Digital
Gold
Institute

The Cryptocurrency Frontier in Monetary Engineering

Bitcoin as Reserve Asset

v2020-10-27

Comments, corrections, and questions: https://drive.google.com/open?id=1T2z4vfRvEv_wooerJI7FgD8IkxeTihlj

Table of Contents

1. **Hayek Money: Elastic Non-discretionary Policy**

2. Hayek Money: Dual Asset Ledger and Proof-of-Payment

Hayek Money, Ametrano (2014)

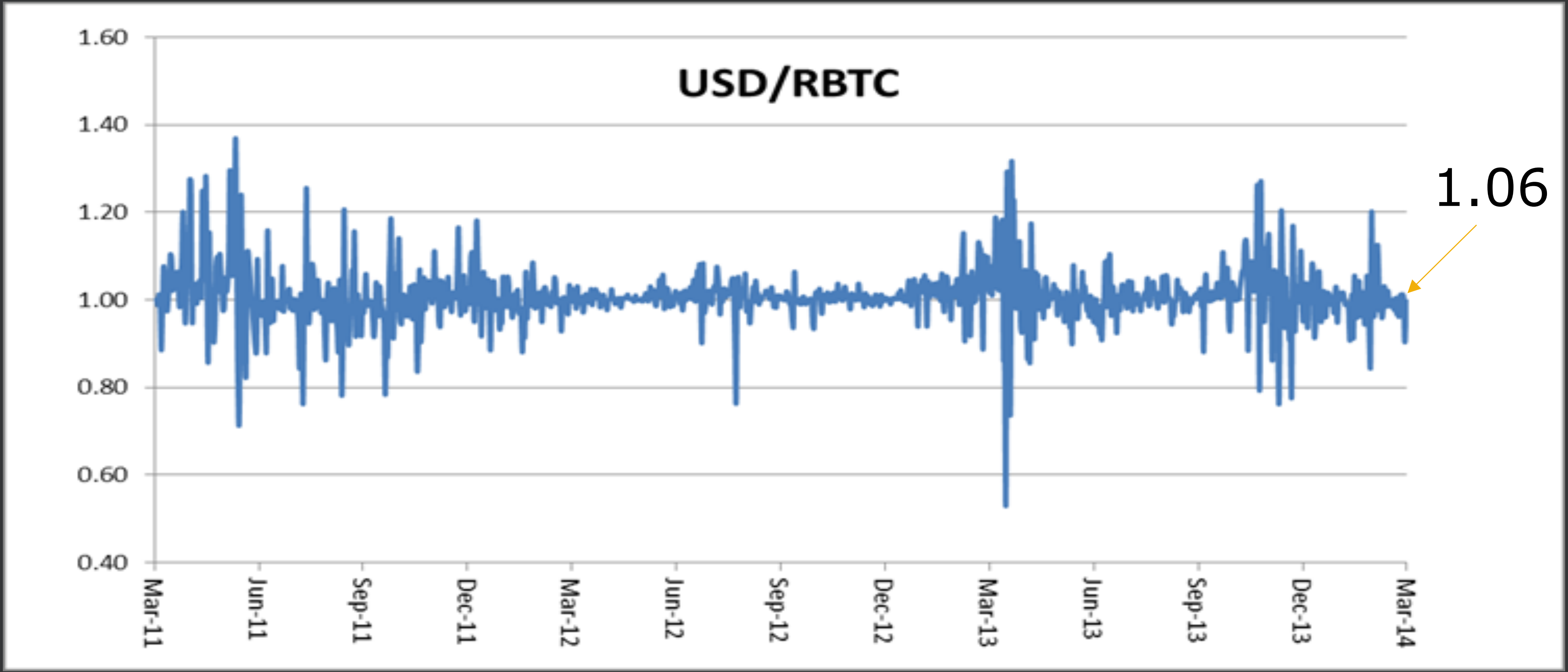
- The cryptocurrency monetary standard of **elastic non-discretionary supply**
- Price stability paradigm with respect to a given reference basket

- USD/BTC: 15-Apr-11 1.0, 29-Mar-14 500.0
- x500 increase for BTC demand relative to USD

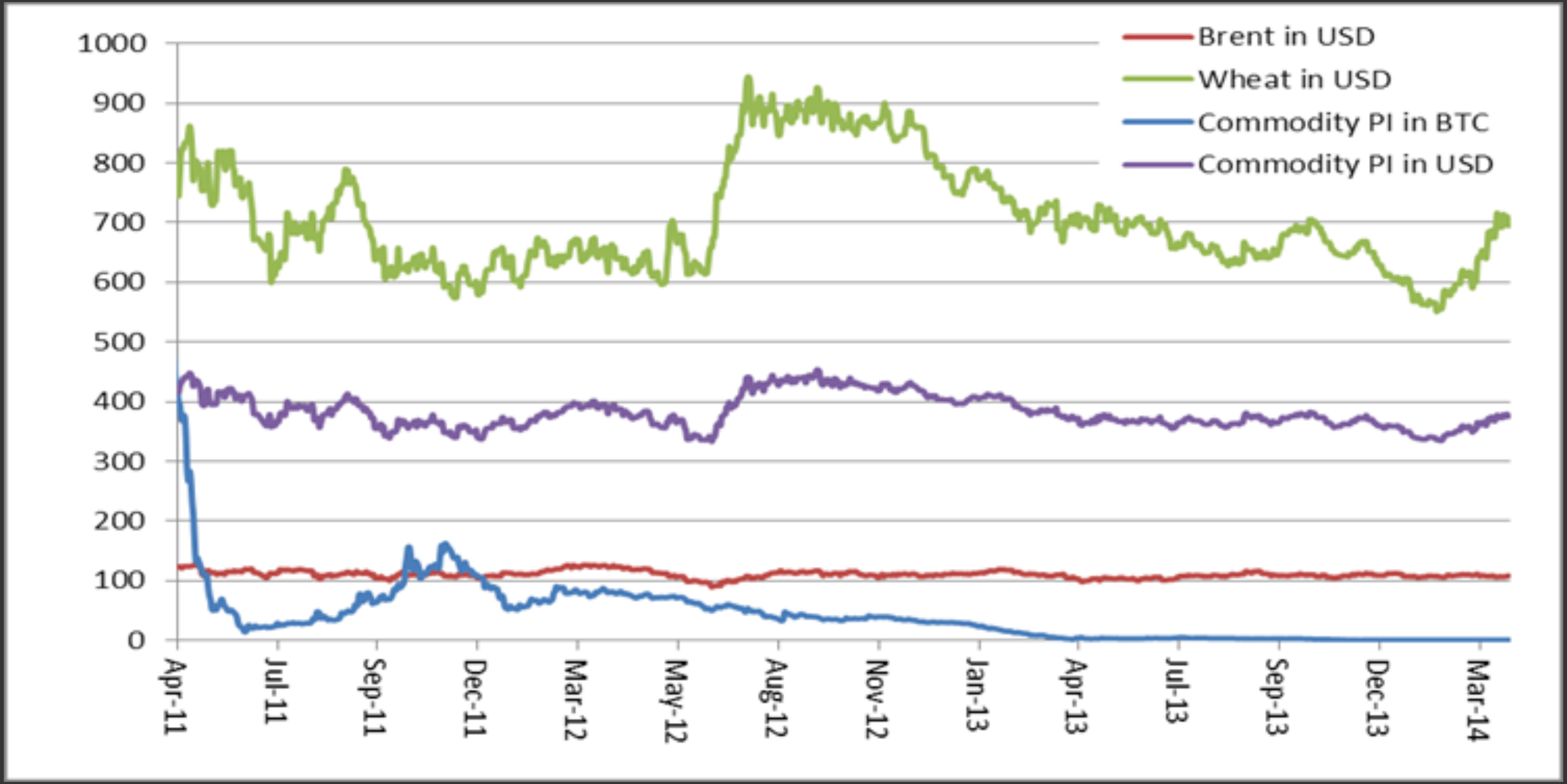
- 29-March-14: 12.5M bitcoins in circulation
- Inflate their number 500 times to 6250M
- On 29-Mar-14 it would have been equivalent to own:
  - 1 BTC worth $500
  - 500 RBTC (*rebased bitcoin*) each worth $1

USD-Parity (Daily) Rebased Bitcoin

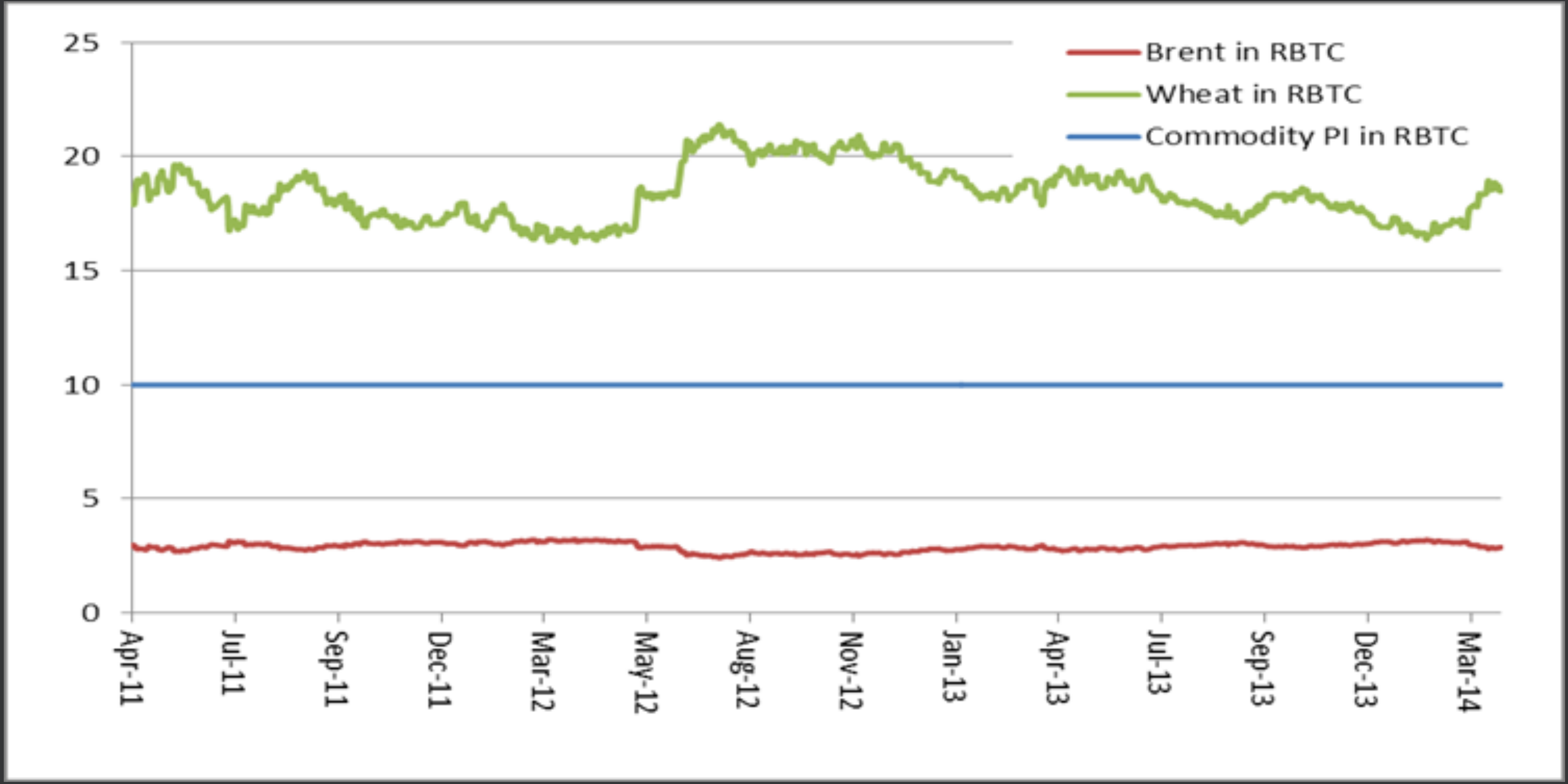
- Adopting the USD Consumer Price Index
- 6% inflation in the period March 2011-2014



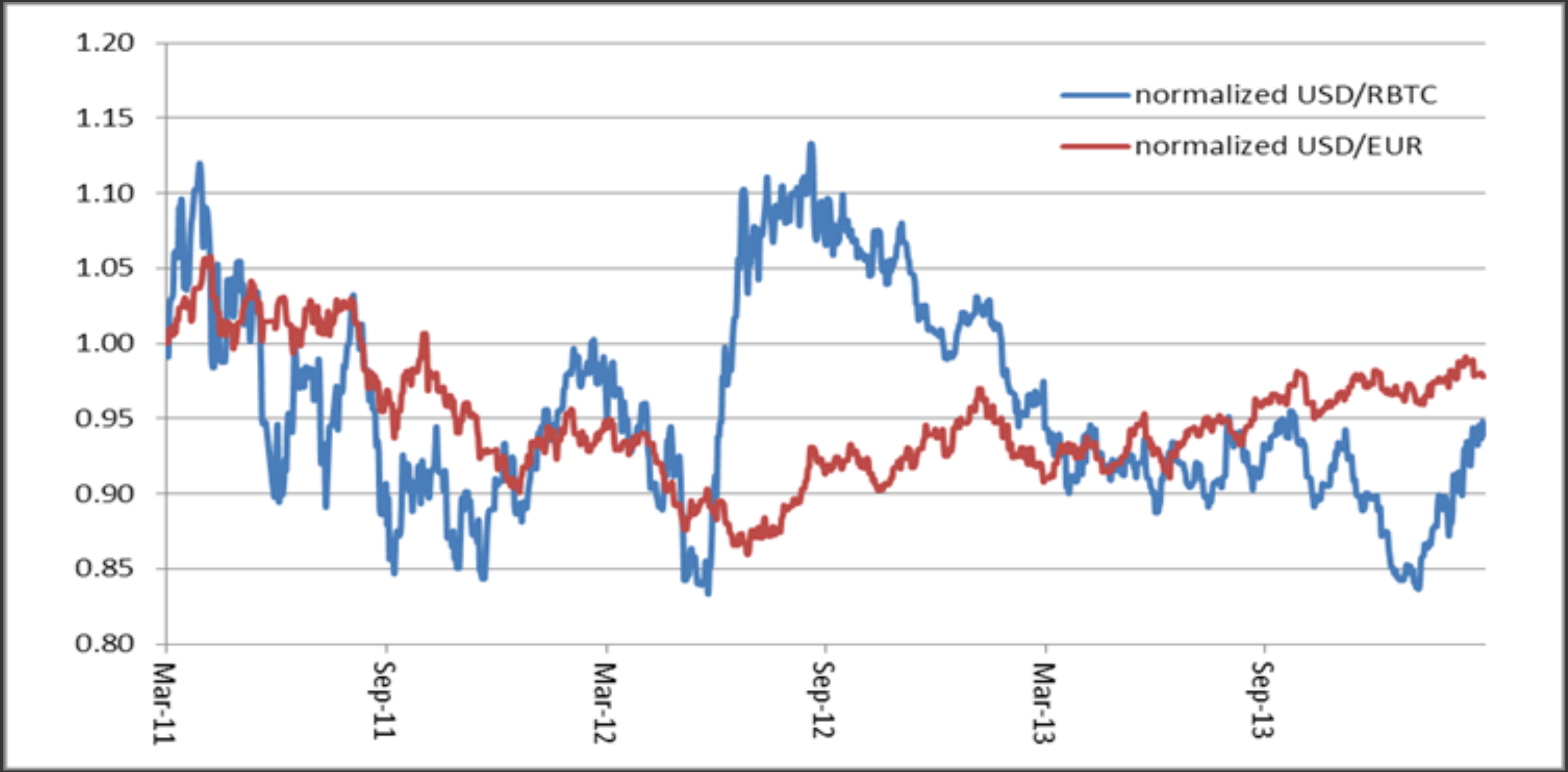
Avoid USD Monetary Policy: Brent-Wheat Basket Price Stability



Brent-Wheat Commodity Price Index Rebased Bitcoin



USD/RBTC vs USD/EUR Exchange Rate



Rebasing Bitcoin?

No, not really!

- Bitcoin was used for the sake of discussion, basically to leverage its historic price time series
- **Bitcoin is good as it is**: it is the digital equivalent of gold, more a cryptocommodity than a cryptocurrency

Hayek Money:
This First Simplistic Implementation (2014)

- Results:
  - Price stability
  - Salaries, mortgages, forward payments are possible

- Problems:
  - Number of coins in a wallet changes without any real cashflow: purchasing power of a given wallet is not stable
  - ***Coins still have speculative investment appeal and so enjoy limited transaction usage*** (do not buy pizza with them)

Early Improvements and Implementations

- M. Morini (2014) suggested to segregate coins in different investment (rebalaced) or saving (non-rebalanced) “wallets”, but failed to clarify how to avoid switching between the two regimes in inflationary/deflationary scenarios
- R. Sams was the first one to understand that two non-fungible different assets were needed: coins and seigniorage shares, but failed to clarify how to avoid exhausting one asset or the other in inflationary/deflationary scenarios

- Early implementation (BitShares, NuBits, Dai, Bancor) have been all naif, wrong, and/or centralized; consequently they failed or faded into insignificance
- Tether has been the only stablecoin successfully targeting USD parity, relying on reserves backing the coin, even if it is suspected to operate on fractional reserve

Table of Contents

1. Hayek Money: Elastic Non-discretionary Policy

2. **Hayek Money: Dual Asset Ledger and Proof-of-Payment**

Hayek Money Dual Asset Ledger

- Split *transactional* and *speculative* money demand with *two non-fungible assets*
- Blockchain technology tracks ownership and transactions for both: *Dual Asset Ledger* (DAL)
- A *Reserve Asset Bank* acts as issuer, issuing both
  - (stable) transactional coins
  - (unstable) speculative shares
- The market will assign respective prices P_C and P_S

Monetary Policy Target

- Make the **coin** **stable** in purchasing power with respect to a given *reference basket*

- The **coin** is pegged to parity:
  - $P_C \cong 1$ unit of the reference basket
  - corridor: $1 - \epsilon < P_C < 1 + \epsilon$ (e.g. $0.95 < P_C < 1.05$)

- **Coin**s must not be inflated/deflated arbitrarily

Monetary Policy Goal

If $P_C \cong 1$ always, **coin**s lose any speculative appeal!

- Money velocity and transaction volume increase

$$MV = PT$$

Where:

- *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.*

Reserve Asset Bank: Market Operations

- The Bank needs reserve assets $ResAss$ to enforces the coin price corridor $0.95 < \boldsymbol{P_C} < 1.05$ by market operations
- Floor enforcement: existing coins are always bought (then burned, destroyed, or removed) at 0.95 using reserves (until completely depleted), avoiding $\boldsymbol{P_C} < 0.95$
- Ceiling enforcement: newly minted coins are always available for sale at 1.05 (increasing reserves), avoiding $\boldsymbol{P_C} > 1.05$
- These enforcements ***should*** be algorithmically deterministic, not discretionary

Reserve Asset Bank: IPO

- Raise *bitcoins* as reserve asset in $ResAss$ quantity

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

- Issue in return C coins and S shares

- $C \cdot 0.95 \ll ResAss$ at IPO
- Hopefully, $C \cdot 0.95 < ResAss$ at every later time

- The market will assign prices P_C and P_S
- The monetary base being backed by $ResAss$, at equilibrium:

$$\boxed{C \cdot P_C + S \cdot P_S = ResAss}$$

© 2020 Digital Gold Institute

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

- Shareholders oversee *reference basket* maintenance;
  it is only fair: it is their coin, they backed it with their capital
- The share price is free to float
- Share value = assets - liabilities

$$S \cdot P_S = ResAss - C \cdot 0.95$$
$$P_S = (ResAss - C \cdot 0.95)/S$$

- Shareholders absorb monetary policy’s profits and losses, shielding coin holders from volatility
- No compelling reason to ever burn/destroy existing shares

$P_C \uparrow 1.05$: Profits for Shareholders

- Ceiling enforcement: newly minted coins are always available for sale at 1.05 (increasing reserves), avoiding $P_C > 1.05$

- For every new minted coin:
  – (reserve) assets increase by 1.05
  – (coin) liabilities increase by 0.95
  – positive net effect for shareholders: $P_S \uparrow$

- Seigniorage shares enjoy seigniorage revenues

$P_C \downarrow 0.95$: Losses for Shareholders

- Floor enforcement: existing coins are always bought (then burned, destroyed, or removed) at 0.95 using reserves (until completely depleted), avoiding $P_C < 0.95$

- If the selling pressure does not stop:
  - If $ResAss < C \cdot 0.95$:
    coin is dead, Bank defaults, $P_S = 0$
  - If $ResAss > C \cdot 0.95$:
    coin is dead, Bank does not default, $P_S > 0$
    i.e. there is no interest for this stable coin; shares are now strictly equivalent to the bitcoins they are entitled to

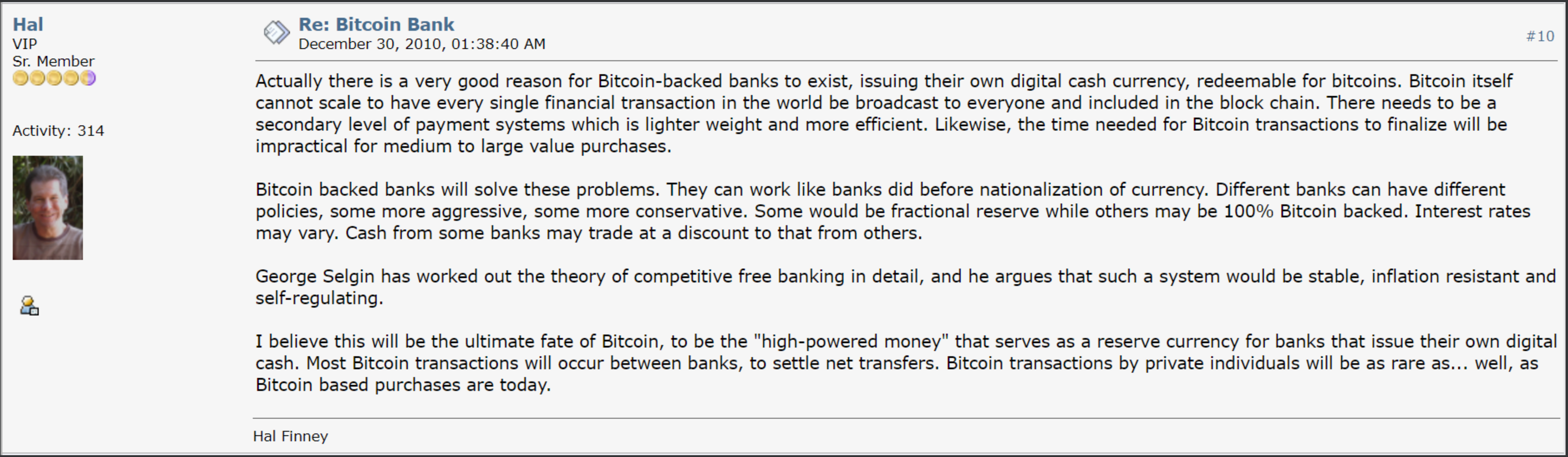
Leverage Bitcoin As Reserve Asset

- 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

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.

Transaction Validation: Proof-of-Payment

- Block generation is rewarded with the issuance of a new shares, one share per block
- Instead of the hardware and electric power costs of the computationally expensive proof-of-work, bitcoins are *irrevocably* paid to the Reserve Asset Bank by validating network nodes (**proof-of-payment**)
- Chances of being appointed for the next block generation are proportional to the overall submitted payments, i.e. to the accumulated proof-of-payment
- When a network node is picked up for block generation its proof-of-payment resets to zero; other nodes are not affected

Transaction Validation: Proof-of-Payment

- If a node is not picked up for block generation, its payments are not lost or discarded: never reimbursed, they are valid for the next block generation lottery
- Since $P_S = (ResAss - C \cdot 0.95)/S$, that should be the maximum price a rational agent is willing to commit as payment
- Share price low bound estimation is obtained as by-product of the block generation lottery
- Existing shareholders are not really diluted: for the issuance of each new share, $ResAss$ increases accordingly (actually, even more considering that **all proof-of-payment cashflows are immediately collected**, then rewarded in the future)

Bibliography

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008) https://bitcoin.org/bitcoin.pdf
- Ferdinando M. Ametrano, Hayek Money: the Cryptocurrency Price Stability Solution (2014), http://ssrn.com/abstract=2425270
- Massimo Morini, Inv/Sav Wallets and the Role of Financial Intermediaries in a Digital Currency (2014), http://ssrn.com/abstract=2458890
- Robert Sams, A Note on Cryptocurrency Stabilisation: Seigniorage Shares (2014), https://github.com/rmsams/stablecoins/blob/master/paper.pdf
- Vitalik Buterin, The Search for a Stable Cryptocurrency (2014), https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/
- Saifedean Ammous, The Bitcoin Standard: The Decentralized Alternative to Central Banking (2018)
- Ferdinando M. Ametrano, Bitcoin: oro digitale per nuovi standard monetary (2018), http://bit.ly/2NQg9VJ
- Ferdinando M. Ametrano, The Cryptocurrency Frontier in Monetary Engineering (2020), http://ssrn.com/abstract=2508296

Hayek Money - Dual Asset Ledger

- Price stability can be achieved with a new generation of cryptocurrencies: Hayek Money

- Multiple cryptocurrencies competing with different
  1. monetary policy definitions
  2. reference basket choices

- Dual Asset Ledger (DAL) can be used to decouple speculative money from transactional money
- Bitcoin payments can be used as economically expensive *Proof-of-Payment* instead of the computational expensive *Proof-of-Work*

The Frontier of Monetary Engineering

- It is about entrepreneurial monetary enterprise: investors risk their capital and gain only if the coin is useful and successful
- DAL fiduciary implementations are possible, reliable technology for a decentralized automated implementation is probably not available yet

- Bitcoin as reserve asset can bootstrap new monetary systems
- Bitcoin, the digital equivalent of gold, could be as relevant as physical gold for the history of civilization and future of money & finance

- Private monies competing with legal tender monies: separation of Money and State?