Hayek Money: the Cryptocurrency Price Stability Solution

Ferdinando M. Ametrano
ferdinando@ametrano.net

University of Milan-Bicocca, QuantLib, Banca IMI IntesaSanpaolo

ssrn.com/abstract=2425270

Bank of Italy, Rome, June 9th 2014
http://creativecommons.org/licenses/by-sa/4.0/
What are bitcoins?

https://bitcoin.org/en/

- decentralized digital currency
- instantaneous peer-to-peer transactions
- no need for trusted third party
- cryptographic security
- low-cost banking for everybody everywhere
- not backed by any government or organization

https://bitcoin.org/en/faq
http://www.coindesk.com/information/
Bitcoin Economy

- Total number of BTC is about 13M
- Market Cap: $8B BTC vs $1,200B USD

http://bitcoincharts.com/charts/bitstampUSD#tgWzm1g10zm2g25zy
What have been said

• Ben Bernanke: long-term promise
• Jared Cohen: crypto-currencies are inevitable
• Marc Andreessen: like Internet in 1994

• Nouriel Roubini: Ponzi game and conduit for criminal/illegal activities
• Alan Greenspan: It’s a bubble. It has to have intrinsic value
Hard to regulate

• Janet Yellen (November 2013 US Senate):
  – Bitcoin is a payment innovation that's taking place outside the banking industry
  – It's not so easy to regulate Bitcoin because there's no central issuer or network operator. This is a decentralized, global [entity]

• ECB (October 2012 report):
  – Governments and central banks would face serious difficulties if they tried to control or ban any virtual currency scheme
  – There is no server that could be shut down if the authorities deemed it necessary
# Table of Contents

1. About Money
2. Hayek: Concurrent Currencies
3. A Bitcoin Primer
4. Hayek Money
5. A New Unfamiliar Paradigm
6. Monetary Rule Implementation
7. Comparisons, Alternatives, and Scenarios
Money as social relation instrument

- Human beings are born into a gift economy
- As the relationship circle is enlarged, the need for an exchange economy arises
- Barter economy, coincidence of wants
- Trade economy based on money as medium of exchange
- Cryptocurrency: money for the global economy of mobile communication, Internet, and social networks.
# Money Comparison

<table>
<thead>
<tr>
<th></th>
<th>Medium of Exchange</th>
<th>Store of Value</th>
<th>Unit of Account</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Live cattle</strong></td>
<td>★★</td>
<td>★★</td>
<td>★★</td>
</tr>
<tr>
<td><strong>Diamonds</strong></td>
<td>★★★★</td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
</tr>
<tr>
<td><strong>Gold</strong></td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
</tr>
<tr>
<td><strong>Fiat coins and notes</strong></td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
</tr>
<tr>
<td><strong>Cryptocurrency</strong></td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
<td>★★★★☆☆☆☆☆☆☆☆☆</td>
</tr>
</tbody>
</table>

- **Live cattle**: swappable, fungible, portable, divisible, recognizable, resistant to counterfeiting
- **Diamonds**: reliably saved, stored, and retrieved, retain usefulness over time, non-perishable or with low preservation cost
- **Gold**: relative worth unit of measure, stable value for stable price comparison, supply must be limited in some way
- **Fiat coins and notes**: ★★★★☆☆☆☆☆☆☆☆☆ ★★★★☆☆☆☆☆☆☆☆☆ ★★★★☆☆☆☆☆☆☆☆☆ ★★★★☆☆☆☆☆☆☆☆☆
- **Cryptocurrency**: ★★★★☆☆☆☆☆☆☆☆☆ ★★★★☆☆☆☆☆☆☆☆☆ ★★★★☆☆☆☆☆☆☆☆☆ ★★★★☆☆☆☆☆☆☆☆☆
From gold standard to fiat money

• Gold: the commodity money standard
  – resistance to corrosion and oxidation
  – high malleability
  – relative easiness of purity assessment
  – Pleasant color
• Gold purity certification
• Representative money
• Fractional receipt money
• Money and currency
• *Fiat* money and legal tender
Money as value yardstick

• Unit against which the value of every other good is measured
• A good in itself: its value is governed by supply and demand
• 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
Inflation and Deflation

• reduction in the purchasing power per unit of money: money value decrease, price level increase

• deflation hinders money’s unit of account role and encourages its hoarding. This can lead to perverse economic crisis.
Monetary policy

• delegated to central banks or equivalent monetary authorities
• institutionally designed to be independents
• central bank’s main objective is to safeguard the value of the national currency
• low and stable rate of inflation is the implicit or explicit goal
Table of Contents

1. About Money
2. Hayek: Concurrent Currencies
3. A Bitcoin Primer
4. Hayek Money
5. A new unfamiliar paradigm
6. Monetary rule implementation
7. Comparisons, Alternatives, and Scenarios
Friedrich 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
Analysis of the Theory and Practice of Concurrent Currencies

• Commercial banks issue their own money:
  – Keep the purchasing power constant
  – Competition between currencies

_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_
Table of Contents

1. About Money
2. Hayek: Concurrent Currencies
3. A Bitcoin Primer
4. Hayek Money
5. A New Unfamiliar Paradigm
6. Monetary Rule Implementation
7. Comparisons, Alternatives, and Scenarios
Bitcoin: a currency and a protocol

• **Bitcoin**: protocol, software, and community

• **bitcoins**: units of the currency.

*bitcoins are sent using Bitcoin*
Bitcoin the protocol

• stroke of genius, major disruptive invention

  replace any processing central authority with decentralized peer-to-peer cryptographically secure equivalent

• This really is Web 3.0
Bitcoin the protocol

• public ledger of transactions:
  – allows to transfer a unique piece of digital property
  – keeps records of each and every transaction forever

• everyone knows the transaction happened, nobody can challenge its legitimacy

• It is a long chain of blocks, each one containing many transactions: block chain

• the protocol is Bitcoin extra-legal tight regulation
«metacoin»s, Ethereum

- Parasitic block chain metacoin: Namecoin, Mastercoin, Counterparty
- Bitcoin-like block chains as public ownership database for digital assets
- Next-Generation Smart Contract and Decentralized Application Platform
- Smart property, smart contracts and decentralized autonomous corporations

https://www.ethereum.org/
bitcoin the currency

• bitcoins are a digital property created inside the Bitcoin protocol

• the first powerful protocol application

• authorities replaced:
  – central banks
  – financial intermediaries
bitcoins

• Not to be found anywhere, they only exist as block chain documented transactions
• A bitcoin wallet is a public address
  1FEz167JCVgBvhJBahpzmrsTNewhiwgWVG
• the block chain certifies for everybody how many bitcoins are associated to the wallet
  
  http://blockexplorer.com/address/1FEz167JCVgBvhJBahpzmrsTNewhiwgWVG

It is mine; you are REALLY encouraged to tip
Pseudonymity, Anonymity

Bitcoin is really *pseudonymous*, not *anonymous*:

- The public key does not provide direct information about the private key owner
- All transactions are transparent to everybody’s inspection. Perfect persistent public account history. The block chain is forever.

[https://blockchain.info/](https://blockchain.info/)
Bitcoin wallet security

• *bitcoins are effectively owned by whoever can spend them*

• Securing a wallet: private key safe storage

• PC client: Bitcoin Core, Armory, Electrum

• Web client: [blockchain.info](http://blockchain.info), [greenaddress.it](http://greenaddress.it)

• Cold storage
Mining

• Miners are the nodes of the network
• Miners provide the computing power for:
  – processing and validating transactions (avoiding double spending)
  – securing the network
  – synchronize the nodes
• Rewarded with the issue of new bitcoins
• Mining privileges obtained by proof-of-work
Bitcoin Monetary Rule

• 2009: 50BTC 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

• digital cash supply free of discretionary intervention
Inelastic Money Supply

![Graph showing the inelastic supply of bitcoins over time. The graph has a horizontal axis labeled from 2009 to 2129 and a vertical axis labeled from 0 to 25,000,000.]
Statement of the Problem

- The Bitcoin protocol has been successful at get rid of any centralized monetary authority
- The bitcoin currency has inadvertently thrown away the flexibility of an elastic monetary policy
Table of Contents

1. About Money
2. Hayek: Concurrent Currencies
3. A Bitcoin Primer
4. Hayek Money
5. A New Unfamiliar Paradigm
6. Monetary Rule Implementation
7. Comparisons, Alternatives, and Scenarios
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)
Fixed USD Exchange Rate

• 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 1BTC worth 500USD
  — or 500BTC each worth 1USD
Rebasing Process Reaction Lag

Daily rebasing

USD/RBTC
Inflation adjusted USD

- Adopting the USD Consumer Price Index
- 6% inflation in the period March 2011-2014
Brent-Wheat Commodity Price Index
Brent-Wheat Commodity Price Index
Brent-Wheat Commodity Price Index
Brent-Wheat Commodity Price Index
Gold Commodity Price Index
Gold Commodity Price Index
Table of Contents

1. About Money
2. Hayek: Concurrent Currencies
3. A Bitcoin Primer
4. Hayek Money
5. A New Unfamiliar Paradigm
6. Monetary Rule Implementation
7. Comparisons, Alternatives, and Scenarios
A new unfamiliar paradigm

The number of coins in a wallet can change without any direct inflows or outflows

Money amount volatility instead of price vol

A historical, cultural, and psychological change of paradigm that will require some effort and time to be accepted
Unit of Account Effectiveness

• Money is a special good whose value changes are better not offloaded to other goods
• If the yardstick changes its length, better fix the yardstick than update the measured lengths of all other objects
• Impacting on wallets is the least irrational and disjointed means of adapting to changes in the value of money
(Un)Fairness of the (Current) Elastic Supply of (Fiat) Money

• Expansionary policy: most are denied of the pro-quota money increase they would deserve

• Contractionary policy: the general loss of value is dumped on borrowers

• Paper money phasing out (2014 Rogoff)
Preserving wallet purchasing power

• The debasement associated with decreasing demand for money is unavoidable

• spreading monetary base purchasing power changes across larger/smaller money stock salvages the currency unit value, but only that
Volatility: intrinsic property of demand dynamics

• rebasing the monetary stock supply absorbs the impact due to variable money demand

• the remaining volatility would be the reference commodity basket variability

• Sudden large variation of demand for a stable (crypto)currency is unlikely: fiat/crypto switches and adoption rate variability will be reduced

• Stable prices will help economic growth
Adaptation to the New Paradigm

• Most people use money without ever wondering about its nature
• The need for education is urgent

• Increasing number of coins will introduce people to variable amount wallets
• Early adopters will enjoy impressive wealth growth: others will follow by emulation
Reintroducing some unfairness to reduce awkwardness

• Reduce the monetary base destroying transaction fees: a countercyclical measure

• Freeze, instead of destroy, transaction fees
Table of Contents

1. About Money
2. Hayek: Concurrent Currencies
3. A Bitcoin Primer
4. Hayek Money
5. A New Unfamiliar Paradigm
6. Monetary Rule Implementation
7. Comparisons, Alternatives, and Scenarios
Observation of Commodity Prices

• Measure prices in a decentralized way, without central authorities
• Miners as agents of the average consensus process
• Shelling points: unbiased market prices are focal prices for the average consensus process
• Miners as (black market) brokers
Commodity Price Index Maintenance

• Commodities’ importance changes, traded volume, relative price stability and sensitivity, and competitive markets might suggest Commodity PI alterations
• The Commodity PI is composed of technically unconstrained numbers
• Nothing could stop the majority of miners from changing the Commodity PI definition
• Proof-of-stake is crucial: the prerogative to change the PI is not oligopolistic power abuse, but the proper right of the majority to rule about its own money
Rebasing Process Reaction Lag
Rebasing Process Reaction Blocks

![Graph showing reaction lag over percent change](image)
Transactions and Rebasing Process

• Processing transaction before/after rebasing

• Make sweeping transactions possible
Table of Contents

1. About Money
2. Hayek: Concurrent Currencies
3. A Bitcoin Primer
4. Hayek Money
5. A New Unfamiliar Paradigm
6. Monetary Rule Implementation
7. Comparisons, Alternatives, and Scenarios
Bitcoin in the Hayek Money Landscape

- bitcoin is the natural Hayek Money candidate
- bitcoin is conservative about radical changes and has gold scarcity paradigm as legitimate monetary rule

- bitcoin’s brilliant intellectual breakthrough is like gold’s pleasant color, but it can be cloned in a digital world

- Evolution should include and leverage the Bitcoin community: transitional bridges from bitcoin to Hayek Money will be of paramount importance
Hayek Money Concurrent Cryptocurrencies

• They will compete in
  – proper monetary policy befitting user needs
  – selected commodity basket standard relevant in the reference economy.

• To keep reserve is not needed or advocated

• Two Hayek Money crypto-families:
  1. Gold, the most brilliant protagonist of the history of money. Maybe Silver.
  2. Mix of petroleums, grains, and industrial metals
Possible Impacts of Hayek Money

- Cancellation of seigniorage and inflation revenues
- Barrier-free frictionless financial system for unbanked people
- Undemocratic regimes are banning cryptocurrencies. Not easy in democratic countries, but huge pressure will grow
- Explicit/stealth technologic attacks: the role of proof-of-stake
- Entertainment industry war against copyright infringing P2P; legal opposition might slow adoption, but cannot stop it
- Early adopters will become rich, emulators will follow
- After wild and abrupt growth, stability will be reached when the monetary base is large enough for billions of people
The Fate of Fiat Currencies

• Unreliable currencies would gradually all be eliminated

• Fiat currencies could issue their own digital Hayek Money crypto-versions: effective if not too late

• It would undermine existing financial/banking system

• Third party authority not compliant with zero-trust ethic, anyway a step forward in terms of transparency and accountability

• The money authority leviathan would have an increased controlling power over everybody’s money
Further Research @
www.hayekmoney.org

• Variable balance wallet awkwardness does really need to be amended?
• Are transaction fees effective as monetary rule?
• Other monetary rules worth implementing?
• Monetary rules technical implementation
• Is the consensus average process robust?
• How to effectively bootstrap a new cryptocurrency?
• How to leverage the bitcoin growth so far?
• CPI definition for concurrent Hayek Money cryptos.
• Lending in a Hayek-cryptocurrency framework?
Hayek Money: 
the good money standard

from barter to money
from money to good money:
stable prices for a new economic era

• Bitcoin is challenging established political and economic theory, Hayek Money will accelerate the transition to a new era

• An opportunity for increased equality, justice, and wellness, it requires responsible actions by good willing people to help smooth the transition