



Stable coins and DeFi: News from the Cryptocurrency Universe

Alexander Lipton
Sila & HUJI & MIT
Field Institute Quant Seminar
Webcast 30th September 2020



Money has been introduced by convention as a kind of substitute for need or demand; and this is why we call it money (*nomisma*), because its value is derived, not from nature, but from law (*nomos*), and can be altered or abolished at will.



Nicholas
Oresme,
De Moneta

When men first began to trade, or to purchase goods with money, the money had no stamp or image, but a quantity of silver or bronze was exchanged for meat and drink and was measured by weight. And since it was tiresome constantly to resort to the scales and difficult to determine the exact equivalent by weighing, and since the seller could not be certain of the metal offered or of its degree of purity, it was wisely ordained by the sages of that time that pieces of money should be made of a given metal and of definite weight and that they should be stamped with a design, known to everybody, to indicate the quality and true weight of the coin, so that suspicion should be averted and the value readily recognized.



1. It must not be changed in value except after ripe deliberation by the government authorities
2. One single place must be chosen for the minting of the money which must be minted in the name of the entire country and not in the name of a single city. ...
3. When the new currency is issued, the old currency must be de-monetized and withdrawn from circulation. ...
4. It is essential to have an inviolable and unchangeable rule to mint only 20 marks and no more from a pound of silver, deducting only the quantity of silver necessary to cover the expenses of coinage. ...
5. Too great a quantity of money must not be issued. ...
6. All the different kinds of coins should be issued at the same time. ...

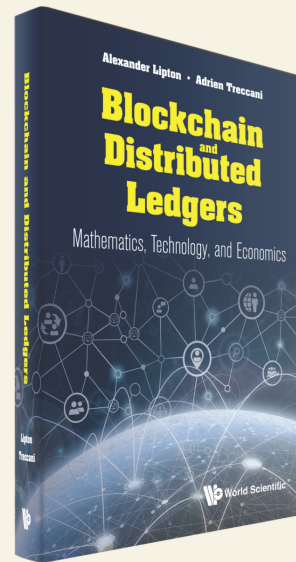
Main references

Blockchain and Distributed Ledgers

Mathematics, Technology, and Economics

by **Alexander Lipton** (Sila Money, USA & Hebrew University of Jerusalem, Israel)

Adrien Treccani (Metaco, Switzerland)



This textbook focuses on distributed ledger technology (DLT) and its potential impact on society at large. The book aims to offer a detailed and self-contained introduction to the founding principles behind DLT accessible to a well-educated but not necessarily mathematically-oriented audience. DLT, which became extremely popular over the last decade, allows solving many complicated problems arising in economics, banking, and finance, industry, trade, and other fields. DLT accomplishes these tasks by developing new mechanisms for distributed consensus, using advanced tools from cryptography, game theory, economics, finance, scientific computing, and others. DLT offers optimal and elegant solutions in many situations. However, to reap the ultimate benefits, one has to overcome some of its inherent limitations and use it judiciously. Not surprisingly, amid increasing applications of DLT, misconceptions are formed over its use, not least because numerous authors identify it with cryptocurrencies such as Bitcoin, Ethereum, Ripple, and their numerous extensions. This situation calls for an impartial assessment of the situation rooted in scientific reasoning, rather than speculation, enthusiastic naivete and personal attacks on one's opponents.

Blockchain and Distributed Ledgers: Mathematics, Technology, and Economics offers a detailed and self-contained introduction to DLT, blockchains, and cryptocurrencies. The book guides the reader through the development and building up of a distributed ledger suitable for one's interest. It covers the basics of cryptography and its applications to cryptocurrencies; provides historical examples of centralized cryptocurrencies; discusses theoretical foundations of decentralized cryptocurrencies, including game theory aspects and Byzantine fault-tolerant consensus; explains operational features of Bitcoin trading platform, including storage, mining, and wallets; covers alternative platforms, including Ethereum, Ripple, Stellar, Zcash, and others; defines smart contracts; covers potential financial and non-financial applications of decentralized ledgers with a detailed analysis of their pros and cons. This introductory text seeks to equip the reader with an ability to participate in the crypto economy meaningfully.

Readership: Students and professionals from quantitatively-oriented fields such as mathematics, computer science, finance, economics, banking, and supply chain management.

CONTENTS

- Background
- Money and the Financial System
- A Primer on Cryptocurrencies and Distributed Ledgers
- Essential Cryptographic Tools
- How to Build Your Own Cryptocurrency? — Epsiloncoin
- Deep-Dive into Bitcoin
- Going Further with Statefulness, Turing-Completeness
- Other Cryptocurrencies
- Cryptocurrencies Management
- Cryptocurrencies and Quantitative Finance
- Central Bank Issued Digital Currencies and Stable Coins
- Case Studies of Financial and Non-Financial Applications Beyond Cryptocurrencies
- DLT and Regulations
- Current Research
- Future of DLT and Cryptocurrencies



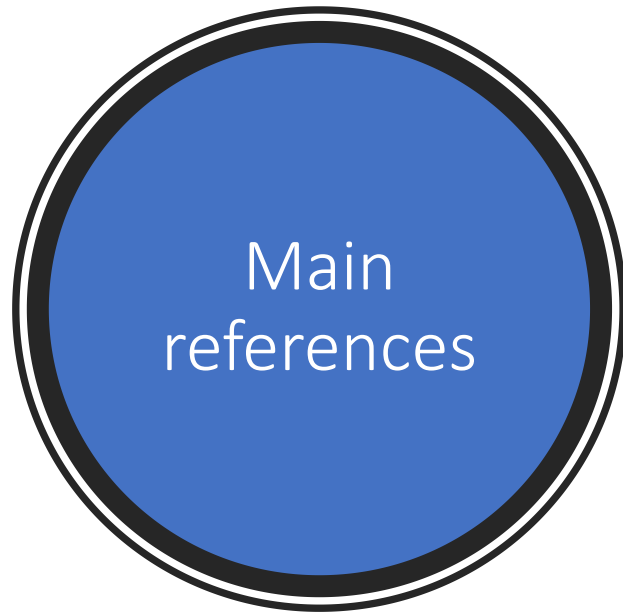
450pp | Pub Date: March 2021

Paperback | US\$45 / £40 | 978-981-122-152-1

Hardcover | US\$95 / £85 | 978-981-122-151-4

Order your copy at <https://doi.org/10.1142/11857>





BUILDING THE NEW ECONOMY

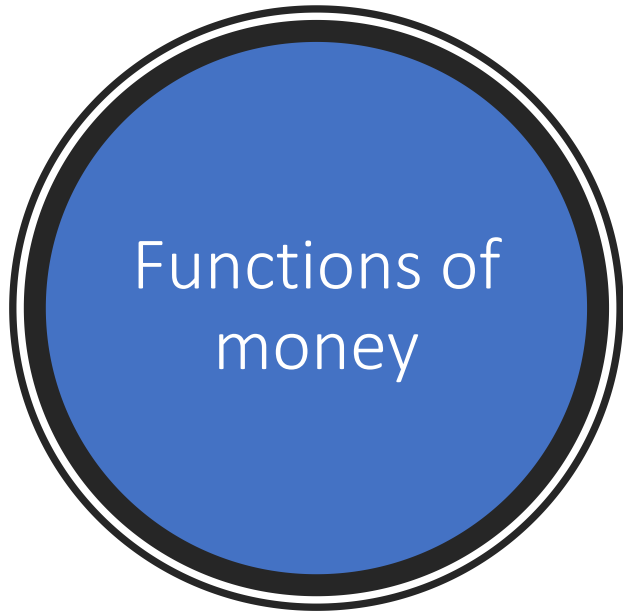
Alex Pentland
Massachusetts Institute of Technology

Alexander Lipton
Massachusetts Institute of Technology

Thomas Hardjono
Massachusetts Institute of Technology

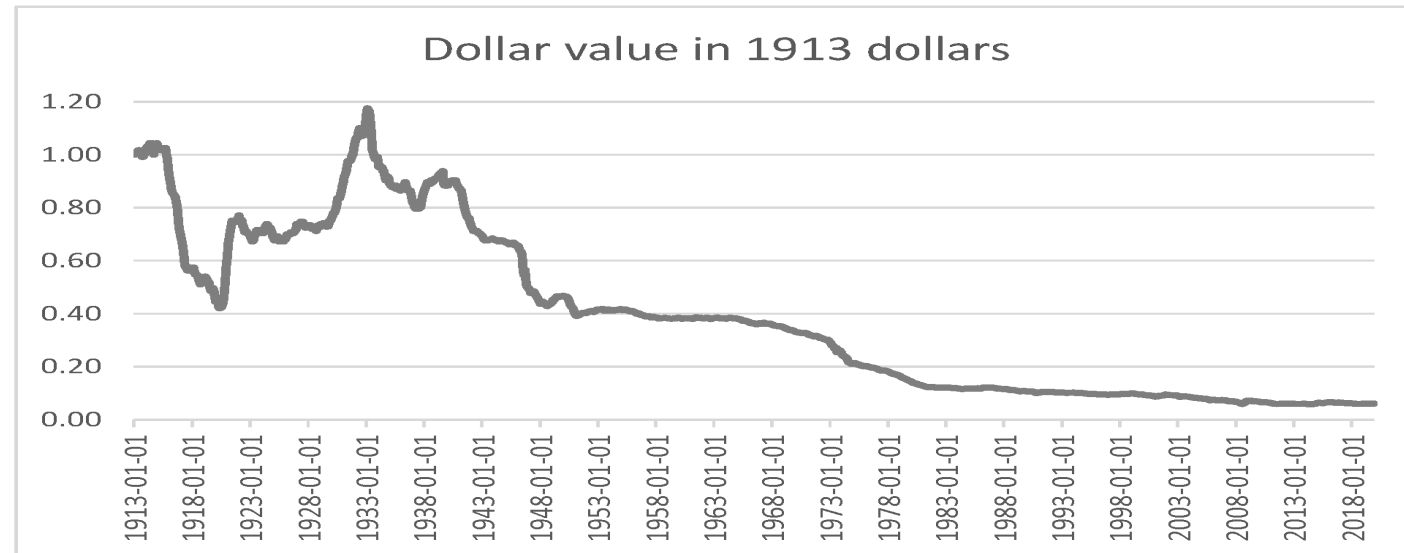
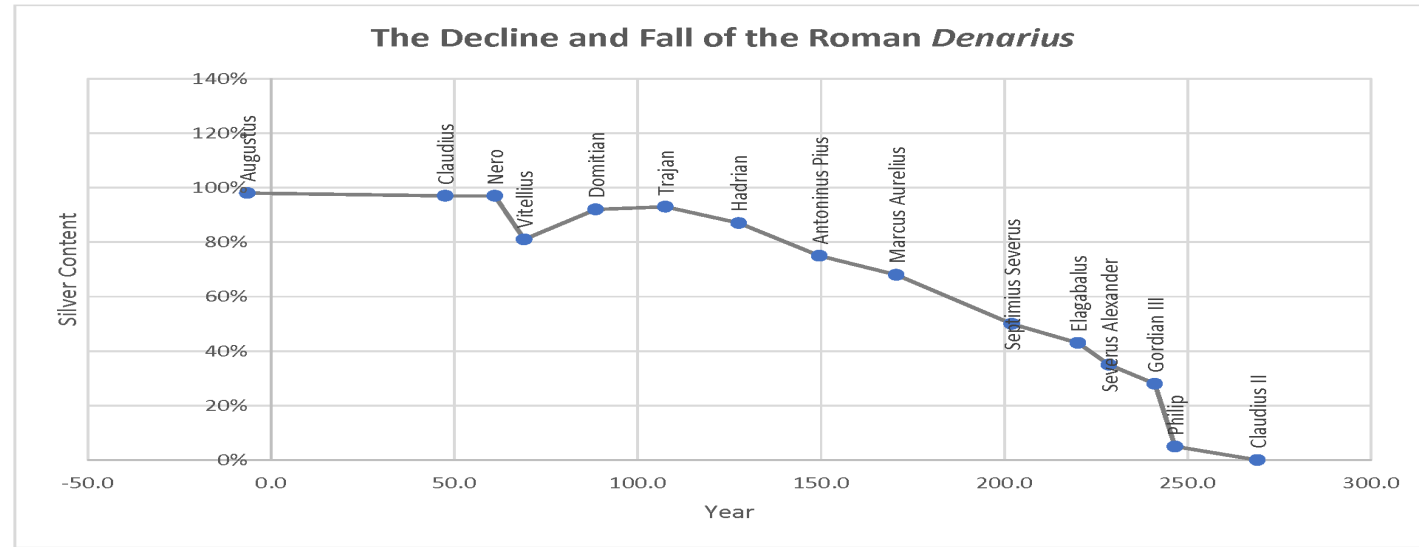


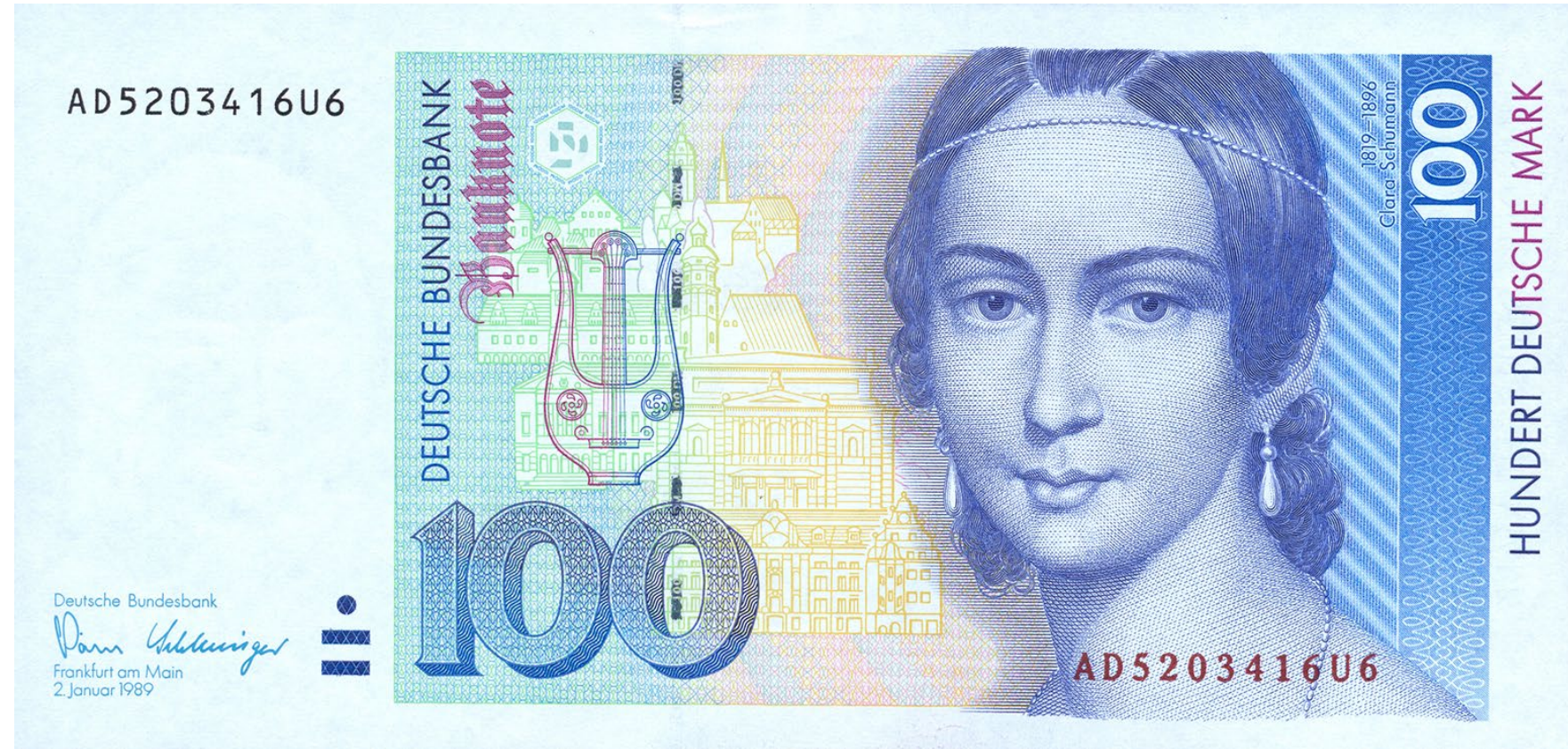
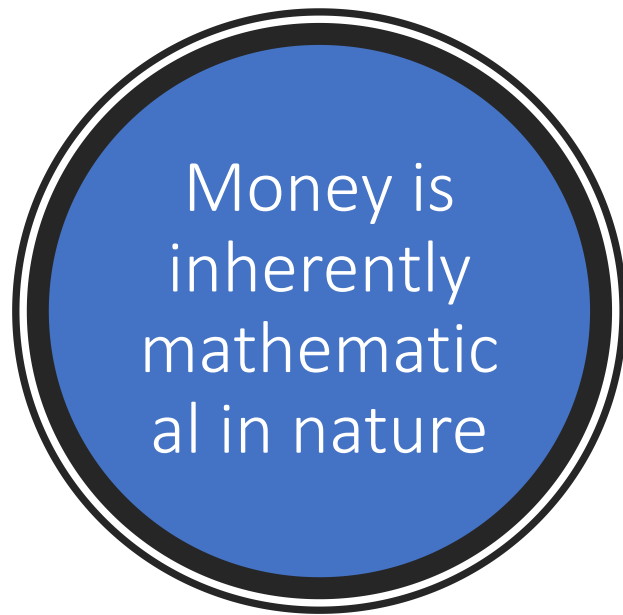
MIT PRESS



- money is a medium of exchange
- money is a means of payments of taxes
- money is a means of payments in general
- money is a store of value
- money is a unit of account
- money is a perpetual call option for acquiring goods and services and discharging one's obligations

Yet, money
is always
unstable





Source: Wikipedia, Yavar Parhizi.



A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

0	1	2	3	4	5	6	7	8	9
1	5	7	6	2	8	3	0	9	4

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

Source: Pavel Tlustý, Marek Šulista, The Algorithm Used for Numbering German Banknotes: What Counterfeiters Might Not Have Known. The International Scientific Conference INPROFORUM 2016.



Orig #	digits	#	$h(n,p)$	sum
A	0	1	1	1
D	1	2	8	9
5	5	3	4	5
2	2	4	5	0
0	0	5	4	4
3	3	6	3	2
4	4	7	9	6
1	1	8	1	5
6	6	9	3	7
U	7	10	1	6
6	6		6	0

Last digit

6

Source: Own calculations

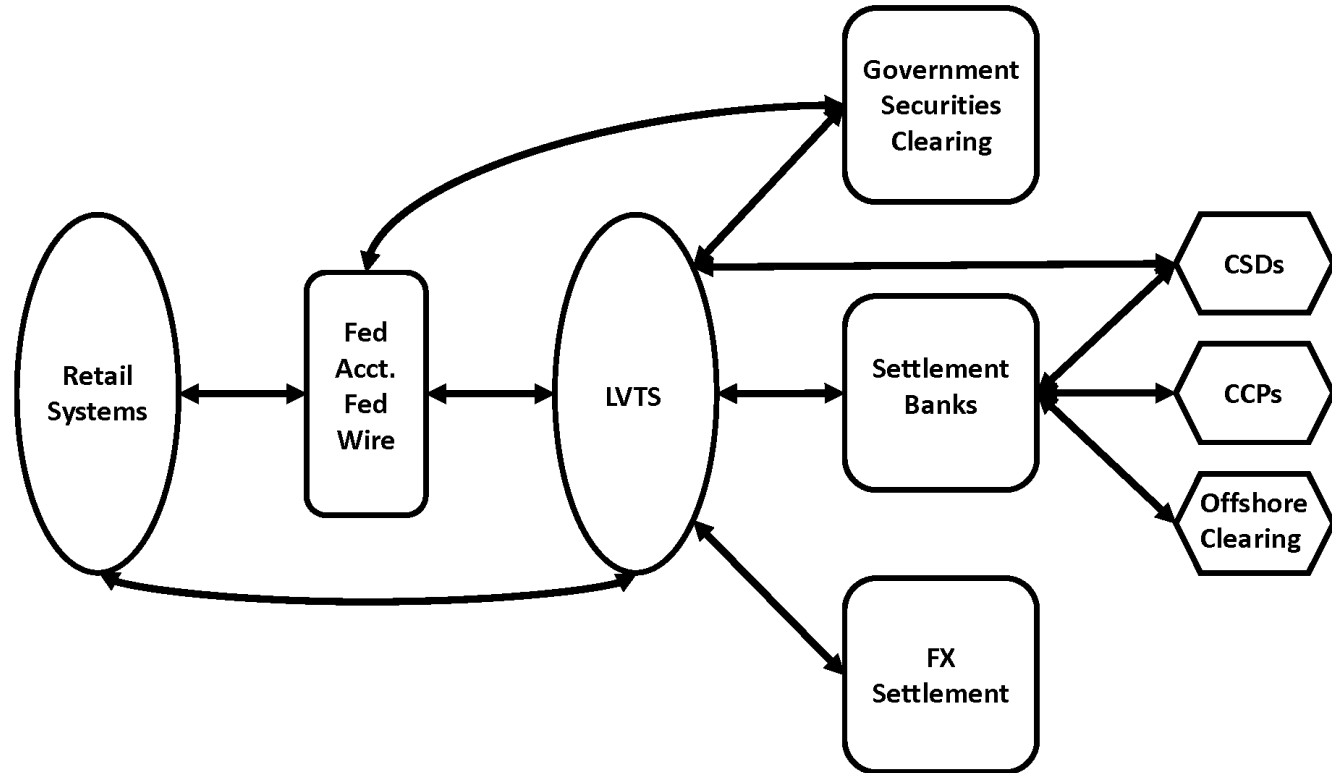


- Existing banking and payment systems, while still working, are obsolete and no longer aligned with the constantly changing requirements of the modern world.
- Financial system the way we know it is on its last legs due to persistent negative or very low positive interest rates.
- While open access Internet protocols have unleashed a wave of creativity and growth in numerous fields, banking is not one of them.
- The reason stems mostly from the fact that successful open access protocols for money and identity, while sorely needed, are conspicuously absent at present.

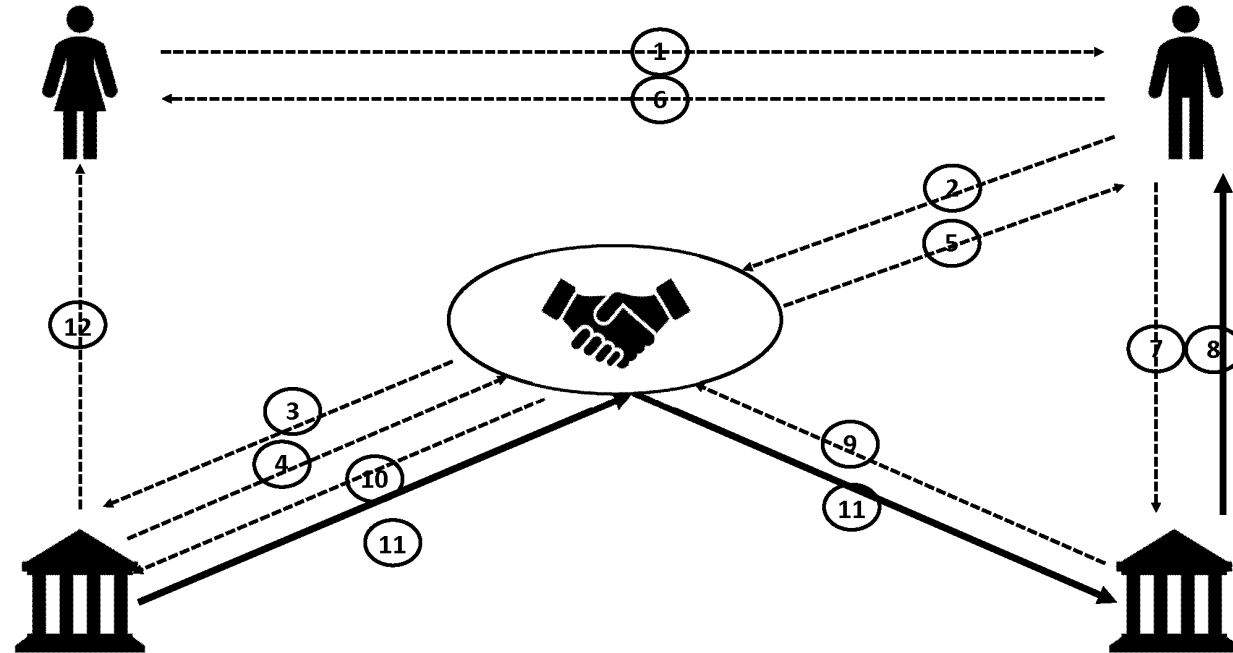


- We argue that a regulatory compliant, fiat-backed tokenized medium of exchange, can help to fill this gap.
- The corresponding tokens can be viewed as an electronic analogue of cash, with all its pluses and minuses.
- Such tokens can have numerous fintech applications.
- Appropriately modified, they can be used by regulated financial institutions in order to build dFMI.

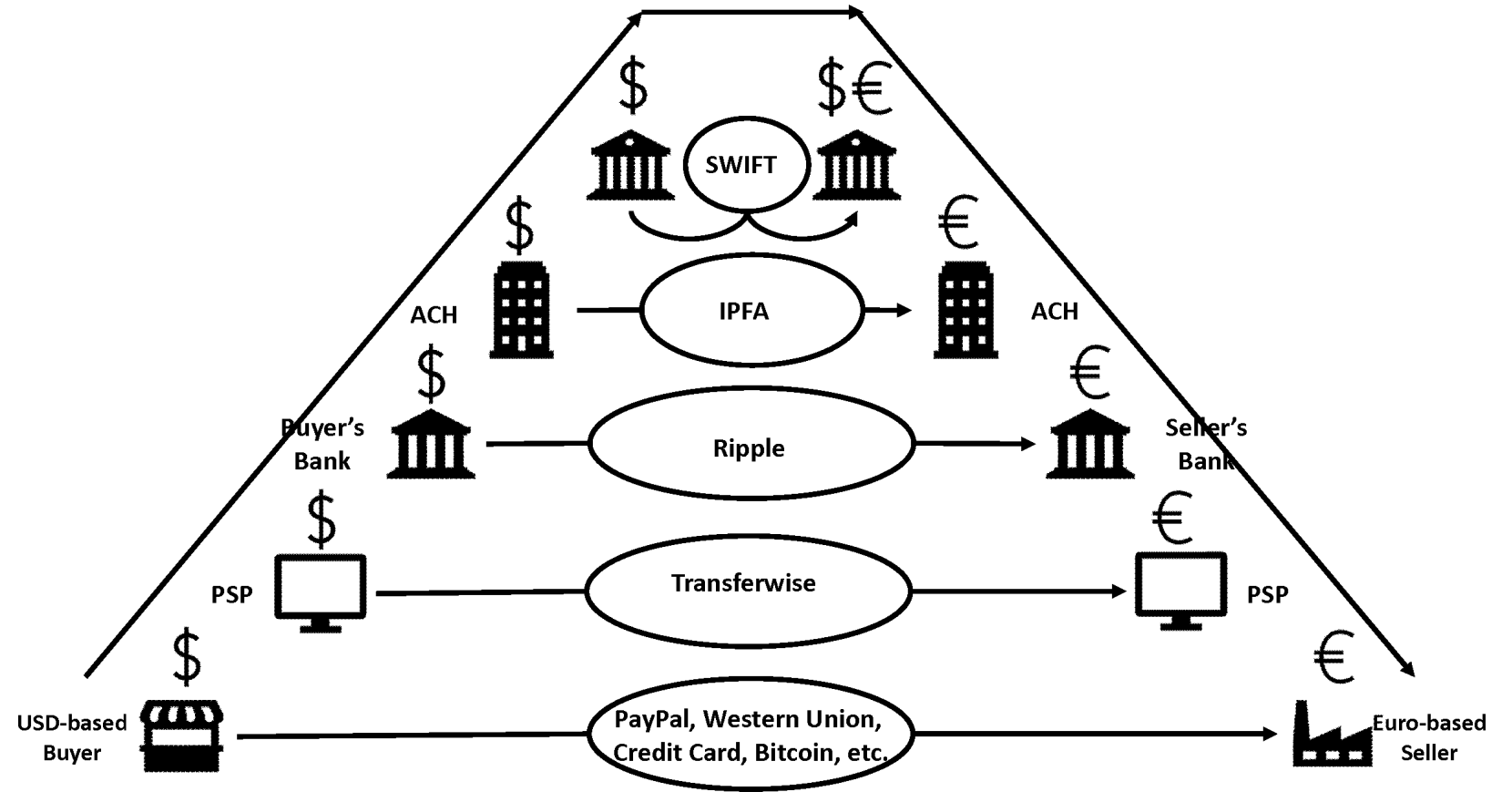
Settlement Systems in the US

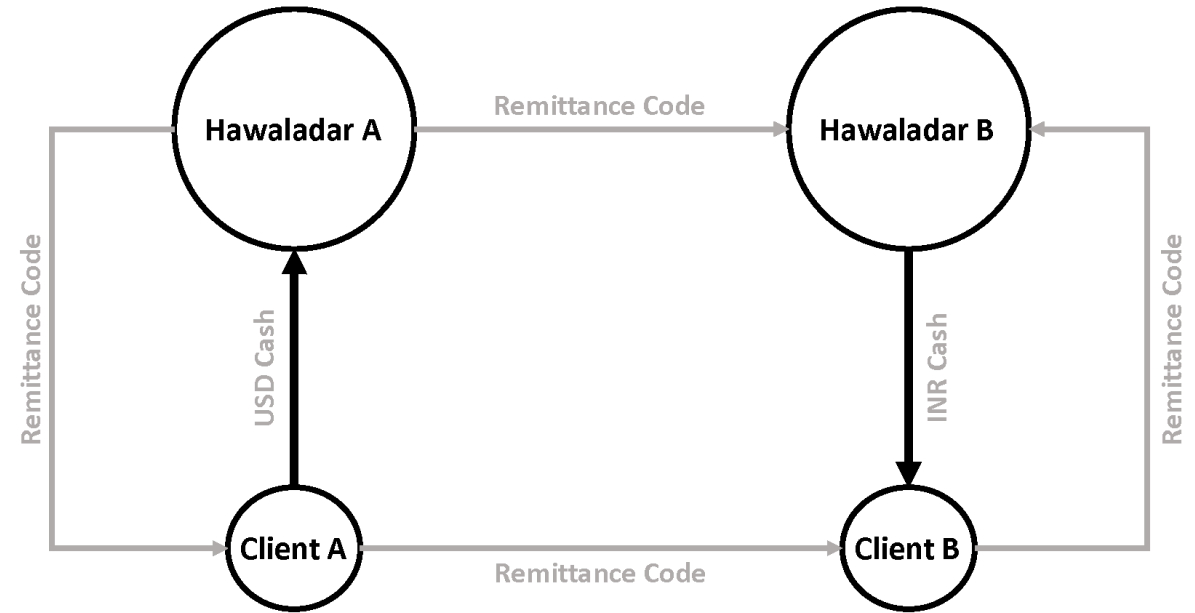
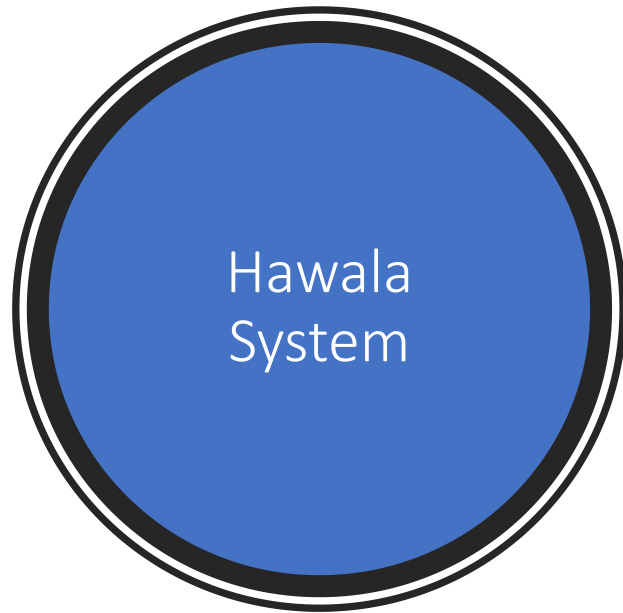


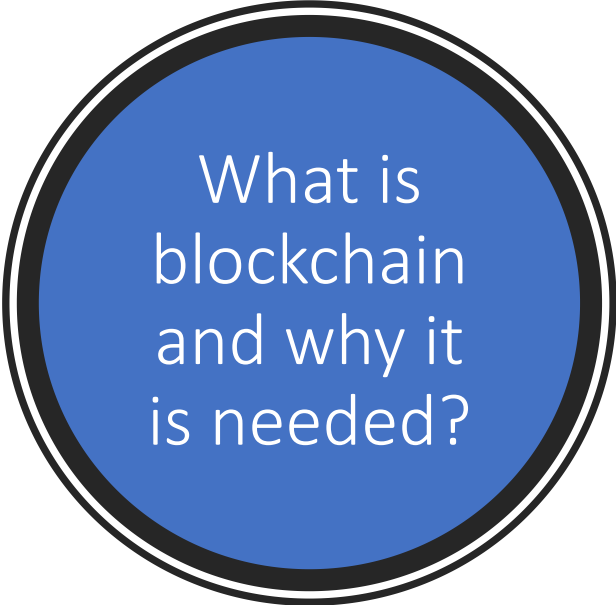
A typical credit card transaction



A typical international transaction





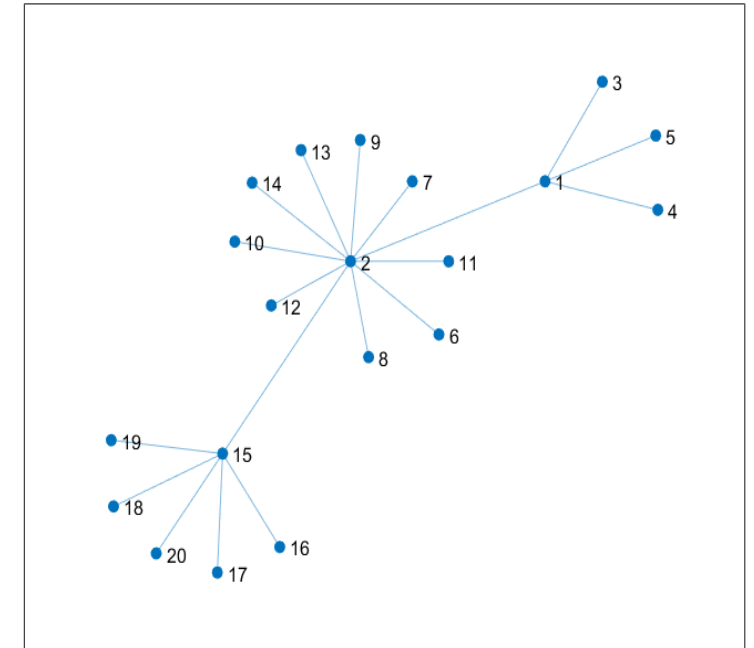
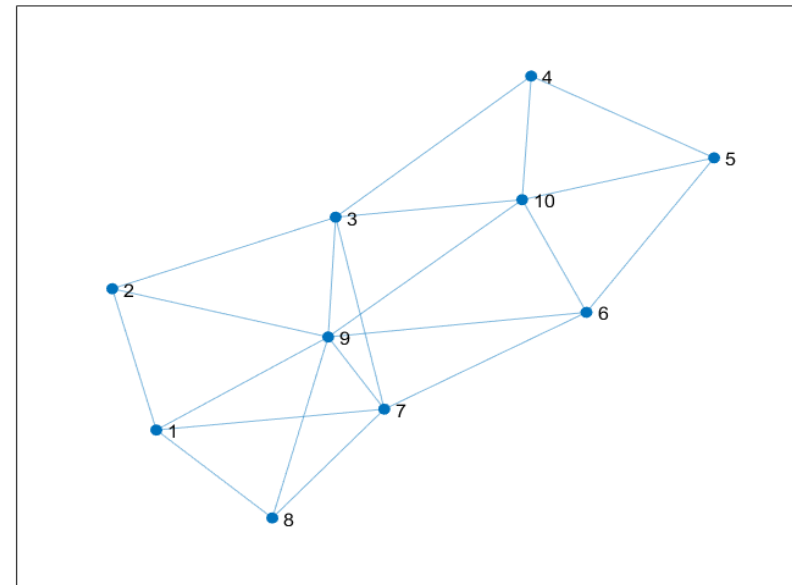
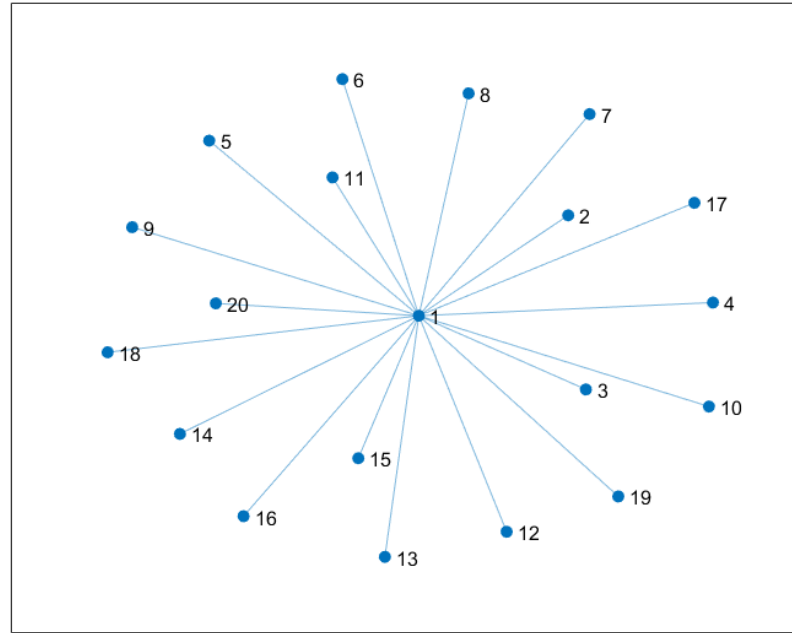


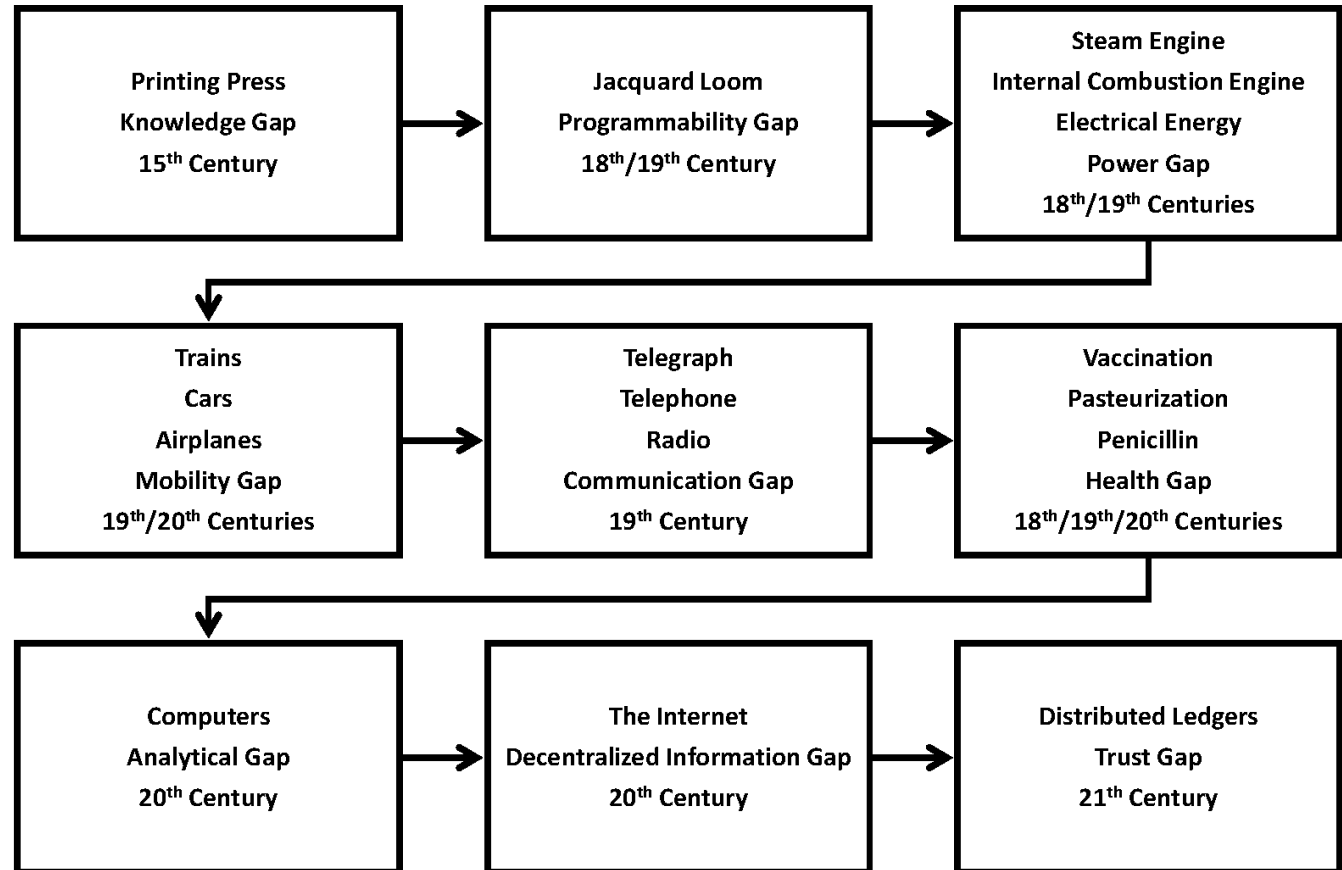
What is
blockchain
and why it
is needed?

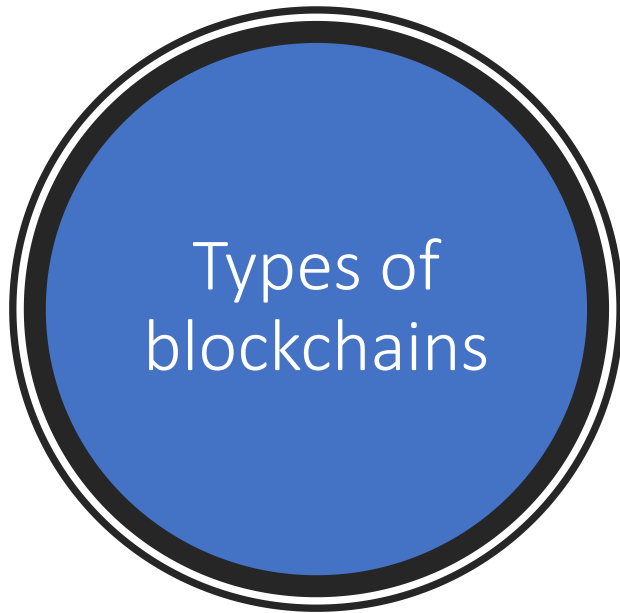
Blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking both tangible and intangible assets in a business network. This can potentially reduce risk and cutting costs for all involved.

Thousands of transactions take place every second. Typically, each participant has his or her own ledger and view of the transaction. This is a recipe for error, fraud and inefficiencies, which can be rectified if a transaction can be tracked in a single ledger.

Informational super structures







Distributed ledgers come in several flavors:

- Unpermissioned public ledger (Bitcoin, Ethereum, and the myriad others)

- Permissioned private ledger (R3, IBM, other similar projects)

- Traditional centralized ledger

To control distributed ledgers a variety of mechanisms can be used such as:

- Proof of work (pow)

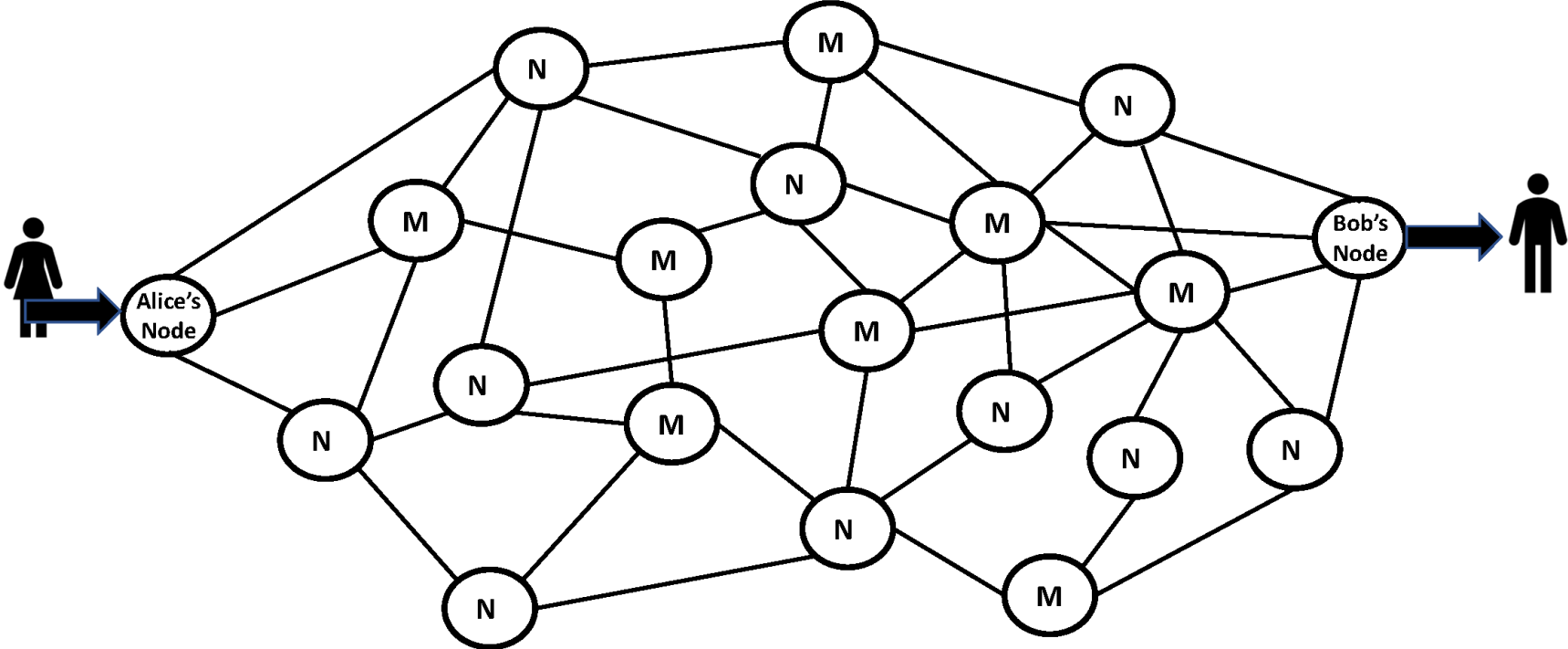
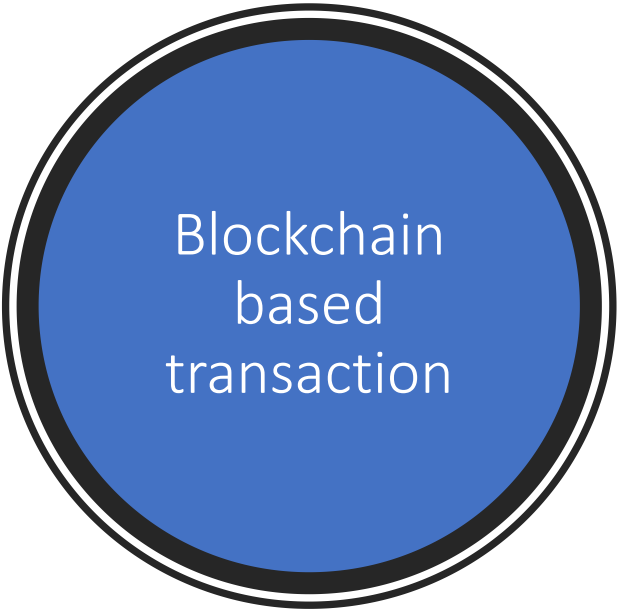
- Proof of stake (pos)

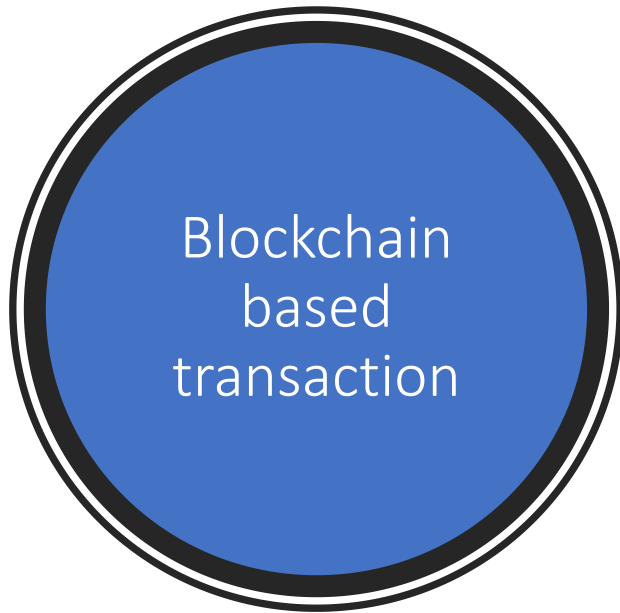
- Proof of burn (pob)

- Practical Byzantine Fault Tolerance PBFT

- and its numerous variations

- Third party verification





What is good about this picture?

- Anyone can participate;
- All transactions are public;
- Middlemen are not assigned from above.

What is bad about this picture?

- Anyone can participate;
- All transactions are public;
- Middlemen are not assigned from above.

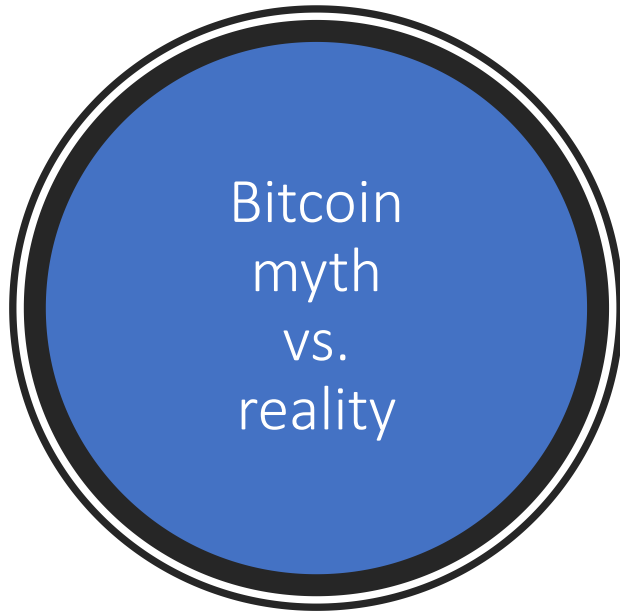
Since all transactions are public, this setup cannot be used by regulated financial institutions.

Rai or Fei -
Yapese stone
money.
Source:
Wikipedia



Medieval
English tally
stick. Source:
Wikipedia





Bitcoin promises are grand:

- Replacement for national currencies
- Removal of money from social and government control
- Anonymity
- Decentralization
- Taking control away from central authorities
- Etc.

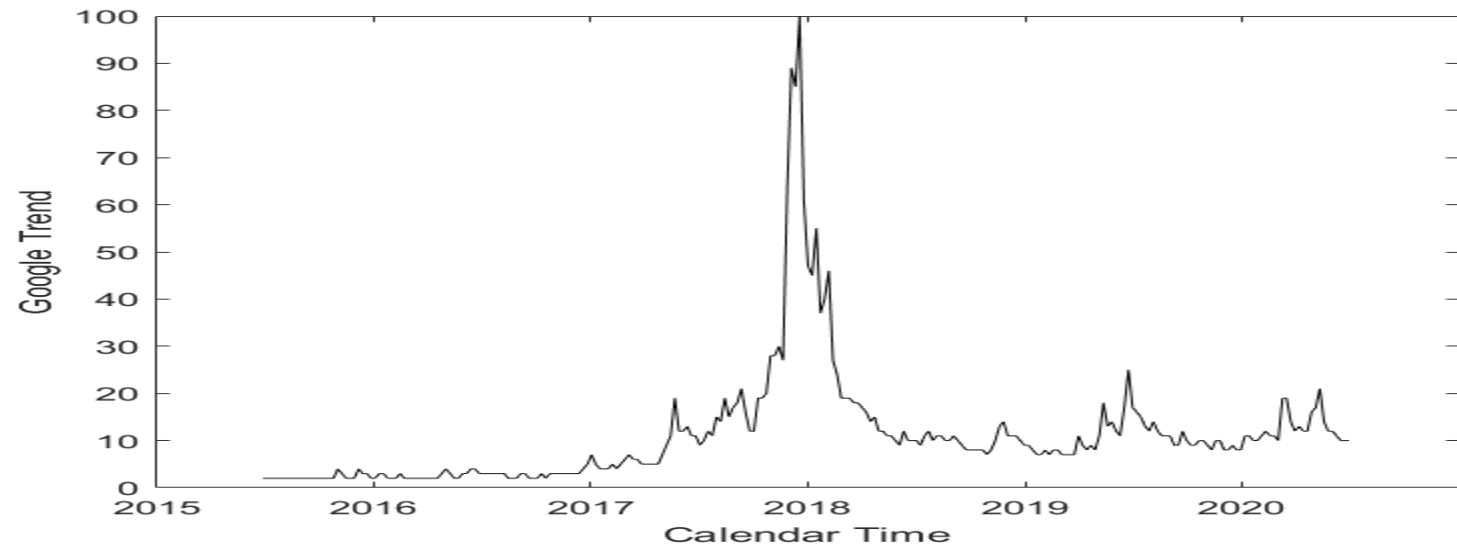
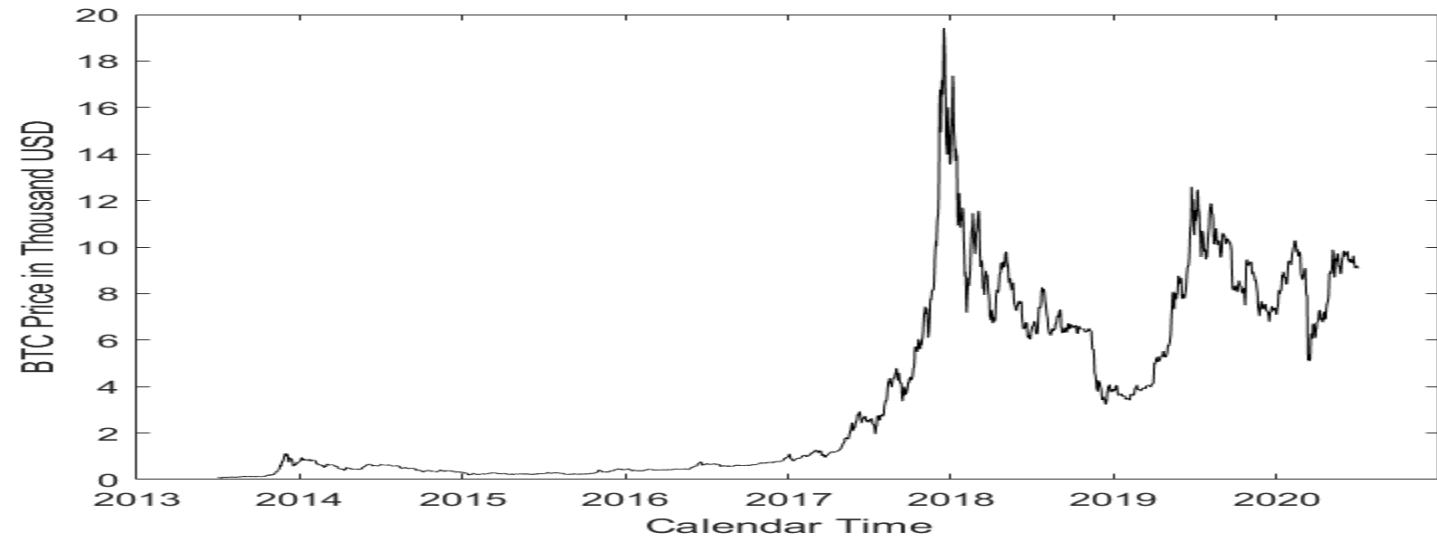
Bitcoin reality is much less so:

- Low TPS and high transaction fees preventing everyday usage
- Struggle for control by different mining and other interests and hard forks
- Pseudonymity (at best)
- Centralization
- Very inefficient consensus algorithm resulting in enormous electricity consumption
- Etc.

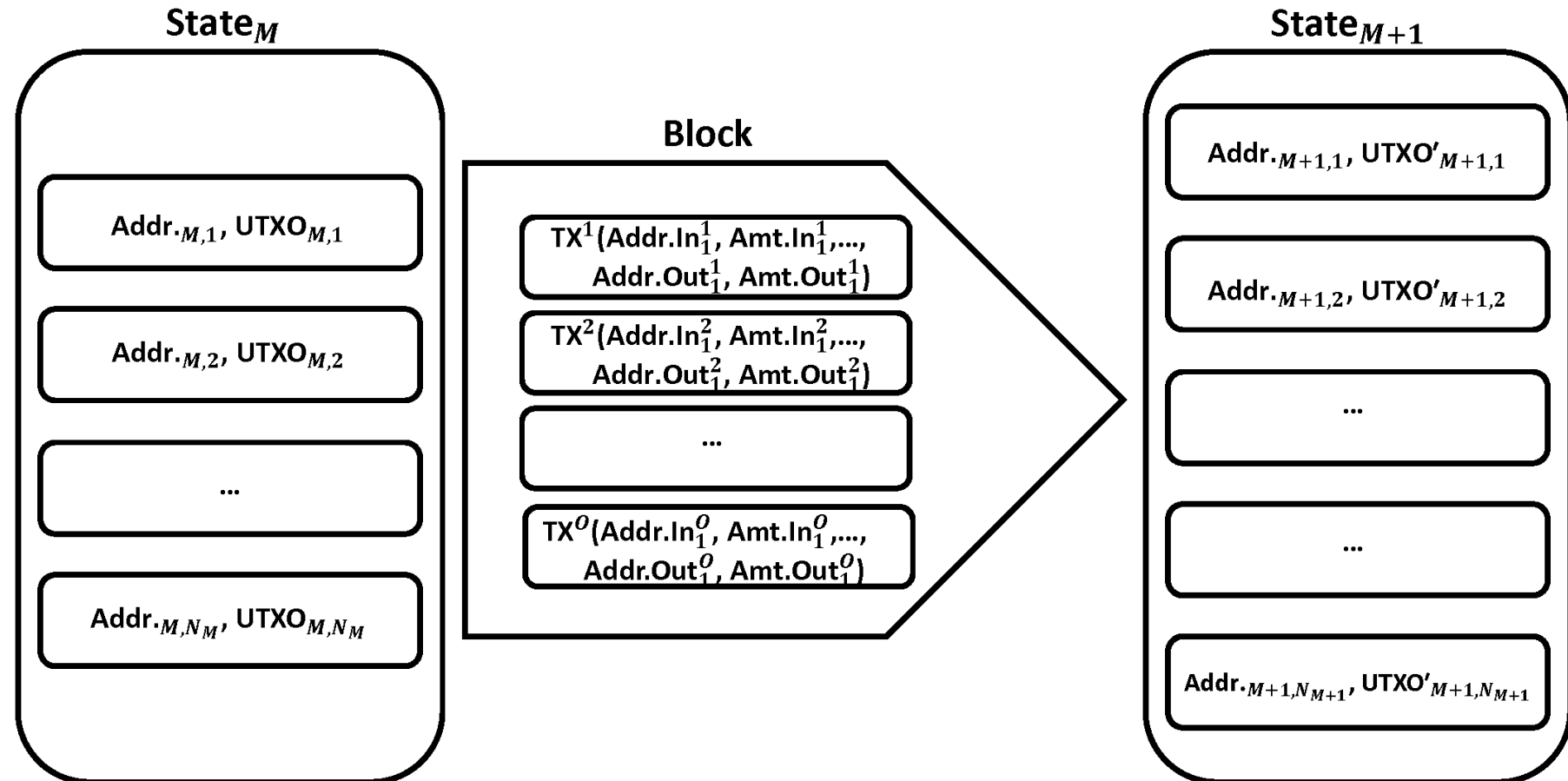
And yet:

- Bitcoin can be viewed as an electronic version of treasure

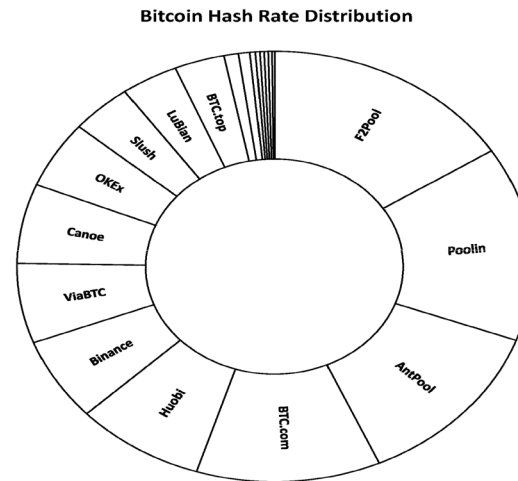
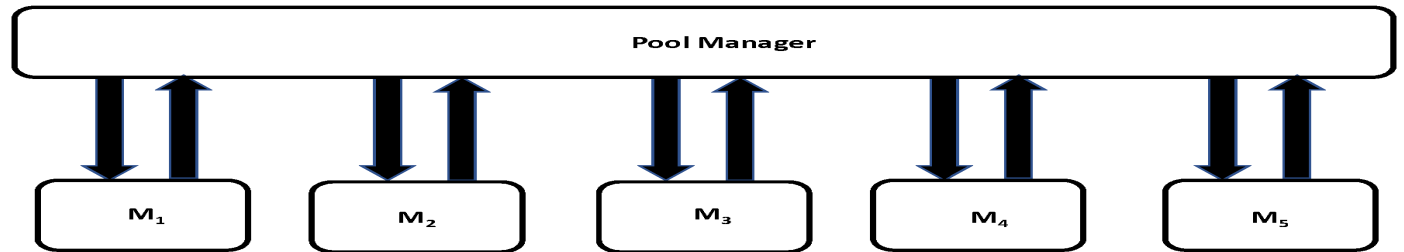
Bitcoin Price.
Source:
<https://coinmarketcap.com/currencies/bitcoin/>
Bitcoin Google
Trend. Source:
Google

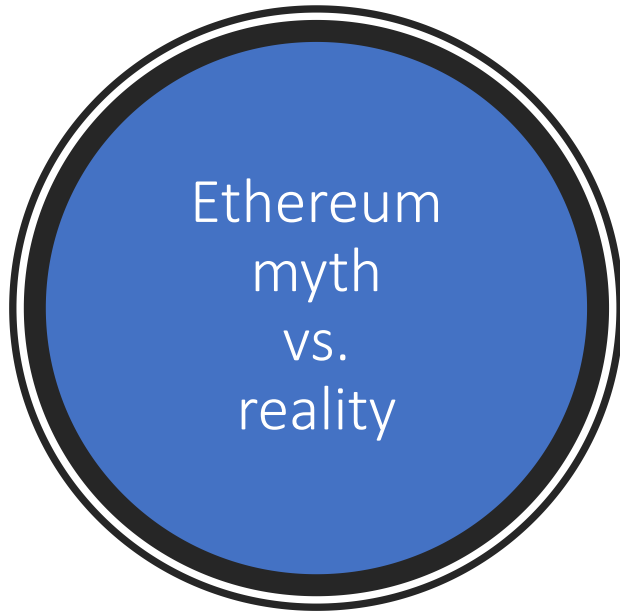


Bitcoin
Blockchain is a
gigantic Markov
Chain
Consensus is
achieved via
Proof-of-Work



Bitcoin hash rate.
Source:
<https://data.bitcoinity.org/bitcoin/hashrate/>





Ethereum promises are even grander than Bitcoin's:

- Ethereum Virtual Machine (EVM)
 - the first distributed Turing-complete computer
- Smart contracts
- Distributed autonomous organizations
- Decentralization
- Etc.

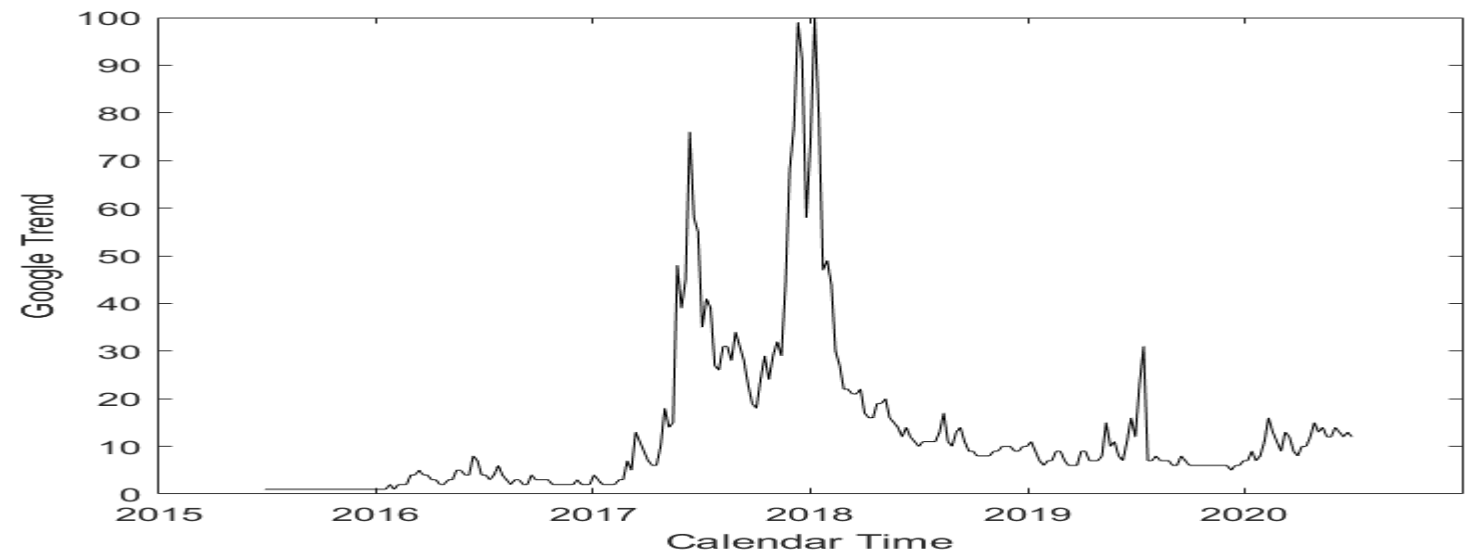
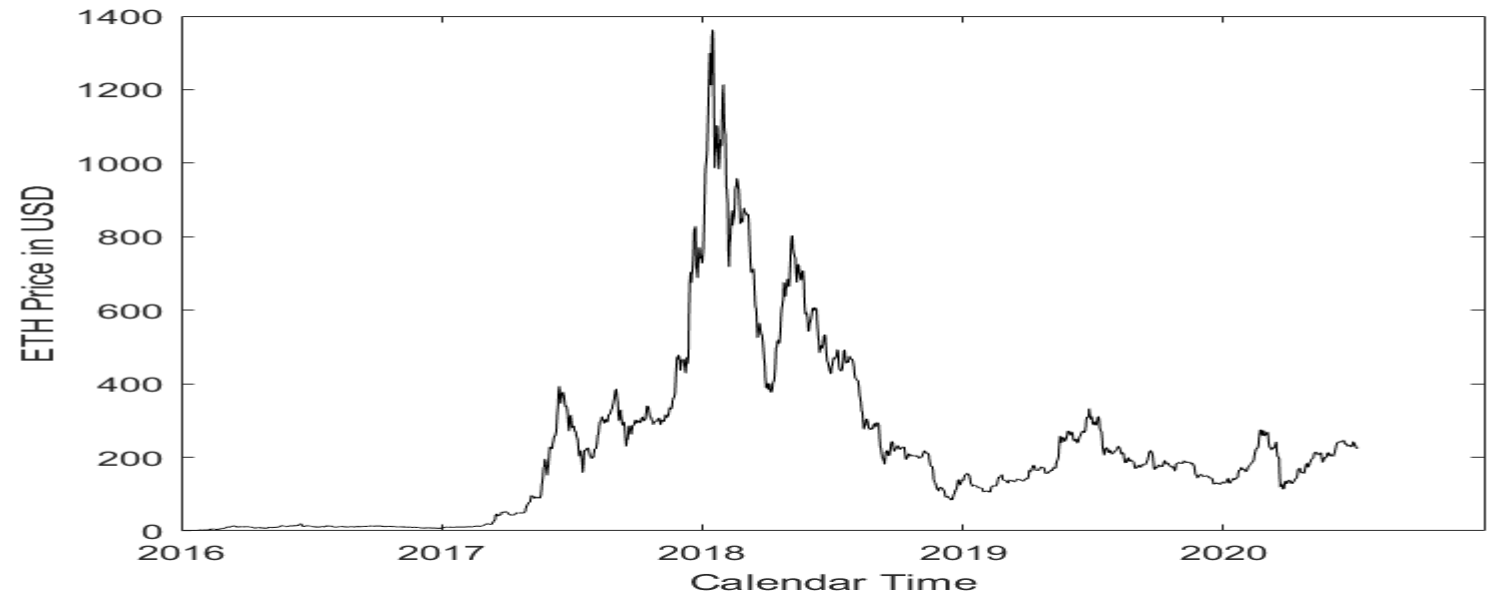
Ethereum reality is much less so:

- Low TPS and high transaction fees preventing everyday usage
- Obsolete payment model based on gas consumption makes EVM a distributed calculator (at best)
- Smart contracts are not smart and prone to unfixable bugs
- Smart contracts are voracious consumers of collateral
- Centralization
- Very inefficient consensus algorithm
- Etc.

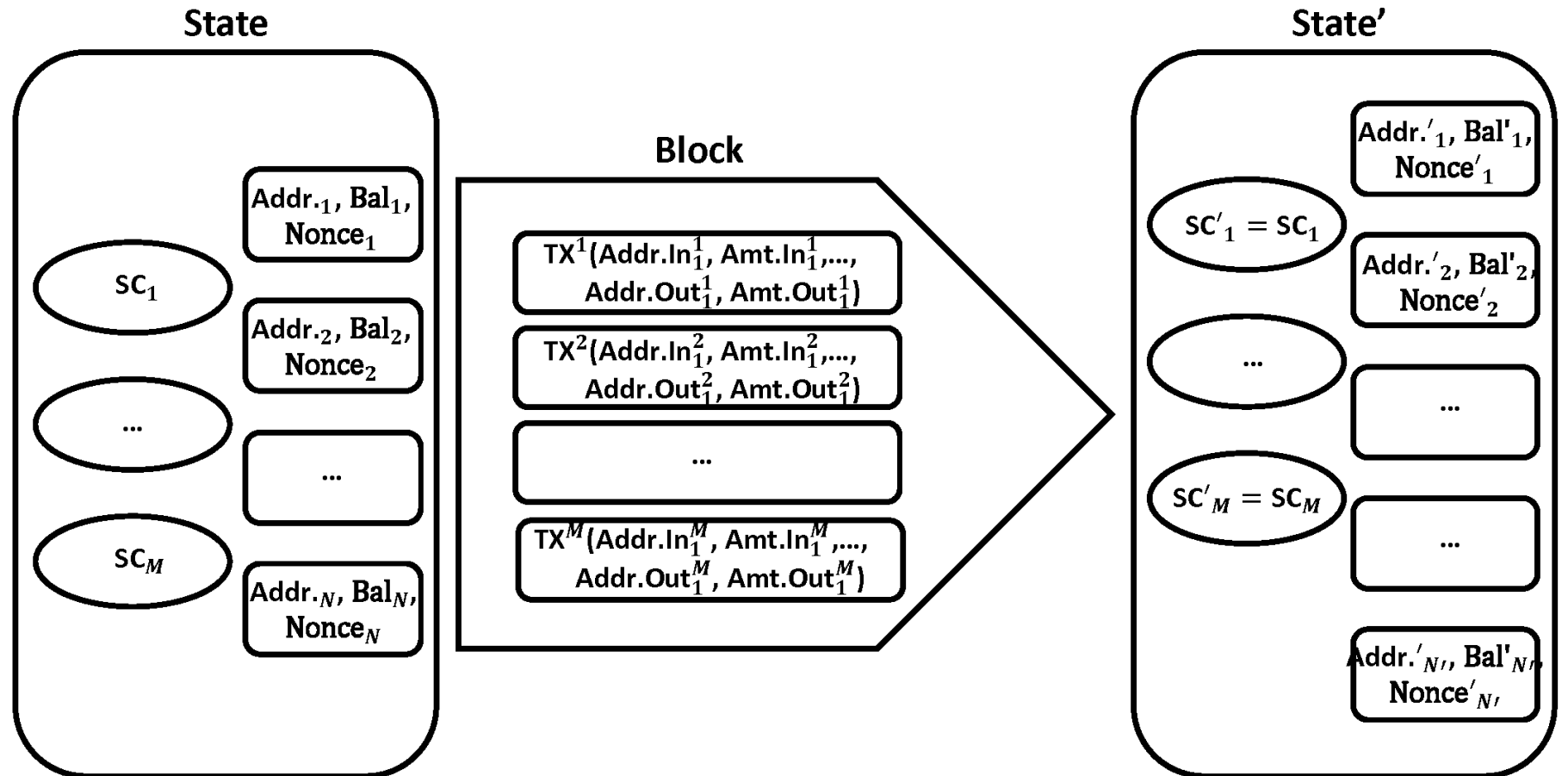
Any yet:

- Convenient for ICO and similar purposes
- Sufficiently robust (when not deliberately forked)

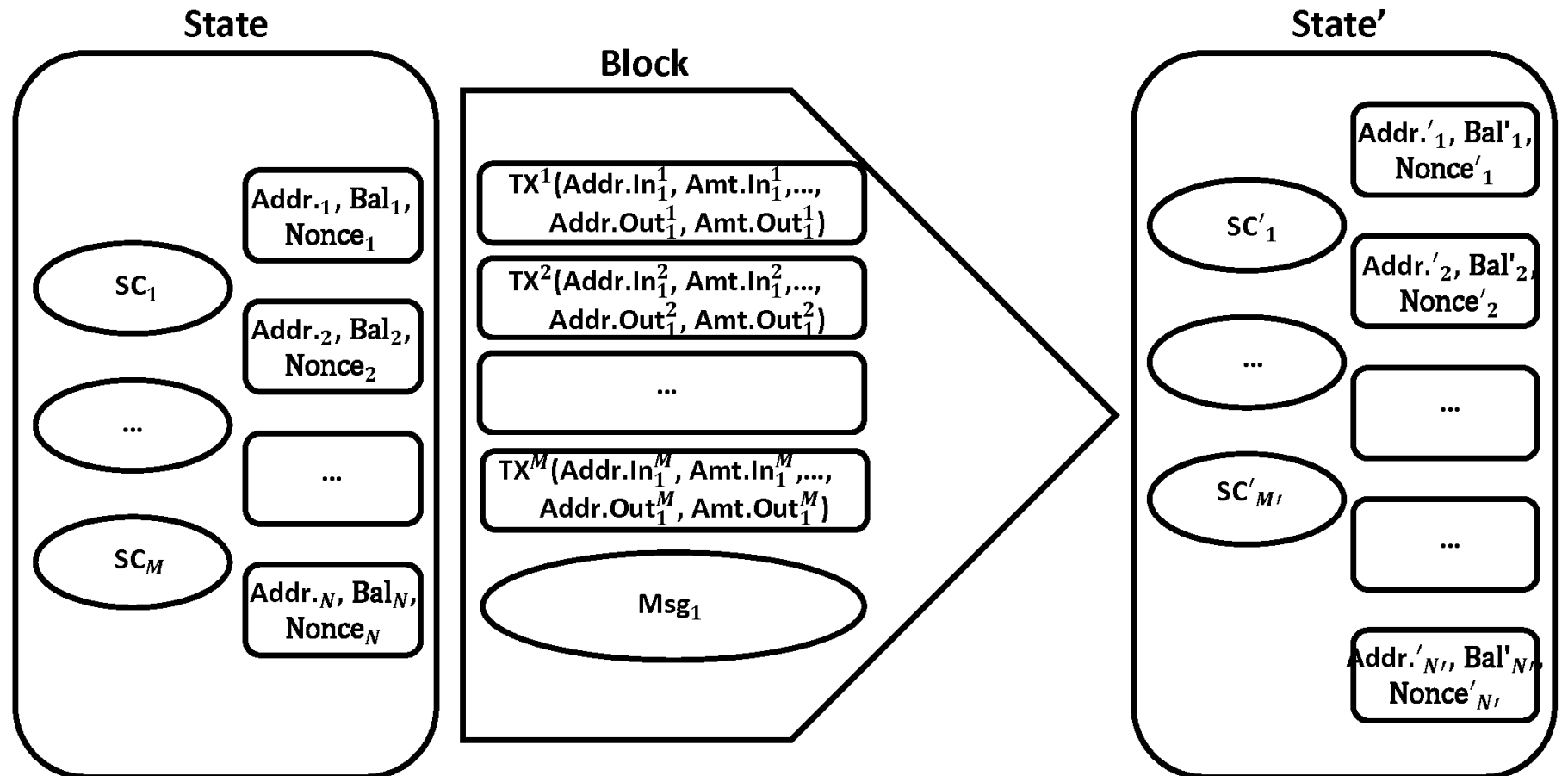
Ethereum price.
Source:
<https://coinmarketcap.com/currencies/Ethereum/>
Ethereum Google
trend. Source:
Google



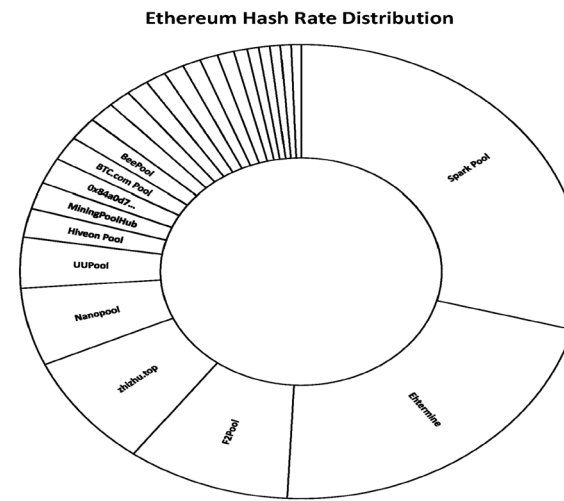
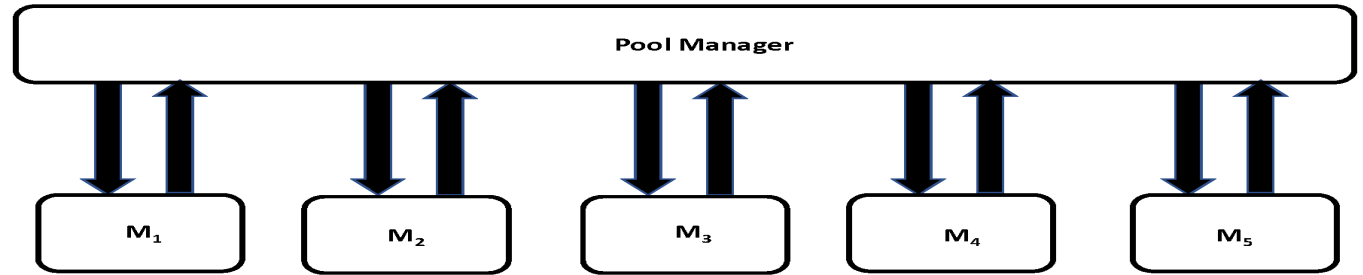
Ethereum
Blockchain is a
gigantic Markov
Chain with Two
Types of Vertices
Consensus is
achieved via
Proof-of-Work



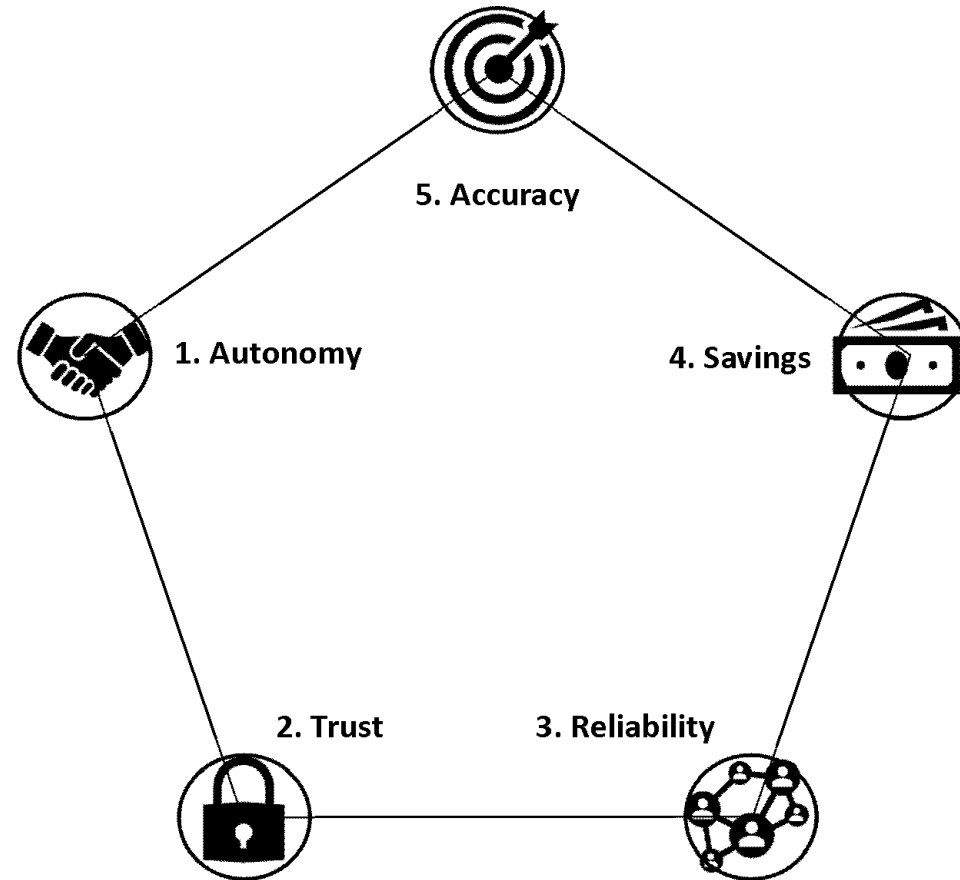
Ethereum
Blockchain is a
gigantic Markov
Chain with Two
Types of Vertices
Consensus is
achieved via
Proof-of-Work



Ethereum hash
rate. Source:
[https://gastracker.i
o/stats/miners/](https://gastracker.io/stats/miners/)



Ethereum
supports Smart
Contracts





Advantages of Smart Contracts

- Smart contracts are programmable financial instruments
- Ethereum provides Consensus as a Service (CaaS) so smart contracts are immutable
- Transactions are visible to all, so smart contracts are visible and auditable by all. This is simultaneously plus and minus
- Blockchain is permissionless, so anyone can write a smart contract
- In many situations, counterparty credit is not an issue since smart contracts are prefunded
- Consensus is VERY expensive
- Smart contracts require external oracles



Quorum attempts to make Ethereum friendly to enterprises in general and banking institutions in particular. Its main features can be summarized as follows:

- Preserves Ethereum Virtual Machine (EVM);
 - the first distributed Turing-complete computer
- Preserves smart contracts;
- Develops efficient (but not particularly robust) consensus algorithms based on PBFT rather than PoW;
- Has high TPS and low transaction fees facilitating everyday usage;
- Employs a flexible payment model;
- Is permissioned in nature;
- Divides transactions into public and private;
- Effectively shards the blockchain.



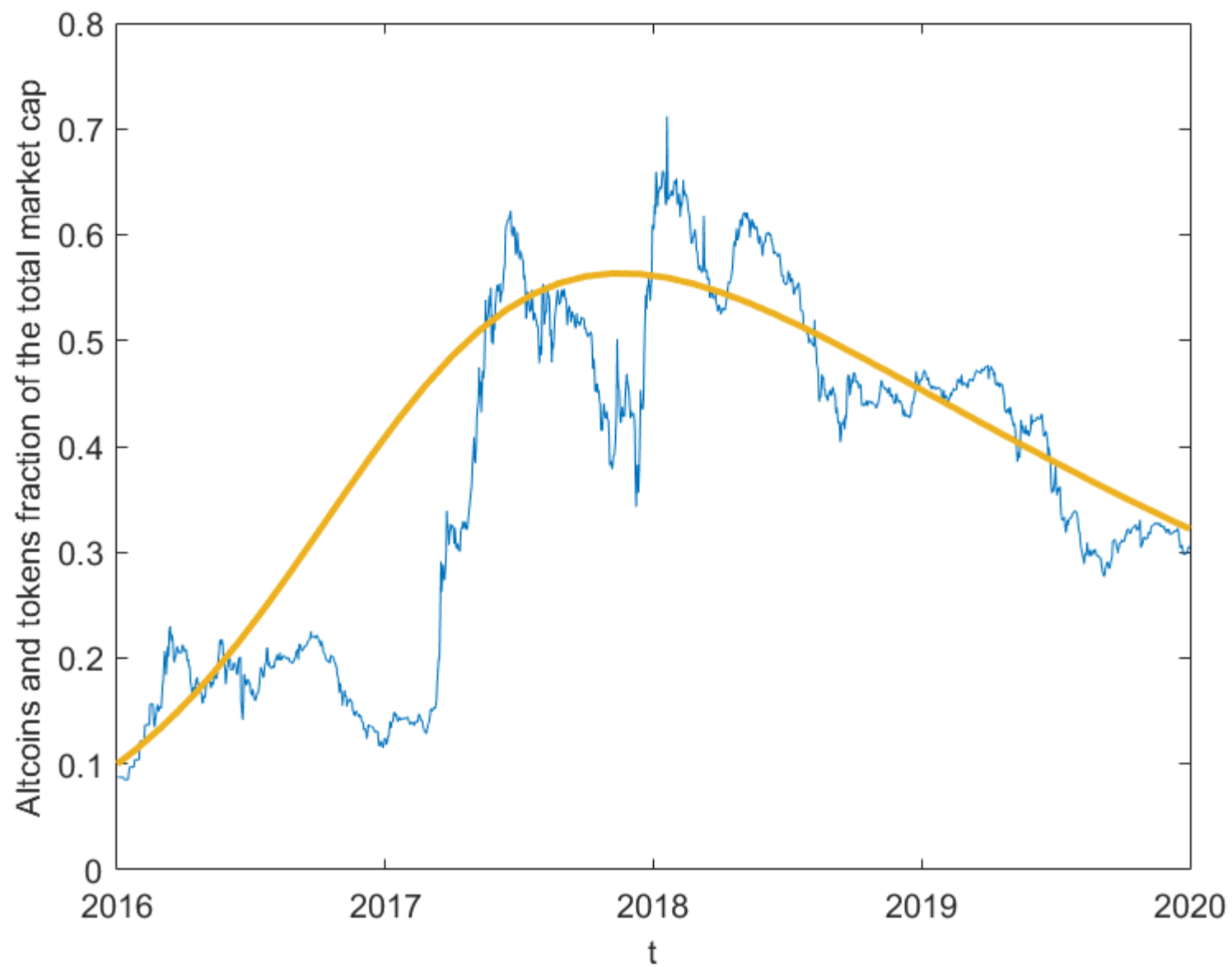
All these implementations are more or less the same:

- Have a version of smart contracts;
- Drop PoW in favor of efficient (but not particularly robust) consensus algorithms based on PBFT rather than PoW;
- Enjoy high TPS and low transaction fees facilitating everyday usage;
- Employ flexible payment models;
- Divide transactions into public and private;
- Effectively sharding of the blockchain and introduce sidechains.

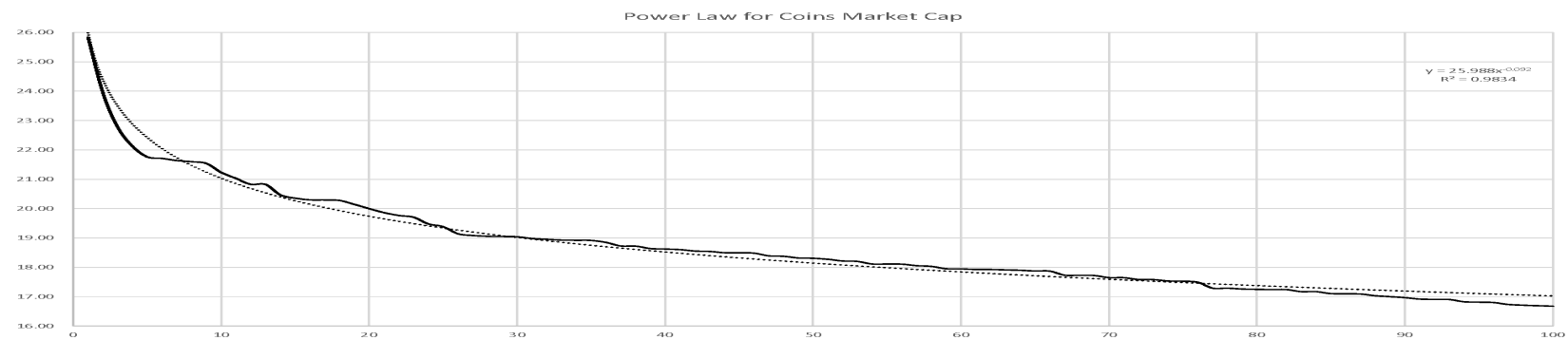
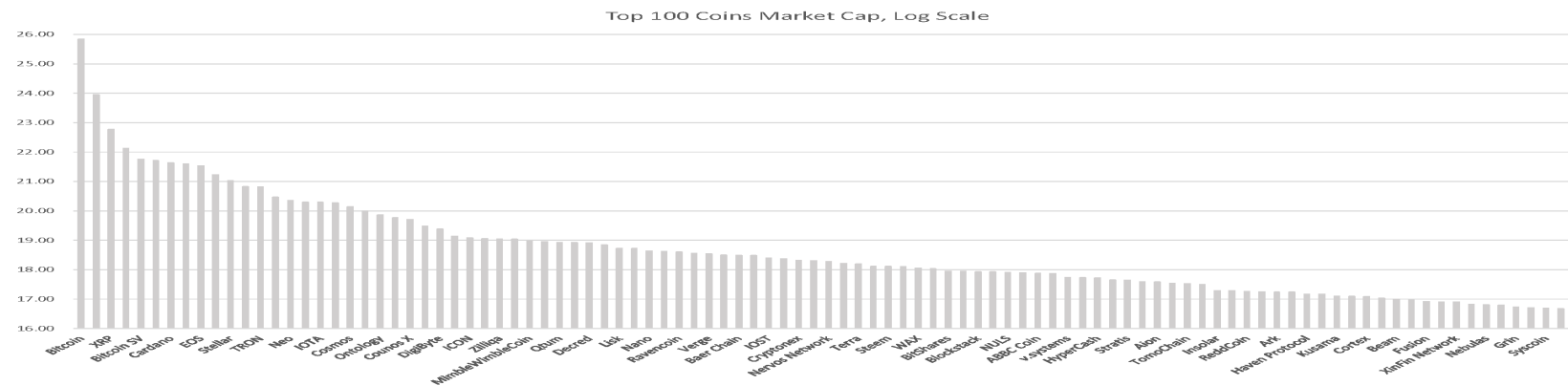


- Efficiency of mathematics is inexplicable.
- In 2019 I undertook a detailed analysis of the so-called Bitcoin dominance.
- To this end I used two models from epidemiology – a deterministic SIR model and a stochastic SIS model.
- The SIR model reads
- $S' = -bSI$, $I' = bSI - cI$, $R' = cI$
- Potential choice of parameters is $b=10$, $c=1$
- We are interested in the ratio $I/(S+R)$, which is shown below

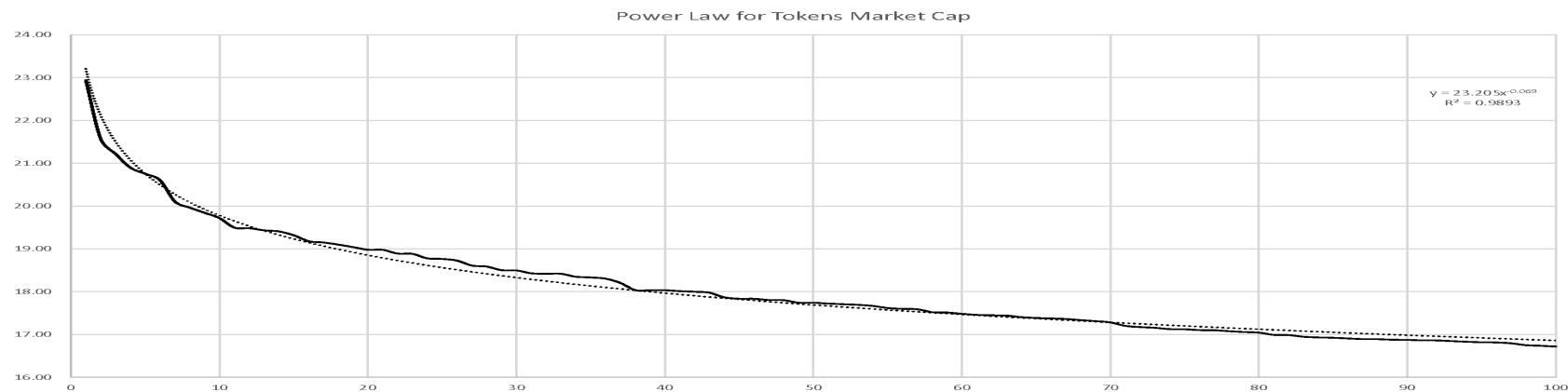
Bitcoin
dominance
via SIR
model



Top 100 coins

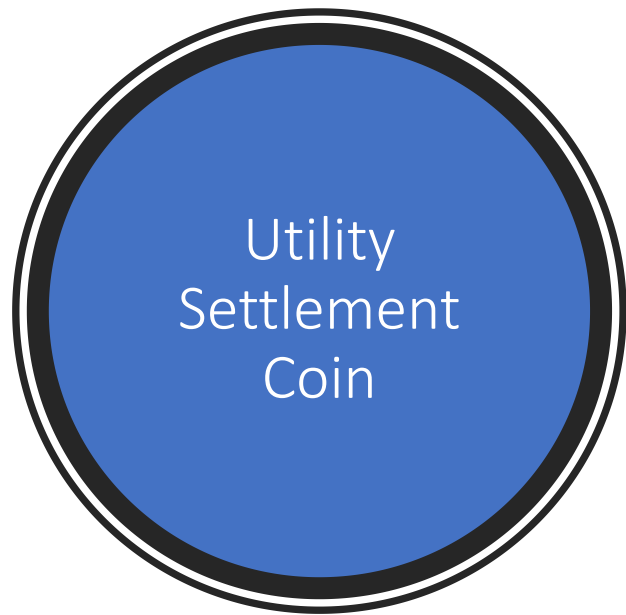


Top 100 tokens





- Potentially, central banks could issue digital cash
- CBDC opens way to a better monetary policy
- But also a possibility of pushing interest rates into a seriously negative territory and other controversial policies
- On the one hand, increasing tax collection, fighting crime, etc.
- On the other hand, excess control over ordinary citizens
- In principle, it would be possible to open a checking account at central bank directly, thus making retail banks obsolete
- In practice, it is more convenient to do by issuing licenses for narrow banks




- CBDC is technically possible but politically complicated
- Hence several alternatives have been proposed
- One promising venue is USC, which is developed by a consortium of
- banks and a fintech startup called Clearmatics
- Initially, USC can be an internal token for a consortium of participating banks
- These coins have to be fully collateralized by electronic cash balances of these banks, which are held by the Central Bank itself
- Eventually, these coins can be circulated among a larger group of participants
- However, in this case, issuance of USCs has to be outsourced to a narrow bank



- Experience shows that all decentralized crypto coins are inherently unstable, which makes them less than useful for commercial applications
- Unfortunately, building a successful stable token is hard
- Contrary to the often-made claims, it is not possible to build a truly decentralized stable token, so that any potentially successful stable coin must be partially centralized
- The degree of decentralization can vary. There are three approaches:
 - Fully collateralized custodial tokens
 - Tokens over collateralized with cryptos
 - Dynamically stabilized tokens
- Only fully collateralized tokens can be stable, even under extreme circumstances
- Tokens collateralized by fiat and tokens collateralized by real assets



- Custodial coins fully collateralized with .at are relatively centralized as their creation and annihilation is performed by a single party.
- Once a coin is created, and before it is destroyed, it can freely move on the corresponding blockchain.
- Given this semi-centralized design, custodial coins are particularly prone to regulatory influences.
- They must be regulatory compliant in order to be able to survive.
- Several coins of this nature, including Tether and TrueUSD, either already exist or are being currently designed.
- (<https://silamoney.com/>) uses a particularly promising framework. Full disclosure – I am CTO of Sila. 



- Saga is one of a new breed of crypto currencies, which are characterized by time-varying degree of collateralization, starting their life as fully collateralized and eventually becoming fully free-floating.
- Such coins cannot be stable in the long run, regardless of the theoretical arguments put forward by their backers.
- History has been brutal to such schemes.
- The moment governments start to manipulate the gold content of their coinage, the value of their coins plummets precipitously.
- The story of the assignats, used as money during the French Revolution illustrates this point with extreme clarity.
- In the 1970s the inflation was triggered after the US dropped the gold peg. Volcker eventually brought it under control by using all the tools available to the Fed.
- Since clear that Saga doesn't have such tools at its disposal and hence is very prone to the death spiral.
- It seems that it is currently inactive.



- An alternative approach to creating stabilized coins is to use unstable native crypto coins, specifically Ether, and smart contracts, which guarantee that stable coins, representing a sliver of the total, are massively overcollateralized.
- This collateral cushion is supposed to create a natural floor for the value of the coin.
- A typical example is Dai issued by MakerDAO.
- As many other crypto ideas, this one can be traced back to conventional financial engineering concepts, specifically, trading on the margin and creation of collateralized debt obligations (CDO) tranches.
- Obviously under normal conditions, the corresponding coins are indeed stable, however, if there is a sudden jump down in the value of the underlying Ether, then the value of the corresponding coin will go below par.
- Experience suggests that it is not even necessary for the actual breach of the floor to occur. A mere perception of such a possibility is enough to make coins value less than par.



- While the idea of dynamic stabilization of a coin contradicts common sense and historical experience, it has recently gripped the imagination of investor community and hence is worth investigating in some detail.
- Basis is a representative example of such a coin.
- Denuded of the amenities, the algorithm works as follows.
 - If the value of the coin is going up (a relatively easy case), then, not surprisingly, new coins are issued and distributed amongst the holders (say proportionally).
 - If the value of the coin is going down (a more complex case), then bond-like instruments are issued in exchange for coins, which are burned. As a result, the number of coins in circulation goes down and, in theory, their price is going up.



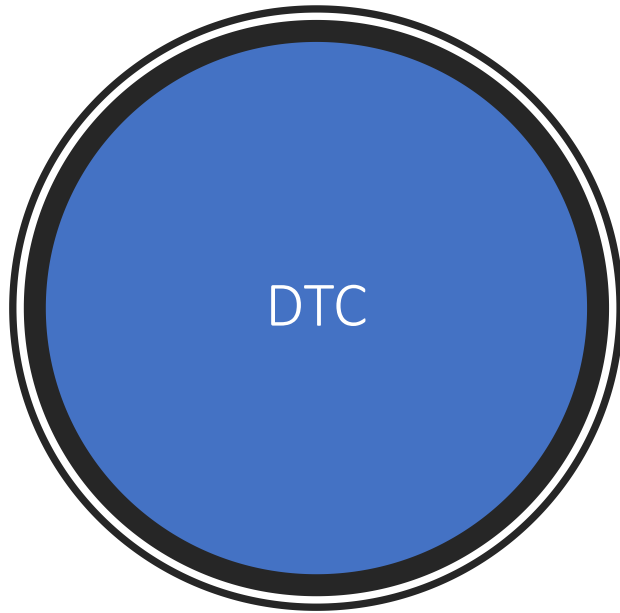
- A simple Gedanken experiment shows that this stabilization cannot work in the long run and will collapse when the bonds will come due.
- Algorithms of this type have been known for a long time. For example, Baron Munchausen is famous for using it and pulling himself and the horse on which he was riding out of a mire by his own hair.
- More recently, similar ideas were entertained by academic economists who proposed a mechanism for fixing the price of gold by a government in terms of its own fiat without keeping any gold in reserve.
- Obviously, even with all the coercion mechanisms at their disposal, no government was ever able to achieve such a feat. The probability of a crypto algorithm lacking such mechanisms to succeed is even lower.
- As an aside, the Quantity Theory of Money (QTM), which is used as a foundational concept underpinning Basis, has been discredited for decades, and doesn't pass muster with scientific analysis, not to mention common sense, see, e.g., Keynes.



- The idea of anchoring value of paper currency in baskets of real assets is old
- Gold and silver as well as bi-metallic standards have been used for centuries
- Two approaches are common: a redeemable currency backed by a basket of commodities; a tabular standard currency indexed to a basket of commodities.
- Joseph Lowe (1822) was the first to explain how to use a tabular standard of value to the price inflation; Poulett Scrope (1833) developed a similar plan based on a basket of 50 commodities; William Jevons (1877) developed these ideas (much) further and proposed an indexation scheme based on a basket of a 100 commodities; Alfred Marshall (1887) proposed a similar tabular standard; Irving Fisher (1911) developed a mixed tabular/gold standard which he called “compensated dollar” proposal.
- Frank Graham (1933), inspired by developments during the Great Depression developed an automatic countercyclical policy based on 100 percent backing of bank deposits by commodities and goods; Benjamin Graham (1933) proposed backing the USD with a commodity basket at 60% and gold at 40%; Friedrich Hayek (1943) extended proposals by Grahams to establishing a universal basket of commodities, which every country would use to back its currency; John Maynard Keynes (1941-1943) proposed the bancor, an international currency defined in terms of a weight of gold (the bancor is supposed to be a multilateral transaction currency); Nicholas Kaldor (1963) proposed a new commodity standard, which he also called bancor, a commodity reserve currency.



- USC and stable coins are helpful from a technical perspective, but it does not solve issues of monetary policy.
- We wish to address this issue by building a counterweight for fiat currencies by backing the DTC by a pool of real assets
- We start with oil, but eventually expand to metals, crops, mooring rights, etc.
- Sponsors bring their oil to the pool administrator, who issues DTC in one-to-one ratio
- DTCs are sold to the public
- The corresponding fiat currencies are deposited with the affiliated narrow bank
- The proceeds are passed through to sponsors



- Today, for the first time ever, there is the possibility of a digital currency that combines the best features of both cash and digital currencies.
- This currency is largely immune to policies of the central banks that control the worlds' reserve currencies.
- Such a currency has enormous potential to improve the stability and competitiveness of trading and natural resource producing economies.
- We propose to develop a trade-oriented asset-backed digital currency, aimed at facilitating international trade and making it as seamless as possible.
- Unlike Bitcoin, it will be fast, scalable, and environmentally friendly.
- It will also be transaction friendly because of its low volatility vs fiat currencies.

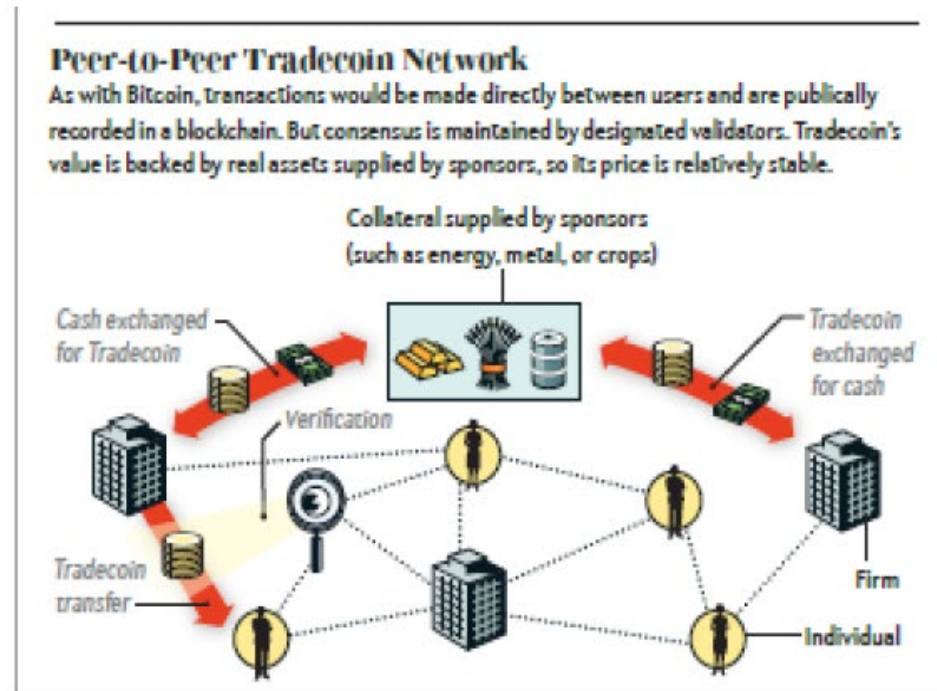
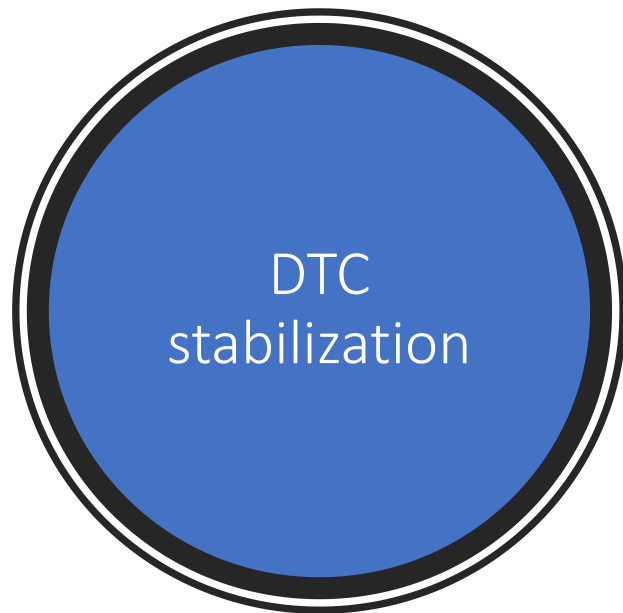


Figure: DTC setup. Source: Scientific American, vol 318, no 1.



Trade Coins on the Silk Road:
silver *drachm* of Sasanian Iran and gold *solidus* of Byzantine empire



Figure: Old Silk Road. Source: Wikipedia

Trade Coins: Spanish Piece of Eight, Austrian thaler,

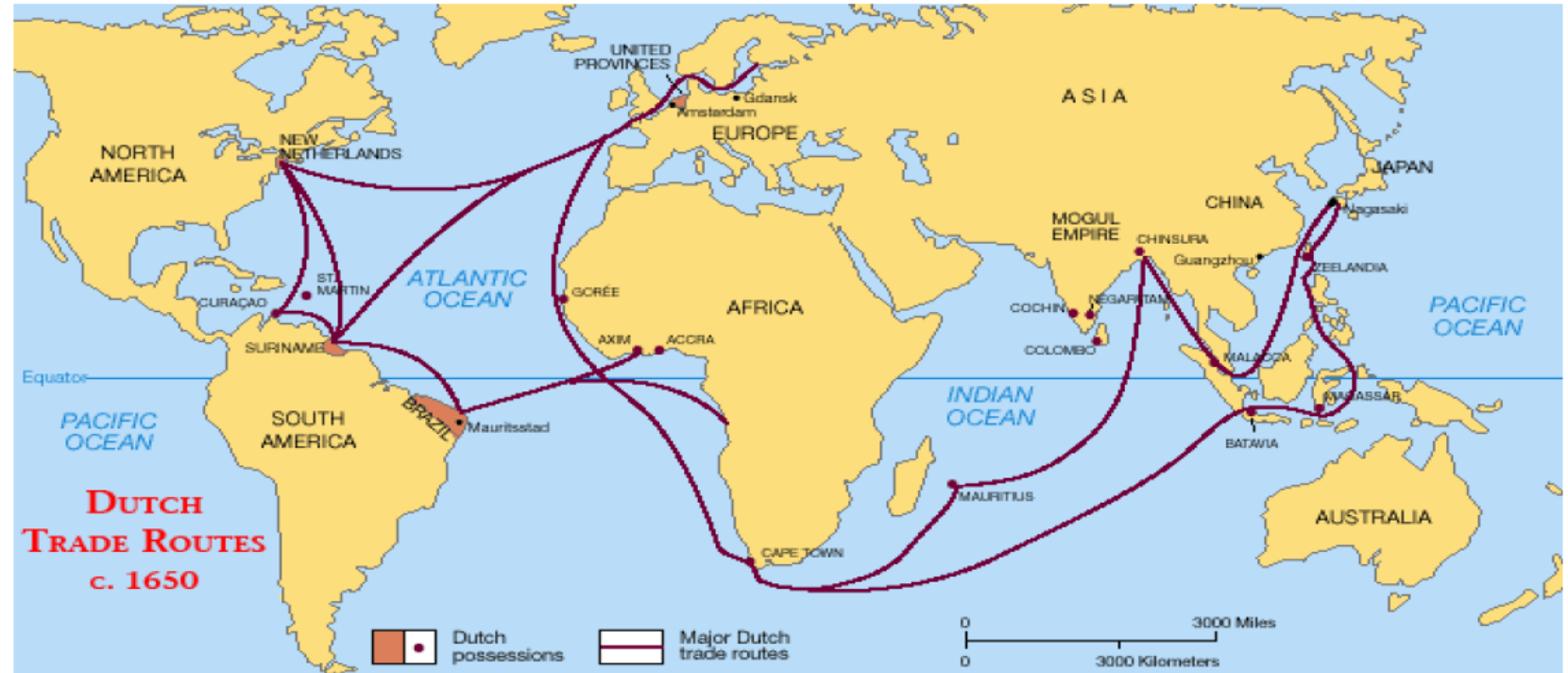
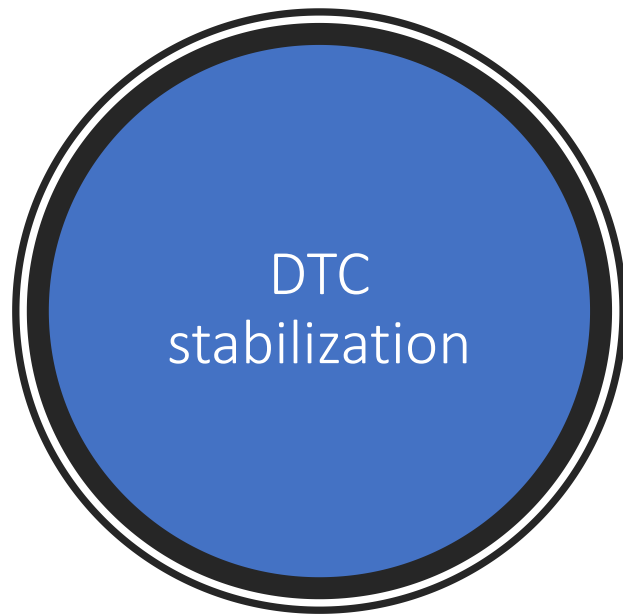


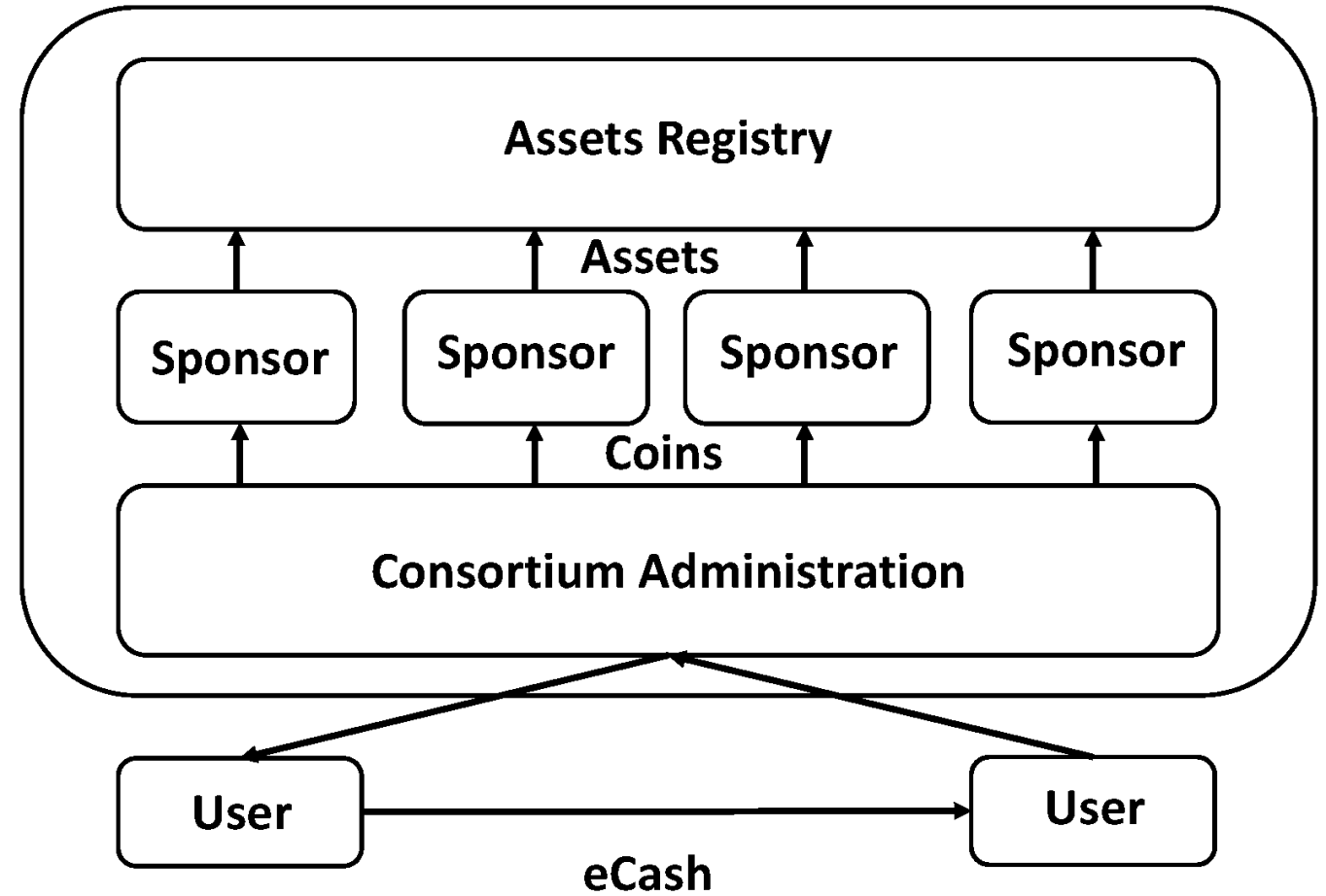
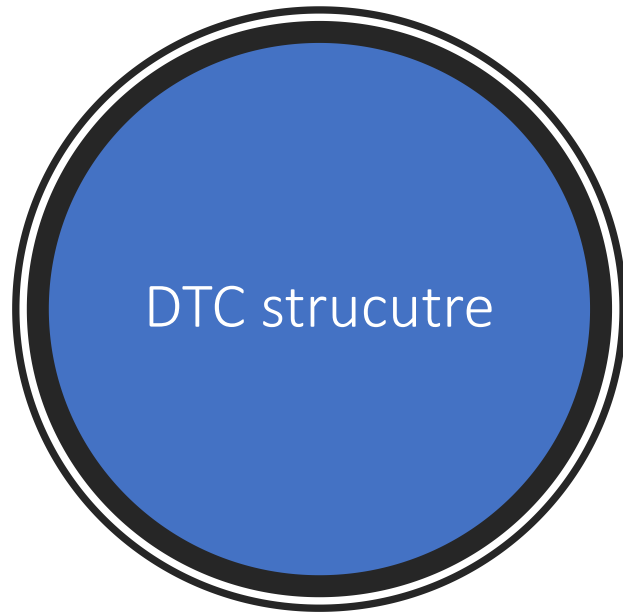
Figure: Spanish Pieces of Eight Source: Wikipedia

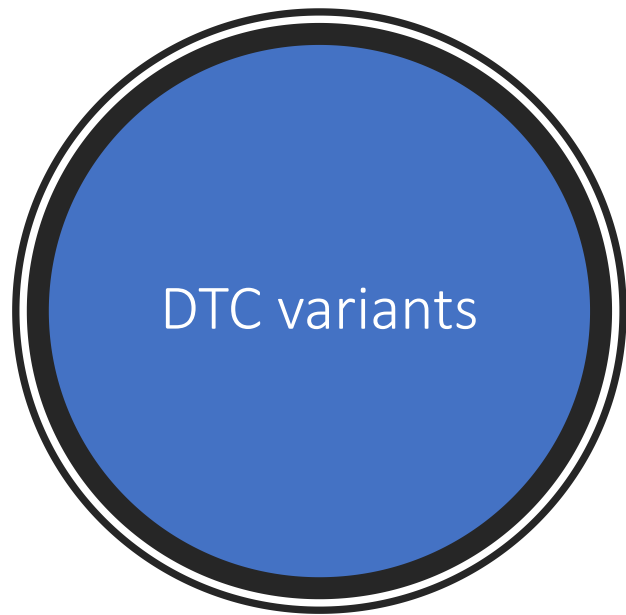


- As a result, the administrator is in possession of real assets, sponsors with fiat currency, general public with DTCs, which can always be converted into fiat at the current market price
- The price P_{DTC} of DTC will be close to (but not exactly at) the market price of the corresponding asset pool, P_M
- Indeed, if P_{DTC} falls significantly below P_M , economic agents will put DTC back to the administrator, who will have sell a fraction of the pool's assets for cash and pass the proceeds to these agents
- If P_{DTC} increases significantly above P_M , sponsors will supply more assets to the administrator, who will issue additional DTC and pass them to sponsors, who will sell them for cash, just pushing the price down
- This mechanism ensures that $|P_{DTC} - P_M| / P_M \ll 1$, a very desirable feature, especially compared for conventional cryptocurrencies, habitually exhibiting extreme volatility
- At the same time, outright manipulation by central banks is not possible either



- DTC has real value
- Accordingly, its price vs a representative basket commodities has very low volatility
- The price of the DTC vs a fiat currency is more volatility but still much lower than the price of bitcoin.
- As a result, it can be used as a transaction currency (think of a mortgage taken in DTC in a country which is naturally aligned with some of the major constituent commodities)
- DTC can be used as a unit of account and a store of value (as much as gold or oil, say, can)





- It goes without saying that fiat currencies can be used to back DTC in lieu of real assets.
- While this must be done very carefully, to avoid inevitable inflation caused by duplication of the money in circulation, it can be done (details to be explained in a due course).
- Provided that the choice of the fiat currencies in the basket and their proportions are done right, the corresponding DTC can be used as a counterpoint to the US dollar, which is much needed to avoid trade imbalances.
- Central bankers start to appreciate the need, as was articulated by Mark Carney at Jackson Hole.



- Libra is a new “cryptocurrency” recently introduced by Facebook.
- As Samuel Johnson famously put it: “Your manuscript is both good and original; but the part that is good is not original, and the part that is original is not good.”
 - It looks like Facebook adds to the list introduced by Marx a new entry:
 - $C-M-C'$
 - $M-C-M'$
 - $M=C$
- Libra will not help to bank the unbanked.
- If Libra becomes popular in developing countries, it will result in a runaway inflation, because its issuance is not immunized.
- Also, it seems rather far fetched and slightly demeaning to suggest a company scrip as a future of money.



Quorum, Fabric, Azure, R3 all pursue broadly similar objectives. Typical banking applications are unglamorous but undeniably important and useful.

Blockchains are used for risk mitigation, cost reductions, improving customer efficiencies, and streamlining operations in general.

- Trade finance;
- Regulatory compliance;
- Commercial insurance;
- Claim processing;
- Etc.

On a more ambitious scale:

- Trade execution, clearing, settlement
- Cross-border payments

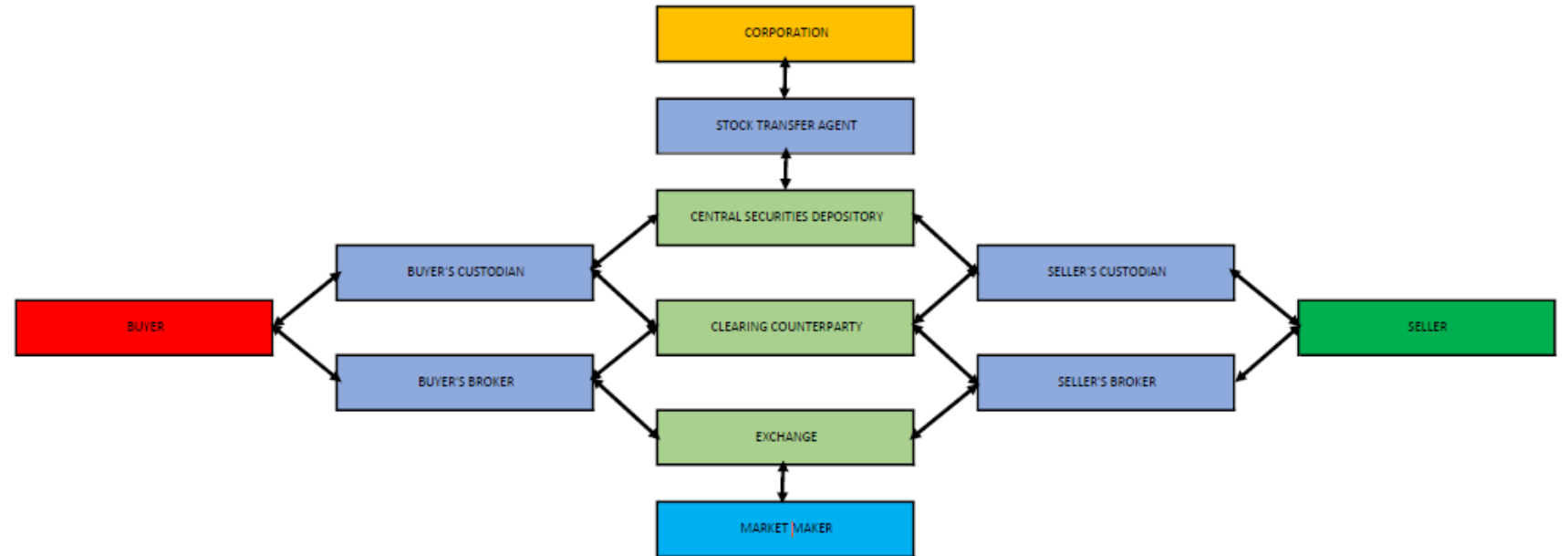


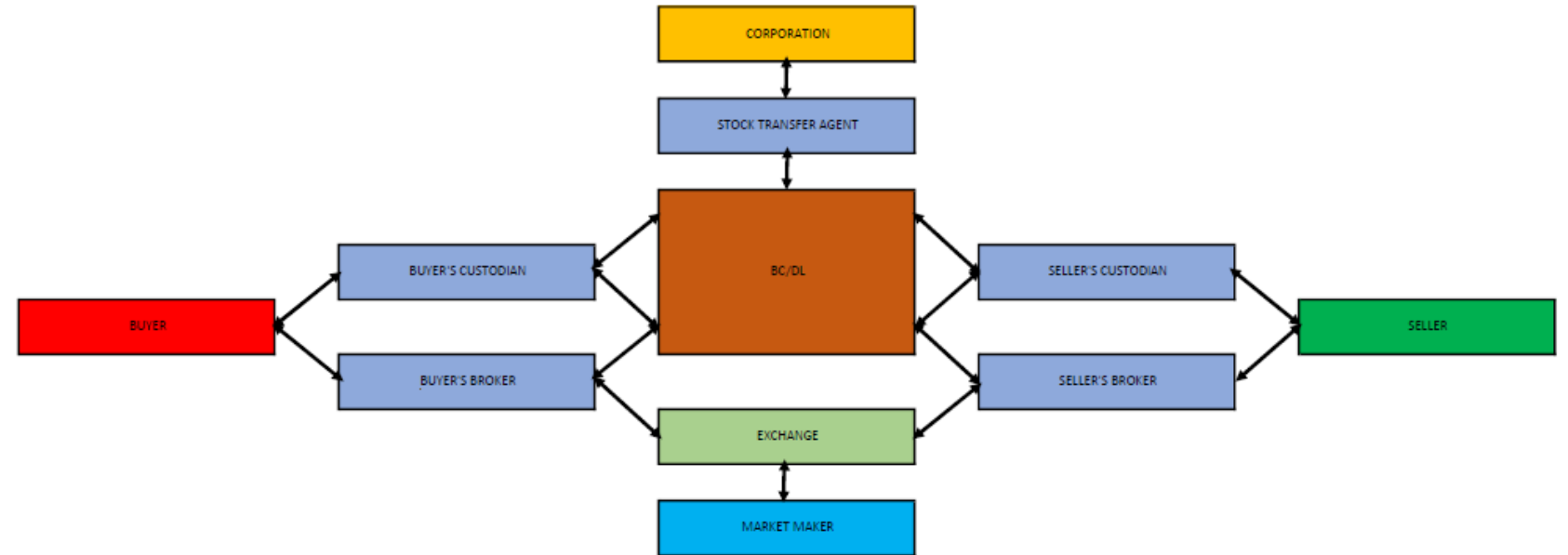
- There are three necessary steps if one wishes to trade public securities
 - A Buyers and sellers have to be matched
 - B Their transaction has to be cleared, i.e. novated to a central clearing counterparty (CCP)
 - C This transaction has to be settled, i.e. delivery vs. payment has to take place; so that title and money are transferred as expected
- These steps are characterized by vastly different time scales - trading often takes place in milliseconds, while clearing and settlement take 1-3 days!
- Although the proverbial T+2, T+3 irritate many people, they might be a bit too fast to push for T+15'
- Actual process is very involved and included investors, custodial banks, brokers (general clearing members, GCMs, of CCPs), exchanges, CCPs, central securities depositories (CSDs), regulators,



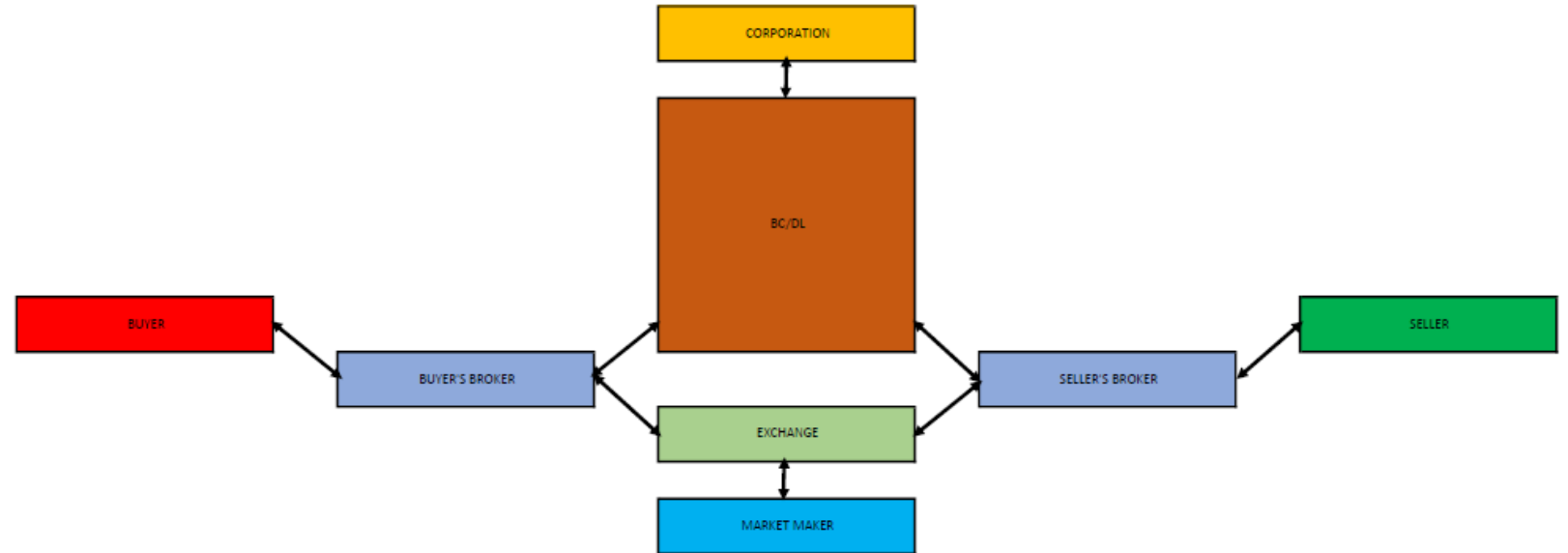
Trade
execution,
clearing,
settlement

- It is clear that straightforward attempt to apply a blockchain to clearing and settlement (thankfully, to the best of my knowledge, nobody wants to use it in trading *per se*) cannot be successful.
- The reasons are not difficult to understand - instantaneous settlement (T+15' as it is occasionally called) obliterates all the advantages of the current system including netting, ability to borrow, anonymity (to some degree), etc.
- It increases the magnitude of money sloshing around by an order of magnitude
- It will not be implemented any time soon (or ever?)
- Thus, speed is not so much a consequence of technological backwardness of exchanges (although they are not always using cutting edge technology), but rather a result of what they do and how they do it



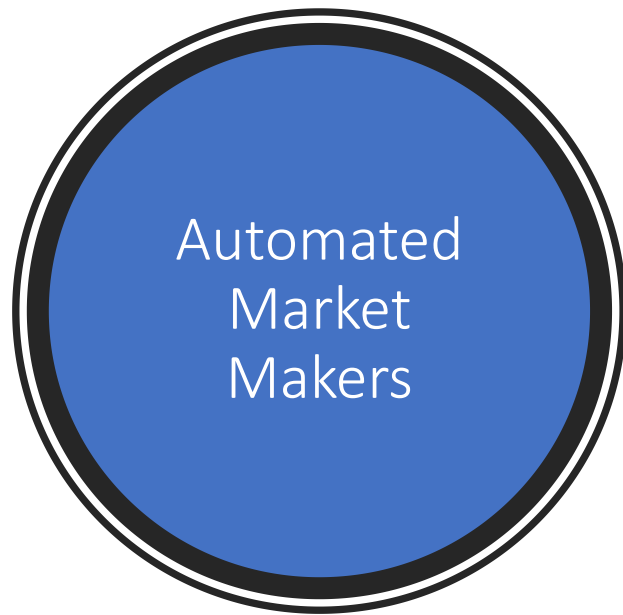


Trade
execution,
clearing,
settlement

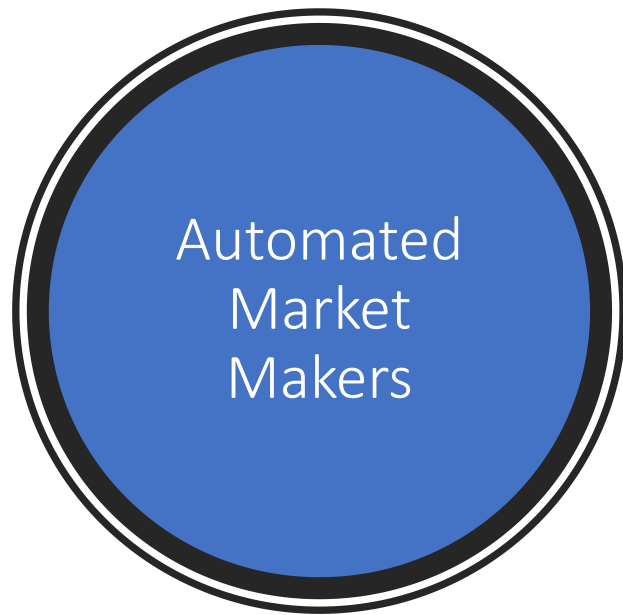




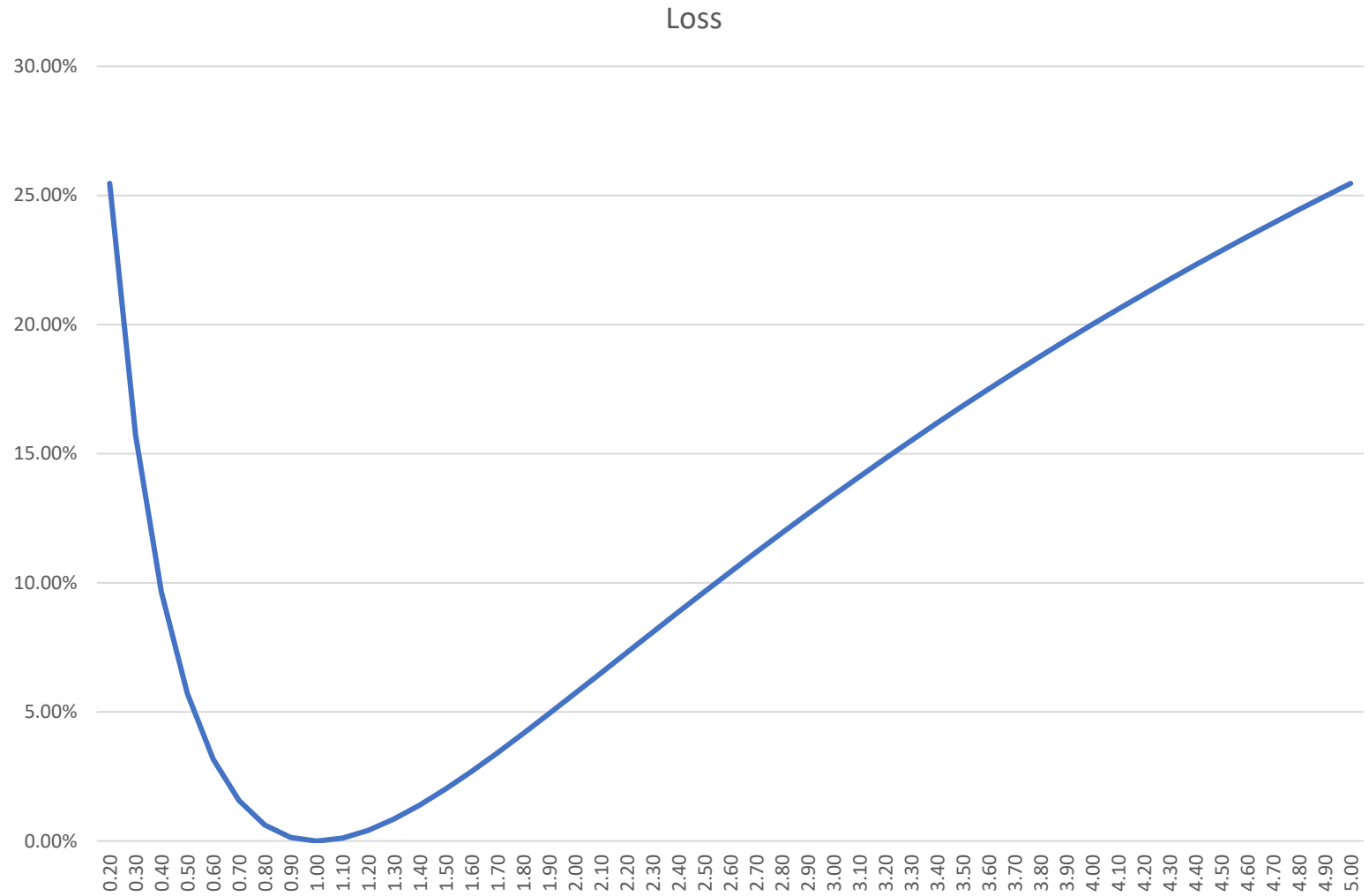
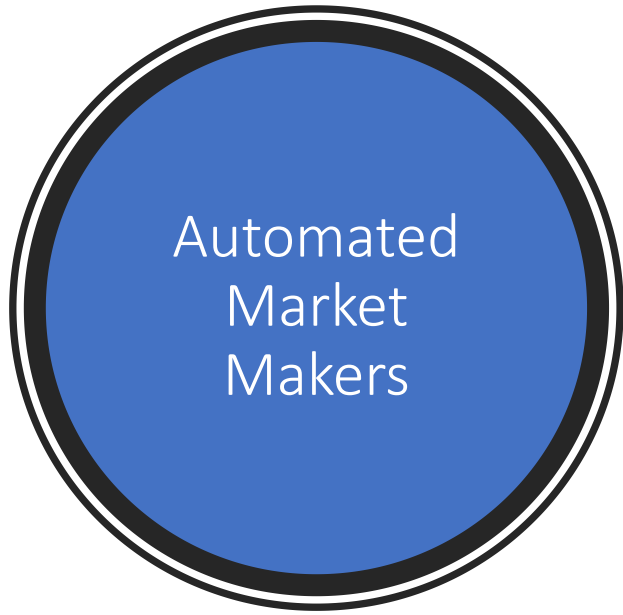
- Ethereum (warts and all) can be viewed as a CaaS provider, although it charges a lot for its services
- This aspect of Ethereum (or other blockchains which have smart contract capabilities) can be used to build Decentralized Finance (DeFi) applications
- DeFi moves away from the centralized system to peer-to-peer finance
- Typical DeFi vehicles:
 - DAOs are decentralized autonomous organizations
 - DEXs are decentralized exchanges
 - Payments and stable coins
 - Yield farming
 - Tokenization
 - Gaming
 - Identity provision

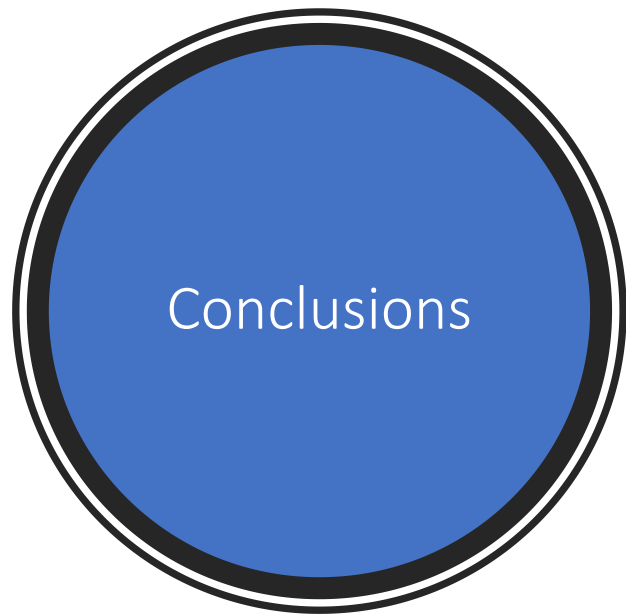


- Automated Market Makers (AMM), such as Uniswap, Balancer and Curve recently became immensely popular
- Overall volume is hard to estimate, but we are talking about 15Billion USD or more
- The original idea is very simple. It can be made more complicated if needed, by providing governance tokens, and similar sweeteners.
- Consider two tokens, which are initially priced at par.
- A participant, who wishes to be an AMM contributes equal number of both to a smart contract
- $N_1 = N_2 = N$
- At any moment in time the product is constant
- $N_1 * N_2 = N^2$
- Every time an arbitrageur changes the composition of the pool, a percentage (say 0.5%) is paid to the pool operator



- Assume that the price P of the second token expressed in terms of the first deviates from its initial value $P=1$
- For example $P>1$
- Then an arbitrageur will step in and purchase the second token by paying for it with the first.
- The optimal positions are as follows
- $N_1 = P^{1/2}N$, $N_2 = P^{-1/2}N$
- The arbitrageur's profit is $(P^{1/2}-1)^2 N$
- Buy and hold portfolio value is $(P+1)N$
- Arbitraged portfolio value is $2P^{1/2} N$
- % loss (also called in the DeFi parlance impermanent loss)
- $L=1-2 P^{1/2}/(P+1)=(P^{1/2}-1)^2/(P+1)$
- The idea is that if the price is mean-reverting, the impermanent loss goes away and transaction fees accumulate to provide 10% return, say.
- Of course, if the price does not mean-revert it is not going to happen, and the loss will be permanent





- The idea of distributed ledgers is not new
- Modern technology gives it a new lease of life
- Potentially, distributed ledgers have numerous applications in finance
- Cryptocurrencies are the best known but not the only ones
- Conventional cryptocurrencies are interesting but not very promising
- Digital cash is very promising avenue
- Retail banks may bifurcate into narrow banks and investment pools
- Asset-backed cryptocurrencies can serve as a much-needed counterpoint for fiat currencies
- DeFi is in its early stages, but if developed further, can provide a viable competitor to the existing centralized framework



- I am grateful to Dr. Marsha Lipton, Prof. Alex (Sandy) Pentland, Dr. Thomas Hardjono, Shamir Karkal, Angela Angelovska-Wilson, Isaac Hines, and Dr. Adrien Treccani for numerous stimulating discussions and the joy of working together.
- This is copyrighted material © Alexander Lipton, 2020
- This material cannot be reproduced in any form without written permission of the copyright holder.