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

Bruno Biais
HEC Paris

Presentation prepared for
the inaugural conference of the Gillmore Centre

London, September 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

Intrinsic value vs means of payment

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

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

Even without intrinsic value, standard currency or cryptocurrency can be valuable as means of payment, solving non-double coincidence of wants problem (Adam Smith, 1776, Jevons, 1875, Wicksell 1901)

Non double coincidence of wants in Wicksell's triangle

Triangle ABC:

- Alice: grows apples but likes bananas
- Bernard: grows bananas but likes cherries
- Claire: grows cherries but likes apples

If meet in centralized market: efficient allocation

If bilateral meetings (+ fruits not storable outside farm): no trade

E.g., if A meets B: A wants B's bananas, but B not interested in A's apples $\longrightarrow$ non double coincidence of wants

Money in Wicksell's triangle

- A goes to bank to borrow money, which she deposits on her account
- When she meets B, A transfers money from her account towards B's account to pay for bananas
- When meeting C, B transfers money to C's account to pay for cherries
- When meeting A, C transfers money to A's account to pay for apples

Money (means of payment created by bank) solves non double coincidence of wants problem

Cryptocurrency in Wicksell's triangle

- Block n: A gets tokens by mining
- Block $n+1$: A transfers tokens to B (to pay for bananas)
- Block $n+2$: B transfers tokens to C (to pay for cherries)
- Block $n+3$: C transfers tokens to A (to pay for apples)

Tokens (means of payment created by blockchain protocol) solve non double coincidence of wants problem:

> *"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" (Nakamoto, 2008)*

Beliefs and volatility

Standard money and cryptocurrencies without intrinsic value

but can solve non double coincidence of wants problem

as means of payment

iff believed to be accepted as means of payment

$\longrightarrow$ fundamental value based on beliefs

change in beliefs $\longrightarrow$ change in value $\longrightarrow$ volatility

Outline

1. Refresher: Model of standard currency as means of payment
2. Extend model to cryptocurrency: similarities and differences

- Sunspot $\longrightarrow$ crash risk
- Costs and benefits, relative to standard currency
- Change in beliefs about sunspot $\longrightarrow$ extrinsic volatility
- Protocol money vs institution money

Non double coincidence and OLG

Non double coincidence of wants because all potential counterparties don't meet at the same time and same place

Meet only subset of agents $\longrightarrow$ no trade with those you don't meet

Money = way to "contract with those you don't meet"

Overlapping generations = way to capture that

- At t, young agents are born and meet old agents born at $t-1$
- Cannot meet and contract with agents to be born at $t+1$

(alternative modeling framework: search, Kiyotaki Wright)

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

Currency supply $= m_t$. Continuum agents born at t, endowed with e_t consumption good, hold currency q_t, 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: $q_t = m_t$

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?

$$p \text{ s.t. } u'(e - mp) = \beta u'(mp)$$

Market cap of money/GDP increasing in discount factor β

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

With power utility:

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

Money and welfare

Utilitarian planner:

$$\max u(c^y) + \beta u(c^o), s.t., c^y + c^o = e$$

$$\max_{c^o} u(e - c^o) + \beta u(c^o)$$

First order condition: $u'(e - c^o) = \beta u'(c^o)$

Same as in strictly positive constant price equilibrium

$p > 0$ equilibrium (agents trust money): Utilitarian optimum
$p = 0$ equilibrium (agents distrust money): Pareto dominated

$\rightarrow$ Trust in money is "common good"

Starr (1974) "The price of money in a pure exchange economy"

$p = 0$ equilibrium eliminated if government requests (large enough) tax to be paid in official money

need to pay tax in money $\longrightarrow$ demand for money $\longrightarrow$ $p > 0$

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

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

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

$$\text{First order condition } u'(e - \sum_i q_i p_1) p_i = \beta u'(\sum_i q_i p_i) p_i$$

Aagin $\exists$ equ with zero price and equ with strictly positive price

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

$$\text{Power utility: } \frac{\sum_i q_i p_1}{e} = \frac{\beta^{\frac{1}{\gamma}}}{1 + \beta^{\frac{1}{\gamma}}}$$

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

Turn from standard currency to cryptocurrency

Same basic structure: crypto-currency as means of payment

+ additional features:

- Sunspot-driven cryptocurrency crash risk
- Costs and benefits, relative to standard currency
- Change in beliefs about sunspot $\longrightarrow$ extrinsic volatility
- Protocol money vs institution money

Crash risk

Standard currency $\longrightarrow$ backed by state $\longrightarrow$ eliminate zero price equilibrium by requesting taxes be paid in currency (Starr, 1974)

Cryptocurrency $\longrightarrow$ no central authority $\longrightarrow$ imposible to use taxation to avoid zero price equilibrium

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

In addition to equ. in which currency price always equal zero

equilibrium in which price

- initially strictly positive
- and at some point crashes to 0

> *"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."*

Model

Crash 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

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"*

Costs and benefits of cryptocurrency

Assumption that standard money more costly to store/trade than crypto not very palatable

In practice, crypto can be quite costly to trade (exchange fees) and store (exchange can be hacked)

But other aspects of crypto can be beneficial for its holders:

- Avoid risk of predation by government
- Avoid regulation/law
- Anonymity
- Avoid capital controls

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

Young consume

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

φ_t = cost of transacting cryptocurrency

Old consume

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

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

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 $p_{2,t+1}$

Constant price equilibrium with CRRA

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

Standard currency as % of GDP if crash (// Samuelson)

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

Currencies 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

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

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

Risk premium

At t, young investors buy crypto.

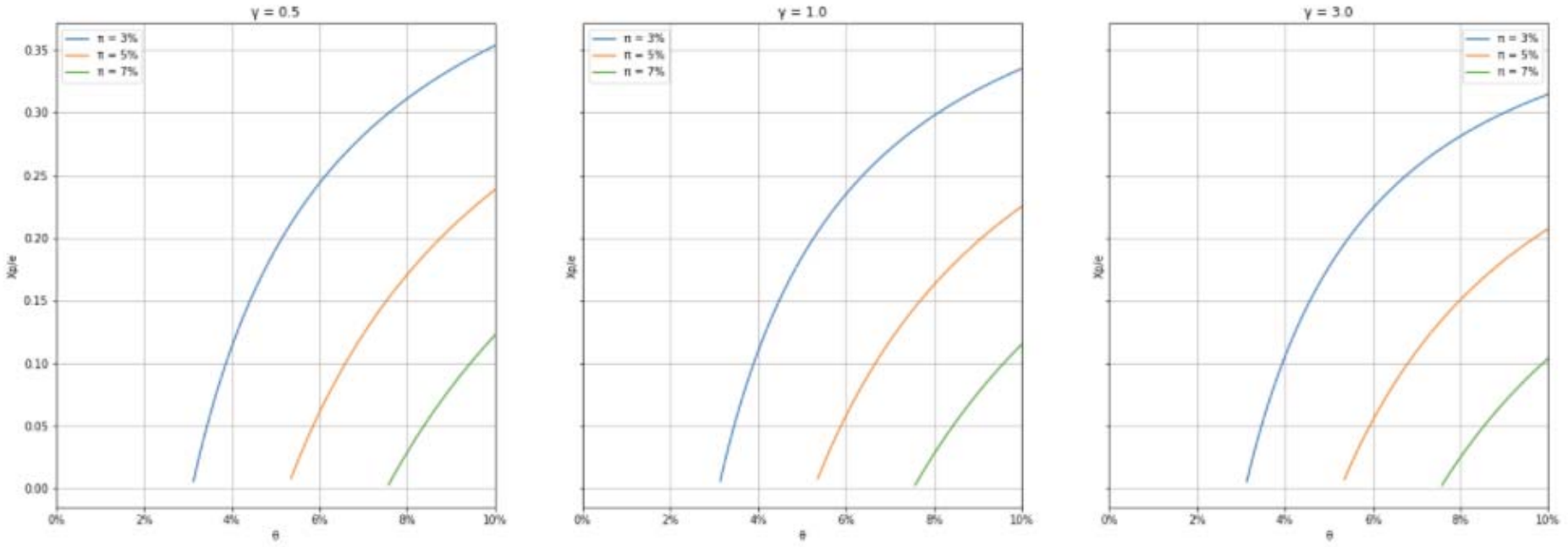
At $t+1$, their consumption is larger if no crash than if crash

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

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

A bit more action

In constant price equilibria analyzed above (Samuelson, Karecken-Garratt-Wallace): price constant, except when crash

Can we construct equilibria in which prices move all the time?

Yes ! with randomly fluctuating belief about crash proba

- State $\omega_t = (t, \varepsilon_{t-1}, \pi_t)$ observed at t
- $\varepsilon_{t-1} = c$ if crash occured before t, nc otherwise
- Markov: time t beliefs about $\omega_{s+1}, s \geq t$, depend on ω_t only

Volatile price equilibrium

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

Before N, ω_t moves around, price pinned down by recursion

$$p_2(\omega_t = (t, \mathbf{c}, \pi_t)) = 0$$

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

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

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

What sunspot?

Sunspot

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

Conclusion

(crypto)currency without intrinsic value valuable as means of payment, if believed to be valuable

but if all believe value is zero then it is

zero price equ. can be avoided for official currency, not for crypto

crypto features:

$\longrightarrow$ sunspot driven crash risk

$\longrightarrow$ extrinsic sunspot driven volatility

Risk factors

In adition to sunspot driven changes in beliefs about crash risk

cryptocurrency volatility can reflect arival of information about reliability & sustainability of blockchain

Protocol design

$\exists$? more sustainable protocol than bitcoin:
$\longrightarrow$ Proof of Stake

Design PoS protocol to ensure robustness to attacks and coordination problems
$\longrightarrow$ committee based BFT blockchains (Amoussou Guénou et al 2021, Auer et al 2022, Halaburda et al 2022)

Interaction protocol $\leftrightarrow$ cryptocurency price (Pagnotta 2022)

Competition between currency & cryptocurrency

Standard currency also comes with its own risk: inflation risk $\longrightarrow$ beliefs about endogenous standard currency supply

Horse race between:

- protocol money: extrinsic volatility, protocol risk
- institution money: political risk, commitment issues