Do cryptocurrencies matter?

B. Biais (HEC), J.C. Rochet (TSE), S. Villeneuve (TSE)

May 19, 2025

Abstract

In our dynamic general equilibrium model, agents can invest in money and in a production technology exposed to shocks. If the government is non-benevolent and has a monopoly over money issuance it issues too much money, to finance excessive public expenditures. We study the effects of a cryptocurrency in limited supply but with crash risk. If the crash risk is not too large, competition from the cryptocurrency constrains the government's monetary policy. If the government is non-benevolent, this constraint improves citizens welfare, but if the government is rather benevolent competition from the cryptocurrency can lower citizens' welfare.

Many thanks for useful feedback to participants at the 2023 Warwick Fintech Conference, the Cardiff University Fintech conference, the CBER Crafting the Crypto-Economy conference at Columbia University, the XIIth Economics of Payments conference in Vienna, the Oxford-Harvard decentralised finance conference, the WashU Essex conference on financial intermediation, the Future(s) of money conference, and seminars at the Oxford Man Institute, Saint Gall University, and the Banque de France. The support of the HEC-TSE-ACPR chair in Risks, Regulation and Systemic Risks is gratefully acknowledged. Biais acknowledges the support of the European Research Council (Grant 882375 WIDE). Rochet acknowledges the support of the European Research Council (Grant 101055239 DIPAMUTA).

1 Introduction

Can cryptocurrencies be useful? With well functioning monetary and financial institutions, official currencies, such as the dollar or the euro, are likely to provide better services than cryptocurrencies, to the extent that they have lower transaction costs and lower volatility.[1] But what if the government is predatory, there is hyperinflation, and political risk is large? In that case, a cryptocurrency, shielded from institutions' dysfunctionality, can offer an attractive alternative to official money.

This may be the reason why the ownership and use of cryptocurrencies has become very large in countries such as Argentina, Egypt, Lebanon, Nigeria, Turkey, and Venezuela. In such countries, cryptocurrencies can be seen as a lifeline, a shield against hyperinflation, and the depreciation of the official currency. According to some estimates, 50% of people in Turkey own cryptocurrency.[2] On 23 February 2024 a *Financial Times* article on Nigeria noted:[3]

> "Digital assets have gained popularity because many people have lost trust in the naira as a reliable store of value. "

Similarly, on 23 March 2024, an article in Coin Telegraph noted:[4]

> "Argentines' efforts to preserve their savings amid the ongoing decline of their national currency, the Argentine peso, have resulted in the nation recently hitting its highest demand for Bitcoin in 20 months."

Large inflation is often attributed to the reliance on excessive money creation to fund large public spending.[5] This causal mechanism is emphasized, e.g., by Lopez and Mitchener (2020) in their study of hyperinflation in Europe after World War 1.[6] Similarly, Pittaluga, Seghezza and Morelli (2021) attribute hyperinflation in Venezuela in the 2010s to inflationary financing of public spending.[7] In his essay entitled "Denationalisation of Money", Hayek (1976) argued that these problems could be avoided thanks to

> "the replacement of the government monopoly of money by competition in currency supplied by private issuers, who, to preserve public confidence, will limit the quantity of their paper issue and thus maintain its value."

[1] The financing of illegal activities is outside the scope of the paper.

[2] See, e.g., https://www.binance.com/en/square/post/1131869

[3] "Nigeria blocks digital asset exchanges as naira plunges,"*Financial Times*, 23rd of February, 2024.

[4] cointelegraph.com/news/bitcoin-demand-argentina-reaches-peak-argentine-peso

[5] See, e.g., the seminal analysis of Cagan (1956).

[6] On page 450 of their article, Lopez and Mitchener (2020, page 450) write "Why do hyperinflations begin? In a mechanical sense, economists have known the answer to this question at least since the monetarist revolution: money is printed in response to unsustainable fiscal policy"

[7] Pittaluga, Seghezza and Morelli (2021) write (pages 337 and 338): "When ... the financing of the existing level of public spending no longer could be sustained by domestic and oil-related taxes, inflationary financing was adopted and hyperinflation ensued. "

Cryptocurrencies are an interesting laboratory to test Hayek's proposition. Cryptocurrencies offer privately supplied means of payment and store of value. Moreover, their issuance rate is determined by the protocol of the blockchain on which they rely, and this protocol is quite difficult to change. This creates the possibility to commit to a predetermined issuance rate, which helps to maintain the value of a currency.

Against this backdrop, our goal is to address the following questions: Can cryptocurrencies be used by private agents when the value of public currencies is undermined by non-benevolent governments' policies ? Can competition from cryptocurrencies discipline non-benevolent governments' monetary and fiscal policies?

To conduct this analysis, we rely on a theoretical model that captures some of the main characteristics of cryptocurrencies: The pace of monetary creation of cryptocurrency is set in advance by the blockchain protocol on which ownership of the cryptocurrency is registered. This protects the cryptocurrency from the excessive inflation plaguing the official currency. Moreover, it is difficult for the government to tax cryptocurrency holdings. But the cryptocurrency is risky and may crash. As in Garratt and Wallace (2019), Rocheteau and Wang (2023), and Biais, Bisière, Bouvard, Casamatta, and Menkveld (2023), the crash can reflect sunspot-driven extrinsic uncertainty. It might also reflect a technology or cybersecurity problem, as in Pagnotta (2022).[8]

We analyze the consequences of these characteristics of cryptocurrencies in a simple general equilibrium model, featuring a government and a continuum of agents operating technologies with i.i.d. productivity shocks. The government does not have the skills to operate these technologies, and therefore must delegate operations to the agents. Because agents are risk averse, they seek to reduce their exposure to random productivity shocks hitting the technologies they operate. We assume, however, the market is incomplete and agents cannot buy insurance against their productivity shocks. While we take this incompleteness as given in the present paper, it can be microfounded by assuming that aents privately observe their productivity shocks, as in Biais, Gersbach, Rochet, von Thadden, and Villeneuve (2023). In this context, agents value the opportunity to hold money, to diversify their portfolio away from their risky production technology. Thus, agents make portfolio choices, deciding what fraction of their wealth to invest in the risky production technology and what fraction to invest in money. The government chooses how much money to issue, and also how much agents' wealth should be taxed, as well as the level of public spending. The budget constraint of the government is that public spending equals tax proceeds plus seigneurage revenues. There is a conflict of interest between the government and the agents, as the government's preferences put more weight on public spending than the agents' preferences.

[8] As written by Garratt and Wallace (2019): "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. The other interpretation of the randomness underlying the equilibrium is that it represents intrinsic uncertainty."

First, as a benchmark, we consider the case in which there is no cryptocurrency, so that the government has a monopoly over money issuance. In that case, we show that a non-benevolent government can rely on seigneurage to fund excessive public spending. When the government is highly non-benevolent, this leads to hyperinflation, which in our theoretical framework is defined as the situation in which agents are unwilling to hold the official currency, the value of which correspondingly goes to zero, not unlike what happened in Venezuela in the 2010s.

Second, we turn to the situation in which there is a cryptocurrency and show that two cases can arise:

- If the cryptocurrency's crash risk is very high, the presence of the cryptocurrency does not change outcomes. It is so risky that it does not offer an attractive store of value, so the government effectively keeps its monopoly power over money issuance. A benevolent government does not find it optimal to go for large inflation, so that agents are happy to hold official currency and, in equilibrium, do not hold cryptocurrency.

- In contrast, if the government is non-benevolent, it would like to go for large inflation. But this is prevented by competition from the cryptocurrency: If the inflation rate of the official currency were too large, agents would not want to hold it and would hold the cryptocurrency instead. Taking this reaction into account, the non-benevolent government finds it optimal to show restraint in its monetary policy. Thus, competition from the cryptocurrency effectively caps inflation in the official currency.

Our analysis thus shows that, while competition from cryptocurrency does not impact benevolent governments, it constrains non-benevolent governments, which makes agents better off. This is in line with Hayek (1976) and rationalizes the following stylized facts:

- First, in many countries, governments and central banks oppose the development of cryptocurrencies, which is in line with the idea that competition from cryptocurrencies constrains governments and central banks.

- Second, ownership of cryptocurrencies is larger in countries in which government and central bank dysfunctionality gives rise to large inflation.

Our paper is related to the literature providing microfoundations for the usefulness of money (dating back to the seminal papers of Allais, 1947, Samuelson, 1958, Tirole, 1985, Weil, 1987, Kiyotaki and Wright, 1989 and 1993, and Lagos and Wright, 2005) and to the literature extending monetary theory to cryptocurrencies (see, e.g., Garatt and Wallace, 2018, Schilling and Uhlig, 2019, Benigno, Schilling, and Uhlig, 2022, and d'Avernas, Vandeweyer and Maurin, 2023). Within this literature, the papers to which our analysis is closest are those studying hyperinflation and those studying competition between currencies. Rocheteau (2024) offers an insightful analysis of equilibria in which the value of the currency progressively declines until it reaches zero. While in Rocheteau (2024) hyperinflation corresponds to a progressive erosion of the value of money due to the self-fulfilling beliefs of the agents, in our analysis hyperinflation corresponds to an instantaneous erosion of the value of the money due to the unsustainability of the government policy. Kareken and Wallace (1981), Garatt and Wallace (2018), Fernandez-Villaverde and Sanches (2019), Biais, Bisière, Bouvard, Casamatta and Menkveld (2023), Rocheteau (2024) and Arifovic, Salle and Schilling (2025) study competition between currencies. The main contribution of the present paper relative to that literature is to offer a microfoundation for the differences in usefulness between cryptocurrencies and public currencies, reflecting endogenous monetary and fiscal policy, and relate it to the conflict of interest between agents and non-benevolent governments.

In our analysis, when inflation in the official currency is high, agents switch to cryptocurrency. This is similar to Thiers' law, in Bernholz (1989) which states that when inflation is high, agents switch from the domestic currency to foreign currency. Pittaluga, Seghezza and Morelli (2021) discuss this switch in the context of the recent hyperinflation crisis in Venezuela.

Our theoretical analysis is also related to empirical analyses of cryptocurrency markets. Luckner, Reinhart, and Rogoff (2023) provide empirical evidence that cryptocurrencies are used to conduct transactions and store value, not unlike in our model. In our model, as long as there is no crash, the demand for cryptocurrency tends to increase faster than its supply, so that the price of the cryptocurrency increases. This is not unlike the mechanism econometrically analyzed by Jermann (2021).

In the next section, we analyze the benchmark case in which there is no cryptocurrency. Section 3 then extends the analysis to the case in which there is a cryptocurrency. Our main result is that competition from the cryptocurrency constrains government policy, which improves citizens' welfare if the government is self-interested but reduces citizens' welfare if the government is benevolent. Section 4 offers a brief comparison between cryptocurrencies and gold. We show that to some extent, well-functioning cryptocurrencies can be seen as the "gold of the 21st century ". Section 5 concludes. Proofs not given in the main text are in the appendix.

2 The Model without Cryptocurrency

In this section, we build a simple macrofinance model with frictions, where a self-interested government has the monopoly of money issuance, and exploits this monopoly power to extract rents from citizens. In the next section, we study how competition from cryptocurrency can constrain the government and whether this increases the welfare of citizens.

2.1 Technology

Time is continuous: $t \in (0, \infty)$. There is a government and a mass 1 continuum of agents, indexed by $i \in (0,1)$. There is only one good, which is produced by agents with a constant return to scale technology, and can be used for private consumption, government consumption, or investment. At date t, agent i operates k_t^i units of capital. Aggregate capital is denoted by K_t:

$$K_t = \int_0^1 k_t^i di. \tag{1}$$

The output of agent i at date t is

$$k_t^i(\mu dt + \sigma dZ_t^i),$$

where the Z_t^i are independent Brownian motions that represent idiosyncratic risks. Under mild regularity assumptions these idiosyncratic risks wash away in aggregate, and total output (GDP) is μK_t.[9] In the absence of frictions, it would be optimal to eliminate idiosyncratic risks by diversification. However, we assume that individual output is not publicly observable. Agents can secretly divert a fraction of their output and secretly consume it. This prevents agents from fully diversifying risks through financial instruments such as equity or insurance contracts. However, they can partially insure their risks by holding money whose supply is entirely controlled by the government.

2.2 Preferences

We denote by c_t^i the consumption flow of agent i and by G_t the flow of public spending. The preferences of the citizens are

$$U^i \equiv \mathbb{E} \int_0^\infty e^{-\rho t}[\log c_t^i + \alpha \log G_t]dt, \tag{2}$$

for agent $i \in (0,1)$, where $\alpha > 0$ is the weight put by citizens on public spending. The preferences of the government are

$$U_G \equiv \int_0^1 U^i di + \beta \mathbb{E} \int_0^\infty e^{-\rho t} \log G_t dt, \tag{3}$$

where $\beta \geq 0$. Equation (3) states that the government maximizes utilitarian welfare but puts an additional weight β on public spending. If $\beta = 0$, the government is fully benevolent. The larger β, the less benevolent the government.

2.3 Government Policy

The government issues M_0 units of fiat money on date $t = 0$ and distributes them equally to the agents, as well as K_0 units of capital.[10] Money supply at

[9] A condition under which idiosyncratic risk washes away is that at each date t, the mapping $i \mapsto k_t^i$ is square-integrable.

[10] This is optimal when the government puts equal welfare weights on all agents.

time t is denoted by M_t. The only market is a spot market in which the physical good is exchanged for money at endogenous price p_t.

Since preferences and technology are constant and utility is logarithmic, there exist balanced-growth stationary equilibria in which all aggregate quantities grow at a constant rate.[11] In such equilibria, money-supply growth is

$$\frac{dM_t}{dt} = g_m M_t,$$

where g_m is a constant, and public spending is a constant fraction of aggregate capital K_t:

$$G_t = \gamma K_t.$$

To balance its budget, the government transfers to the citizens the difference between the revenue from the issuance of money (seigneuriage) $\frac{dM_t}{dt}$ and the public expenditures $p_t G_t$. This difference can be positive (subsidy) or negative (tax). We assume that these transfers are allocated proportionally to agents' wealth. Because growth is balanced, the transfer rate τ is constant.

2.4 Individual behavior

Agents form rational expectations about the price p_t of the good at all future dates and choose their consumption c_t, money holdings m_t and investment k_t to maximize

$$\mathbb{E}[\int_0^\infty e^{-\rho t} \log c_t dt]. \tag{4}$$

under their budget constraint.[12] Public spending also enters in the utility of the agent, but additively, and is not controlled by the agents. So we don't need to include it in the optimization problem of the agent.

On a balanced growth path the inflation rate π and the growth rate g of capital are constant:

$$p_t = p_0 e^{\pi t}, K_t = K_0 e^{gt}. \tag{5}$$

Agents' real wealth is the sum of their capital holdings and real balances:

$$w_t = k_t + \frac{m_t}{p_t}. \tag{6}$$

Since there are no transaction costs, agents can immediately and costlessly adjust the composition of their wealth at any time. Thus, w_t is the single state variable for each agent. The dynamics of w_t is given by the state-equation:

$$dw_t = k_t(\mu dt + \sigma dZ_t) + (\tau w_t - c_t - \pi(w_t - k_t))\, dt. \tag{7}$$

[11] Biais, Gersbach, Rochet, von Thadden and Villeneuve (2025) offer a micro-foundation in which the monetary equilibrium on which we focus in the present paper can implement second-best allocations.

[12] Hereafter, to avoid cumbersome notations, we omit the index i, but the reader should bear in mind that there are many agents, with different asset holdings and consumption.

The change in real wealth is output plus government transfers minus consumption and depreciation due to inflation. Denoting by $u(w)$ the value function of the agent, we can write the Bellman equation

$$\rho u(w) = \max_{c,k} \Big(\log c + u'(w)[\mu k + \tau w - c - \pi(w-k)] + \frac{\sigma^2 k^2}{2} u''(w) \Big), \tag{8}$$

where the maximum is subject to the constraint that money holdings cannot be negative, which is equivalent to $k \leq w$. As in Merton (1969), the homogeneity of the agent's program and the logarithmic utility of consumption imply that $u(w)$ is also logarithmic:

$$u(w) = \frac{\log w}{\rho} + u(1),$$

so that

$$wu'(w) = -w^2 u''(w) = \frac{1}{\rho}. \tag{9}$$

The agent's decision problem therefore simplifies to

$$\max_{c,k} \log c + \frac{1}{\rho} \left(\frac{(\mu+\pi)k}{w} + \tau - \frac{c}{w} - \pi \right) - \frac{\sigma^2 k^2}{2\rho w^2},$$

under the constraint that $k \leq w$. The first order condition with respect to c implies that optimal consumption is a constant fraction ρ of the wealth of the agents:

$$c = \rho w.$$

The propensity to consume is thus constant and equal to ρ : it increases with the impatience of the agent. Because agents have logarithmic utility, their propensity to consume is not affected by other parameters, such as the transfer rate or the inflation rate.

The first order condition with respect to k implies that optimal investment in capital is a constant fraction x of agents' wealth with:

$$x = \min \left[\frac{\mu+\pi}{\sigma^2}, 1 \right] \tag{10}$$

So, when $\pi < \sigma^2 - \mu$, the capital investment share x chosen by the agent is smaller than 1. Therefore

$$\mu + \pi = \sigma^2 x. \tag{11}$$

The left-hand side of this equation is the benefit of capital investment, equal to the expected return μ plus the benefit of being protected from inflation. Thus, x increases with inflation, an important feature to which we will return later. The right-hand side of equation (11) is the cost of capital investment, namely the productivity risk. The higher this risk, the lower the propensity of agents to invest in capital. In contrast, since the agents invest the fraction $(1-x)$ of their of wealth in money, condition (11) implies that money holdings decrease with inflation but increase with productivity risk. The latter reflects the fact that money is valued by agents because it is a safe asset. Finally, note that the agent's portfolio choice x does not depend on the transfer rate τ because transfers are proportional to total wealth.

2.5 Rational expectations equilibrium

Having characterized individual behavior as a function of anticipated inflation π, we now study rational expectations equilibria in the markets for goods and money, for a given choice of policy instruments (g_m, γ). Equilibrium on the good market is characterized by the equality of savings and investment:

$$\frac{dK_t}{dt} = \mu K_t - C_t - \gamma K_t \tag{12}$$

Since there is no depreciation of capital, the growth of aggregate capital $(\frac{dK_t}{dt})$ is equal to investment. Market clearing implies that this investment is equal to savings, that is, output μK_t minus agents' consumption C_t and government spending γK_t. Moreover, since the agent's optimality conditions imply that his consumption is $c_t = \rho w_t$ and his capital holdings are $k_t = x w_t$, the agent's consumption is also proportional to his capital: $c_t = \rho \frac{k_t}{x}$. Aggregating between agents, we see that aggregate wealth is $W_t = \frac{K_t}{x}$, while agregate agents' consumption is $C_t = \frac{\rho}{x} K_t$. Hence, the growth rate of capital is:

$$g = \mu - \frac{\rho}{x} - \gamma. \tag{13}$$

The higher the investment x, the lower the consumption and the higher the growth rate. In addition, the larger ρ, the more impatient the agents, the larger their consumption, and therefore the lower their aggregate investment. Thus, the growth rate g decreases with the agent discount rate ρ.

The rate τ of public transfers is determined by government's budget balance: total transfers τW_t equal seigneurage $g_m(1-x)W_t$ minus public spending $\gamma x W_t$, which implies

$$\tau = g_m(1-x) - \gamma x. \tag{14}$$

The third step of our equilibrium analysis is to equalize money supply and money demand. We have seen that agents want to keep a constant fraction $(1-x)$ of their wealth in money and the rest in capital. Therefore, the aggregate money demand is $\frac{(1-x)}{x} p_t K_t$. It is proportional to the nominal value of the aggregate capital stock $p_t K_t$. Since money supply grows at rate g_m, the equality between money supply and money demand gives:

$$M_0 e^{g_m t} = \frac{(1-x)}{x} p_t K_t = \frac{(1-x)}{x} p_0 e^{\pi t} K_0 e^{g t}. \tag{15}$$

Condition (15) shows that there always exists a rational expectation equilibrium in which money has no value. In fact, when all agents anticipate that $p_0 = \infty$, they invest only in capital ($1-x=0$). We interpret this situation as (an extreme form of) hyperinflation: money has no value, and agents do not use it.

But there may also exist a monetary equilibrium, that is, an equilibrium in which money has a strictly positive value (p_t is finite for all t) and the demand for money is strictly positive ($x < 1$). In a monetary equilibrium, equality between money supply and money demand at time 0 yields

$$M_0 = \frac{(1-x)}{x} p_0 K_0. \tag{16}$$

Substituting (16) into (15), in a monetary equilibrium we have

$$g_m = g + \pi, \tag{17}$$

expressing that nominal growth equals real growth plus the inflation rate. We can reformulate condition (17) by replacing g and π by their expressions given by (11) and (13). We obtain an equation that determines x, with two regimes:

- When the demand for money is strictly positive ($x < 1$), $\pi = \sigma^2 x - \mu$ and $g = \mu - \frac{\rho}{x} - \gamma$. By adding up these two conditions, we obtain an implicit equation for x:

  $$\sigma^2 x - \frac{\rho}{x} = g_m + \gamma. \tag{18}$$

  Since the left hand side of (18) is increasing in x, there is a unique solution. It satisfies $x < 1$ when

  $$g_m + \gamma < \sigma^2 - \rho. \tag{19}$$

- On the contrary when

  $$g_m + \gamma \geq \sigma^2 - \rho,$$

  the only equilibrium is non monetary ($x = 1$): the demand for money is zero and money has no value.

This yields our first proposition:

Proposition 1 *When government expenditures and money creation are not too high, as (19) holds, there is a unique monetary equilibrium, characterized by an inflation rate $\pi = \sigma^2 x - \mu$, where $x < 1$ is the unique solution of*

$$\sigma^2 x - \frac{\rho}{x} = g_m + \gamma. \tag{20}$$

Otherwise, if (19) does not hold, the only equilibrium corresponds to hyperinflation: the value of money is zero and agents invest all their wealth in productive capital ($x = 1$).

The proposition shows that the nature of the equilibrium (monetary or not) and the level of inflation are completely determined by $I \equiv (g_m + \gamma)$, which can be interpreted as an index of inflationary pressure. It aggregates the growth rate of the money supply with the government expenditure rate. The inflation rate π is increasing in I. If I is too large, the only equilibrium corresponds to hyperinflation: $x = 1$ and $p_t \equiv \infty$. Finally, when $x < 1$ (monetary equilibrium) the level of prices is determined by equation (16): p_0 is proportional to M_0. This is a weak form of neutrality in the sense that the initial price level is proportional to the initial money supply. However, the inflation rate is determined by other policy variables (g_m, γ), aggregated into the index of inflationary pressure I.

2.6 Citizens' welfare and government's objective

Government policy boils down to monetary policy, i.e., the money-supply growth rate g_m, and budget policy, i.e., the public spending rate γ.[13] Proposition 1 shows that the equilibrium value of x is determined by the sum of these policy rates. The next subsection characterizes the welfare of the citizens U and the government's objective U_G as a function of government policy. We then compute the optimal policy, maximizing U_G.

Assuming initial wealth, $W_0 = \frac{K_0}{x}$, is equally distributed among agents at time $t = 0$, the initial welfare of each citizen is equal to

$$U \equiv \mathbb{E} \int_0^\infty e^{-\rho t}[\log c_t + \alpha \log G_t]dt, \tag{21}$$

where $c_t = \rho w_t$ and $G_t = \gamma K_t$. Moreover $K_t = K_0 e^{gt}$, where $g = \mu - \frac{\rho}{x} - \gamma$. Finally, rearranging (7) we obtain

$$\frac{dw_t}{w_t} = gdt + \sigma x dZ_t.$$

These conditions imply that

$$\log c_t = \log \frac{\rho K_0}{x} + (g - \frac{\sigma^2 x^2}{2})t + \sigma x Z_t,$$

and

$$\log G_t = \log \gamma K_0 + gt.$$

Easy computations give

$$\rho U = \log \frac{\rho K_0}{x} + \alpha \log \gamma K_0 + \frac{1}{\rho}[(1+\alpha)(\mu - \frac{\rho}{x} - \gamma) - \frac{\sigma^2 x^2}{2}]. \tag{22}$$

The interpretation of equation (22) is that agents put weight 1 on the utility from consuming a fraction ρ/x of their capital and weight α on the utility from public spendings, equal to fraction γ of aggregate capital, and that aggregate capital deterministically grows at rate $\mu - \rho/x - \gamma$, while agents' wealth is exposed to shocks with instantaneous variance $\sigma^2 x^2$.

Similarly, the government objective function U_G is such that

$$\rho U_G = \log \frac{\rho K_0}{x} + (\alpha + \beta) \log \gamma K_0 + \frac{1}{\rho}[(1+\alpha+\beta)(\mu - \frac{\rho}{x} - \gamma) - \frac{\sigma^2 x^2}{2}]. \tag{23}$$

[13] The transfer rate τ does not impact individual decisions. It is determined by the government budget constraint.

2.7 Policy choices and impact on citizens

The government maximizes expression (23) with respect to (x, γ) under the constraint $x \leq 1$. He chooses the public spending rate

$$\gamma_M = \frac{\rho(\alpha + \beta)}{1 + \alpha + \beta}, \tag{24}$$

where the subscript M refers to the monopoly of money issuance. The maximum with respect to x is obtained for $x = \min(1, x_M(\beta))$, where $x_M(\beta)$ is the unique solution of the cubic equation

$$\frac{\sigma^2}{\rho} x^3 + x = 1 + \alpha + \beta. \tag{25}$$

Note that $x_M(\beta) < 1$ if and only if $\beta < \frac{\sigma^2}{\rho} - \alpha$. This gives our next proposition:

Proposition 2 *1. The government chooses the spending rate given by (24).*

2. When $\beta < \frac{\sigma^2}{\rho} - \alpha$, the government implements a monetary equilibrium with $x = x_M(\beta) < 1$.

3. When $\beta \geq \frac{\sigma^2}{\rho} - \alpha$, the government implements the hyperinflation equilibrium and the agents do not use money: $x = 1$.

The policy decisions that maximize the welfare of citizens are obtained by taking $\beta = 0$ in the above formulas:

$$\gamma^* = \frac{\rho\alpha}{1 + \alpha}, x^* = x_M(0). \tag{26}$$

The comparison with the policy chosen by the government is immediate. From the point of view of the citizens, the level of public expenditures is too high $(\gamma_M > \gamma^*)$.

To analyze money issuance, we assume from now on that $\alpha < \frac{\sigma^2}{\rho}$. This condition ensures that $x^* < 1$: Citizens would never choose hyperinflation spontaneously. Hyperinflation occurs only in our model when the intensity β of government failure is high: $\beta > \frac{\sigma^2}{\rho} - \alpha$. The proposition also implies that, even when there is no hyperinflation, the inflation rate $\pi_M = \sigma^2 x_M(\beta) - \mu$ is higher (and the welfare of the citizens lower) than what the citizens would like. The interpretation of these results is natural: a self-interested government uses its monopoly power to issue too much money in order to finance excessive expenditures.

2.8 The determinants of inflation and growth

In our model, the level of inflation and the growth rate of the economy are determined by political-economy considerations and the fundamentals of the economy. To shed light on this detemination, we hereafter derive comparative-statics properties of the monetary equilibrium ($x < 1$). We focus on three parameters: β, the intensity of government failure, μ the marginal productivity of capital, and σ, the volatility of productivity risk.

Proposition 3 *1. The inflation rate π_M is an increasing function of β and σ, and a decreasing function of μ.*

2. The real growth rate g_M is a U-shaped function of β, a decreasing function of σ, and an increasing function of μ.

When the government is not benevolent (that is, when β is large), it wants to spend a lot. To fund this spending, the government needs high growth and correspondingly large investments. But agents may be reluctant to invest a lot in capital because their output is risky. To ensure that agents invest enough, a self-interested government finds it optimal to go for high inflation.

If the government is highly non-benevolent, we have $x_M(\beta) > 1$, which implies that agents only invest in capital and do not demand money. They do so because inflation is so large that it is not worth holding money, that is, there is hyperinflation. In hyperinflation, the welfare of agents is low as their risk exposure is large, since they cannot hold money to buffer productivity shocks. As we will see in the next section, in this context, the ability to hold cryptocurrency can be valuable for agents.

3 Competition between public and private currencies

3.1 Introducing a cryptocurrency in the model

We now consider the case where, at $t = 0$, $\hat{M}_0$ cryptocurrency tokens are issued and distributed equally to all agents. The ownership of the tokens is recorded on a blockchain that the government cannot manipulate. The issuance of cryptocurrencies is determined by the blockchain protocol. For simplicity and without effect on our qualitative results, we assume that it takes place only at time 0. The supply of cryptocurrency at times $t > 0$ is kept constant: $\hat{M}_t \equiv \hat{M}_0$.

To capture the risky nature of the cryptocurrency, we assume it can crash. More precisely, we assume there is an exogenous Poisson process N_t with intensity λ, which all agents observe. At the first jump in this process, cryptocurrency tokens become worthless, that is, $\hat{p}_t$ goes to infinity. As in Garatt and Wallace (2018) and Biais et al.(2023), there are two possible interpretations of the crash. The first interpretation is that the jump of the Poisson process is a sunspot: When agents observe this sunspot, they rationally anticipate that the token has no value. This is because the cryptocurrency, just like the official currency, is a pure bubble, without any real counterpart or dividend, whose value stems from the belief that it is valuable. In this context, the belief that the cryptocurrency has no value is self-fulfilling. The second interpretation is that the

Poisson process jumps when a major technological problem in the blockchain occurs, e.g., Byzantine nodes successfully attack the blockchain protocol (see, e.g., Pagnotta, 2022).

We hereafter denote the time of the first jump of the Poisson process by T. At any time $t < T$ an agent holds capital k_t and real balances m_t in official currency and $\hat{m}_t$ in cryptocurrency. The price of the good in cryptocurrency is denoted by $\hat{p}_t$. Consequently, the composition of the real wealth w_t of a typical agent is as follows:

$$w_t = k_t + \frac{m_t}{p_t} + \frac{\hat{m}_t}{\hat{p}_t}.$$

As in the previous section, because utility is logarithmic and the environment is stationary (until the first jump of the Poisson process), portfolio shares are constant. We denote by x the fraction of real wealth w_t invested in capital and by b the fraction invested in public money. The share invested in cryptocurrency is $(1 - b - x)$. So we have

$$k_t = xw_t, \frac{m_t}{p_t} = bw_t, \frac{\hat{m}_t}{\hat{p}_t} = (1 - b - x)w_t.$$

At the time of the cryptocurrency crash, the price of the official currency jumps from p_T to p_{T^+} (we use the superscript + to denote what happens after the crash). Also, at the time of the crash, the agent's wealth jumps to

$$w_{T^+} = k_T + \frac{m_T}{p_{T^+}} = w_T(x + b\frac{p_T}{p_{T^+}}).$$

3.2 Agents' optimal decisions

We consider a rational expectations equilibrium that is stationary until time T, with constant money-supply growth rate g_m, constant inflation rates, π for the official currency and $\hat{\pi}$ for the cryptocurrency, and constant transfer rate τ. The transfer to (if $\tau > 0$) or from (if $\tau < 0$) citizens is proportional to the part $(b + x)w$ of the wealth of the citizens that is observable by the government.[14] The rest of the citizens' wealth is invested in cryptocurrency.

The dynamics of an agent's wealth is given by:

$$\frac{dw_t}{w_t} = x(\mu dt + \sigma dB_t) + \left(\tau(b + x) - \frac{c_t}{w_t} - \pi b - \hat{\pi}(1 - b - x)\right) dt - (1 - x - b\frac{p_t}{p_t^+})dN_t.$$

The last term reflects the possibility of a cryptocurrency crash, a Poisson event with intensity λ. When the Poisson process jumps, so that $dN_t = 1$, agents lose a fraction $(1 - x - b\frac{p_t}{p_t^+})$ of their wealth.

[14] Citizens could report their currency holdings to public authorities but in practice they seem to keep them secret, especially when $\tau < 0$ (taxes). For example, Meling et al. (2024) find evidence that 80 percent of the Norwegian citizens who hold cryptocurrencies do not report them to the tax authorities.

As in the previous section, because the utility function is logarithmic, the value function is also logarithmic. Before the cryptocurrency crash, there is a constant $\hat{u}(1)$ such that the value function of an agent is

$$\hat{u}(w) = \frac{\log w}{\rho} + \hat{u}(1).$$

The Bellman equation for an agent is

$$\rho\hat{u}(w) = \max_{c,x,b} \log c + \frac{1}{\rho}(\mu x + \tau(b+x) - (\pi b + \hat{\pi}(1-b-x)) - \frac{c}{w}) \tag{27}$$

$$-\frac{\sigma^2 x^2}{2\rho} - \frac{\lambda}{\rho} log \frac{w}{w(x + b\frac{p}{p^+})}. \tag{28}$$

c, x, and b must be non negative but these constraints don't bind. In contrast, the constraint that $x + b$ be lower than or equal to one can bind. As in the case without cryptocurrency, the first-order condition with respect to consumption yields

$$c = \rho w.$$

The portfolio problem of the agent is to choose $x \leq 1$ and b to maximize

$$\mu x + \tau(b+x) - \pi b - \hat{\pi}(1-b-x)i - \frac{\sigma^2 x^2}{2} + \lambda log(x + b\frac{p}{p^+}).$$

The Lagrangian of this problem is

$$\mathbb{L} = \mu x + \tau(b+x) - \pi b - \hat{\pi}(1-b-x) - \frac{\sigma^2 x^2}{2} + \lambda log(x + b\frac{p}{p^+}) + \nu(1-b-x),$$

where ν is the multiplier associated with the constraint that $x + b \leq 1$. The first order conditions are

$$\mu + \tau + \hat{\pi} - \sigma^2 x + \frac{\lambda}{x + b\frac{p}{p^+}} = \nu,$$

with respect to x and

$$\tau - \pi + \hat{\pi} + \frac{\lambda\frac{p}{p^+}}{x + b\frac{p}{p^+}} = \nu,$$

with respect to b.

The first condition states that the optimal portfolio is such that the marginal benefit of investing in productive capital, $\mu + \tau - \sigma^2 x + \frac{\lambda}{x+b\frac{p}{p^+}} - \nu$ is equal to the marginal benefit $-\hat{\pi}$ of investing in the cryptocurrency. The marginal benefit of investing in productive capital is equal to expected productivity μ, plus public transfer rate τ, minus risk premium $\sigma^2 x$, plus the hedging value of capital against a cryptocurrency crash, minus the shadow cost ν of the constraint $x + b \leq 1$. The marginal benefit of investing in cryptocurrency is the expectation of an increase in the real value of cryptocurrency, that is, $-\hat{\pi}$.

The second condition expresses that the marginal benefit of holding official money equals the marginal benefit $-\hat{\pi}$ of holding cryptocurrency. The benefit of holding official money is the transfer rate τ minus inflation π plus the hedging value of official money in relation to a cryptocurrency crash,[15] and minus the shadow cost ν of the constraint $x + b \leq 1$.

3.3 Equilibrium conditions

After the crash the cryptocurrency is valueless. So agents can only invest their wealth in productive capital and official currency. Denote by W_{T^+} the aggregate wealth of the agents after the crash. Agents rationally anticipate that after the crash government policy and equilibrium will be the same as when there is no cryptocurrency. Consequently, when $\beta < \frac{\sigma^2}{\rho} - \alpha$, government policy after the crash is such that agents invest fraction x_M of their wealth in capital and the rest in money, where x_M is defined by the cubic equation (25). In this case, the aggregate demand for capital is

$$K_T = x_M W_{T^+}.$$

Before the cryptocurrency crash, agents have a fraction x of their wealth invested in productive capital. Noting that the aggregate stock of productive capital is unchanged after the crash, we obtain a condition imposed by the conservation of capital

$$K_T = x W_T = x_M W_{T^+}.$$

Considering that, at the time of the cryptocurrency crash, the wealth of agents jumps from W_T to $W_{T^+} = W_T(x + b\frac{p_T}{p_T^+})$, we have

$$\frac{W_T^+}{W_T} = x + b\frac{p_T}{p_T^+}.$$

Combining this equation with the conservation of capital condition we have

$$x + b\frac{p_T}{p_T^+} = \frac{x}{x_M}. \tag{29}$$

Thus, the total wealth of agents is reduced by a factor $\frac{x}{x_M}$ after the cryptocurrency crash. Note that productive capital and official money offer different hedging values to citizens, because the real value of money is affected by the price change $\frac{p_T}{p_T^+}$. By (29), this price change is

$$\frac{p_T}{p_T^+} = \frac{x(1 - x_M)}{b x_M}. \tag{30}$$

We also need to take into account the government budget constraint

$$(\gamma + \tau)\, x = (g_m - \tau) b, \tag{31}$$

[15] Note that this hedging value is generally different from the hedging value of capital, due to the price increase that follows the cryptocurrency crash

together with the condition that gives the growth rate of the economy, which is the same as in the previous section

$$g = \mu - \gamma - \frac{\rho}{x}, \tag{32}$$

and the inflation rate of the cryptocurrency, which is

$$\hat{\pi} = -g, \tag{33}$$

since the supply of cryptocurrency is constant while the economy grows at a rate g. Finally, the growth of the money supply must be equal to the sum of inflation and real growth

$$g_m = \pi + g, \tag{34}$$

Note that this condition implies that, in any stationary equilibrium, the growth rate of the price of the cryptocurrency expressed in official currency, that is $(\pi - \hat{\pi})$ is equal to g_m, the rate of growth of the supply of official money.

We are now in a position to characterize the competitive equilibrium between currencies.

3.4 The outcome of competition between currencies

We now characterize the competitive equilibrium in the presence of a cryptocurrency as a function of government policy (γ, g_m). As before, there always exists a nonmonetary equilibrium $(x = 1)$ where both currencies have no value because agents anticipate that they will not be accepted by other agents. We focus on monetary equilibria $(x < 1)$ where one or both currencies are accepted for trade. They are characterized in the next proposition (whose proof is in the appendix).

Proposition 4 *When $x_C \equiv \frac{\sqrt{\rho+\lambda}}{\sigma} < min(1, x_M)$, there exists a monetary equilibrium. Its characteristics depend on the index of inflationary pressure $I = \gamma + g_m$:*

- *If $I > \frac{\lambda(1-x_M)}{x_C(1-x_C)}$, the equilibrium is interior: $x + b < 1$ and $x = x_C$. The fraction invested in cryptocurrency increases with I.*
- *In contrast, if $I \leq \frac{\lambda(1-x_M)}{x_C(1-x_C)}$, we have a boundary equilibrium where agents do not hold the cryptocurrency and $x \leq x_C$.*

When $x_C \equiv \frac{\sqrt{\rho+\lambda}}{\sigma} \geq min(1, x_M)$, the cryptocurrency has no impact: the equilibrium is the same as in Proposition 1.

Proposition 4 is the counterpart of Proposition 1. It shows that, when the probability of a cryptocurrency crash is small enough $(\lambda < \sigma^2 - \rho)$ so that $x_C < 1$, the monetary equilibrium always exists, even if the government would prefer a hyperinflation equilibrium $(x_M \geq 1)$. The presence of a cryptocurrency guarantees the possibility of a monetary equilibrium and the nature of this equilibrium depends on the index of inflationary pressure I.[16] If this index is high, the cryptocurrency is held by the agents. If this index is low, the cryptocurrency is not held by the agents, and the share of the wealth of the agents that is invested in productive capital is low, as $x < x_C$. In both cases, the existence of a monetary equilibrium is guaranteed whenever $x \leq x_C < 1$. The government can implement any $x \leq x_C$ by an appropriate choice of g_m, but cannot reach any $x > x_C$.

In contrast, when the probability of crash is high, so that $x_C \geq 1$, the cryptocurrency has no impact: the equilibrium is the same as when the government has the monopoly of money issuance, including the possibility of hyperinflation if β is too high. We now examine how the presence of the cryptocurrency impacts the policy choices of the government.

3.5 Government policy

The objective of the government is similar to that of its counterpart without cryptocurrency. The only difference is that, when there is a cryptocurrency, the government must take into account the possibility that this cryptocurrency crashes. After the crash, we are back to the initial situation, and the government adopts the policy characterized in Proposition 2. Before the crash, the government is limited by the presence of cryptocurrency, as shown in Proposition 4: x cannot exceed x_C. The choice of x_t may therefore be time dependent, since this constraint disappears after the random date T at which the cryptocurrency crashes. Because optimal investment is constant before and after the cryptocurrency crash, we consider the following dynamic for x_t,

$$x_t = x \mathbb{1}_{t<T} + x_M \mathbb{1}_{t \geq T}.$$

In contrast, the choice of γ is not affected by the cryptocurrency and is thus time-independent. So the value function of the government is U_G such that:

$$\rho U_G = E \int_0^\infty \rho e^{-\rho t} \left[\log \rho w_t + (\alpha + \beta) \log \gamma K_t\right] dt,$$

where

$$\frac{dw_t}{w_t} = (\mu - \gamma - \frac{\rho}{x_t})dt + \sigma x_t dt - (1 - \frac{x_t}{x_M})dN_t.$$

Standard computations show that, up to a constant

$$\rho U_G = (\alpha + \beta) \log \gamma + (1 + \alpha + \beta)(\frac{\mu - \gamma}{\rho} - \frac{\rho}{x(\rho + \lambda)}) - \frac{1}{\rho + \lambda}\big(\rho \log x + \frac{\sigma^2 x^2}{2}\big).$$

The government chooses (x, γ, δ) to maximize this expression under the constraint $x \leq \min(1, x_C)$. The optimal government policy is described in our next proposition.[17]

[16] The cryptocurrency, however, does not eliminate the possibility of hyperinflation, since the non monetary equilibrium always exists.

[17] The proof of the proposition is immediate since U_G is quasi-concave in x and has an unconstrained maximum for $x = x_M(\beta)$.

Proposition 5 *The existence of a cryptocurrency has no impact on government spending, that is, $\gamma = \gamma_M$. However, since the government cannot force agents to invest more than a fraction x_C of their wealth in capital, for monetary policy two situations are possible:*

- *When $x_C < min(1, x_M)$ the government policy choice is such that agents choose $x_t = x_C, \forall t \leq T$, and invest the rest of their wealth in the two currencies.*
- *When $x_C \geq min(1, x_M)$, the cryptocurrency has no impact.*

When the government is rather benevolent (that is, β is low), it does not want to set inflation too high. Consequently, it does not want to set x too high. This corresponds to a value of $x_M(\beta)$ below $x_C(\lambda)$. In that case, agents are satisfied with holding capital and the official currency and do not find it optimal to hold cryptocurrency. So, the government is not constrained in its monetary policy by the competition of the cryptocurrency.

In contrast, when the government is quite non-benevolent (that is, β is high), it would like to conduct monetary policy such that inflation would be high and correspondingly x would be high, since $x_M(\beta) > x_C(\lambda)$. In that case, competition from the cryptocurrency prevents the government from conducting such a predatory policy. It reduces inflation and caps x at $x_C(\lambda)$. In that case, agents hold cryptocurrency.

Note that $x_C(\lambda) = \frac{\sqrt{\rho+\lambda}}{\sigma}$ increases with the risk of a cryptocurrency crash (λ). If the cryptocurrency is very risky, agents are reluctant to hold it. Therefore, the competitive pressure exerted by the cryptocurrency is weak and does not restrict the government very much.

The proposition also has implications for the macroeconomic impact of cryptocurrency. When the government is non-benevolent and the cryptocurrency is not too risky, agents bear less risk and consume more with the cryptocurrency than without it. This suggests that the presence of the cryptocurrency could make agents better off. We examine this point in the next subsection.

3.6 Are citizens better off with the cryptocurrency?

Proposition 5 shows that cryptocurrency does not impact public spending. However, it changes the composition of the portfolio of households when $x_C < \min(1, x_M)$. The difference between the welfare of citizens with cryptocurrency and without it is proportional to $U(x_C) - U(x_M)$ where

$$U(x) = -\left[\log x + \frac{\sigma^2 x^2}{2\rho} + \frac{1+\alpha}{x}\right].$$

We know that $U(x)$ is maximum for $x = x^*$ and that $x_M > x^*$. Since U is quasi-concave and unbounded below, for all $x_M > x^*$, there is a unique $x = \phi(x_M)$ that satisfies the two conditions $U(x) = U(x_M)$ and $x < x_M$. Intuitively, $\phi(x_M)$ is the unique value of x in the domain $x < x_M$ (where U is increasing) that gives the same utility as x_M: $U(\phi(x_M)) = U(x_M)$. Therefore, $U(x_C) < U(x_M)$ if and only if $x_C < \phi(x_M)$.

Thus, the cryptocurrency hurts the citizens if and only if $x_C < \phi(x_M)$. It benefits the citizens when $\phi(x_M) < x_C < x_M$ and has no impact when $x_C > \min(1, x_M)$. These results are summarized in the following proposition.

Proposition 6 *Three configurations are possible:*

1. *When $x_C > \min(x_M, 1)$, the cryptocurrency has no impact. This occurs when λ is large and β is small.*
2. *When $\phi(x_M) < x_C < x_M$, the cryptocurrency improves the welfare of citizens This occurs when β is large.*
3. *When $x_C < \phi(x_M)$, cryptocurrency is bad for the citizens. This occurs when both λ and β are small.*

The result that the cryptocurrency may hurt citizens may be surprising, since no one is forced to use it. However, we have seen that its presence restricts the feasible policy tools that the government can use. This may be good for citizens if the government is strongly self-interested (β is large). But, as stated in the proposition, this is bad when β and λ are small.

4 Gold

In our model, the cryptocurrency is an alternative to official money with two essential features: Private holdings are not observable by the government, and citizens have a second store of value that protects them if the government becomes extortive. Similar protection has been provided for many years by precious metals such as gold or silver. What is different with cryptocurrencies?

In this section, we study how gold compares with a cryptocurrency as a store of value providing protection to citizens. We apply the same model as before but change the interpretation: individuals invest a fraction x of their wealth in productive capital, a fraction b in official money and a fraction $b_G = 1 - b - x$ in gold. We assume that the aggregate quantity of gold is constant and that the government cannot tax or even seize individual gold holdings because they are not publicly observable. However, they can be stolen by thieves. By analogy to cryptocurrency, we assume that individual thefts are governed by Poisson processes N_t^G with intensity λ_G. There is, however, an important difference: While the risk of cryptocurrency crash is aggregate (the Poisson process N_t is the same for all agents), the risk of gold theft is idiosyncratic (we assume that the Poisson processes N_t^G are independent between agents). An individual theft does not affect the market price or the government policy does not change. Thus, equilibrium conditions with gold are similar to their counterparts with cryptocurrency, except that there is no regime change after the theft, in particular, $p^+ = p$. The Bellman equation is

$$\rho\hat{u}(w) = \max_{c,x,b} \log c + \frac{1}{\rho}\left(\mu x + \tau(b+x) - (\pi b + \hat{\pi}(1-b-x)) - \frac{c}{w}\right)$$
$$-\frac{\sigma^2 x^2}{2\rho} - \frac{\lambda_G}{\rho} log \frac{w}{w(x+b)},$$

and we obtain the following proposition:

Proposition 7 *When there is no cryptocurrency, but agents can secretly store gold, the competitive equilibrium has the following properties: When* $x_G \equiv \frac{\sqrt{\rho+\lambda_G}}{\sigma} < 1$, *there exists a monetary equilibrium. It is such that* $x \leq x_G$. *In this equilibrium,* x *is determined by*

$$I = \sigma^2 x - \frac{\rho}{x},$$

where $I = g_m + \gamma$ *is the index of inflationary pressure.*

We now determine the policy choice of the government in the model with gold but without cryptocurrency. Contrary to the previous model (with cryptocurrency but without gold), x is stationary (since there is no aggregate shock) but agents are exposed to individual risks of theft of their gold holdings, in which case they lose a fraction $b_G = 1 - x - b$ of their wealth. Easy computations show that

$$\rho\hat{U}_G = \log\frac{\rho}{x} + (1+\alpha+\beta)(\log K_0 + \frac{\mu-\gamma}{\rho} - \frac{1}{x}) + (\alpha+\beta)\log\gamma - \frac{\sigma^2 x^2}{2\rho} + \frac{\lambda_G}{\rho}\log(x+b).$$

We see that contrarily to the case of cryptocurrency, citizens' money holdings b appear in the objective function of the government, because they impact the size of losses in case of theft. Thus, independently of β, the government will always want to protect citizens against this risk of theft by choosing transfers τ that are high enough so that $x + b = 1$. The choice of x is similar to the case of a cryptocurrency. We can state the main result of this section, which is the exact counterpart of Proposition 6.

Proposition 8 *The possibility of secretly holding gold has no impact when* $x_G > \min(x_M, 1)$, *which occurs when* λ_G *is large and* β *is small. The possibility of secretly holding gold improves the welfare of citizens when* $\phi(x_M) < x_G < x_M$, *which occurs when* β *is large. The possibility of secretly holding gold hurts citizens when* $x_G < \phi(x_M)$, *which occurs when both* λ_G *and* β *are small.*

Thus, in our model, comparing the impact of gold to that of cryptocurrency is essentially a matter of comparing x_G and x_C, and therefore λ_G and λ. In particular, gold can discipline an extortive government only when the risk of theft λ_G is relatively small. To the extent that $\lambda < \lambda_G$, cryptocurrencies can be viewed as a modern and efficient substitute for gold. This suggests cryptocurrencies should be particularly useful in countries in which government is predatory (i.e., β is large) and public safety is low (i.e., λ_G is large).

5 Conclusion and directions for future research

In our model, money has no intrinsic value and is not backed by any real asset, but it is valuable because it is a store of value, useful for agents who seek to buffer uninsurable productivity shocks.

When a non-benevolent government has the monopoly in the issuance of money, it runs an expansionary monetary policy, giving rise to high inflation, compelling agents to save by investing in risky productive assets. Since these assets are productive, they generate large aggregate output, which the government can tax to indulge in large public spending. In the limit, when the government is highly non-benevolent, this leads to hyperinflation, in which case money is valueless and agents only invest in risky assets. The correspondingly large risk exposure reduces the agents' welfare.

A cryptocurrency, competing with the official currency, can prevent the government from inflating too much. Thus the cryptocurrency increases the welfare of citizens when the government is highly non-benevolent. To the extent that cryptocurrency is private money, this result echoes Hayek's (1976) advocacy for the denationalization of money. In contrast, when the government is benevolent, if competition from the cryptocurrency constrains the government policy this reduces citizens' welfare.

The role played by cryptocurrency in our model is not unlike that of gold, which citizens can secretly hoard to hedge against inflation and avoid excessive taxation. Government failure, however, is likely to deteriorate public safety as well as economic policy. For citizens exposed to a high risk of theft, gold hoarding is unattractiveness. In that context, cryptocurrencies can offer a modern and potentially more efficient alternative to gold.

References

Allais, M., 1947, Economie et Intérêt, Paris, Imprimerie Nationale.‘

Arifovic, J., I. Salle, L. Schilling, 2025, “Currency competition, Monetary policy and Transaction Costs: Theory and Experiments”, Working Paper.

d’Avernas, A, V. Maurin, and Q. Vandeweyer, 2023, “Can Stablecoins be Stable?”Working paper, HEC.

Benigno, P. L. Schilling and H. Uhlig, 2019, “Cryptocurrencies, Currency Competition, and the Impossible Trinity”, *Journal of International Economics.*

Bernholz, P., 1989, “Currency competition, inflation, Gresham’s law and exchange rate. ”*Journal of Institutional and Theoretical Economics*, pp. 465-488.

Biais, B., C. Bisière, M. Bouvard, C. Casamatta and A. Menkveld, 2023, “Equilibrium bitcoin pricing”, *Journal of Finance.*

Biais, B., H. Gersbach, J.C. Rochet, E. von Thadden, and S. Villeneuve, 2023, “Dynamic contracting with many agents,”Working paper, HEC.

Cagan, P., 1956, “The monetary dynamics of hyperinfl ation,”in Friedman, M., Ed., Studies in the Quantity Theory of Money, The University of Chicago Press, Chicago, 25-117.

Cass, D., and K. Shell, 1983, “Do Sunspots Matter?”*Journal of Political Economy*, pp.193-227.

Fernández-Villaverde, J., and Daniel Sanches, 2019, “Can currency competition work? ”*Journal of Monetary Economics*, pp. 1-15.

Garratt, R. and N. Wallace, 2018, “Bitcoin 1, bitcoin 2, . . . An experiment in privately issued outside monies” *Economic Inquiry* pp 1887-1897.

von Hayek, F., 1976, “Denationalization of Money,” Hobart Paper, 70, Institute of Economic Affairs.

Jermann, U., 2021, “Cryptocurrencies and Cagan’s model of hyperinflation ” *Journal of Macroeconomics*, pp 1-9.

Kareken, J. and N. Wallace, 1981, “On the Indeterminacy of Equilibrium Exchange Rates”, *Quarterly Journal of Economics*, pp. 207-222.

Kiyotaki and Wright, 1993, “A Search-Theoretic Approach to Monetary Economics”, *The American Economic Review*, pp. 63-77.

Kiyotaki and Wright, 1989, “On Money as a Medium of Exchange,” *The Journal of Political Economy*, pp. 927-54.

Lagos, L. and R. Wright, 2005, “A Unified Framework for Monetary Theory and Policy Analysis”, *Journal of Political Economy*, pp. 463-484.

Lopez, J., and J. Mitchener, 2020, “Uncertainty and hyperinflation: European inflation dynamics after World War 1, ”*Economic Journal*, pp 450-475.

von Luckner, C., C. Reinhart, and K. Rogoff, “Decrypting new age international capital flows,”*Journal of Monetary Economics*, pages 104-122.

Meling, T., M. Mogstad, and A. Vestre, 2024, “Crypto Tax Evasion ” *Working Paper NO. 2024-106, Becker Friedman Institute, Chicago.*

Merton, R., 1969, “Lifetime Portfolio Selection under Uncertainty: The Continuous-Time Case, ”*The Review of Economics and Statistics*, pp. 247-257.

Pagnotta, E., 2022, “Decentralizing Money: Bitcoin Prices and Blockchain Security, ” *The Review of Financial Studies*, Volume 35, Issue 2, February 2022, Pages 866–907.

Pittaluga, G., E. Seghezza, and P. Morelli, 2021, “The political economy of hyperinflation in Venezuela”, *Public Choice*, pp 337-350.

Prat, J., and B. Walter, 2021, “An equilibrium model of bitcoin mining”, *Journal of Political Economy*, pp 2415-2452.

Rocheteau, G., and L. Wang, 2023, “Endogenous liquidity and volatility, ”forthcoming *Journal of Economic Theory*.

Rocheteau, G., 2024, “When money dies: The dynamics of speculative hyperinflation,”Working paper, University of California, Irvine.

Samuelson, P., 1958, “An exact consumption-loan model of interest with or without the social contrivance of money,” *Journal of Political Economy*, pp 467-482.

Schilling, L. and H. Uhlig, 2019, “Some Simple Bitcoin Economics”, *Journal of Monetary Economics*, pp. 16-26.

Tirole, J., 1985, “Asset bubbles and overlapping generations,” *Econometrica*, pp 1071-1100.

Weil, P., 1987, “Confidence and the real value of money in an overlapping generations economy,” *Quarterly Journal of Economics*, pp 1-22.

Appendix: Proofs

Proof of Proposition 3: Part 1: the monotonicity of π with respect to β and μ is immediate, since $\pi = \sigma^2 x_M(\beta) - \mu$ while $x_M(\beta)$, given implicitly by the cubic equation (25), is an increasing function of β and does not depend on μ. Now, the total differentiation of this cubic equation with respect to σ^2 gives

$$\frac{x^3}{\rho} + \frac{\sigma^2(3x^2+1)}{\rho}\frac{dx}{d\sigma^2} = 0,$$

or

$$\frac{dx}{d\sigma^2} = -\frac{x^3}{\sigma^2(3x^2+1)}.$$

Since $\pi = \sigma^2 x - \mu$, we have

$$\frac{d\pi}{d\sigma^2} = x + \sigma^2\frac{dx}{d\sigma^2} = x - \frac{x^3}{3x^2+1} = \frac{2x^3+x}{3x^2+1} > 0,$$

which ends the proof of part 1.

Part 2: first note that $g = \mu - \frac{\rho(\alpha+\beta)}{1+\alpha+\beta)} - \frac{\rho}{x_M(\beta)}$, which can be expressed more conveniently as a function of $x = x_M(\beta)$ rather than β. We obtain:

$$g = \mu - \rho\frac{\frac{\sigma^2}{\rho}x^3 + x - 1}{\frac{\sigma^2}{\rho}x^3 + x} - \frac{\rho}{x} = \mu - \rho - \frac{1}{\frac{x}{\rho} + \frac{1}{\sigma^2 x}},$$

which is U-shaped in $x = x_M(\beta)$, and thus in β. The two other properties are immediate.

Proof of Proposition 4: Using the equilibrium conditions (32) and (34), the first order conditions of the agent's portfolio problem can be transformed into:

$$\tau + \frac{\rho}{x} + \gamma + \delta - \sigma^2 x + \frac{\lambda}{x + b\frac{p}{p^+}} = \nu,$$

and

$$\tau - g_m + \frac{\lambda\frac{p}{p^+}}{x + b\frac{p}{p^+}} = \nu.$$

Multiplying the first condition by x, the second by b and adding the two, we obtain

$$(\tau + \gamma + \delta)x + (\tau - g_m)b + \rho - \sigma^2 x^2 + \lambda = \nu, , \qquad (35)$$

where we have used the complementarity slackness condition

$$\nu(x + b - 1) = 0.$$

The first two terms in the previous equation add to zero by the budget constraint of the government. We obtain finally

$$\sigma^2 x^2 = \rho + \lambda - \nu,$$

that is

$$x = \frac{\sqrt{\rho + \lambda - \nu}}{\sigma}.$$

The multiplier ν being nonnegative, this establishes the first part of the proposition: $x \leq x_C$. This implies the existence of a monetary equilibrium ($x < 1$) when $x_C < 1$.

Using conditions (29) and (30), the first order conditions become

$$\tau + \frac{\rho}{x} + \gamma + \delta - \sigma^2 x + \frac{\lambda x_M}{x} = \tau - g_m + \frac{\lambda(1 - x_M)}{b} = \nu.$$

Computing the difference between these two conditions, we see that

$$I = g_m + \gamma + \delta = \sigma^2 x - \frac{\rho}{x} + \lambda(\frac{1 - x_M}{b} - \frac{x_M}{x}). \tag{36}$$

If the equilibrium is interior ($x + b < 1$), the holdings of cryptocurrency are positive, $\nu = 0$ and $x = x_C$. On the other hand, in a boundary equilibrium ($x + b = 1$), agents do not hold any cryptocurrency and $x \leq x_C$. Thus there are two cases:

1. $\nu = 0, x = x_C$ and

$$\frac{\lambda(1 - x_M)}{b} = I - \frac{\lambda(1 - x_M)}{x_C}.$$

   Then $b < 1 - x_C$ if and only if

$$I > \lambda(1 - x_M)[\frac{1}{1 - x_C} + \frac{1}{x_C}] = \frac{\lambda(1 - x_M)}{x_C(1 - x_C)},$$

2. $\nu > 0, x < x_C$ and $b = 1 - x$, where x is determined by the equation

$$I = \sigma^2 x - \frac{\rho}{x} - \frac{\lambda x_M}{x} + \frac{\lambda(1 - x_M)}{1 - x}.$$

   Thus $x \leq x_C$ if and only if $I \leq \frac{\lambda(1-x_M)}{x_C(1-x_C)}$.

This establishes the first part of Proposition 4. Note also that money holdings are always positive, since putting $b = 0$ in (36) would imply an infinite I. The second part of the proposition is immediate since $x_C \geq 1$ implies that the cryptocurrency has no impact on the equilibrium.

QED

Proof of Proposition 7

The first order conditions of portfolio optimization become

$$\mu + \tau + \hat{\pi} - \sigma^2 x + \frac{\lambda_G}{x + b} = \nu, \tag{37}$$

respect to x and

$$\tau - \pi + \hat{\pi} + \frac{\lambda_G}{x+b} = \nu, \tag{38}$$

with respect to b, where ν is the multiplier associated with the constraint $b+x \leq 1$.[18] We use a similar method as above to determine the characteristics of the equilibrium. By subtracting (38) from (37), we find that

$$\pi = \sigma^2 x - \mu.$$

Moreover, stationarity conditions imply that

$$\hat{\pi} = -g = \gamma + \frac{\rho}{x} - \mu,$$

and

$$g_m = g + \pi = \sigma^2 x - \frac{\rho}{x} - \gamma.$$

Thus

$$I = g_m + \gamma = \sigma^2 x - \frac{\rho}{x}.$$

Multiplying (37) by x, (38) by b, adding them and using the stationarity conditions, we find that

$$(\tau + \gamma)x + \rho - \sigma^2 x^2 + \lambda_G + (\tau - g_m)b = \nu(x+b) = \nu.$$

Using the budget constraint of the government

$$(\gamma + \tau)\, x = (g_m - \tau)b, \tag{39}$$

we finally find

$$x = \frac{\sqrt{\rho + \lambda_G - \nu}}{\sigma} \leq x_G \equiv \frac{\sqrt{\rho + \lambda_G}}{\sigma}$$

and

$$\frac{\lambda_G}{x+b} = \nu - \tau + g_m.$$

Thus, the government can influence citizens' portfolio choice (x, b) up to the following constraints:

$$x \leq min(x_G, 1), x + b \leq 1.$$

If we assume $x_G < min(x_M, 1)$ (otherwise, gold has no disciplining power) there are in fact two cases:

1. $\nu = 0, x = x_G, x + b \leq 1$
2. $\nu > 0, x < x_G, x + b = 1.$

QED

[18] As we will see, the constraint $b \geq 0$ is never binding.