Dynamic Modeling for Optimal Cryptoeconomic Policies

Mingxuan He
ECMA 33603
Prof. Andre Silva

July 24, 2023

Abstract

This paper introduces the idea of my thesis research project and documents my work so far. I provide a research topic description, discuss relevant literature including my replication for a baseline model, and report the current progress on my extended model, which combines two ideas from Stage 1 of the project.

I Introduction

In December 2018, the market capitalization of cryptocurrencies reached nearly 400 billion US Dollars, equivalent to 11% of M1 in the USA (Schilling & Uhlig, 2019b). As the size of blockchain and cryptocurrency networks grew, there has been increasing discussion around volatility and welfare in cryptoeconomies, and ways for the issuer of the cryptocurrency protocol to implement policies to ensure there is sustainable benefits for the network of token holders. These policies are often referred to as the protocol's "tokenomics".

As of today, most cryptoeconomic policies are static, which means the supply of tokens grows or shrinks according to a deterministic mechanism. For example, the supply of Bitcoin grows at a deterministic and decreasing rate. Many protocols cite these static policies act as an important aspect of decentralization: as the protocol pre-commits to a set of token issuance and burning policies, it reduces the requirement for trust from users in the procotol's governance. However, as demonstrated by both academic literature and recent events, the lack of response mechanisms can lead to devastating results when the cryptoeconomy faces exogenous shocks.

In many modern blockchain protocols, "staking" and "burning" are the primary coded policy rules in the underlying blockchain system. Staking is a mechanism where the user chooses to stake their token in the protocol for a period of time, after which the protocol rewards them with a staking yield that is paid out by newly minted tokens. In monetary economics terms, staking increases the total token supply by introducing new tokens into circulation, while reduces the amount of tokens in circulation due to illiquidity of the staked tokens. On the other hand, burning is a mechanism where the protocol burns (permanently destroys) some tokens from the supply, which usually comes from the transaction fees paid by users to conduct blockchain transactions.

Current staking and burning policy rules were primarily designed for the purpose of offering user incentives and/or preventing inflation from over-issuance. Most importantly, they do not respond to shock factors. My research aims to develop a model framework where staking and burning rules can be set dynamically to maximize the welfare of relevant actors in the cryptoeconomy.

This paper is organized as follows: Section II provides an overview of the established literature. Section III outlines the baseline model by Biais et al. (2020) and replicates its solutions (3.1) and outlines the current progress of my extended model (3.2).

II Literature Review

My research is related to the emerging literature on modeling cryptocurrencies and the blockchain economy. Following Yermack (2015) that argued that Bitcoin is not a currency, there was an interest in studying Bitcoin as a financial asset. Athey et al. (2016), Biais et al. (2020), Garratt and Wallace (2018), and Pagnotta (2022) studied equilibria in asset pricing models for Bitcoin. Schilling and Uhlig (2019a, 2019b) focused on the interactions between Bitcoin and the real economy, including dollar exchange rate and currency substitution. A broader set of models for Bitcoin include Bolt and Van Oordt (2020), Catalini and Gans (2020), Chiu and Koeppl (2017), Hinzen et al. (2022), and Huberman et al. (2021). For Proof-of-Stake protocols, Saleh (2019, 2021) modeled their general volatility and welfare, while Catalini et al. (2020) examined their tokenomics in the presence of an attack. A common result of the aforementioned asset pricing models is that static token supply causes all shocks are absorbed by the token price, which explains the high volatility of Bitcoin. This provides the motivation for an endogenous token supply in my model, which adds response mechanisms in terms of dynamic policy rules therefore can potentially mitigate the price effect of exogenous shocks.

Another set of literature has attempted to identify optimal policy rules for special types of tokens. Cong et al. (2021, 2022) built an asset pricing model featuring token issuance as means of platform financing and user growth leveraging network effects. Sockin and Xiong (2023a, 2023b) modeled cryptocurrencies as platform utility tokens and discussed elastic token issuance. d'Avernas et al. (2022) studied how stablecoin issuers can profit from seigniorage while maintaining the stablecoin's peg. Fernández-Villaverde et al. (2021) and Zhu and Hendry (2019) are examples of papers proposing optimal monetary policies for CBDCs. While the policy goals of utility tokens are very specific (defending peg for stablecoins/CBDCs, making profit for stablecoins/platform tokens), I adopt the general policy goal of maximizing user welfare, measured by consumption and transactional benefits.

My research is also related to the large literature on cryptocurrencies. Notable empirical researches include Liu and Tsyvinski, 2021 on the risk factors of cryptocurrencies, Makarov and Schoar, 2020 on the arbitrage spreads among different cryptocurrency markets. Griffin and Shams, 2020 studied the relationship between Tether purchases and cryptocurrency prices. Studies on the microeconomics of blockchain mechanisms include Biais et al. (2019), Budish (2018), Gans and Gandal (2019), Gans and Holden (2022), and Huberman et al. (2021).

III Model

3.1 Baseline model

This model was proposed by Biais, Bisiere, Bouvard, Casamatta, and Menkveld in their 2020 paper in The Journal of Finance titled "Equilibrium Bitcoin Pricing". Their main idea is that the fundamental value of cryptocurrencies comes from the stream of future transactional benefits (e.g. access to unique goods, not expropriated/taxed/constrained by government, direct internet access). The primary result is that Bitcoin price changes partly due to changes in fundamentals (net transactional benefits) but mostly due to extrinsic volatility.

The model is a two-period cryptoeconomy with overlapping generations of users. The cryptoeconomy includes three representative agents (user, validator, and hacker), three financial assets (risk-free asset, standard currency, and cryptocurrency). It features a fixed schedule money supply.

3.1.1 Users

In each period, young users receive some endowment in numeraire goods, which they spend on consumption goods and the three financial assets. They pay a fee on any cryptocurrency purchased. Old users consume all their savings from the previous period and receive transactional benefits on their cryptocurrencies. A portion of their crypto savings gets hacked. The users' budget constraints are:

$$c_t^y = e_t - s_t - (1+\varphi_t)q_t p_t - \hat{q}_t \hat{p}_t \tag{1}$$

$$c_{t+1}^o = s_t(1+r_t) + (1-h_{t+1})q_t p_{t+1} + \hat{q}_t \hat{p}_{t+1} + \theta_{t+1}(1-h_{t+1})q_t p_{t+1} \tag{2}$$

e_t: endowment
s_t: quantity of risk-free assets held
$q_t, \hat{q}_t$: quantities of crypto and dollars held
$p_t, \hat{p}_t$: prices (in units of consumption goods) of crypto and dollars
h_{t+1}: portion of crypto hacked by hackers
φ_t: transaction fees involved in using crypto (exog.)[1]
θ_{t+1}: transactional benefits from using crypto (exog.) (assume $\theta_{t+1} \geq -1$)

3.1.2 Validators

Validators receive newly minted tokens as block rewards, similar to a lump-sum transfer of money. The validators' budget constraint is:

$$c_{t+1}^v = (X_{t+1} - X_t)p_{t+1} + \varphi_{t+1} q_{t+1} p_{t+1} \tag{3}$$

X_t: stock token supply
$X_{t+1} - X_t$: increase in token supply (newly minted tokens)

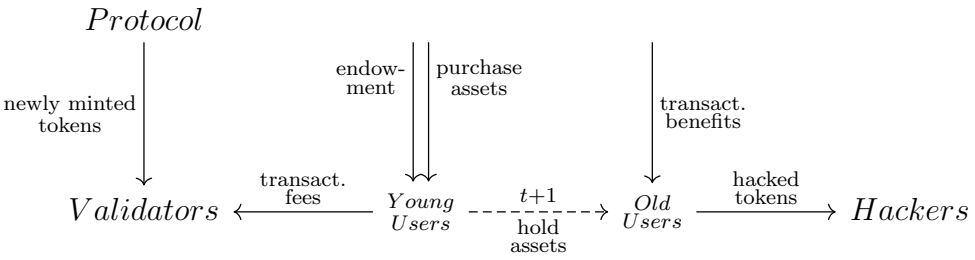
[1] The analysis remain largely unchanged if we include a transaction cost when selling crypto in period $t+1$ as well.

3.1.3 Hackers

Hackers hack a portion of users' crypto. The hackers' budget constraint is:

$$c_{t+1}^h = h_{t+1} q_t p_{t+1} \tag{4}$$

I made a graph summarizing of the interaction of the agents in two periods: Figure 5.



(5)

3.1.4 Solution

Here are my own steps for obtaining the pricing equations for cryptocurrency and standard currency.
The market clearing condition for the three financial assets are:

$$\text{crypto: } q_t = X_t \tag{6}$$
$$\text{dollars: } \hat{q}_t = m \tag{7}$$
$$\text{risk-free assets: } s_t = 0 \tag{8}$$
$$\tag{9}$$

Market for consumption goods also clears (by Walras's Law):

$$c_t^y + c_t^o + c_t^v + c_t^h = e_t \tag{10}$$

A young user in period t solves:

$$\max_{s_t, q_t, \hat{q}_t} u(c_t^y) + \beta \mathbb{E}_t u(c_{t+1}^o) \tag{11}$$
$$\text{subject to user's budget constraints and } c_t^y \geq 0$$

* Information set at period t includes $\{\theta_t, \varphi_t, \pi_t\}$
The Lagrangian is

$$\begin{aligned}
\mathcal{L} &= u(c_t^y) + \beta \mathbb{E}_t u(c_{t+1}^o) + \lambda c_t^y \\
&= u(e_t - s_t - (1+\varphi_t) q_t p_t - \hat{q}_t \hat{p}_t) \\
&\quad + \beta \mathbb{E}_t \left[u(s_t(1+r_t) + (1-h_{t+1}) q_t p_{t+1} + \hat{q}_t \hat{p}_{t+1} + \theta_{t+1}(1-h_{t+1}) q_t p_{t+1}) \right] \\
&\quad + \lambda(e_t - s_t - (1+\varphi_t) q_t p_t - \hat{q}_t \hat{p}_t)
\end{aligned} \tag{12}$$

First-order conditions:

$$s_t : -u'(c_t^y) + \beta(1+r_t)\mathbb{E}_t[u'(c_{t+1}^o)] = \lambda \tag{13}$$
$$q_t : -(1+\varphi_t) p_t u'(c_t^y) + \beta \mathbb{E}_t[u'(c_{t+1}^o)(1-h_{t+1})(1+\theta_{t+1}) p_{t+1}] = \lambda(1+\varphi_t) p_t \tag{14}$$
$$\hat{q}_t : -\hat{p}_t u'(c_t^y) + \beta \mathbb{E}_t[u'(c_{t+1}^o) \hat{p}_{t+1}] = \lambda \hat{p}_t \tag{15}$$

For Eqn. 14, substitute λ with LHS of Eqn. 13:

$$\begin{aligned} & -(1+\varphi_t)p_t u'(c_t^y) + \beta \mathbb{E}_t[u'(c_{t+1}^o)(1-h_{t+1})(1+\theta_{t+1})p_{t+1}] \\ &= (1+\varphi_t)p_t\{-u'(c_t^y) + \beta(1+r_t)\mathbb{E}_t[u'(c_{t+1}^o)]\} \qquad (16) \\ &\Rightarrow \\ & \beta \mathbb{E}_t[u'(c_{t+1}^o)(1-h_{t+1})(1+\theta_{t+1})p_{t+1}] \\ &= (1+\varphi_t)p_t\beta(1+r_t)\mathbb{E}_t[u'(c_{t+1}^o)] \qquad (17) \\ &\Rightarrow \end{aligned}$$

$$p_t = \frac{1}{1+r_t}\frac{1}{1+\varphi_t}\mathbb{E}_t[u'(c_{t+1}^o)]^{-1}\mathbb{E}_t[u'(c_{t+1}^o)(1-h_{t+1})(1+\theta_{t+1})p_{t+1}] \qquad (18)$$

Eqn. 18 is the pricing equation for cryptocurrency. Intuitively, $\frac{1}{1+r_t}$ is a discount by the interest rate, $1-h_{t+1}$ is the hack risk, $\frac{1+\theta_{t+1}}{1+\varphi_t}$ measures the net transactional benefits generating the currency's fundamental value, $\mathbb{E}_t[u'(c_{t+1}^o)]^{-1}u'(c_{t+1}^o)$ is the risk-neutral probability, and p_{t+1} is the resale value. This pricing equation provides a viewpoint that Bitcoin prices reflect both fundamentals and extrinsic factors.

We can also consider Eqn. 15, and substitute λ with LHS of Eqn. 13:

$$\begin{aligned} & -\hat{p}_t u'(c_t^y) + \beta \mathbb{E}_t[u'(c_{t+1}^o)\hat{p}_{t+1}] \\ &= \hat{p}_t\{-u'(c_t^y) + \beta(1+r_t)\mathbb{E}_t[u'(c_{t+1}^o)]\} \qquad (19) \\ &\Rightarrow \\ & \beta \mathbb{E}_t[u'(c_{t+1}^o)\hat{p}_{t+1}] \\ &= \hat{p}_t\beta(1+r_t)\mathbb{E}_t[u'(c_{t+1}^o)] \qquad (20) \\ &\Rightarrow \end{aligned}$$

$$\hat{p}_t = \frac{1}{1+r_t}\mathbb{E}_t[u'(c_{t+1}^o)]^{-1}\mathbb{E}_t[u'(c_{t+1}^o)\hat{p}_{t+1}] \qquad (21)$$

Eqn. 21 provides an expression for the return on dollars in the cryptoeconomy, in relation to the risk-neutral probability as well as the interest rate.

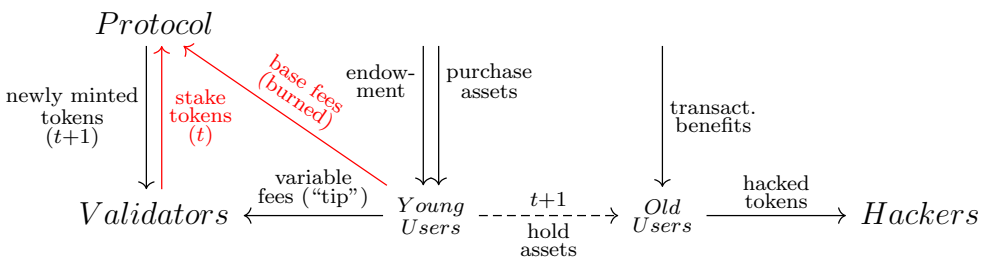
3.2 Extended model

3.2.1 Staking and burning

In my extended model, I introduce two new mechanisms:

- Two-part transaction fee with burning
- Interest-bearing staking

The protocol controls the staking yield ("interest rate") and the base transaction fee rate (burn rate). The figure below illustrates the new dynamics:



(22)

Define new variables, following notation in the ideas step:
L_t: amount of staked tokens
δ_t: staking yield (set by protocol)
φ_t^b: base fee (set by protocol)
φ_t^v: variable fee (competitively determined by validators and users)
The new budget constraints are:

$$\text{Young users: } c_t^y = e_t - s_t - (1 + \varphi_t^b + \varphi_t^v) q_t p_t - \hat{q}_t \hat{p}_t \tag{23}$$

$$\begin{aligned}\text{Old users: } c_{t+1}^o &= s_t(1 + r_t) + (1 - h_{t+1}) q_t p_{t+1} + \hat{q}_t \hat{p}_{t+1} \\ &\quad + \theta_{t+1}(1 - h_{t+1}) q_t p_{t+1}\end{aligned} \tag{24}$$

$$\text{Validators: } c_{t+1}^v = (1 + \delta_t) L_t p_{t+1} + \varphi_{t+1}^v q_{t+1} p_{t+1} - L_{t+1} p_{t+1} \tag{25}$$

$$\text{Hackers: } c_{t+1}^h = h_{t+1} q_t p_{t+1} \tag{26}$$

3.2.2 Endogenous token supply

Instead of a predetermined exogenous supply of tokens, now the supply is endogenous and dependent on the staking yield and base fee rate:

$$\begin{aligned}M_{t+1} &= (M_t - L_t) + L_t(1 + \delta_t) - \varphi_t^b X_t \\ &= M_t + \delta_t L_t - \varphi_t^b X_t\end{aligned} \tag{27}$$

M_t: total token supply
$X_t \equiv M_t - L_t$: circulating supply (Now the market clearing condition is $X_t = q_t$)

3.2.3 Validator's problem

Since the amount staked is an active choice by the validators, we now have a new optimization problem by the validators:

$$\begin{aligned}&\max_{L_{t+1}} \; u((1 + \delta_t) L_t p_{t+1} + \varphi_{t+1}^v q_{t+1} p_{t+1} - L_{t+1} p_{t+1}) \\ &\text{s.t. } q_{t+1} \leq M_{t+1} - L_{t+1}\end{aligned} \tag{28}$$

This problem describes the following trade off by the validators:

$$\text{more staking at } t \Rightarrow \begin{cases}\text{more staking yield at } t+1 \\ \text{less circulating supply} \Rightarrow \text{less transact. fees at } t\end{cases}$$

Intuitively, the budget constraint should be binding since there should not be idle tokens in the economy: all tokens either enter the circulating supply or be staked to generate yields. Formally, we can apply Karush-Kuhn-Tucker to solve the optimization problem.

The solution to this problem, and a general equilibrium solution for the extended model, are currently work in progress.

References

Athey, S., Parashkevov, I., Sarukkai, V., & Xia, J. (2016). *Bitcoin pricing, adoption, and usage: Theory and evidence* (tech. rep.). Stanford University Graduate School of Business Research Paper.

Biais, B., Bisiere, C., Bouvard, M., & Casamatta, C. (2019). The blockchain folk theorem. *The Review of Financial Studies*, *32*(5), 1662–1715.

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C., & Menkveld, A. J. (2020). Equilibrium bitcoin pricing. *The Journal of Finance*.

Bolt, W., & Van Oordt, M. R. (2020). On the value of virtual currencies. *Journal of Money, Credit and Banking*, *52*(4), 835–862.

Budish, E. (2018). *The economic limits of bitcoin and the blockchain* (tech. rep.). National Bureau of Economic Research.

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Communications of the ACM*, *63*(7), 80–90.

Catalini, C., Jagadeesan, R., & Kominers, S. D. (2020). Markets for crypto tokens, and security under proof of stake. *Available at SSRN 3740654*.

Chiu, J., & Koeppl, T. V. (2017). The economics of cryptocurrencies–bitcoin and beyond. *Available at SSRN 3048124*.

Cong, L. W., Li, Y., & Wang, N. (2021). Tokenomics: Dynamic adoption and valuation. *The Review of Financial Studies*, *34*(3), 1105–1155.

Cong, L. W., Li, Y., & Wang, N. (2022). Token-based platform finance. *Journal of Financial Economics*, *144*(3), 972–991.

d'Avernas, A., Maurin, V., & Vandeweyer, Q. (2022). Can stablecoins be stable? *University of Chicago, Becker Friedman Institute for Economics Working Paper*, (2022-131).

Fernández-Villaverde, J., Sanches, D., Schilling, L., & Uhlig, H. (2021). Central bank digital currency: Central banking for all? *Review of Economic Dynamics*, *41*, 225–242.

Gans, J. S., & Gandal, N. (2019). *More (or less) economic limits of the blockchain* (tech. rep.). National Bureau of Economic Research.

Gans, J. S., & Holden, R. T. (2022). *Mechanism design approaches to blockchain consensus* (tech. rep.). National Bureau of Economic Research.

Garratt, R., & Wallace, N. (2018). Bitcoin 1, bitcoin 2,....: An experiment in privately issued outside monies. *Economic Inquiry*, *56*(3), 1887–1897.

Griffin, J. M., & Shams, A. (2020). Is bitcoin really untethered? *The Journal of Finance*, *75*(4), 1913–1964.

Hinzen, F. J., John, K., & Saleh, F. (2022). Bitcoin's limited adoption problem. *Journal of Financial Economics*, *144*(2), 347–369.

Huberman, G., Leshno, J. D., & Moallemi, C. (2021). Monopoly without a monopolist: An economic analysis of the bitcoin payment system. *The Review of Economic Studies*, *88*(6), 3011–3040.

Liu, Y., & Tsyvinski, A. (2021). Risks and returns of cryptocurrency. *The Review of Financial Studies*, *34*(6), 2689–2727.

Makarov, I., & Schoar, A. (2020). Trading and arbitrage in cryptocurrency markets. *Journal of Financial Economics*, *135*(2), 293–319.

Pagnotta, E. S. (2022). Decentralizing money: Bitcoin prices and blockchain security. *The Review of Financial Studies*, *35*(2), 866–907.

Saleh, F. (2019). *Volatility and welfare in a crypto economy* (Vol. 3235467). SSRN.

Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of financial studies*, *34*(3), 1156–1190.

Schilling, L., & Uhlig, H. (2019a). Currency substitution under transaction costs. *AEA Papers and Proceedings*, *109*, 83–87.

Schilling, L., & Uhlig, H. (2019b). Some simple bitcoin economics. *Journal of Monetary Economics*, *106*, 16–26.

Sockin, M., & Xiong, W. (2023a). Decentralization through tokenization. *The Journal of Finance*, *78*(1), 247–299.

Sockin, M., & Xiong, W. (2023b). A model of cryptocurrencies. *Management Science*.

Yermack, D. (2015). Is bitcoin a real currency? an economic appraisal. In *Handbook of digital currency* (pp. 31–43). Elsevier.

Zhu, Y., & Hendry, S. (2019). *A framework for analyzing monetary policy in an economy with e-money* (tech. rep.). Bank of Canada Staff Working Paper.