Bitcoin and the Future of Money

ferdinando@ametrano.net
https://twitter.com/Ferdinando1970
https://speakerdeck.com/nando1970
https://it.linkedin.com/in/ferdinandoametrano
Why Bitcoin Is Hard to Understand

At the crossroads of:

• Game theory
• Cryptography
• Computer networking and data transmission
• Economic and monetary theory

Mainly not a technology,

a cultural paradigm shift instead
Bitcoin: Elements of Economic and Monetary Theory

1. Bitcoin as Private Money
2. Bitcoin as Digital Gold
3. Bitcoin as Unit of Account
4. Hayek Money
5. Dual Asset Ledger and Reserve Asset Bank
Private Monies

• A widely accepted medium of exchange or payment
  – 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

- 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

• 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’
Precursors

• ECash, David Chaum, 1982 (blind signature)
• Hashcash, Adam Back, 1997 (Proof-of-Work)
• B-money, Wei Dau, 1988 (distributed database)
• Bit gold, Nick Szabo, 1998 (distributed database, sequential money creation)
• Anonymous Electronic Cash, Tomas Sander and Amnon Ta-Shma, 1999 (anonymity)
• Reusable P-o-W, Hal Finney, 2004
Digital Transfer of Value

• To securely (cryptographically) transfer value digitally has been possible for decades
• However it had always required the creation of a centralized trusted party to prevent double spending
• Bitcoin
  – does not require a central trusted party
  – is designed to resist attacks of malicious agents, as long as they do not control network majority
Bitcoin Monetary Rule

• 2009: 50BTC every 10 minutes
  – halving every 4Y, currently is 12.5BTC
• 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
Inelastic Money Supply
Deterministic Decreasing Supply Rate

- 2029: issued 96.88% of all BTC
- 2141: issued last 0.00000001 BTC

Ferdinando Ametrano 2017
What Makes Bitcoin Special?

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

*Bitcoin is digital gold*
this is the brilliant groundbreaking achievement by Satoshi Nakamoto
Friedrich August von Hayek
Denationalisation of Money

• I am more convinced than ever that if we ever again are going to have a decent money, it will not come from government. Good money [...] imposes on the issuer a discipline to which the government has never been and cannot be subject.

• 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*


Money as Social Relation Instrument

- Human beings are born into a gift economy
- Enlarged relationship circle requires exchange economy
- Barter economy, coincidence of wants
- Trade economy, money as medium of exchange
- Bitcoin is money for the information economy
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?
Bitcoin:
Money for the Information Economy

- Decentralized: no authority
- Permissionless: no regulator
- Censorship resistant: no frozen funds
- Open-access: no discrimination, no amount limits, 24/7, 365 days
- Free: negligible transaction costs
- Borderless: no geographic boundaries
- Transnational: no specific jurisdiction applies
- Secure: non falsifiable, non repudiable transactions
- Resilient: nothing has been able to stop it or break it

Ferdinando Ametrano 2017
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
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

Ferdinando Ametrano 2017
Bitcoin Economy

http://bitcoincharts.com/charts/bitstampUSD#tgWzm1g10zm2g25

- BTC Market Cap: about $20B (USD M0 1959-2017 average has been $680B)
Statement of the Bitcoin Problem

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

<table>
<thead>
<tr>
<th></th>
<th>Medium of Exchange</th>
<th>Store of Constant Value</th>
<th>Unit of Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live cattle</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
</tr>
<tr>
<td>Diamonds</td>
<td>⭐️⭐️</td>
<td>⭐️⭐️⭐️⭐️⭐️⭐️</td>
<td>⭐️⭐️⭐️⭐️⭐️</td>
</tr>
<tr>
<td>Gold</td>
<td>⭐️⭐️⭐️</td>
<td>⭐️⭐️⭐️⭐️⭐️⭐️</td>
<td>⭐️⭐️⭐️⭐️⭐️</td>
</tr>
<tr>
<td>Fiat coins and notes</td>
<td>⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️</td>
<td>⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️</td>
<td>⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️</td>
</tr>
<tr>
<td>Bitcoin</td>
<td>⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️</td>
<td>⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️</td>
<td>⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️⭐️</td>
</tr>
</tbody>
</table>

- 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
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 BTC1 worth $500
  - or (rebased) RBTC500 each worth $1
USD-Parity Rebased Bitcoin
Brent-Wheat Commodity Price Index

The graph shows the price index of Brent and Wheat commodities over time in USD and BTC. The price of Brent and Wheat shows fluctuations, with Wheat generally remaining higher than Brent throughout the period from April 2011 to March 2014.
Brent-Wheat Commodity Price Index
Rebased Bitcoin
Brent-Wheat Commodity Price Index

The chart shows the normalized USD/RBTC and normalized USD/EUR prices from March 2011 to September 2013. The blue line represents the normalized USD/RBTC, while the red line represents the normalized USD/EUR. The prices fluctuate over time, with periods of increase and decrease.
Limits of This First Simplistic Implementation of Hayek Money

• The number of coins in a wallet changes without any direct inflows or outflows

• Prices are stable (salaries and mortgages are now possible!), but the purchasing power of a given wallet is not stable

• Coins still have speculative investment appeal and so enjoy limited transaction usage
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
Reserve Asset Bank IPO

• Raise bitcoins as reserve asset in $ResAss$ quantity
• Issue $C$ coins, with $C \ll ResAss$
• Target $P_C = 1$, allowing for a corridor, e.g. $0.95 < P_C < 1.05$
• Issue $S$ shares, implicitly fixing $P_S$ as in $C + P_S S = ResAss$
Coins

• The supply is regulated to peg the coin to a given price index parity
  – Expansionary monetary phases: newly minted coins are sold by the Reserve Asset Bank for bitcoin
  – Contractionary monetary phases: coins are bought by the Reserve Asset Bank paying with bitcoin
• When $P_C \cong 1$, coins give up any speculative value
• Money velocity and transaction volume increase
Distributed Central 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

Miners are replaced by shareholders entitled to seigniorage revenues as compensation for being:

– obliged to validation task duties
– responsible for network security, node synchronization, etc.
– subjected to the costs associated to coin stability
Seigniorage Shares

- The share price is free to float, but it is basically anchored to:
  \[ P_s S = ResAss - P_C C \]
- Shareholders absorb all monetary policy’s costs and benefits, shielding coin holders from volatility
- Shares are never burned/destroyed
- Transaction validation is rewarded with the issuance of new shares, not coins
- Block validation right is gained with proof-of-payment: increasing ResAss and obtaining a new share in an action-like process
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 to:
  – scale to huge (cash + bank accounts + credit cards) number of transactions
  – support economically inefficient micropayments
  – lower confirmation time
• The Reserve Bank IPO: raise bitcoins, issue seigniorage shares
Conclusions

1. Bitcoin is digital gold: cryptocommodity more than cryptocurrency
2. Hayek Money is the price stability paradigm of cryptocurrency with elastic non-discretionary money supply
3. Coin/share dual asset ledger can decouple transactional and speculative money demand
4. Bitcoin can be used as reserve asset for a DeCentralized Reserve Bank (DAO) that performs market operations
5. *Proof-of-Payment* can avoid increasing socially inefficient usage of seigniorage revenues for transaction verification
Bibliography


