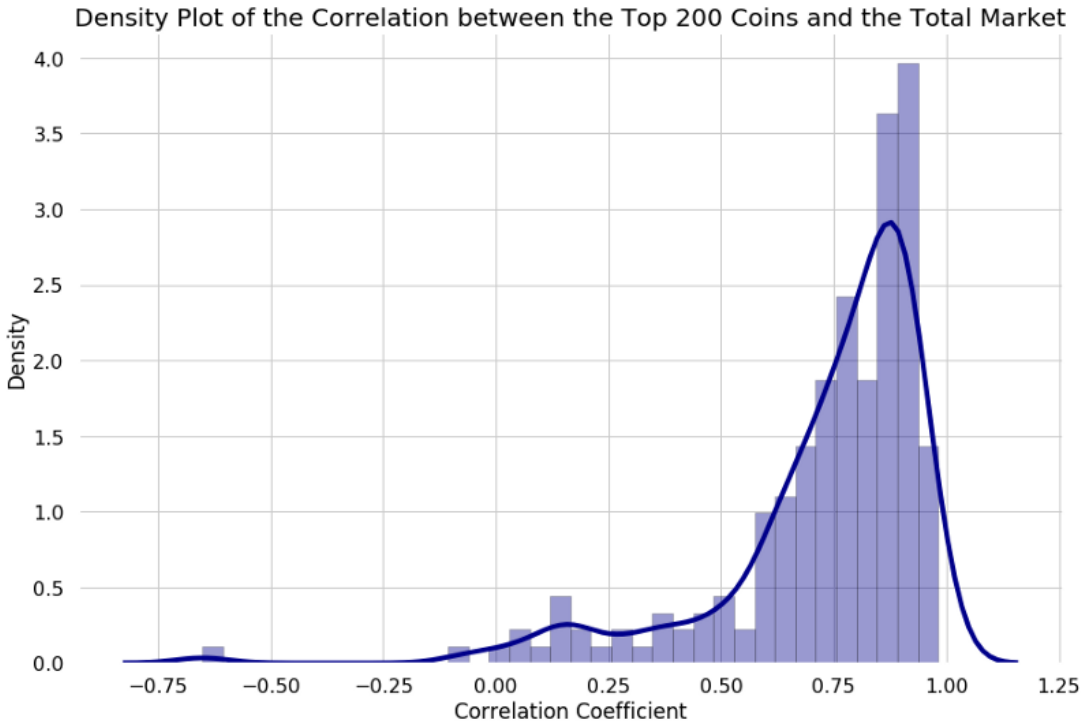
- **Economic Circumstances:**
  - Exchange Traded Funds ruling
  - ICOs (Initial Coin Offerings)
  - Venture Capital funding for crypto companies

- **2020 DeFi :**
  - Comes the many defi innovations

Initial Coin Offering

- **ICO – a form of crowd-funding where a company offers new digital tokens in exchange for cryptocurrencies such as Bitcoin, Ether, or fiat currency**
- **Three types of tokens:**
  - Cryptocurrencies
  - Utility tokens – future access to product or service
  - Security tokens – ownership rights, subject to regulations
- **Risk of ICO**
  - Lack of investor protection
  - Market risks (volatility) – speculative investment
  - Susceptibility of being hacked
  - Risks of money laundering and terrorist activities
- **Benefits of ICO**
  - Fund raising mechanism – whether blockchain is necessary
  - Synergy with VCs
  - Liquidity – 24/7, dry period

Many Cryptocurrencies Follow the Market



- **75% of the top 200 coins have a correlation of 0.67 or higher.**
- **50% of the top 200 coins have a correlation of 0.80 or higher.**

How Cryptocurrencies Correlated to Each Other

	bitcoin	ethereum	ripple	bitcoin-cash	eos	litecoin	stellar	cardano	iota	tron	tether	neo	dash	monero	binance-coin	nem	vechain	ethereum-classic	qtum	omisego
bitcoin	1	0.91	0.82	0.87	0.47	0.96	0.81	0.67	0.93	0.43	0.76	0.82	0.96	0.97	0.42	0.84	0.045	0.91	0.79	0.73
ethereum	0.91	1	0.89	0.76	0.68	0.93	0.93	0.89	0.76	0.73	0.84	0.95	0.9	0.95	0.7	0.88	0.66	0.92	0.83	0.89
ripple	0.82	0.89	1	0.76	0.53	0.86	0.91	0.95	0.73	0.81	0.7	0.83	0.86	0.89	0.61	0.94	0.39	0.81	0.91	0.81
bitcoin-cash	0.87	0.76	0.76	1	0.46	0.84	0.67	0.75	0.87	0.54	0.33	0.6	0.93	0.88	0.44	0.8	0.13	0.84	0.88	0.74
eos	0.47	0.68	0.53	0.46	1	0.57	0.78	0.43	0.51	0.71	0.85	0.61	0.31	0.57	0.9	0.33	0.78	0.37	0.46	0.62
litecoin	0.96	0.93	0.86	0.84	0.57	1	0.87	0.76	0.88	0.58	0.81	0.87	0.94	0.98	0.56	0.85	0.38	0.91	0.85	0.82
stellar	0.81	0.93	0.91	0.67	0.78	0.87	1	0.9	0.71	0.86	0.86	0.93	0.79	0.9	0.82	0.83	0.76	0.77	0.78	0.85
cardano	0.67	0.89	0.95	0.75	0.43	0.76	0.9	1	0.72	0.81	0.3	0.78	0.76	0.85	0.53	0.94	0.44	0.75	0.91	0.88
iota	0.93	0.76	0.73	0.87	0.51	0.88	0.71	0.72	1	0.51	0.44	0.64	0.9	0.88	0.45	0.79	0.14	0.81	0.81	0.72
tron	0.43	0.73	0.81	0.54	0.71	0.58	0.86	0.81	0.51	1	0.56	0.6	0.42	0.63	0.78	0.67	0.6	0.46	0.67	0.76
tether	0.76	0.84	0.7	0.33	0.85	0.81	0.86	0.3	0.44	0.56	1	0.82	0.66	0.81	0.88	0.57	0.87	0.69	0.39	0.58
neo	0.82	0.95	0.83	0.6	0.61	0.87	0.93	0.78	0.64	0.6	0.82	1	0.81	0.91	0.64	0.79	0.72	0.82	0.73	0.85
dash	0.96	0.9	0.86	0.93	0.31	0.94	0.79	0.76	0.9	0.42	0.66	0.81	1	0.96	0.28	0.91	-0.0013	0.92	0.89	0.74
monero	0.97	0.95	0.89	0.88	0.57	0.98	0.9	0.85	0.88	0.63	0.81	0.91	0.96	1	0.58	0.88	0.39	0.91	0.88	0.89
binance-coin	0.42	0.7	0.61	0.44	0.9	0.56	0.82	0.53	0.45	0.78	0.88	0.64	0.28	0.58	1	0.4	0.78	0.36	0.5	0.66
nem	0.84	0.88	0.94	0.8	0.33	0.85	0.83	0.94	0.79	0.67	0.57	0.79	0.91	0.88	0.4	1	0.17	0.84	0.92	0.74
vechain	0.045	0.66	0.39	0.13	0.78	0.38	0.76	0.44	0.14	0.6	0.87	0.72	-0.0013	0.39	0.78	0.17	1	0.27	0.25	0.59
ethereum-classic	0.91	0.92	0.81	0.84	0.37	0.91	0.77	0.75	0.81	0.46	0.69	0.82	0.92	0.91	0.36	0.84	0.27	1	0.81	0.76
qtum	0.79	0.83	0.91	0.88	0.46	0.85	0.78	0.91	0.81	0.67	0.39	0.73	0.89	0.88	0.5	0.92	0.25	0.81	1	0.81
omisego	0.73	0.89	0.81	0.74	0.62	0.82	0.85	0.88	0.72	0.76	0.58	0.85	0.74	0.89	0.66	0.74	0.59	0.76	0.81	1

Cryptocurrencies Concept Classes

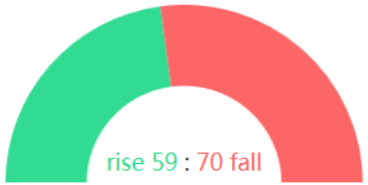
Cryptocurrency Market Cap : $126.9B Volume : $4.862B	58 : 76	-0.80%
Financial Services Market Cap : $16.54B Volume : $442.5M	59 : 70	-1.51%
Public Chain Market Cap : $147.7B Volume : $7.897B	18 : 46	-0.52%
Game Market Cap : $417.1M Volume : $16.21M	21 : 35	+0.46%
Payment and Settlement Market Cap : $15.75B Volume : $402.6M	19 : 29	-1.41%
Content Copyright Market Cap : $466.3M Volume : $36.32M	23 : 25	-1.25%

Financial Services

Ratio = 59 : 70 -1.51%

Market Cap : $16.54B

Volume(24h) : $442.5M



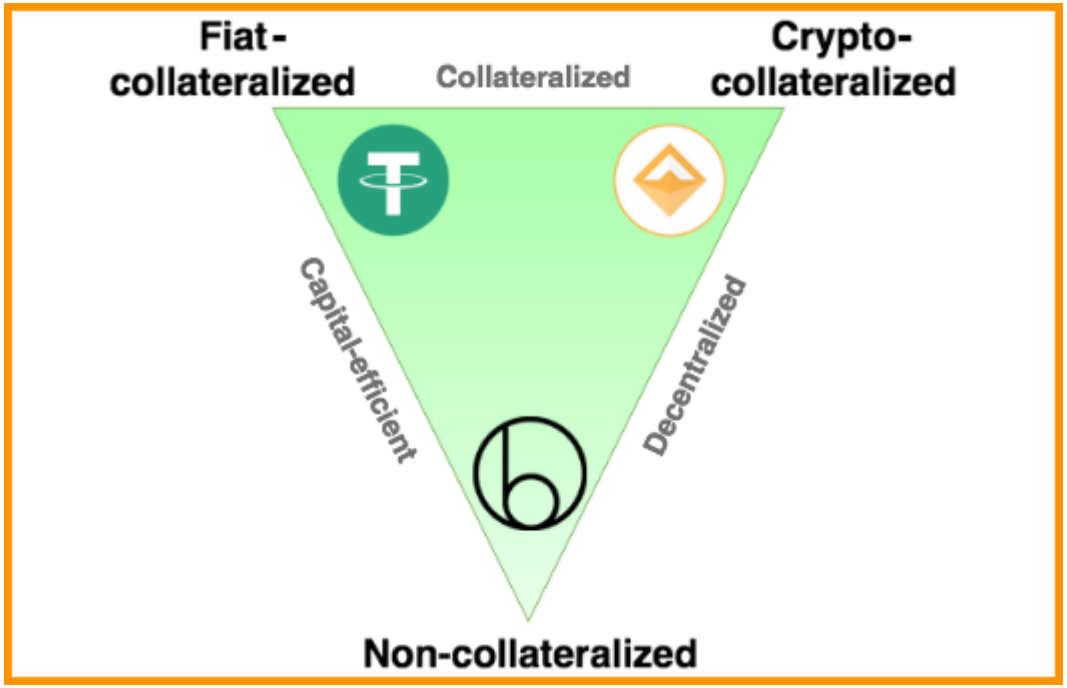
24hour	Market Cap	Price	Change
XRP-XRP	$11B	$0.277	-1.45%
XLM-Stellar	$3.772B	$0.201	-3.88%
OMG-OmiseGO	$484.7M	$3.454	+1.07%
NPXS-Pundi X	$154.8M	$0.001	-7.09%
PPT-Populous	$118.6M	$3.206	-5.95%
MCO-MCO	$74.81M	$4.232	-5.70%
PAY-TenX	$69.35M	$0.634	-1.12%
KNC-Kyber Network	$49.85M	$0.374	+0.53%
ETN-Electroneum	$43.13M	$0.005	-0.31%
POLY-Polymath	$39.3M	$0.139	-4.99%
GVT-Genesis Vision	$35.75M	$8.514	-1.89%

https://www.tokenclub.com

Stablecoins in The Crypto Market

- Stablecoins are cryptocurrencies pegged (or linked) to real-world assets such as fiat to keep their value stable

Stablecoins in The Crypto Market



- Fiat-Collateralized Stablecoins: backed by fiat reserves such as USD (like treasure debt). E.g. Tether (USDT), TrueCoin, TrueUSD
- Crypto-Collateralized Stablecoins: backed by other reserves of crypto currencies. a bucket of cryptocurrencies account for the price stability (like ABS), e.g. MakerDao, Bitshares, Havven
- Non-Collateralized Stablecoins: supply is algorithmically governed by its smart contracts which keeps expanding or contracting to keep the price stable (like central bank – algo bank), e.g. Basecoin, Nubits, Caborn

Stablecoin Shortcomings

- Stablecoin's supply manipulation and crypto market manipulation e.g. USDT
- They can run into a problem of not being backed by any assets at all
- Tends to be more centralized as one company controls it.
- They also historically dipped or risen up to (+/-) 10%
- All three types run into blockchain oracle problem - digital world needs to "know" about the physical world

US-Audited Stablecoins

- Debut on 10 Sept. 2018, two U.S. regulated stablecoins launched: Gemini Dollar (GUSD) and Paxos Standard (PAX)
- World's first-ever regulated stablecoins, approved and regulated by the New York State Department of Financial Services (NYDFS)
- Fully collateralized 1:1 by the U.S. dollar (in FDIC-insured U.S. bank accounts), which means tokens in circulation exactly match dollars in reserve
- USD balances audited externally on a monthly basis
- Built on Ethereum ERC-20 standard, so can be stored in any Ethereum wallet
- Use for hedging against the volatility of other cryptoassets, settling transactions outside of banking hours, or eliminating cross-border transaction fees
- Subject to the stringent requirements of the NYDFS:
  - implement, monitor and update effective risk-based controls, e.g. AML, illegal activity, market manipulation, or other similar misconduct
  - warn consumers if stablecoins may be forfeited or affected for illegal activities

ERC20 in a Nutshell

- The ERC-20 defines a common list of rules for all Ethereum tokens to follow, meaning that this particular token empowers developers of all types to accurately predict how new tokens will function within the larger Ethereum system

```
contract ERC20Interface {
   function totalSupply() constant returns (uint256 totalSupply);
   function balanceOf(address _owner) constant returns (uint256 balance);
   function transfer(address _to, uint256 _value) returns (bool success);
   function transferFrom(address _from, address _to, uint256 _value) returns (bool success);
   function approve(address _spender, uint256 _value) returns (bool success);
   function allowance(address _owner, address _spender) constant returns (uint256 remaining);
   event Transfer(address indexed _from, address indexed _to, uint256 _value);
   event Approval(address indexed _owner, address indexed _spender, uint256 _value);
}
```

Non-Fungible Token – ERC-721

- Non-Fungible Tokens (NFT) is to identify something in a unique way. It is used for collectible items, access keys, lottery tickets, numbered seats for concerts and sports matches
- All NFTs have a uint256 variable called tokenId, so for any ERC-721 Contract, the pair "contract address, uint256 tokenId" must be globally unique. Once deployed, it will be responsible to keep track of the created tokens on Ethereum.

Methods

```
1        function balanceOf(address _owner) external view returns (uint256);
2        function ownerOf(uint256 _tokenId) external view returns (address);
3        function safeTransferFrom(address _from, address _to, uint256
    _tokenId, bytes data) external payable;
4        function safeTransferFrom(address _from, address _to, uint256
    _tokenId) external payable;
5        function transferFrom(address _from, address _to, uint256 _tokenId)
    external payable;
6        function approve(address _approved, uint256 _tokenId) external
    payable;
7        function setApprovalForAll(address _operator, bool _approved)
    external;
8        function getApproved(uint256 _tokenId) external view returns
    (address);
9        function isApprovedForAll(address _owner, address _operator)
    external view returns (bool);
```

```
1        event Transfer(address indexed _from, address indexed _to, uint256
    indexed _tokenId);
2        event Approval(address indexed _owner, address indexed _approved,
    uint256 indexed _tokenId);
3        event ApprovalForAll(address indexed _owner, address indexed
    _operator, bool _approved);
```

Events

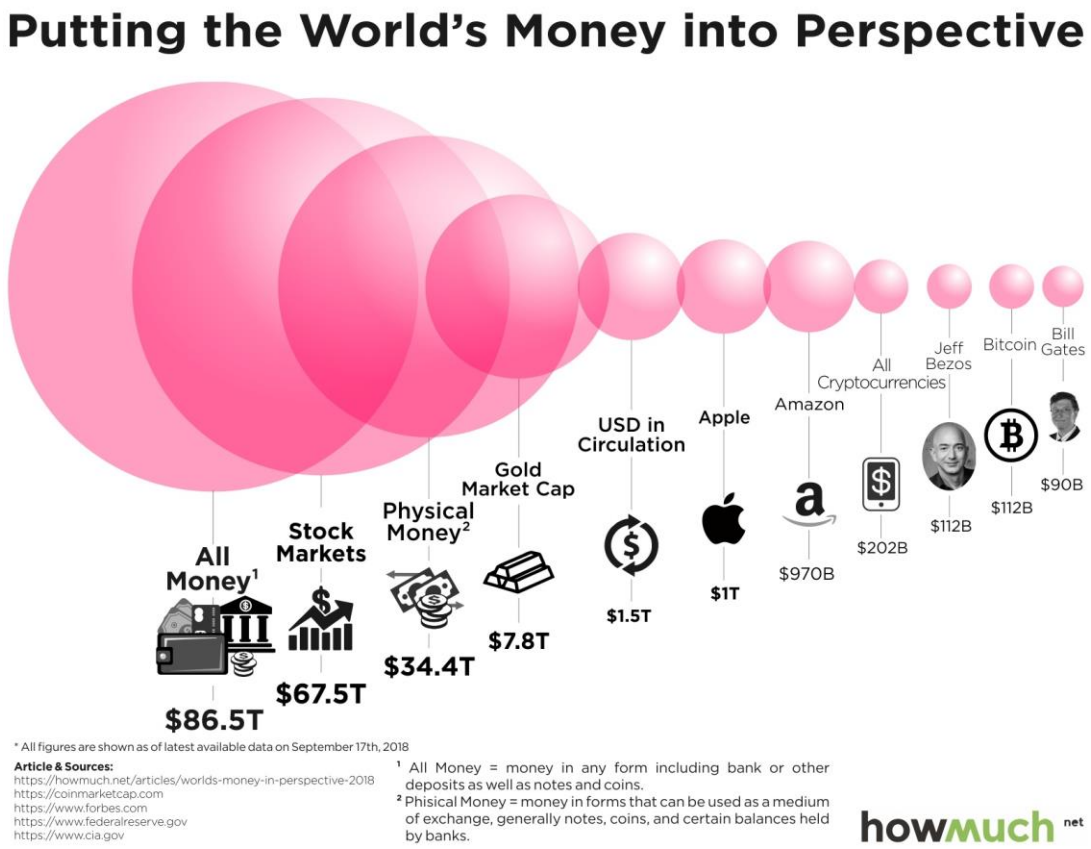
Hybrid Token – Security Token Standard ERC-1400 - Tokenization of Assets

- Purpose: being compliant with financial regulators
- Security tokens are designed to represent complete or fractional ownership in assets.
- Can restrict its usage based on identity, jurisdiction and asset category:
  - regulate holding period in a wallet
  - whitelist all potential buyers/sellers
  - KYC wallets and restrict sales when KYC expired
  - put a threshold on transactions
  - limit the number of tokens per wallet
- ERC-1594: Core Security Token Standard - support off-chain injection of data into transfers, issuance, redemption, and to check the validity of a transfer and on-chain functionality that could determine whether a transfer will succeed
- Token Issuance and Redemption
- ERC-1410: Partially Fungible Tokens - attaching of metadata
- ERC-1643: Document Management Standard - attaching of doc to security token contracts
- ERC-1644: Controller Operations - allows a party, e.g., an issuer or regulator acting as a controller, who can force the transfer of security tokens between addresses

Project: Tokenization of Tesla & Components

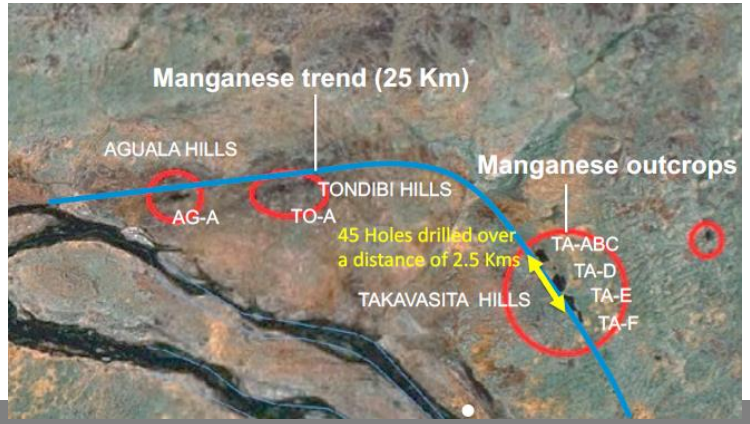
- 1 Bitcoin = 1 Tesla ?

- How about other components? … supply chain … whole economy – what portion of GDP



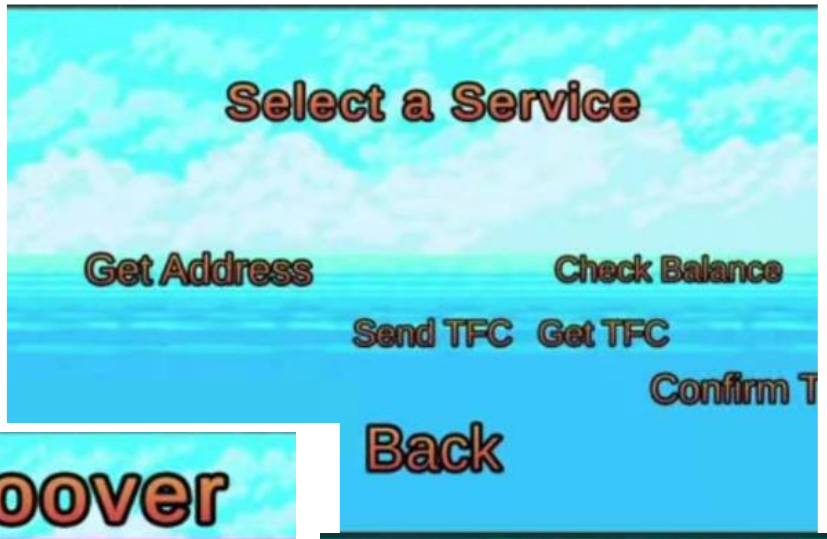
Project: Tokenization of High-Grade Manganese

- Manganese is a free element in nature and over 90% of manganese is used to make steel. manganese is used to make batteries for electric vehicle market
- High grade manganese market is opaque with only 5 producers controlling over 90% of the global market. There is no trading platform enabling small investors to buy manganese or “Black Gold” as they can buy gold, silver, platinum and other metal commodities or, food supplies like soybean.
- This Token offering is intended to be the beginning of creating broad participant trading in “Black Gold. Large buyers will trade the price down and large suppliers will trade the price up. The small investor can now be part of the trading, just like buying and selling gold.
- Unit Being Offered: Each Asset based Token (“Token”) is equivalent to one Dry Metric Ton Unit (“DMTU”) of 44% grade manganese oxide
- Token Price: Each Token sold is discounted by 25% to market value
- Size of Offering: Up to 150,000 Tokens



Project: NFT – Game Items

- Project: Game engine, back-end API, token issurances



Project: NFT – Game Items API

```
* Registering an Account
Request Method: POST
Path: [TFC_URI]/account
Response Body:
{
    int code,
    struct data {
        string address,
        string pubkeyHex,
        string privkeyHex
    },
    string msg
}

* Checking the Balance
Request Method: GET
Path: [TFC_URI]/balance/[ADDRESS]
Response Body:
{
    int code,
    struct data {
        string activeTFC,
        string lockedTFC
    },
    string msg
}
```

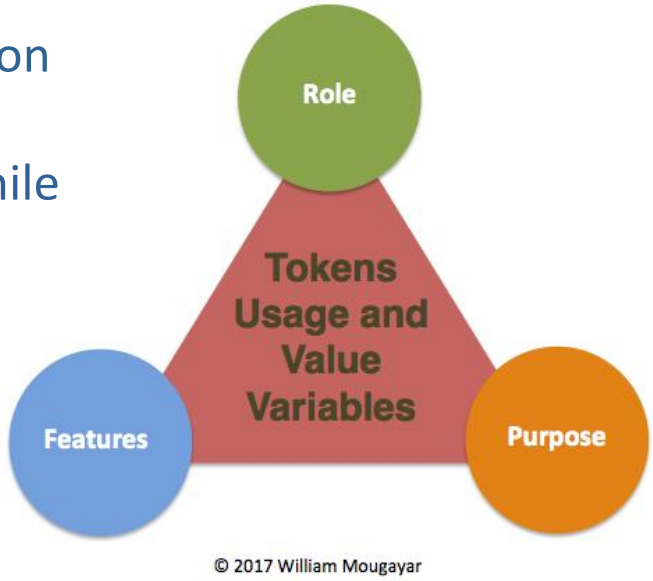
```
* Initiating a Transfer Request
Request Method: POST
Path: [TFC_URI]/transferTx
Content Type: application/json
Request Body:
{
    string from,
    string to,
    int amount,
    string auxdata,
    int carryFee
}
Response Body:
{
    int code,
    struct data {
        struct tx {
            string id,
            int timestamp,
            string from,
            int accountNonce,
            string to,
            int amount,
            int carryFee,
            int txType,
            string payload,
            string signature
        }
    },
    string msg
}
```

```
* Confirmation of Transaction
Request Method: POST
Path: [TFC_URI]/signedTx
Content Type: application/json
Request Body:
{
    string id,
    int timestamp,
    string from,
    int accountNonce,
    string to,
    int amount,
    int carryFee,
    int txType,
    string payload,
    string signature
}
Response Body:
{
    int code,
    struct data,
    string msg
}

* Verification of Transaction
Request Method: POST
Path: [TFC_URI]/verification
Content Type: application/json
Request Body:
{
    string from,
    string to,
    string amount,
    string txid
}
Response Body:
{
    int code,
    string msg
}
```

Tokenomics – Token Usage, Utility and Value

- **Cryptoeconomics -** the mechanics and specifics of token distribution, according to a given sale and ownership structure **– about token sale**
- **Tokenomics –** A unit of value (token) an organization creates to self-govern its business model, and empower its users to interact with its products, while facilitating the distribution and sharing of rewards and benefits to all of its stakeholders **– about business model**
- Key objective of a DAO is value creation or production, there needs to be a specific linkage between **user actions** and the **resulting effects** on the overall value to the organizations
- Usage without value linkage will backlash. A new DAO is like a startup. It requires a **product fit**, **business model realization** and **users**



A Guide to Crypto Tokens Usage and Value

ROLE	PURPOSE	FEATURES
RIGHT	Bootstrapping engagement	Product usage, Voting, Governance, Product Access, Contribution, Ownership
VALUE EXCHANGE	Economy creation	Work rewards, Selling something, Buying, Active/Passive work, Spending, Creating a product
TOLL	Skin in the game	Running smart contracts, Security deposit, Usage fees
FUNCTION	Enriching user experience	Joining a network, Connecting with users, Incentive for usage
CURRENCY	Frictionless transactions	Payment unit, Transaction unit
EARNINGS	Distributing benefits	Profit sharing, Benefits sharing, Inflation benefits

Assessing the Token Utility – Token to Market Fit

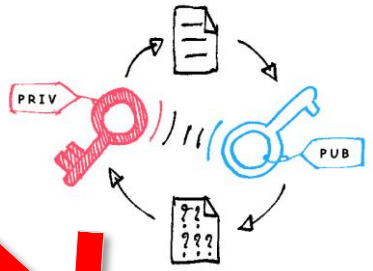
- ❑ Is the token tied to a product usage, i.e. exclusive access or interaction rights?
- ❑ Does it grant a governance action, like voting or other decision-making factor?
- ❑ Does it enable the user to contribute to a value-adding action?
- ❑ Does it grant an ownership of sorts, whether real or proxy to a value?
- ❑ Does it result in a monetizable reward based on an action by the user (active work)?
- ❑ Does it grant the user a value based on sharing or disclosing some data (passive work)?
- ❑ Is buying something part of the business model?
- ❑ Is selling something part of the business model?
- ❑ Can users create a new product or service?
- ❑ Is it required to run a smart contract or to fund an oracle?
- ❑ Is it required as a security deposit to secure some aspect of the blockchain's operation?
- ❑ Is it (or a derivative of it, like a stable coin or gas unit) used to pay for some usage?
- ❑ Is it required to join a network or other related entity?
- ❑ Does it enable a real connection between users?
- ❑ Is it given away or offered at a discount, as an incentive to encourage usage?
- ❑ Is it your principal payment unit, essentially functioning as an internal currency?
- ❑ Is it (or derivative of it) the principal accounting unit for all internal transactions?
- ❑ Does your blockchain autonomously distribute profits to token holders?
- ❑ Does your blockchain autonomously distribute other benefits to token holders?
- ❑ Is there a related benefit to your users, resulting from built-in currency inflation?

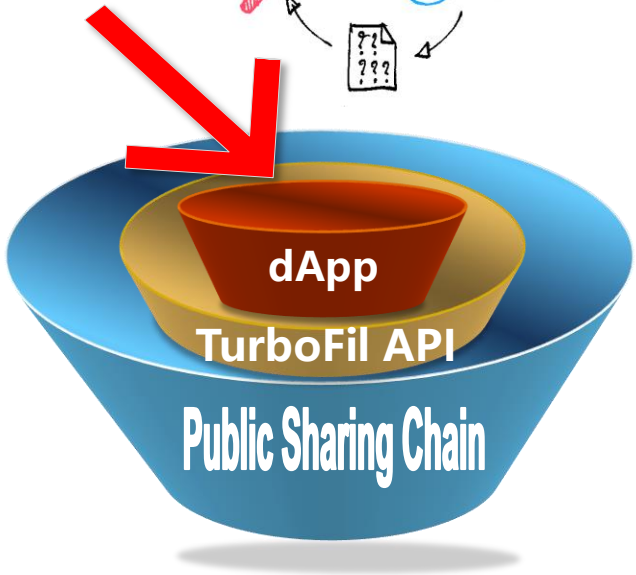
Crypto Market Players - Miners

How would you invest in crypto currencies/assets today?

- ❑ Buy
- ❑ Transfer
- ❑ Business
- ❑ Earn/work
- ❑ Mine (hardware)
- ❑ Project
- ❑ Crowd funding
- ❑ ICO
- ❑ STO

Every sales transaction is a crypto mining opportunity





Community e-commerce with Defi

❑Project Description:

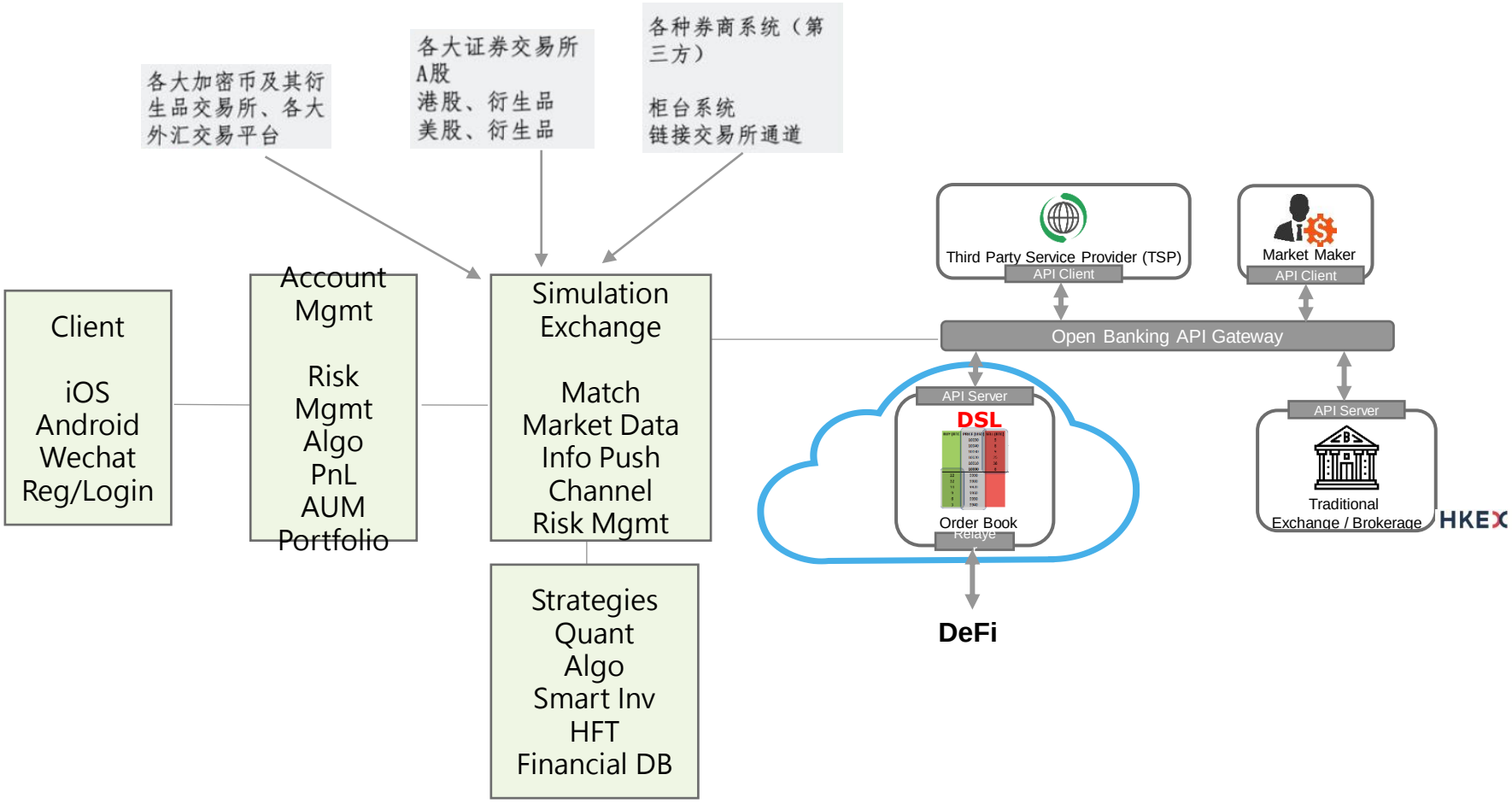
- ❖ The first-generation e-commerce giant such as Amazon revolutionized the cloud computing landscape.
- ❖ The new unicorn such as Pinduoduo explored the social commerce and big data to its full advantage.
- ❖ Defi and crypto technologies will further change the landscape of community e-commerce because every sales transaction is a crypto mining opportunity.
- ❖ This project will ride and materialize this upcoming trend.

❑Skills required: app programming, front end development, basic crypto knowledge;

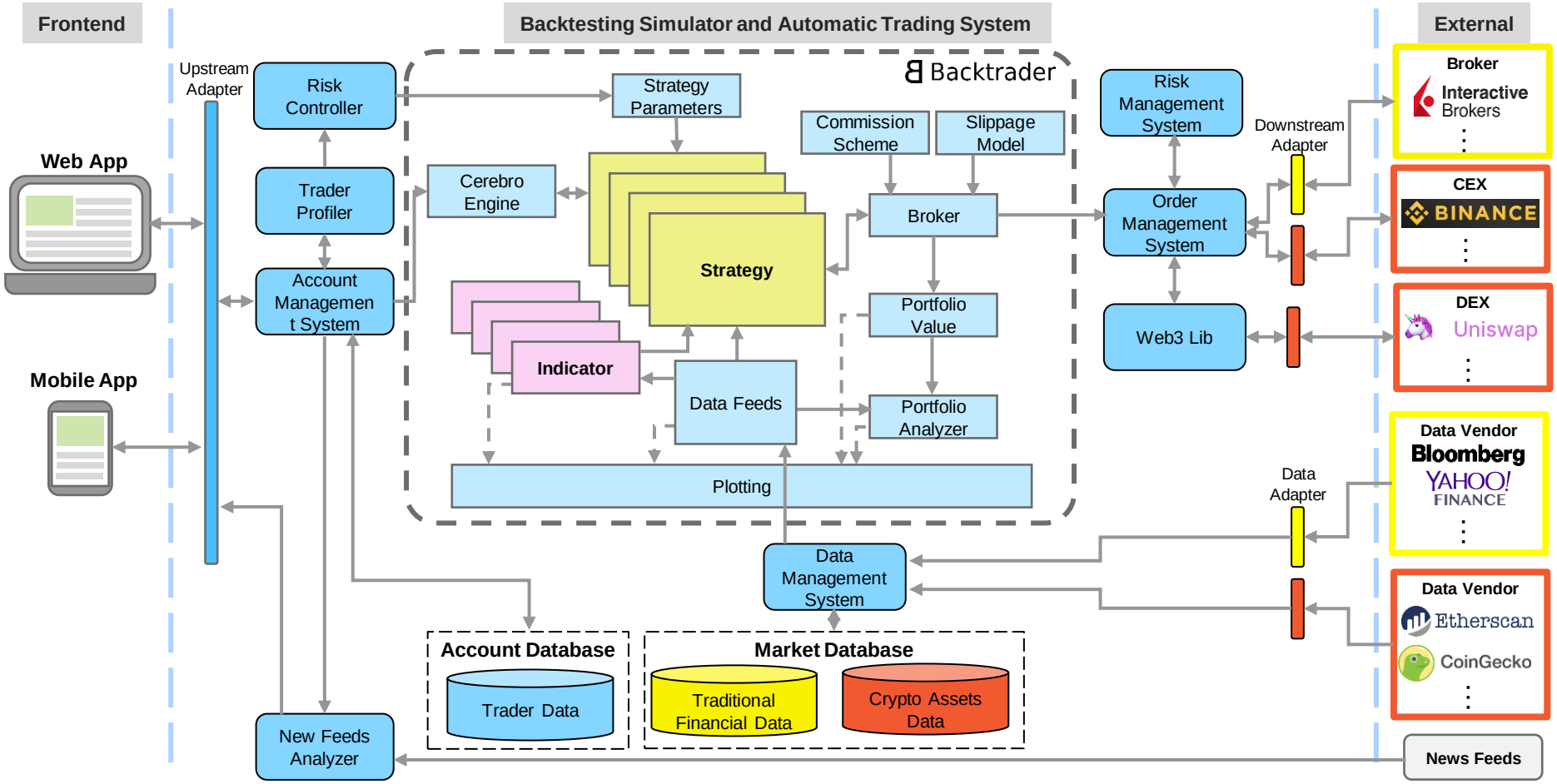
Course Project

- Tokenization – assets, e-commerce
- Token Apps – games, NFT
- DeFi – Quant investments
- Social network – video sharing, Super Star Ranking, prof. network
- Infra - DID (de-centralized ID) / DDNS (next class)
- 2B2C – SaaS, Virtual Assistant/cocoPDA

Project: Unified CeFi/DeFi Platform



Backtesting Simulator and Automatic Trading System, e.g. Filecoin



Project: Super Star Ranking

- Different platforms rank stars differently – bias, commercial purpose
- Build composite ranking from all sites, and let fans to vote against
- Popular sites:
  - https://weibo.com/ 30%
  - http://index.baidu.com/v2/rank/index.html?#/industryrank/star?tab=0 20%
  - Tiktok 15%
  - Wechat 12.5%
  - Kuaishou 10%
  - Taobao, jd, little red book, netease, QQ …. 2.5%*n