From Adam Smith to Nakamoto: A survey of (crypto)currency theories

Bruno Biais
HEC Paris

June 2022

Cryptocurrencies have no intrinsic value

"bitcoin is a pure bubble, an asset without intrinsic value — its price will fall to zero if trust vanishes"
Jean Tirole, TSE, 2017

"Cryptocurrencies basically have no value and they don't produce anything. They don't reproduce, they can't mail you a check, they can't do anything, and what you hope is that somebody else comes along and pays you more money for them later on, but then that person's got the problem. In terms of value: zero."
Warren Buffett CNBC February 2020

Yet... one bitcoin worth more than $ 15,000

Can we make sense of that?

Can such high (and volatile) valuation be rationalized, microfounded?

Two types of microfoundations for the value of cryptocurrencies

1. Cryptocurrency = token giving access to platform $\longrightarrow$ surplus: Cong, Li & Wang (2021), Sockin & Xiong (2022)
2. Cryptocurrency = means of payment // standard currencies

This talk focuses on 2

Means of payment

bitcoins have no intrinsic value (no dividend, no real assets)

Just like standard currencies ($, £, €, ...)

$\longrightarrow$ fiat money

Even without intrinsic value, fiat money valuable, as means of payment, solving non-double coincidence of wants problem (Adam Smith, 1776, Jevons, 1875)

Beliefs

I accept to be paid in fiat currency now, because I believe others will accept it in the future when I want to use it to pay

Fiat money current valuation depends on beliefs about its future valuation/acceptance

Beliefs about bitcoin acceptance can fluctuate (either due to changes in intrinsic variables, e.g. regulatory framework or technology, or extrinsic sunspots)

Belief fluctuations $\longrightarrow$ volatility

Sunspots?

Sunspot

Capture d'écran du compte d'Elon Musk, vendredi 29 janvier 2021. Twitter

Samuelson (1958): An exact consumption loan model of interest with or without the social contrivance of money

Currency supply $= m_t$. Continuum of investors born at time t, endowed with e_t consumption good, chose holdings of currency q_t, and consume

$$c_t^y = e_t - q_t p_t$$

At $t+1$, investor born at t is old and consumes (then dies)

$$c_{t+1}^o = q_t p_{t+1}$$

Young investors solve $\mathcal{P}_t$:

$$\max_{q_t} u(c_t^y) + \beta u(c_{t+1}^o)$$

Equilibrium $=$ prices and investment choices solving $\mathcal{P}_t$ given rational expectations about prices, and s.t. markets clear: $q_t = m_t$

Samuelson: Constant price equilibrium

Constant endowment e and money supply m

$$\text{Equilibrium: } \arg\max_q u(e - qp) + \beta u(qp) = m$$

$$\text{First order condition: } u'(e - qp)p = \beta u'(qp)p$$

0 is an equilibrium, and what else ? With power utility

$$\frac{mp}{e} = \frac{\beta^{\frac{1}{\gamma}}}{1 + \beta^{\frac{1}{\gamma}}}$$

Market cap of money/GDP increasing in discount factor β

Patient $\longrightarrow$ eager to save $\longrightarrow$ demand money

Kareken Wallace (1981): On the indeterminacy of equilibrium exchange rates

Currency: $i = 1$ (\$), 2 (€). Constant price equilibrium:

$$\arg\max_{q_i} u(e - \sum_i q_i p_i) + \beta u(\sum_i q_i p_i) = m_i, \forall i$$

First order condition

$$u'(e - \sum_i q_i p_1) p_i = \beta u'(\sum_i q_i p_i) p_i$$

Power utility

$$\frac{m_1 p_1 + m_{2p_2}}{e} = \frac{\beta^{\frac{1}{\gamma}}}{1 + \beta^{\frac{1}{\gamma}}}$$

Only total capitalization of money matters, not how it is split

Nakamoto, 2008: Bitcoin: A Peer-to-Peer Electronic Cash System

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."

Garatt Wallace (2018): Bitcoin 1, bitcoin 2, . . . An experiment in privately issued outside monies

"The best theory of the value of bitcoin is that it rests on what are called self-fulfilling beliefs and that the set of beliefs that can be self fufilling is huge...

People's beliefs over bitcoin prices include the possibility of a collapse... One interpretation is that the uncertainty is purely extrinsic. . . a publicly observed sunspot variable à la Cass and Shell (1983). The appearance of a sunspot triggers a change in beliefs that leaves bitcoin valueless. This interpretation is consistent with our message that equilibrium prices depend upon beliefs. . . "

Garatt & Wallace: Model

Crash can occur with probability π

As long as no crash, constant price (p_1, p_2)

$$\text{at } t \text{ young consume: } c_t^y = e - \sum_i q_{i,t} p_i$$

$$\text{at } t+1 \text{ old consume: } \sum_i q_{i,t} p_i$$

If crash at $t+1$, \$ price $= p_1^c$, crypto price $= 0$, old consume $q_{i,t} p_1^c$

Young investors solve

$$\max_{q_{i,t}} u(e - \sum_i q_{i,t} p_i) + \beta \left[(1-\pi) u(\sum_i q_{i,t} p_i) + \pi u(q_{i,t} p_1^c) \right] - \xi q_{1,t}$$

$\xi =$ cost of storing money in utility terms

Garatt & Wallace: Constant price equilibrium (until crash)

Standard money costly to store but bitcoin exposed to crash risk

> *"pessimistic beliefs on bitcoin's future equilibrium price path are sufficient to offset the real financial cost of storing [the standard currency]..."*

Equilibria:

> *"six equations and six unknowns that (for suitable parameter choices that permit interior solutions) describe the equilibrium... Equilibria also exist ... in which the price of either or both monies are zero"*

Schilling Uhlig (2019): Some simple bitcoin economics

Central bank $\longrightarrow$ supply of standard money (\$) $\longrightarrow$ inflation target

Bitcoin supply grows deterministically

Two possible equilibria:

- "Conventional scenario": btc price $\longrightarrow$ central bank policy
- "Unconventional scenario": central bank policy $\longrightarrow$ btc price

Biais, Bisière, Bouvard, Casamatta, Menkveld (2022): Equilibrium bitcoin pricing

Young consume

$$c_t^y = e_t - s_t - \sum_i q_{i,t} p_{i,t} - \varphi_t q_{2,t} p_{2,t}$$

s_t = savings in risk-free asset
φ_t = cost of transacting cryptocurrency

Old consume

$$c_{t+1}^o = s_t(1 + r_t) + q_{1,t} p_{1,t+1} + (1 - h_{t+1})\theta_{t+1} q_{2,t} p_{2,t+1}$$

h_{t+1} = fraction of btc hacked
θ_{t+1} = transactional benefits of using crypto (anonymity, international payment, internet/on chain)

BBBCM: Equilibrium

$$p_{2,t} = \beta(1-\pi_t)E_t\left[\frac{u'(c^o_{t+1})}{u'(c^y_t)}(1-h_{t+1})\frac{1+\theta_{t+1}}{1+\varphi_t}p_{2,t+1}\middle|\text{no crash at } t\right]$$

$\frac{u'(c^o_{t+1})}{u'(c^y_t)}$: intertemporal marginal rate of substitution

$\theta, \varphi \longrightarrow$ net transactional benefit of crypto $\longrightarrow$ fundamental

// dividend for stock, but here fundamental depends on $p_{2,t+1}$

$\longrightarrow$ equilibrium multiplicity:

- different price processes can satisfy equilibrium equation
- $p_{2,t} = 0$ is an equ., we also characterize equ. with $p_{2,t} > 0$

BBBCM: Constant price equilibrium with CRRA

Generalized discount factor $D(\pi) \equiv \beta(1-\pi)(1+\theta)$

Standard currency as % of GDP if crash

$$\frac{mp_1^c}{e} = \frac{\beta^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}$$

Crypto as % of GDP if no crash (// Kareken Wallace)

$$\frac{Xp_2}{e}\frac{1+\theta+D^{\frac{1}{\gamma}}}{1+D^{\frac{1}{\gamma}}} + \frac{mp_1}{e} = \frac{D^{\frac{1}{\gamma}}}{1+D^{\frac{1}{\gamma}}}$$

Standard currency if no crash pinned down ($\neq$ Kareken Wallace)

$$p_1\theta(1-\pi)\left(\frac{(1+\theta)D^{\frac{1}{\gamma}} - \theta D^{\frac{1}{\gamma}} mp_1}{1+\theta+D^{\frac{1}{\gamma}}}\right)^{-\gamma} = \pi\left(mp_1^c\right)^{-\gamma} p_1^c$$

BBBCM: Multiple constant price equilibria

For each crash proba $\pi \in [0, \bar{\pi}]$, $\exists$ constant price equilibrium

$\longrightarrow$ continuum of equilibria based on self-fulfilling sunspot beliefs

BBBCM: Risk premium

At t, young investors buy crypto.

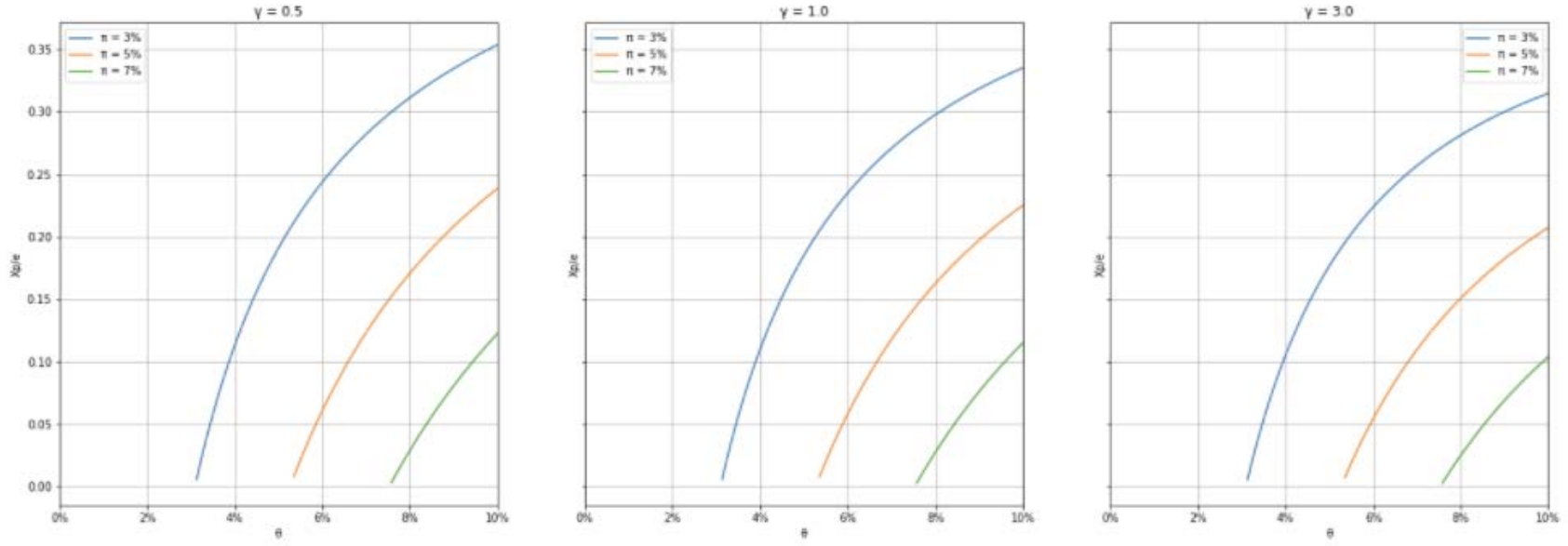
At $t+1$, their consumption is larger if no crash than if crash

To compensate for that risk, cryptocurrency expected return larger than risk free asset return

$$(1-\pi)(1+\theta) > 1+r$$

Bitcoin cap/GDP when agents have power utility

Equilibria with constant price until crash can be characterized numerically:
CRRA γ between .5 and 3. π between 3% and 7%. θ between 3% and 10%



btc goes down with γ: investors less willing to bear crash risk
btc goes down with crash risk π and increases with transactional benefit θ

BBBCM: Volatile price equilibrium

Randomly fluctuating state $\omega_t = (t, \xi_{t-1}, \pi_t)$ observed at t
$\xi_{t-1} = c$ if crash occured, nc otherwise, $p_2(t, c, \pi_t) = 0$

Markov: time t beliefs about $\omega_{s+1}, s \geq t$, depend on ω_t only

After N, crash probability constant $\pi_N \longrightarrow$ constant price equ

Before N, price pinned down by recursion

$$p_2(\omega_t) = D(\omega_t) E_t \left[\frac{u'(c_{t+1})}{u'(c_t)} \; p_2(\omega_{t+1}) | \text{no crash} \right]$$

$$\frac{u'(c_{t+1})}{u'(c_t)} = \left(\frac{e - X p_2(\omega_t) - m p_1(\omega_t)}{X p_2(\omega_{t+1})(1+\theta) + m p_1(\omega_{t+1})} \right)^{\gamma}$$

Fluctuation in $\omega_t \longrightarrow$ extrinsic, sunspot driven, volatility

Conclusion

Fundamental of cryptocurrency = transactional services it provides

Transactional services depend on price

Fundamental depends on beliefs about price

Variability in beliefs (sunspots) $\longrightarrow$ cryptocurrency volatility

Volatility

Why crypto so much more volatile than standard currencies?

Is it because standard currencies are anchored by legal tender status (can be used to pay taxes)?

Is it because central banks stabilise/coordinate beliefs?

Institution's money vs distributed money

Institutions: state, central bank, financial institutions

- can foster coordination $\longrightarrow$ reduce volatility
- only if trustworthy $\longrightarrow$ limited commitment/agency problems

Distributed ledger: protocol, nodes

- can achieve commitment $\longrightarrow$ limit opportunistic behaviour
- but coordination problems $\longrightarrow$ volatility

Interaction means of payment - unit of account

Are standard currencies more stable than crypto, because they are unit of account and prices are sticky?

Stable regime: unit of account $\longrightarrow$ stable $\longrightarrow$ unit of account

Unstable: not unit of account $\longrightarrow$ volatile $\longrightarrow$ not unit of account

Interaction blockchain technology - cryptocurrency pricing

Pagnotta (2020): price $\longrightarrow$ mining $\longrightarrow$ blockchain security $\longrightarrow$ price

Blockchain technology: smart contract, defi,...

- $\longrightarrow$ token useful on platform (Cong, Li & Wang, 2021)
- $\longrightarrow$ intrinsic value
- $\longrightarrow$ interaction: intrinsic value / means of payment?
- $\longrightarrow$ can intrinsic value reduce volatility?

Stablecoins

Stablecoins $\longrightarrow$ stability + onchain

If stablecoin stable because issued by institution that holds \$
$\longrightarrow$ rely on institution
$\longrightarrow$ need to trust institution
$\longrightarrow$ what Nakamoto (2008) wanted to avoid

E.g., concerns about whether Tether's reserves really risk-free:
back to classical agency problems with financial intermediaries

Algorithmic stablecoins? ... Terra-Luna