Central Bank Digital Currency and Private Monies

Milan, May 10, 2018

ferdinando@ametrano.net
https://github.com/fametrano
https://twitter.com/Ferdinando1970
https://speakerdeck.com/nando1970
https://www.reddit.com/user/Nando1970/
https://www.slideshare.net/Ferdinando1970
https://it.linkedin.com/in/ferdinandoametrano
https://www.youtube.com/c/FerdinandoMAmetrano

POLITECNICO
MILANO 1863

UNIVERSITÀ DEGLI STUDI DI MILANO
BICOCCA

The Information Economy

- Data is transferred with zero marginal cost
- Why pay a fee to move bytes representing wealth?
- Why only 9-5, Monday-Friday, two days settlement?
- Who (and when) will gift humanity with a global instantaneous free p2p payment network?

Reliable E-Cash
Will Be Developed on the Internet

The one thing that's missing, but that'll soon be developed, is a reliable e-cash, a method whereby on the internet you can transfer funds from A to B, without A knowing B or B knowing A, the way I can take a 20 Dollar bill and hand it over to you...

Milton Friedman, 1999

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

Agenda

1. **Central Bank and Private Digital Cash**
2. About Money and Innovationa
3. Private Monies and Bitcoin
4. Hayek Money

Central Bank Digital Currency

"[… it] is appealing […] it would mean people have direct access to the ultimate risk-free asset [...] it could exacerbate liquidity risk by lowering the frictions involved in running to central bank money [...] it could fundamentally and perhaps abruptly re-shape banking"

Mark Carney, Governor of the Bank of England, June 2016

http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf

Central Bank Digital Currency

"Allowing the public to hold claims on the central bank might make their liquid assets safer, because a central bank cannot become insolvent. This is an feature which will become relevant especially in times of crisis – when there will be a strong incentive for money holders to switch bank deposits into the official digital currency simply at the push of a button. But what might be a boon for savers in search of safety might be a bane for banks, as this makes a bank run potentially even easier."

Jens Weidmann, President of Bundesbank, June 2017
https://www.ft.com/content/414072b7-0de5-3864-9493-14438eab30ae

Cash On The Ledger:
Imperative for Delivery vs Payment

- Hardly provided by Central Banks
- IMF sponsored blockchain tokens might replace Special Drawing Rights: unrealistic as it would severely undermine US dollar predominance
- absent from the agenda of prominent players promising DLT solutions
- A free instantaneous P2P payment network is a great opportunity for retail banks (probably worth a consortium)

Cash or Electronic Money

- Cash is a privacy preserving bearer asset
- Electronic money is attributed to a given customer and can be recovered

Cash Digitization: Proof of Concept

- Bitcoin core codebase
- Mining, i.e. transaction finalization, reserved to vetted nodes (block signing from Elements)
- Thousands transactions per second
- Apps: wallets (iOS, Android, Desktop), blockexplorer, issuer dashboard

Cash Digitization: Security and Guarantees

- Coin issuance backed by fiat currency reserves
- Entrance/exit gateway (fiat currency <-> digital cash) monitored with KYC and AML processes
- Issuer/admin able to confiscate coins to any address if needed/required

Cash Digitization: Regulators' Feedback

Transactions must be attributed to known customers

-> Electronic money, not cash

Alllowed applications must be certified, i.e. closed network

-> Client-server approach, not peer-to-peer

Digital Currency
Does Not Need Blockchain

- Client-server solutions can be explored, e.g. SatisPay, even with bitcoin-like transactions
- What is relevant is which reserve asset is backing the digital currency (if not issued by a central bank)
- If customers are identified, then it is electronic money, not cash

Why is finance fascinated with blockchain?

Blockchain transactions are immediately validated, then cleared and settled shortly thereafter, automatically without a central authority

- In the financial world, ***cash*** transactions are cleared and settled automatically without a central authority

Consensus by Reconciliation

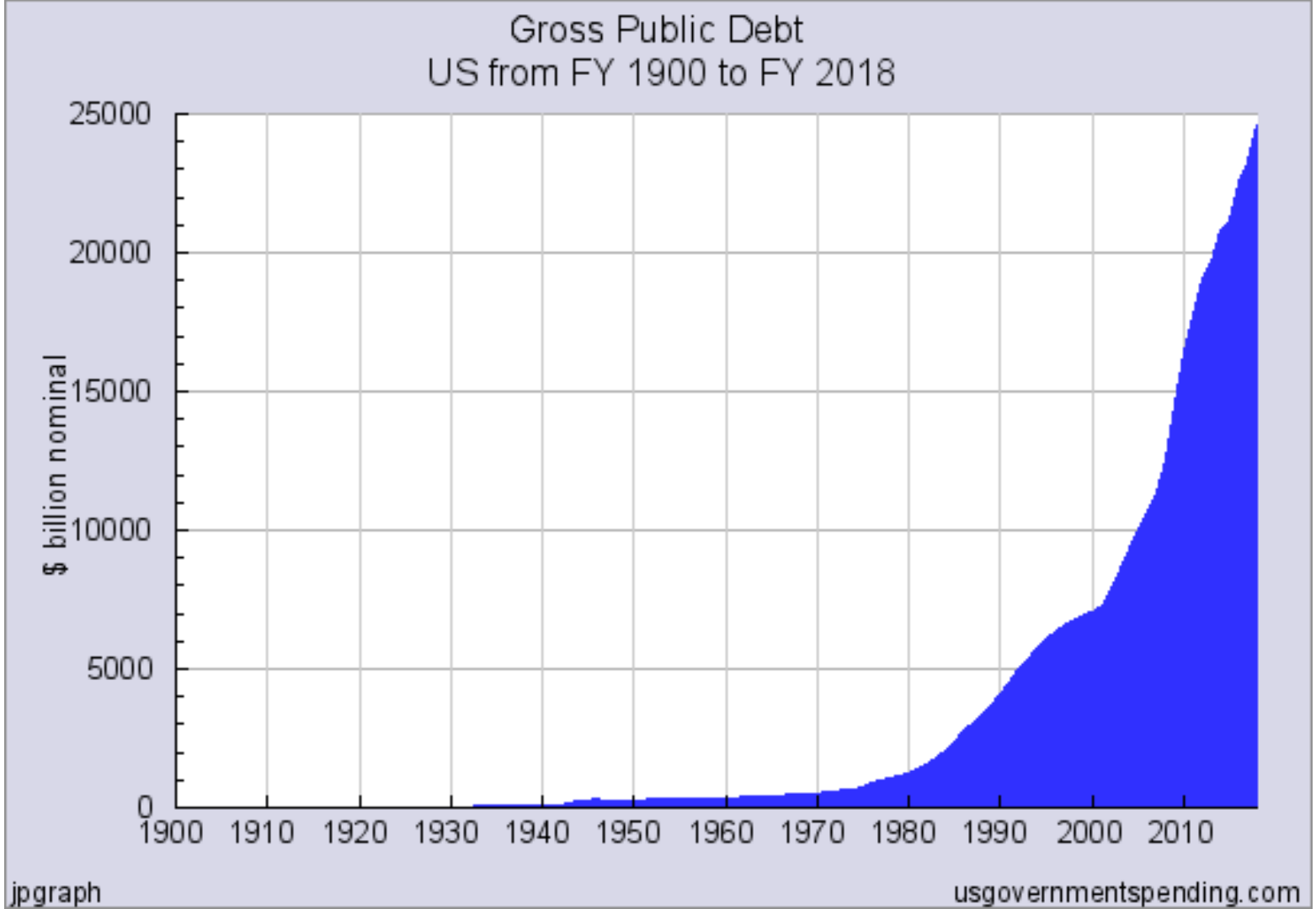
- Non-cash financial transactions, e.g. stock trading, can be executed in nanoseconds, but are cleared and settled in days
- Not a technological problem
- Consensus by reconciliation of multiple independent ledgers: a *checks and balances* system that allows for prescriptions, corrections, and restrictions

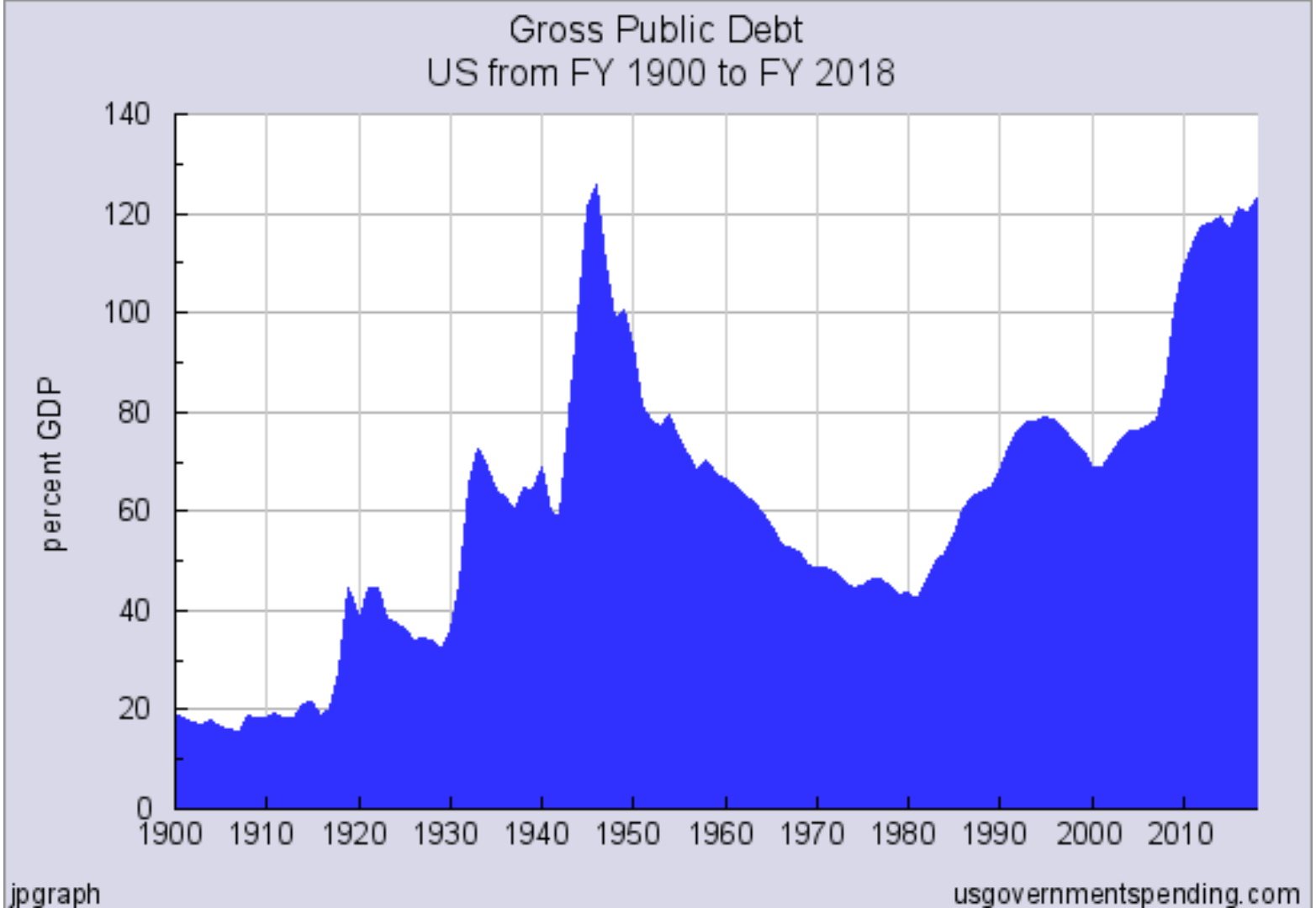
Agenda

1. Central Bank and Private Digital Cash
2. **About Money and Innovation**
3. Private Monies and Bitcoin
4. Hayek Money

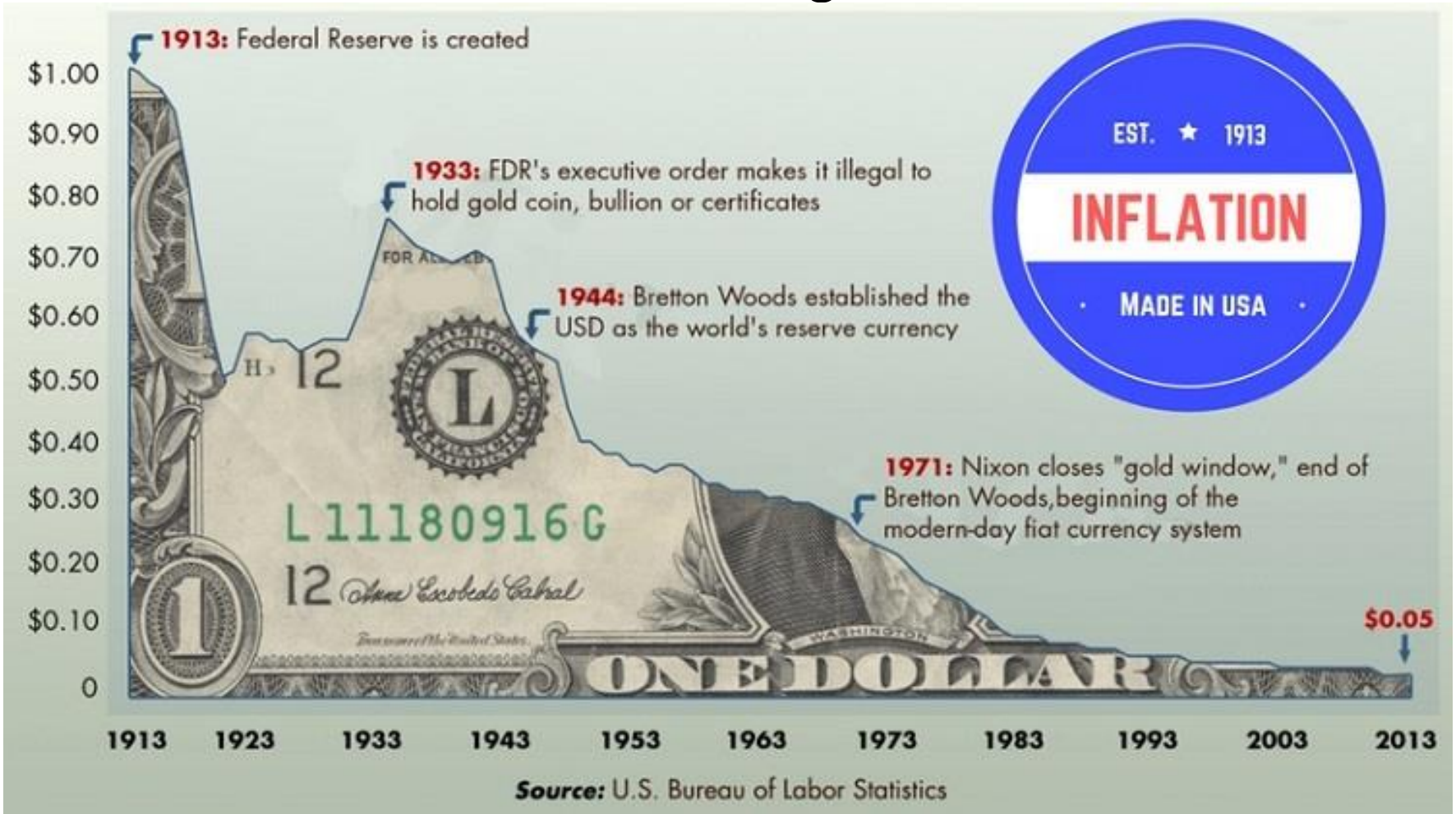
Trade Economy
From Gold Standard to Fiat Money

- Gold: the commodity money standard
  - scarce
  - pleasant color, i.e. resistant to corrosion and oxidation
  - high malleability
  - relative easiness of its purity assessment
- Gold purity certification
- Representative money
- Fractional receipt money
- *Fiat* money and legal tender


Gross Public Debt
US from FY 1900 to FY 2018
$ billion nominal
25000
20000
15000
10000
5000
0
1900
1910
1920
1930
1940
1950
1960
1970
1980
1990
2000
2010
jpgraph
usgovernmentspending.com


Gross Public Debt
US from FY 1900 to FY 2018
percent GDP
140
120
100
80
60
40
20
0
1900
1910
1920
1930
1940
1950
1960
1970
1980
1990
2000
2010
jpgraph
usgovernmentspending.com

USD Purchasing Power



Take Money out of the Hands of Government

I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop.

F. A. Hayek

https://youtu.be/EYhEDxFwFRU?t=19m23s

Friedrich August von Hayek
Denationalisation of Money

- history of coinage is an almost uninterrupted story of debasements; history is largely a history of inflation engineered by governments for their gain
- why government monopoly of the provision of money is regarded as indispensable? It deprived public of the opportunity to discover and use a better reliable money

Blessed will be the day when it will no longer be from the benevolence of the government that we expect good money but from the regard of the banks for their own interest

A Free-Market Monetary System, Gold and Monetary Conference, New Orleans, Nov. 1977, https://mises.org/daily/3204

Hayek, F. A., Denationalisation of Money, The Institute of Economic Affairs, http://www.mises.org/books/denationalisation.pdf

Money As A Social Relation Instrument

1. Human beings are born into a gift economy
2. Enlarged relationship circle requires exchange economy
3. Barter economy: coincidence of wants
4. Trade economy: money as medium of exchange
5. Global information economy: supranational digital money

Permissionless Innovation Fast and Effective

- No centralized security mechanism, no barrier to enter, no editorial control
  - Email has not been designed by a consortium of postal agencies
  - Internet has not been developed by a consortium of telcos
- Will a decentralized transactional network be designed by a consortium of banks?

Agenda

1. Central Bank and Private Digital Cash
2. About Money and innovation
3. **Private Monies and Bitcoin**
4. Hayek Money

Private Monies

- A medium of exchange issued by a non-governmental body, without legal privileges
- Private monies do not have to be generally acceptable; they merely have to be accepted in a given economic community
- Public demand for private currencies:
  - hold them in the expectation that they will not diminish in purchasing power as state money has
  - wish to be part of a movement against increasing state control of economic and personal behavior
  - conduct illegal activity
  - just want better money

Double Spending Problem

- To securely transfer value using digital means has been possible for decades
- In digital cash schemes, a single digital token, being just a file that can be duplicated, can be spent twice
- A centralized trusted party has always been required to prevent ***double spending***

Liberty Dollar: 1998-2009

- Private mint that issued gold and silver coins; also issued notes redeemable in precious metals
- Periodically revalued against USD: the value of the latter fell over time against precious metals
- Specifically designed to function in parallel with and in competition to USD
- Never marketed or represented as official US currency
- Highly successful: it became the second most popular currency in the US
- Its use declared a federal crime by the US government
- Its founders convicted for counterfeiting, fraud and conspiracy against the United States

E-gold: 1996-2007

- Digital payment system with gold as unit of account
- User accounts backed by gold reserves
- By 2005, e-gold had grown to be second only to PayPal in the online payments industry: 1.2M accounts and $1.5B transactions
- Indicted in April 2007 by US law enforcement services
- Charges: unlicensed money-transmitting entity and a means of moving the proceeds of illegal activities
- Never proven and even the judge expressed major doubts
- ‘Offshore’ payment system rather than a money transmitter or bank as defined under then-existing regulations, not least because gold was not legally ‘money’

Distributed Consensus

- Without a central trusted party, how does the Bitcoin protocol reach consensus on transaction history?
- Consensus in an asynchronous network with faulty (or malicious) nodes is proved to be impossible
- A problem known as Byzantine General Problem

Mining

- All network nodes validate all transactions; those also providing the computational power for clearing and settlement are called ***miners***
- Miners compete to finalize a new block of transactions: the winner providing *proof-of-work* is rewarded with the issue of new bitcoins in a special *coinbase* transaction included in the block
- Miners solve the double spending problem:
  - double spending (or invalid) transactions would invalidate the block
  - an invalid block would be rejected from the network
  - the bitcoin reward would be removed from transaction history
  - miner would have wasted his work

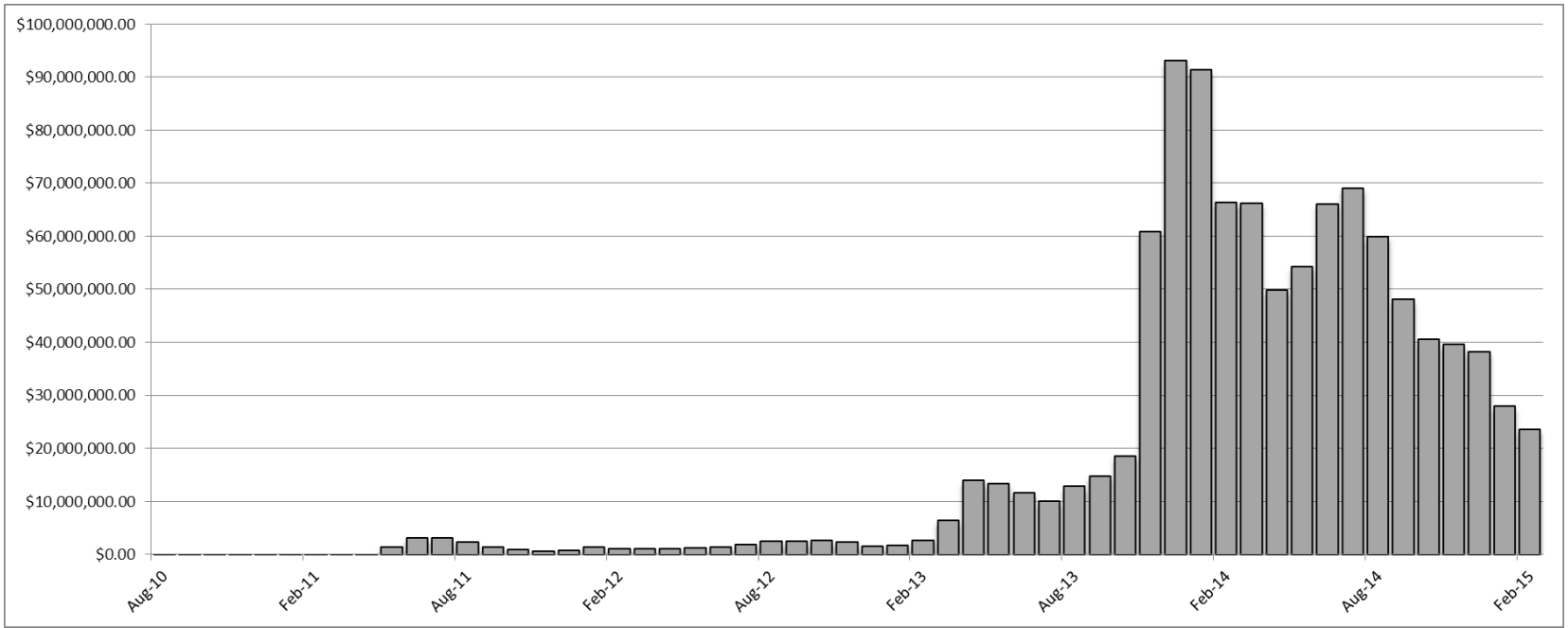
Bitcoin Distributed Consensus

- Practical Byzantine Fault Tolerant (PBFT) *distributed consensus* is achieved using *(game theory) economic incentive* for the mining nodes to be honest.
- Double spending is solved without a central trusted party
- Bitcoin can resist attacks of malicious agents, as long as they do not control network majority
- Miners are compensated for their *proof-of-work* using seigniorage revenues, i.e. with issuance of new bitcoins

Seigniorage Revenues Cover Consensus Cost

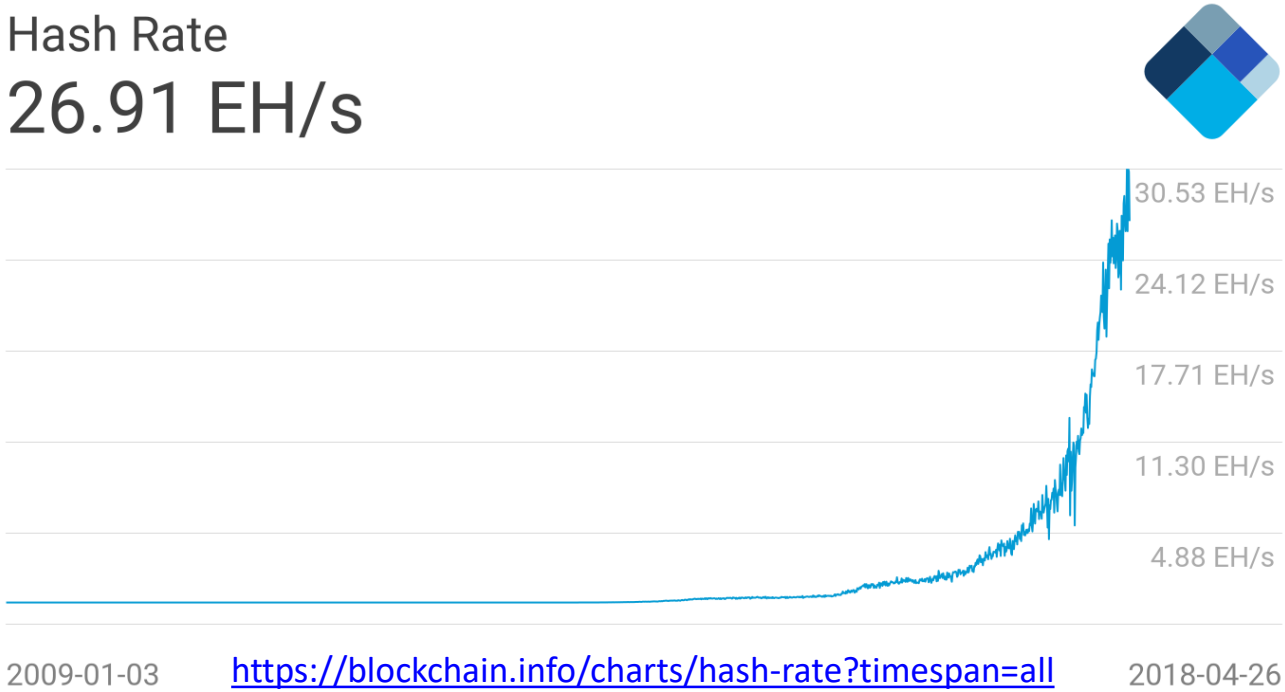
- Seigniorage revenues subsidize the network, making transactions cheap
- 144 block/day, 365 day/year, 12.5 BTC/block, $10,000 per BTC

Currently about $7 billions per year (as of November 2017)



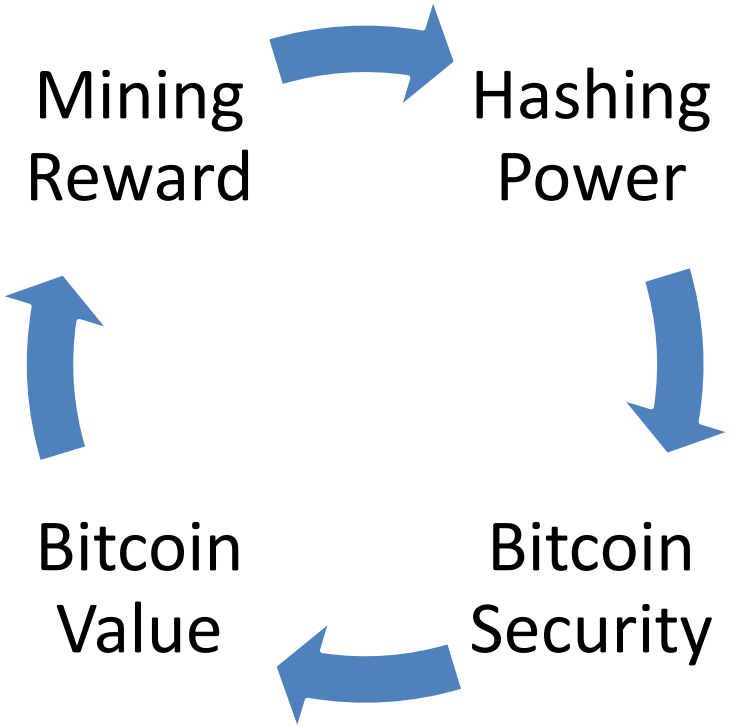
Network Hash Rate

- 100,000s times more powerful than the world top 500 supercomputers
- To manipolate blocks 51% of the Hash Rate is required



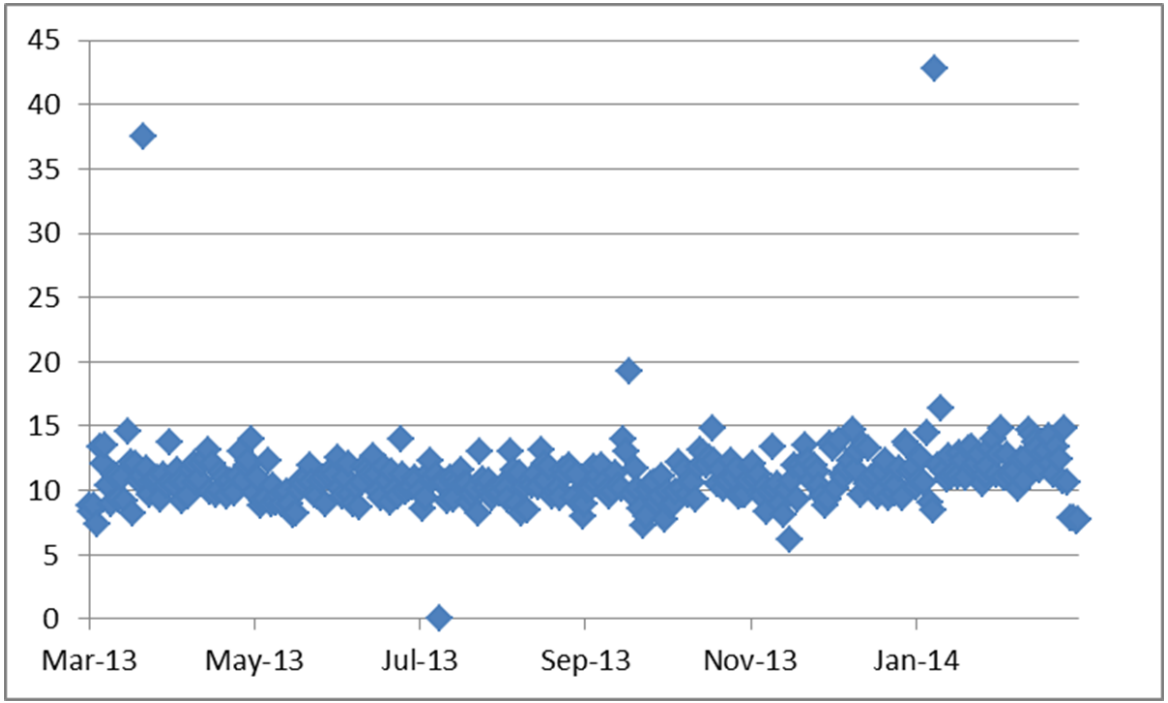
https://blockchain.info/charts/hash-rate?timespan=all

Virtuous Cycle



Validation Process: Block Generation

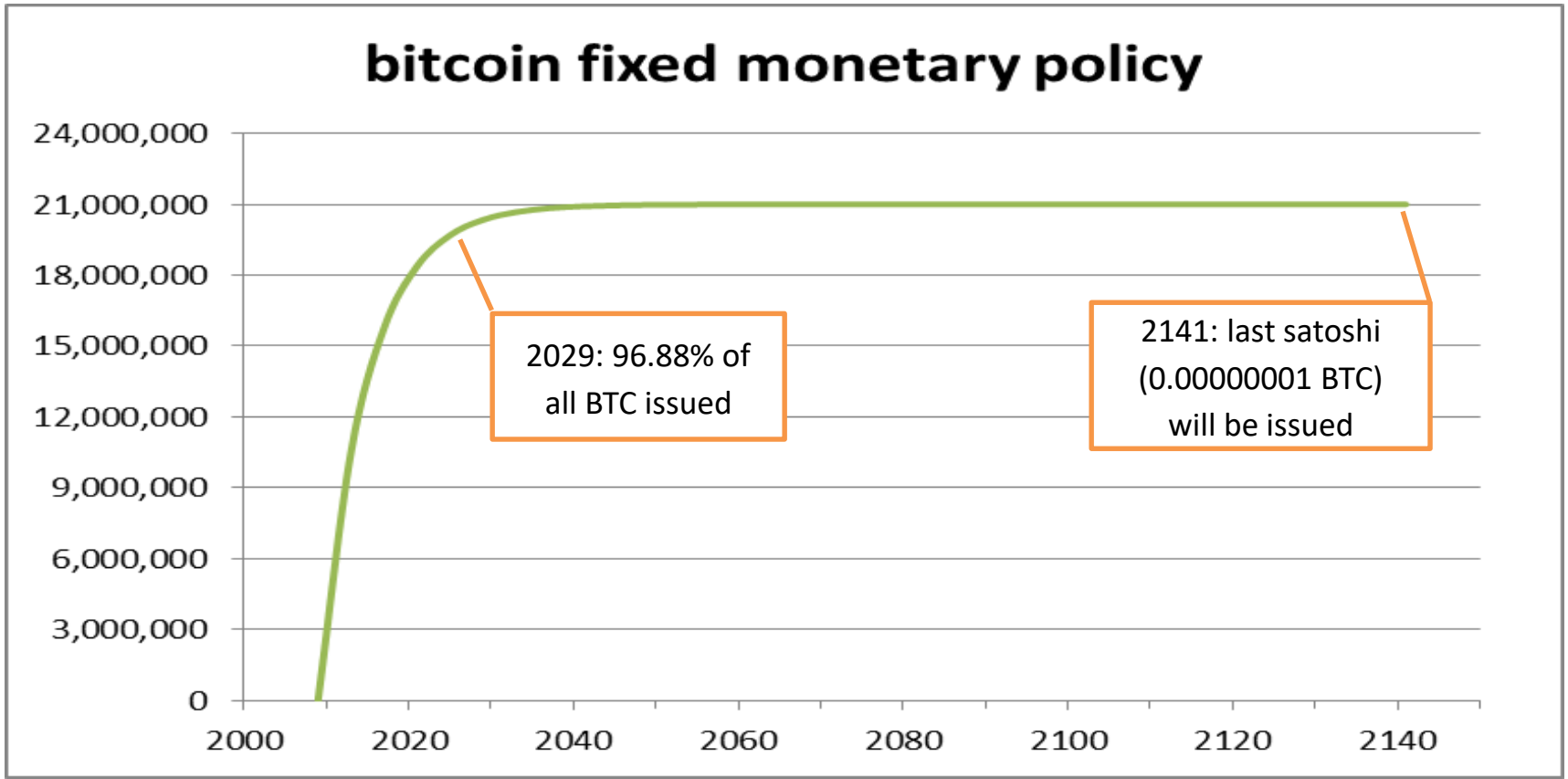
The proof-of-work *difficulty* is adapted to the overall available computing power to ensure an average of one block every ten minutes



Bitcoin Monetary Rule

- 2009: 50BTC per block, every 10 minutes
  - halving every 4Y
- This is the only way new bitcoins are released
- It is called mining because of its similarity with the progressive scarcity of gold extraction
- Supply free of discretionary intervention

Bitcoin Inelastic Supply: Deterministic Decreasing Rate



What Makes Bitcoin Special?

- Digital and scriptural: it only exists as validated transaction
- Asset, not liability
- Bearer instrument
- It can be transferred but not duplicated
  (i.e. it can be spent, but not double-spent)
- Scarce in digital realm, as nothing else before
- Mimicking gold monetary policy

Bitcoin is digital gold

this is the groundbreaking achievement by Satoshi Nakamoto

- More a crypto-commodity then a crypto-currency

Bitcoin Relevance

If one thinks about the role of physical gold in the history of civilization, money, and finance

the digital equivalent of gold could be disruptive

in the current digital civilization and the future of money and finance

Gold Is Not Loved

- 1933 Gold Act "forbidding the hoarding of gold coin, gold bullion, and gold certificates within the continental United States".
- 1966 Greenspan: “This is the shabby secret of the welfare statists' tirades against gold. Deficit spending is simply a scheme for the confiscation of wealth. Gold stands in the way of this insidious process. It stands as a protector of property rights. If one grasps this, one has no difficulty in understanding the statists' antagonism toward the gold standard.”
- 1972 Nixon shock: unilateral cancellation of the convertibility of the United States dollar to gold.

Bitcoin as (Digital) Gold in the History of (Crypto)Money

gold

- Its adoption was not centrally planned
- For centuries it has been the most successful form of money
- It has bootstrapped all monetary systems we know of
- It has been surpassed by other kind of money without becoming obsolete

bitcoin

- Its adoption has not been centrally planned
- It is the most successful form of cryptocurrency
- It will bootstrap new monetary systems
- It might be surpassed by more advanced type of cryptocurrencies without becoming obsolete

The Ultimate Fate of Bitcoin: To Serve as a Reserve Currency

Hal
VIP
Sr. Member

Activity: 314

Re: Bitcoin Bank
December 30, 2010, 01:38:40 AM

#10

Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital cash currency, redeemable for bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. Likewise, the time needed for Bitcoin transactions to finalize will be impractical for medium to large value purchases.

Bitcoin backed banks will solve these problems. They can work like banks did before nationalization of currency. Different banks can have different policies, some more aggressive, some more conservative. Some would be fractional reserve while others may be 100% Bitcoin backed. Interest rates may vary. Cash from some banks may trade at a discount to that from others.

George Selgin has worked out the theory of competitive free banking in detail, and he argues that such a system would be stable, inflation resistant and self-regulating.

I believe this will be the ultimate fate of Bitcoin, to be the "high-powered money" that serves as a reserve currency for banks that issue their own digital cash. Most Bitcoin transactions will occur between banks, to settle net transfers. Bitcoin transactions by private individuals will be as rare as... well, as Bitcoin based purchases are today.

Hal Finney

https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211

Hal Finney (1956–2014) was a noted cryptographic activist. He was the second PGP Corporation developer hired after Phil Zimmermann. He created the first reusable proof-of-work. He was an early bitcoin user and received the first bitcoin transaction from bitcoin's creator Satoshi Nakamoto.

Agenda

1. Central Bank and Private Digital Cash
2. About Money and Innovation
3. Private Monies and Bitcoin
4. **Hayek Money**

The Holy Grail of Stable Prices

- Gold standard, bimetallism, symmetallism
- Fixed value of bullion (Aneurin Williams 1892)
- Compensated dollar (1911-20 Irving Fisher)
- Commodity Reserve Currency (1932 J. Goudriaan, 1937-44 B. Graham, 1942 F. Graham, 1951 M. Friedman)
- ANCAP basket (1982 Robert Hall)
- Futures contracts (1984 Miles, 1989-95 Sumner)
- Quasi-futures contract (1994 Kevin Dowd)
- Price index option (2000 Kevin Dowd)

Unit of Account: Money as Numeraire

- Money is the unit of account against which the value of every other good is measured
- The price system measures the value of goods relative to the value of money

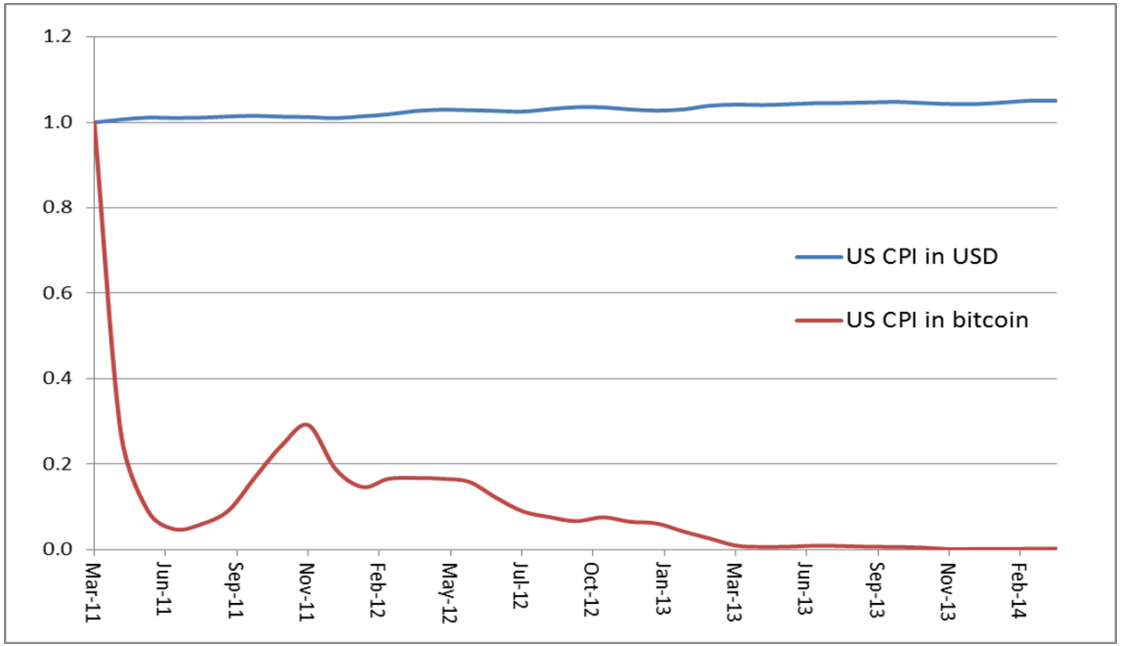
Good money should provide stable prices to best perform its role as unit of account

Money Comparison

	Medium of Exchange	*Store of ~~Constant~~ Value*	*Unit of Account*
Live cattle			
Diamonds			
Gold			
Fiat coins and notes			
Bitcoin			
	• swappable • fungible • portable • divisible • recognizable • resistant to counterfeiting	• reliably saved, stored, and retrieved • retain usefulness over time • Maintain its storage properties • non-perishable or with low preservation cost	• relative worth unit of measure • stable value for stable price comparison • supply must be controlled in some way

Bitcoin, Being Digital Gold, Is Not a Good Unit of Account

- no salaries, no mortgages, no stable purchasing power
- *successful at getting rid of a centralized monetary authority, it has given up the flexibility of an elastic supply of money*



Hayek Money:
A New Generation of Cryptocurrencies

- The cryptocurrency monetary standard of **elastic <u>non-discretionary</u>** supply
- Price stability paradigm with respect to a given reference basket
- Concurrent cryptocurrencies will compete in monetary policy definition and reference basket choices
- Bitcoin can be used as reserve asset

Hayek Money Implemented as Dual Asset Ledger

Split *transactional* and *speculative* money demand with *two non-fungible assets*:

- (stable) transactional coins
- (unstable) speculative shares

Blockchain technology tracks ownership and transactions for both: *dual asset ledger*

Reserve Asset Bank IPO

- Raise bitcoins as reserve asset in $ResAss$ quantity

  Better to avoid non-crypto reserve assets or a custodian legal entity would be required, re-introducing centralization

- Issue C coins and S shares

Monetary base is backed by $ResAss$:

$$C \cdot P_C + S \cdot P_S = ResAss$$

Reserve Asset Bank: Stable Coins

- When $P_C \cong 1$, coins give up any speculative value
- Money velocity and transaction volume increase

$$MV = PT$$

M is the money supply (total amount of money in circulation;
V is the velocity of money for all transactions in a given time frame;
P is the price level;
T is the aggregate real value of transactions in a given time frame.

- Coins not to be inflated/deflated arbitrarily
- Transaction validation to be rewarded with issuance of new shares, not coins

Reserve Asset Bank: Seigniorage Shares

Seigniorage: profit made by a currency issuer, especially the difference between the face value of coins and notes and their production costs

- Shares are never burned/destroyed
- Shareholders are in charge of *reference basket* maintenance

- The share price is free to float: shareholders absorb all monetary policy's costs and benefits, shielding coin holders from volatility
- Share value = assets - liabilities

$$S \cdot P_S = ResAss - C \cdot 0.95$$

Monetary Policy Target

Coin is pegged to a given *reference basket* for price parity:

$P_C \cong 1$, allowing for a corridor, e.g. $0.95 < P_C < 1.05$

- Must be $C \ll ResAss$ at IPO
- Hopefully $C < ResAss$ any time later on

The Reserve Asset Bank (even as Decentralized Autonomous Organization) enforces price boundaries by market operations using reserve assets

Monetary Phases

Expansionary monetary phases (when $P_C \uparrow 1.05$):

- new coins are minted by the Reserve Asset Bank and sold for 1.05 in exchange for bitcoin (increasing reserves)

Contractionary monetary phases (when $P_C \downarrow 0.95$):

- existing coins are bought at 0.95 (and destroyed) by the Reserve Asset Bank using bitcoin (until reserves are depleted)

Leverage Bitcoin As Reserve Asset

- Bitcoin is the first and most successful instance of an intrinsically scarce digital asset: it’s digital gold
- When used as reserve asset, its qualities are magnified!
- Its limits are lessened. No more need for:
  - scaling to huge (cash + bank accounts + credit cards) number of transactions
  - supporting economically inefficient micropayments
  - lowering confirmation time
- The Reserve Bank IPO raises bitcoins, issues seigniorage shares and stable coins

Bibliography

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) https://bitcoin.org/bitcoin.pdf
- *Hayek Money: the Cryptocurrency Price Stability Solution (2014)*, http://ssrn.com/abstract=2425270
- *Bitcoin, Blockchain and Distributed Ledger Technology: Hype or Reality?* (2017) https://ssrn.com/abstract=2832249
- Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (2018)
- *Bitcoin as Digital Gold* (2018), United Nations Department of Economic and Social Affairs; video: https://goo.gl/NkEC9w; slides: https://goo.gl/szzBXh
- *Blockchain Needs A Native Digital Asset*, https://www.finextra.com/videoarticle/1241/blockchain-needs-a-native-digital-asset
- *Bitcoin*, YouTube videos, https://goo.gl/qDvKXi

Takeaways

Thank You

1. Central bank digital currency is not going to happen anytime soon
2. Private digital cash backed by fiat currency reserves is possible
3. In both cases blockchain technology is not really needed
4. Bitcoin, being digital gold, could be as relevant as physical gold for history of civilization and future of money & finance
5. Bitcoin is bootstrapping new monetary systems
6. Price stability can be reached with Hayek Money