CRYPTOCURRENCY AND CURRENCY LOSS

Nicholas Glenn
Department of Economics
University of Alabama
Tuscaloosa, AL 35487
nglenn@crimson.ua.edu

Robert Reed*
Department of Economics
University of Alabama
Tuscaloosa, AL 35487
rreed@cba.ua.edu

July 13, 2021

ABSTRACT

In recent years, there has been increased enthusiasm regarding the viability of cryptocurrencies. Consequently, an academic literature studying cryptocurrency has also emerged. In terms of thinking about the viability of cryptocurrency, there has also been increasing awareness of the costs of producing such forms of money. In this sense, the costs of producing digitally issued money can be significantly higher than pieces of paper issued by sovereign governments. Yet, in addition to the relatively unique features of the costs of producing digital money, cryptocurrencies are also embedded with unique security features. Notably, a unique feature of cryptocurrency is that such forms of private outside money are based on cryptography as holders of coins store their currencies such as Bitcoin at an address on a decentralized ledger that is linked to both a private and public key. If a private key is lost or damaged, the coins are permanently missing. This aspect of many cryptocurrencies is typically omitted from previous work that studies whether privately issued outside money would circulate over time. Consequently, failing to account for permanent coin loss may fundamentally alter the conditions where private money circulates. It is also likely to impact whether the supply of private money over time would be socially efficient. In light of this gap in the existing literature, the objective of this paper is to study how exogenous token loss affects the conditions where privately produced money circulates. In particular, we discuss how the relationship between the price of coins and the degree of token loss also depends on the shape of the cost function.

JEL Classification: E40, E42, E52

Keywords: Private Money, Token Loss, Production Costs

I. Introduction

In recent years, there has been increased enthusiasm regarding the viability of cryptocurrencies. For example, the value of Bitcoin, the cryptocurrency with the largest circulation, has recently been established near $60,000. In addition, there has been significant appreciation of other cryptocurrencies such as Ethereum and Dogecoin in the past several years. Consequently, an academic literature studying cryptocurrency has also emerged. In particular, the ideas put forward by Hayek (1999) are often invoked when considering whether privately created outside monies could circulate in equilibrium.

In terms of thinking about the viability of cryptocurrency, there has also been increasing awareness of the costs of producing such forms of money. In this sense, the costs of producing digitally issued money can be significantly higher than pieces of paper issued by sovereign governments. Notably, a recent contribution by Fernandez-Villaverde and Sanches (2019, hereafter, FVS) has

*Corresponding Author

emphasized how the technologies for producing digital money play a significant role in determining whether private forms of money would exist. In particular, their framework shows that the shape of the cost function determines the relationship between equilibrium prices and the incentive to produce money over time. To be specific, an equilibrium with stable prices can only exist if the cost function is strictly increasing and locally linear around the origin. That is, if the marginal cost of producing tokens is equal to zero, there would be incentives to produce money until it eventually becomes worthless.

Yet, in addition to the relatively unique features of the costs of producing digital money, cryptocurrencies are also embedded with distinctive security features. For example, a special feature of cryptocurrency is that such forms of private outside money are based on cryptography – holders of coins store their currencies such as Bitcoin at an address on a decentralized ledger that is linked to both a private and public key.[2] As the identity of the individual behind the public address is unknown, public key cryptography is necessary for network verification. Similar to a pen name, the public address acts as a pseudonym for the owner of the cryptocurrency. In order to transfer Bitcoin from an address, the crypto holder must use the private key to digitally sign the message containing the request to send Bitcoin.[3] The Bitcoin network completes the transfer once the signature is verified by the public key. The verification process illustrates how possession of the private key allows for control of the corresponding address's funds. Moreover, security of the private key is critical to the use of cryptocurrency.

Interestingly, Kahn et al. (2020) study the degree of attention that is required for security of a private key. In particular, crypto owners store their private key in what is known as a wallet – wallets can be broadly placed in two categories. First, a hot wallet stores the private keys on a device that is connected to the internet. Holding the private keys in hot storage provides more convenience due to easier access, but this accessibility comes with a cost. Due to a connection to a network, the private keys are always at risk from an external web-based attack. In order to prevent this, crypto owners often use a second type of wallet. That is, Bitcoin owners store their private key on a hardware wallet offline in "cold storage".[4] However, this comes with the downside of requiring extra effort by the coin holder. Moreover, if the hardware wallet is lost, damaged or the passcode to the device is forgotten, access to the tokens is permanently lost.[5] The losses are far from trivial. In fact, recent estimates from Chainalysis[6] indicates that as of 2017, nearly 4 million bitcoins alone have been lost which is around one-quarter of the aggregate supply of existing bitcoins.[7] This aspect of many cryptocurrencies is typically omitted from models such as FSV and Martin and Schreft (2006) who study whether privately issued outside money would circulate over time. Consequently, failing to account for permanent coin loss may fundamentally alter the conditions where private money circulates. It is also likely to impact whether the supply of

[2]The private key is known as the signing key and is only known by the address owner. In contrast, the public key used for verification is made available to the Bitcoin network.

[3]A good analogy comes from the 80's film "The Scarlet Pimpernel". While his deeds are known, the identity of the hero is unknown to the public. In order to verify his communications, he signs his letters with a wax insignia shaped like a scarlet pimpernel.

[4]The hardware wallet is a type of flash drive that performs the function of a crypto wallet. For example, the Bitcoin wallet is responsible for generating the random private key that is a 256-bit number identified by 64 characters in the range 0-9 or A-F. The wallet then uses the public key, which is mathematically related to the private key, to create the public address.

[5]Due to the pseudoanomyity and the decentralized nature of crypto networks, it is not possible to go to a trusted third party and retrieve your private key or gain access to your money with an ID.

[6]Chainalysis is a crypto forensics company based in New York that will often assist Interpol and U.S. law agencies in tracking down cyber criminals. For a discussion on their relevance to current events, see "The rise of crypto laundries: how criminals cash out of bitcoin." (Murphy, Financial Times, May 28, 2021).

[7]For example, the CEO of the crypto exchange QuadrigaCX died and took with him any knowledge of the private keys to $190 million in several different types of cryptocurrency. In addition, Stefan Thomas, a German programmer based in San Francisco, forgot the password that unlocked his small hard drive, called the IronKey, that would allow him to access 7,002 bitcoin, which was worth $220 million. For additional discussion, see "Lost Passwords Lock Millionaires Out of Their Bitcoin." (Popper, New York Times, January 12, 2021).

private money over time would be socially efficient.

In light of this gap in the existing literature, the objective of this paper is to study how exogenous token loss affects the conditions where privately produced money circulates. To do so, we include the potential to lose tokens in the model of FVS. As in FVS, we are able to show how the circulation of private money depends on the shape of the cost function. Yet, in stark contrast to FVS, we show that a stable price equilibrium can exist even if the costs are strictly convex and equal to zero at the origin as new coins need to be produced in order to offset the amount of tokens that are lost over time. Moreover, we discuss how the relationship between the price of coins and the degree of token loss also depends on the shape of the cost function. To be specific, if the cost function is strictly convex, the price of tokens adjusts to the rate of token loss along with the equilibrium money stock. Under linear costs, the money stock entirely absorbs the degree of loss.

The remainder of the paper proceeds as follows. In the next section, we construct a model to show the effects of currency loss. In order to replicate the issue of crypto holders losing access to their private key, we introduce the potential to lose tokens in the model. In this context, we show that a stable-price equilibrium can exist with no cap on production of tokens. Next, we examine whether a stable price equilbrium can exist if there is a cap on token production. We proceed to conduct welfare analysis and then look to examine conditions where government money can displace privately produced outside money that is susceptible to token loss.

II. Model

There is a [0,1] set of infinitely-lived consumers who consume and produce goods at different points in discrete time. Further, individuals meet in both a centralized market (CM) and a decentralized market (DM). Consumers also have the ability to transform labor into a perishable good known as the CM good through the use of a linear technology. In addition to consumers, following FVS, there are also entrepreneurs (miners) who create tokens. In the first subperiod, both types of agents interact in the CM and consume the CM good.

In the second sub-period, consumers meet in pairs in the DM but the entrepreneurs are idle. During this time, consumers produce differentiated goods which are also divisible. Due to their specialized tastes and production capabilities, it will never be the case that two consumers would desire what the other produces. This friction creates a role for a medium of exchange. First, a consumer has the ability to produce a good for the other individual with probability $\sigma \in (0, 1/2)$ and will therefore be a seller. Second, there is also the probability $\sigma \in (0, 1/2)$ that he will be a buyer in a given match. Lastly, with probability $(1 - 2\sigma)$, neither individual would desire to trade.

By comparison, entrepreneurs have access to a technology that can create tokens. These tokens can come in either physical or digital form. Counterfeiting is not an issue with the tokens as they can be verified publicly at zero cost. Entrepreneurs create identical tokens, and bear the same costs of production $c : \mathbb{R}_+ \to \mathbb{R}_+$ for minting tokens. We refer to the entrepreneurs as miners when the tokens created are cryptocurrency. In the case of miners, the cost comes from the miners solving a complex computational problem that requires input. For example, the cryptocurrency will have a protocol that determines the amount of work required to solve the problem. To capture these costs, the cost function is strictly increasing and weakly convex: $c'(\Delta) > 0, c''(\Delta) \geq 0$, and $c(0) = 0$. The entrepreneurs will create these tokens to maximize profits which enable trade between buyers and sellers in the DM.

Let $x_t \in \mathbb{R}$ denote the consumer's net consumption of the CM good, and $q_t \in \mathbb{R}_+$ denote consumption of the DM good. In addition, $n_t \in \mathbb{R}_+$ reflects the effort to produce the DM good.

Thus, an individual consumer's preferences are denoted by

$$U(x_t, q_t) = x_t + u(q_t) - w(n_t).$$

Note that $u : \mathbb{R}_+ \to \mathbb{R}$ is continuously differentiable, increasing, and strictly concave: $u'(\cdot) > 0$, $u''(\cdot) < 0$, $u'(0) = \infty$, and $u(0) = 0$. Also, $w : \mathbb{R}_+ \to \mathbb{R}_+$ is continuously differentiable, increasing, and weakly convex: $w'(\cdot) > 0$, $w''(\cdot) \geq 0$, and $w(0) = 0$. With regards to $u(q)$ and $w(q)$, one of the inequalities of the second derivative must be strict. All consumers have the same discount factor $\beta \in (0, 1)$ between dates t and $t + 1$.

By comparison, $x_t^e \in \mathbb{R}_+$ denotes an entrepreneur's consumption of the CM good, and $\Delta_t \in \mathbb{R}_+$ is the production of tokens. The preferences of an entrepreneur are denoted by

$$U^e(x_t^e, \Delta_t) = x_t^e - c(\Delta_t)$$

Meetings in the DM are anonymous, precluding any chance of credit. This friction, along with the double coincidence of wants problem, makes a medium of exchange necessary to facilitate trade. Therefore, although a token is intrinsically worthless, it obtains its value from use as a medium of exchange.

Since the entrepreneurs' only concern is maximizing profits, their behavior can be predicted by other agents. This allows agents to form expectations about the future money supply and use this to determine the relative price level.

Consumers

The value function for the consumer in the CM is denoted by $W(M_{t-1}^c, t)$. The agent will start period t with $M_{t-1}^c \in \mathbb{R}_+$ in his portfolio. Further, $V(M_t^c, t)$ denotes the consumer's value function in the DM. The Bellman equation for the consumer in the CM is

$$W\big(M_{t-1}^c, t\big) = \max_{x_t, M_t^c} \big[x_t + V(M_t^c, t)\big]$$

subject to:

$$\phi_t \cdot M_t^c + x_t = \phi_t \cdot M_{t-1}^c$$

The budget constraint rearranges to:

$$x_t = \phi_t \cdot M_{t-1}^c - \phi_t \cdot M_t^c$$

Substituting into the Bellman Equation:

$$W\big(M_{t-1}^c, t\big) = \max_{M_t^c} \big\{\phi_t \cdot M_{t-1}^c - \phi_t \cdot M_t^c + V(M_t^c, t)\big\}$$

Next, $W(0, t)$ below represents the value function for the consumer at the end of the first subperiod. The agent will choose between the disutility from producing goods and acquiring tokens in the CM versus the value of tokens for use in the DM :

$$W(0, t) = \max_{M_t^c} \big[- \phi_t \cdot M_t^c + V\big(M_t^c, t\big)\big] \tag{1}$$

In contrast to FVS, we introduce the potential for consumers to lose tokens in the model. For example, this could be due to an individual losing access to their private key. The loss of the private key would occur in the DM before they match up with another consumer. Once in the DM, the tokens will be lost with a probability of $\psi \in (0,1)$. We also let $\overline{q}$ represent the anticipated amount of the consumption good to be traded in a match in the DM. In addition, $\overline{d}$ denotes the transfer of tokens to a seller.

Below we present the value function for a consumer at the beginning of the DM. First, with probability ψ, the individual loses his tokens. Further, with probability σ, the individual would like to be a buyer but does not have any tokens to give up in exchange. As a result, consumption will not occur and the individual will return to the CM in the following period. Moreover, with probability $\sigma\psi$, the consumer would have the ability to produce a good for a buyer but the buyer has also lost his tokens. In either scenario, the consumer will return to the CM empty-handed.

$$
\begin{aligned}
V(M_t^c, t) = \psi\big\{ & \underbrace{\sigma(u(0) + \beta W(0, t+1))}_{match \quad w/ \quad seller} + \underbrace{\sigma\psi[-w(0) + \beta W(0+0, t+1)]}_{potential \quad buyer \quad lost \quad currency} + \\
& \underbrace{\sigma(1-\psi)[-w(\overline{q}) + \beta W(0+\overline{d}, t+1)}_{successful \quad match \quad w/ \quad buyer} + \underbrace{(1-2\sigma)\beta W(0, t+1)}_{no \quad match} \big\} \\
+ (1-\psi)\big\{ & \underbrace{\sigma[u(q) + \beta W(M_t^c - d)]}_{match \quad w/ \quad seller} + \underbrace{\sigma\psi[-w(0) + \beta W(M_t^c + 0)]}_{potential \quad buyer \quad lost \quad currency} \\
& \underbrace{\sigma(1-\psi)[-w(\overline{q}) + \beta W(M_t^c + \overline{d})]}_{successful \quad match \quad w/ \quad buyer} + \underbrace{(1-2\sigma)\beta W(M_t^c, t+1)}_{no \quad match} \big\}
\end{aligned}
\tag{2}
$$

However, with probability $\sigma(1-\psi)$, the consumer produces a good for a buyer that has not lost their tokens. The consumer will take the tokens given in exchange for the DM goods produced into the next period. Lastly, with probability (1-2σ), the consumer will not be a buyer or seller in the DM. Thus, the consumer will not consume a DM good and would go to the next period without any tokens.

Alternatively, with a probability of $(1-\psi)$, the consumer does not lose his tokens. Conditional on his money holdings, with a probability of σ, the individual is a buyer and transfers his tokens over to the seller in exchange for the seller's DM good. As a consequence, consumption of the DM good occurs and the individual will not take any tokens into the next period. In addition, with probability $\sigma\psi$, the consumer is capable of producing a good for a buyer but the buyer has lost his tokens. As a result, the consumer will then enter the next period with only his tokens in hand.

With probability $\sigma(1-\psi)$, the consumer produces a good for a buyer in exchange for tokens. This results in the individual bringing his and the buyer's tokens into the following period. Lastly, with probability $(1-2\sigma)$, the consumer will not be a buyer or seller. As a result, consumption does not take place and the individual goes into the next period with his tokens.

Simplifying instances where no trade occurs produces the equation below. Notably, in situations where the individual loses his tokens, we can combine all the instances where no trade occurs. This results in zero utility for the consumer, and such possibilities in (2) drop out entirely. With a probabiliy of $(1-\sigma(1-\psi))$, no trade occurs in the DM. Therefore, no consumption occurs and the consumer enters the next period with no tokens.

$$V(M_t^c,t)=\psi\{\underbrace{\sigma(1-\psi)[-w(\overline{q})+\beta W(0+\overline{d},t+1)]}_{successful\quad match\quad w/\quad buyer}+\quad\underbrace{(1-\sigma(1-\psi))\beta W(0,t+1)}_{no\quad money\quad taken\quad to\quad next\quad period}\quad\}+$$

$$(1-\psi)\{\underbrace{\sigma[u(q)+\beta W(M_t^c-d)]}_{match\quad w/\quad seller}+ \tag{3}$$

$$\underbrace{\sigma(1-\psi)[-w(\overline{q})+\beta W(M_t^c+\overline{d},t+1)]}_{successful\quad match\quad w/\quad buyer}+\quad\underbrace{(1-\sigma(1+(1-\psi)))\beta W(M_t^c,t+1)}_{no\quad consumption,\quad takes\quad money\quad to\quad next\quad period}\quad\}$$

Thus, (2) simplifies to (3) above which only includes scenarios in which one of the consumers does not lose their tokens and trade occurs. Further, with the same probability of $\sigma(1-\psi)$, the consumer produces a good for the buyer and receives tokens from the buyer. As a result, the individual enters the next period with the buyer's tokens.

By comparison, we only eliminate the meetings where the potential buyer has no currency if the consumer does not lose his tokens. In this particular case, no production occurs and the consumer does not gain any tokens. Thus, he will head into the next period with his tokens only with a probability of (1-$\sigma(1+(1-\psi))$). Identically before simplification, with probability $\sigma(1-\psi)$, the consumer produces a good for a buyer in exchange for tokens. Additionally, with a probability of σ, the individual buys the DM good from a seller in exchange for his money holdings. Further, if $\psi=0$, one obtains the standard probability of $(1-2\sigma)$.

We use Nash bargaining to determine the terms of trade between the two consumers in the DM. We let $\theta\in[0,1]$ be the bargaining power of the consumer when he acts as a buyer. The terms of trade $(q,d)\in\mathbb{R}_+^2$ in the DM are determined by solving

$$\max_{(q,d)\in\mathbb{R}_+^2}\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big]^{\theta}\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]^{1-\theta} \tag{4}$$

subject to the participation constraint of each agent.

Next, we have the buyer's participation constraint:

$$u(q)-\beta\cdot\phi_{t+1}\cdot d\geq 0$$

And, the seller's constraint:

$$-w(q)+\beta\cdot\phi_{t+1}\cdot d\geq 0,$$

Finally, we have the buyer's liquidity constraint:

$$d\leq M_t^c,$$

The amount of production in the DM satisfies:

$$u'(q) = w'(q) \tag{5}$$

where q^* satisfies $u'(q^*) = w'(q^*)$, so that there is a socially efficient level of production in DM if the liquidity constraint does not bind. Next, we find d when the liquidity constraint is not binding:

$$(1-\theta)u(q^*) + \theta w(q^*) = \beta\phi_{t+1} \cdot d \tag{6}$$

That is, the discounted real value of the total tokens to be exchanged is a weighted average of the buyer's utility and the seller's disutility. If the buyer has more bargaining power, then the value of the tokens depends more on the disutility of the seller since they incur a loss of utility in production.

In summary, if the liquidity constraint does not bind, bargaining power does not affect the amount of production in the DM – it only affects the cost in terms of the value of the tokens exchanged.

Next, we can use the bargaining solution to express the value of money exchanged. The amount of production of the DM good will allow for the expression of money traded in terms of the buyer's utility and the seller's effort. $m : \mathbb{R}_+ \to \mathbb{R}_+$ represents the real value of money holdings. Set $m(q)$ equal to $\beta \cdot \phi_{t+1} \cdot d$, and you have:

$$m(q) \equiv \frac{\theta w(q)u'(q) + (1-\theta)u(q)w'(q)}{\theta u'(q) + (1-\theta)w'(q)}$$

We will let $\beta \cdot \phi \cdot M_0$ represent the real value of the consumer's portfolio in the steady state. When the liquidity constraint is binding, we will have $\beta \cdot \phi_{t+1} \cdot d_t = \beta \cdot \phi_{t+1} \cdot M_t^c$:

$$\beta\phi_{t+1}M_t^c = \frac{\theta w(q)u'(q) + (1-\theta)u(q)w'(q)}{\theta u'(q) + (1-\theta)w'(q)}$$

Thus, q can be obtained from the inverse function:

$$q = m^{-1}(\beta\phi_{t+1}M_t^c)$$

For the general case, the solution to the bargaining problem is given by:

$$q(M_t^c, t) = \begin{cases} m^{-1}(\beta \cdot \phi_{t+1} \cdot M_t^c) & if \\ \phi_{t+1} \cdot M_t^c < \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)] & \\ & \\ q* & if \\ \phi_{t+1} \cdot M_t^c \geq \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)] & \end{cases}$$

and:

$$\phi_{t+1} \cdot d(M_t^c, t) = \begin{cases} \phi_{t+1} \cdot M_t^c & if \\ \phi_{t+1} \cdot M_t^c < \beta^{-1}[\theta w(q*) + (1-\theta)u(q*)] & \\ & \\ \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)] & if \\ \phi_{t+1} \cdot M_t^c \geq \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)] & \end{cases}$$

Special Case. In order to simplify our analysis, consider a case where the buyer has all the bargaining power ($\theta = 1$) :

$$w(q^*) = \beta\phi_{t+1} \cdot d$$

Because the buyer has all of the bargaining power, he extracts all of the surplus from the transaction in the meeting. The buyer will only transfer enough tokens to just cover the effort from the seller.

In the case when d is binding:

$$\phi_{t+1} \cdot d = \phi_{t+1} M_t^c$$

If the buyer has full bargaining power:

$$m(q) \equiv w(q)$$

and so

$$w(q) = \beta\phi_{t+1} M_t^c$$

Upon solving to get the quantity of the DM good produced in terms of the real value of tokens:

$$\beta\phi_{t+1} M_t^c = w^{-1}(\beta\phi_{t+1} M_t^c) \tag{7}$$

We let q represent the amount of the DM good produced for the buyer. The seller will receive no surplus in this transaction. The seller's effort will be equivalent to the real value of tokens offered. Thus, the amount of the DM good produced by the seller is increasing in the real value of a token until the buyer's liquidity constraint no longer binds.

In the case where the buyer has all the bargaining power ($\theta = 1$), the solution to the bargaining problem for the general cost function becomes:

$$q(M_t^c, t) = \begin{cases} w^{-1}(\beta \cdot \phi_{t+1} \cdot M_t^c) & if \\ \phi_{t+1} \cdot M_t^c < \beta^{-1} w(q^*) & \\ & \\ q^* & if \\ \phi_{t+1} \cdot M_t^c \geq \beta^{-1} w(q^*) & \end{cases}$$

and

$$\phi_{t+1} \cdot d(M_t^c, t) = \begin{cases} \phi_{t+1} \cdot M_t^c & if \\ \phi_{t+1} \cdot M_t^c < \beta^{-1} w(q^*) & \\ & \\ \beta^{-1} w(q^*) & if \\ \phi_{t+1} \cdot M_t^c \geq \beta^{-1} w(q^*) & \end{cases}$$

The solution to the bargaining problem characterizes real expenditures in the DM, $\phi_{t+1} \cdot M_t^c$, as a function of the real value of buyer's portfolio.

Portfolio Choice

For the portfolio choice the producer will only need to consider the disutility from producing the CM good to acquire money balances, and the gains from trade when the tokens are not lost. We also include from the value function all the possibilities for the agent in the event his tokens are not lost. This will give the agent all the information he needs to determine the optimal amount of tokens to carry into the DM.

$$-\phi_t M_t^c + (1-\psi)\Big\{\sigma[u(q) + \beta W(M_t^c - d(M_t^c, t))] + \sigma[(1-\psi)(-w(\overline{q}) + \beta W(M_t^c + \overline{d}(M_t^c, t+1), t+1)$$
$$+\psi(-w(0) + \beta W(M_t^c + 0, t+1))] + (1-2\sigma)\beta W(M_t^c, t+1)\Big\}$$

We can substitute $\beta\phi_{t+1}M_t$ for $W(M_t^c, t+1)$ and simplify:

$$\underbrace{-\phi_t M_t^c}_{value\ \ foregone\ \ in\ \ CM} + \underbrace{\sigma(1-\psi)[u(q) - \beta\phi_{t+1}d]}_{(utility\ -\ money\ \ transfer)\ \ w/\ \ match} + \underbrace{(1-\psi)\beta\phi_{t+1}M_t^c}_{value\ \ taken\ \ to\ \ next\ \ period} \tag{8}$$

The consumer will maximize utility based on equation (8). First, the agent considers the disutility required to carry tokens out of the CM. Next, the agent takes into account the meetings with agents who produce a good for him. This will only occur if the consumer does not lose his tokens. Thus, with a probability of $\sigma(1-\psi)$ the consumer will use his tokens to purchase goods from another agent. Lastly, the consumer will consider the value of tokens taken into the CM in the next period. This only occurs if the consumer does not lose his tokens with a probability of $(1-\psi)$.

The first-order condition for money balances is:

$$-\phi_t + (1-\psi)\Big\{\sigma(u'(q)\frac{\partial q_t}{\partial M_t^c} - \beta\phi_{t+1}) + \beta\phi_{t+1}\Big\} = 0$$

We let $A = \phi_{t+1} \cdot M_t^c$ and substitute into the first-order condition along with $\frac{\partial q(M_t^c, t)}{\partial M_t^c} = \frac{\beta\phi_{t+1}}{m'(q(M_t^c, t))}$ to get:

$$\phi_t = \beta\phi_{t+1}\Big(\sigma(1-\psi)\frac{u'(m^{-1}(\beta A))}{m'(m^{-1}(\beta A))} + (1-\sigma)(1-\psi)\Big)$$

If the buyer's liquidity constraint no longer binds, $\sigma(1-\psi)[u(q)-\beta\phi_{t+1}d]$ remains constant with any change in M_t^c. The first-order condition for money balances will now become:

$$\phi_t = \beta\phi_{t+1}(1-\psi)$$

Thus, the optimal choice satisfies:

$$\phi_t = \beta\phi_{t+1}L_\theta(\phi_{t+1}\cdot M_t^c).$$

We can define $\gamma_{t+1} = \frac{\phi_{t+1}}{\phi_t}$ and express in terms of the rate of return

$$1 = \beta\gamma_{t+1}L_\theta(\gamma_{t+1}\phi_t M_t^c)$$

along with the transversality condition

$$\lim_{t\to\infty}\beta^t\cdot\phi_t\cdot M_t^c$$

where $L_\theta : \mathbb{R}_+ \to \mathbb{R}_+$ is given by:

$$L_\theta(A) = \begin{cases} \sigma(1-\psi)\frac{u'(m^{-1}(\beta A))}{m'(m^{-1}(\beta A))} + (1-\sigma)(1-\psi) & if\ A < \beta^{-1}\left(\theta w(q^*) + (1-\theta)u(q^*)\right) \\ 1-\psi & if\ A \geq \beta^{-1}\left(\theta w(q^*) + (1-\theta)u(q^*)\right) \end{cases}$$

This function represents the marginal benefit of taking additional tokens into the DM. The term $\sigma(1-\psi)\frac{u'(m^{-1}(\beta A))}{m'(m^{-1}(\beta A))}$ represents the utility from consuming the DM good produced by an agent in the DM. This will occur if the liquidity constraint does not bind. If it does bind, no more DM goods will be purchased with an increase in tokens brought to the DM. The only value the additional tokens will have is in the CM next period. This will of course be affected by the probability of loss of currency (ψ). The greater the chance of currency loss, the lower the benefit of taking tokens in the DM. Without the currency, the agent will not have the ability to purchase a DM good and will lose any potential value of holding tokens in the next period.

We will now solve for the portfolio problem for our previous special case. In turn, this allows us to solve for a special case with functional forms. We substitute $\frac{u'(m^{-1}(\beta A))}{m'(m^{-1}(\beta A))} = \frac{u'(w^{-1}(\beta A))}{w'(w^{-1}(\beta A))}$ and $L_1 : \mathbb{R}_+ \to \mathbb{R}_+$ is given by:

$$L_1(A) = \begin{cases} \sigma(1-\psi)\frac{u'(w^{-1}(\beta A))}{w'(w^{-1}(\beta A))} + (1-\sigma)(1-\psi) & if\ A < \beta^{-1}w(q^*) \\ 1-\psi & if\ A \geq \beta^{-1}w(q^*) \end{cases}$$

We continue with the assumption the buyer has all the bargaining power. In addition, let's say the utility from consumption can be defined as $u(q) = 2q^{1/2}$, and $w(q) = q$ represents the cost of producing DM goods. We solve and the special case with functional forms $L_1 : \mathbb{R}_+ \to \mathbb{R}_+$ is given by:

$$L_1(\phi_{t+1}M_t^c) = \begin{cases} \sigma(1-\psi)\frac{1}{\sqrt{\beta\phi_{t+1}M_t^c}} + (1-\sigma)(1-\psi) & if\ \phi_{t+1}M_t^c < \beta^{-1}w(q^*) \\ 1-\psi & if\ \phi_{t+1}M_t^c \geq \beta^{-1}w(q^*) \end{cases}$$

With our functional forms, it becomes obvious that the liquidity benefit from carrying money into the DM decreases in real money holdings.

Entrepreneur's Problem

We now turn our focus to the supply of tokens in the economy. With no central bank, entrepreneurs determine the quantity of money in the economy. For the entrepreneur's problem, we first denote $M_t \in \mathbb{R}_+$ as the per capita supply of currency in period t. Next, we denote $\Delta_t \in \mathbb{R}$ as the entrepreneur's net circulation of newly minted tokens in period t (mined if new cryptocurrency). Along with the probability of currency loss ψ, we can now denote the law of motion for the total amount of tokens at the beginning of period t by

$$M_t = \Delta_t + M_{t-1} - \psi M_{t-1},$$

The term ψM_{t-1} represent the currency loss from the DM. We denote the entrepreneur's money holdings with $M_t^e \in \mathbb{R}_+$. As long as $\Delta_t \geq 0$, then the the entrepreneur's budget constraint can be shown as:

$$x_t + \phi_t M_t^e = \phi_t \Delta_t + \phi_t M_{t-1}^e \quad \forall t \geq 0$$

Recall that the entrepreneur only consumes the CM good and will not participate in the DM. So unless $\beta(1-\psi)\phi_{t+1} \geq \phi_t$, the entrepreneur will choose not to hold currency across time periods. Consequently, $M_t^e = M_{t+1}^e = 0$, and the budget constraint can be rewritten as

$$x_t = \phi_t \Delta_t$$

The entrepreneur will consume an amount of the CM good equal to the amount of new tokens created. Since $x_t \geq 0$, our previous assumption $\Delta_t \geq 0$ must be true.

Entrepreneurs take the price of tokens as given. We have $\Delta_t^* \in \mathbb{R}_+$ as the solution to the profit maximization problem of an entrepreneur is given by

$$\Delta_t^* \in arg \max_{\Delta \in \mathbb{R}_+} \big[\phi_t \Delta - c(\Delta)\big].$$

The amount of new token creation will adjust accordingly to any price change of tokens. Therefore, the solution to the entrepreneur's profit maximization problem implies:

$$M_t = \Delta_t^* + (1-\psi)M_{t-1} \quad \forall t \geq 0.$$

Importantly, there are two factors that determine the change of the money stock from one period to the next. In the process of maximizing profits, the entrepreneurs will add to the money stock. In

addition, any tokens misplaced will be lost permanently from the money stock each period. The equation highlights an important distinction between currency loss and theft. In particular, theft will cause the consumer to lose access to his tokens, but not remove tokens from the money supply.[8]

III. Equilibrium

The market-clearing condition for money is

$$M_t = M_t^c + M_t^e, \quad \forall t$$

As shown earlier, $M_t^e = 0$ and the market-clearing condition becomes

$$M_t = M_t^c$$

We now move to define a monetary equilibrium in our framework

Definition 1: *A perfect-foresight monetary equilibrium is an array* $\{M_t, M_t^c, \Delta_t^*, \phi_t\}_{t=0}^{\infty}$ *satisfying the following conditions at all dates* $t \geq 0$.

5 Conditions for Equilibrium

i. Money Demand for DM

$$\phi_t = \beta \phi_{t+1} L_\theta(\phi_{t+1} \cdot M_t^c) \tag{9}$$

ii. Transversality Condition

$$\lim_{t \to \infty} \beta^t (\phi_t \cdot M_t^c) = 0 \tag{10}$$

iii. Profit Maximization for Entrepreneur

$$\Delta_t^* \in arg \max_{\Delta_t \in \mathbb{R}_+} \left[\phi_t \Delta_t - c(\Delta_t)\right] \tag{11}$$

iv. Law of Motion for Currency Creation

$$M_t = \Delta_t^* + (1 - \psi) M_{t-1}, \quad \forall t \geq 0. \tag{12}$$

v. Money Market Clearing Condition

$$M_t = M_t^c. \tag{13}$$

Our analysis begins with entrepreneurs having a strictly convex cost function. The first proposition shows conditions with price stability:

Proposition 1: *Suppose that* $\psi > 0$ *and buyers have all the bargaining power, (*$\theta = 1$*). In addition, consider the following functions for utility from consumption,* $u(q) = 2q^{\frac{1}{2}}$*, the cost of producing DM goods* $w(q) = q$*, and the costs of producing new tokens* $c(\Delta) = \Delta^2$*. Under these conditions, there exists a steady state price* $\overline{\phi} = \frac{\sigma(1-\psi)\sqrt{2\beta\psi}}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))}$*. At the steady-state price, entrepreneurs will maintain a steady state level of tokens* $\overline{M} = \frac{\sqrt{\beta}\sigma(1-\psi)}{\sqrt{2\psi}(1-\beta(1-\psi)+\beta\sigma(1-\psi))}$*. The steady-state price of*

[8] He et al. (2008) introduce theft in model to highlight the security properties of banking. Thieves steal money from the honest agents in order to spend money in the following CM. While this affects the value of money and production, the stock of money remains unchanged.

tokens is decreasing in the rate of currency loss, and increasing in the probability of a successful trade. Finally, the steady-state money supply is decreasing in the rate of currency loss, and increasing in the likelihood of a successful trade.

The results show that a steady-state monetary equilibrium with a stable price is possible with a strictly convex cost function for entrepreneurs, $c(\Delta) = \Delta^2$. The proposition also shows the effect of currency loss on production of new tokens in the steady-state. In particular, the steady-state money supply $\overline{M}$ is decreasing in the rate of currency loss ψ. The increase in loss of tokens will directly lower the money supply. In addition, the steady-state price of tokens is decreasing in the rate of currency loss. As tokens get their value from their purchasing power in the decentralized market, consumers make purchases less often in the decentralized market when the rate of currency loss is higher. As a result, the tokens will be worth less to the consumer. Moreover, this also indirectly lowers the steady-state money supply since entrepreneurs would have reduced incentives to produce additional tokens if the price of tokens is lower.

In addition, the proposition shows the effect of a higher matching rate in the decentralized market. Notably, the steady-state price $\overline{\phi}$ is increasing in the probability of a successful trade (σ) in the decentralized market. As mentioned in the previous paragraph, tokens derive their value from use in trade for goods in the decentralized market. As a result, the tokens gain value due to the increased chance of trade. Moreover, this leads to the steady-state money supply $\overline{M}$ increasing in successful trades. The higher price provides additional incentives for entrepreneurs to produce new tokens.

In light of the results presented in our Propostion 1, we would like to compare how our results stand in relationship to previous work. First, in stark contrast to our analysis, FVS argue that a stable price equilibrium does not generally exist when the costs of producing new tokens is strictly convex. In particular, the marginal cost of producing tokens is zero at production of zero tokens. Thus, entrepreneurs will continue to produce new tokens as long as the price of tokens is not zero — in turn, consumers expect entrepreneurs to produce new tokens until prices are driven to zero.

In fact, in order to generate a stable price equilibrium, FVS require that a hard cap is placed on token production at a future date. Since consumers believe that token production will eventually cease, a stable price equilibrium is possible. In contrast, we show that such caps are not required — as token loss occurs over time, new tokens need to be produced so that *the supply of tokens will remain constant & prices are stable.* In comparison to FVS where the price of tokens converges monotonically to zero, the introduction of token loss leads to the currency converging to a positive price. As a result, this helps the cryptocurrency to avoid self-fulfilling inflationary episodes.

Martin & Schreft were also able to establish the existence of an equilibrium for a privately-issued currency. The authors use a mechanism that is similar to the one used by FVS. In their model, Martin & Schreft instill agents with a belief that any money minted after a specified threshold number will be worthless. Therefore, once the number of units of money has reached the threshold, agents will have no incentive to mint new currency. In both models, agents have reason to believe that money creation will not be unbounded. As a result, conditions for an equilibrium do exist.

Our results have particular importance for cryptocurrencies without an algorithm that places a limit on total token production. Notably, Dogecoin, Monero, and Ethereum are all cryptocurrencies without limitations on total production. Consequently, token loss increases the potential for stability of cryptocurrencies. Moreover, the results also pertain to cryptocurrency with a cap at a finite date.

Instead of a date in the future, the cryptocurrency would automatically converge to a stable price.

We now look to establish that a steady-state is also consistent with a linear cost function for entrepreneurs.

Proposition 2: *Suppose consumers have the same utility functions from the previous proposition but $c(\Delta) = c_0\Delta$ represents the cost of producing tokens for entrepreneurs. Then there exists a steady-state price $\overline{\phi} = c_0$ and steady-state money supply $\overline{M} = \frac{1}{c_0}\frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$.*

The steady-state price when the entrepreneur has a linear cost function does not adjust with changes in the rate of currency loss. Therefore, the steady-state money supply is more sensitive to a change in the rate of currency loss with a lower c_0. In equilibrium, a higher priced cryptocurrency will have a higher cost c_0 to produce than a lower priced cryptocurrency. As a result of the higher price, it takes less of a decrease in token supply to meet the lower demand for real money balances caused by the increase in currency loss.

Consequently at lower prices, the steady-state money supply of a cryptocurrency with a linear cost function for entrepreneurs is more sensitive to a change in the rate of currency loss than a cryptocurrency with a strictly convex cost function. However, at higher prices the cryptocurrency with a strictly convex cost function requires larger adjustments to maintain the steady-state level of the money supply than a cryptocurrency with a linear cost function.

Finite Supply of Tokens

Up until this point, miners face no constraint on minting new currency. However, in the case of most cryptocurrencies, the protocol sets an upper limit on token creation. For example, due to the Bitcoin algorithm, mining of new Bitcoins will stop in 2140 after 21 million have been created. Similar to Bitcoin, we consider a cap on the amount of cryptocurrency that can be mined at each date. In addition, miners cannot create any new tokens past a certain date. Let $\overline{\Delta}_t \in \mathbb{R}_+$ denote the date-t cap on cryptocurrency.

The entrepreneur's profit maximization problem can be shown as

$$\Delta_t^* \in arg \max_{0\leq\Delta\leq\overline{\Delta}_t} [\phi_t\Delta - c(\Delta)].$$

Now, with the new constraints, we prove that a steady-state does not exist regardless of the cost function.

Proposition 3 *Suppose there is a set of caps $\{\overline{\Delta}_{t=0}^{\infty}\}$ on token creation. These caps are such that $\overline{\Delta}_t > 0$ at dates $0 \leq t \leq T$ and $\overline{\Delta}_t = 0$ at all subsequent dates $t \geq T+1$, given a finite date $T > 0$. A stable price steady-state does not exist under this set of conditions as long as $\psi > 0$.*

In contrast to FVS, a stable price equilibrium is not possible when cryptocurrency production is capped. This would preclude a stable price for a lot of cryptocurrencies. Bitcoin, Litecoin and Bitcoin cash all have a hard cap as part of their protocol. Once tokens are no longer created, the token loss would introduce deflationary pressure that makes a stable price impossible. That is, price stability would only be possible if token loss $\psi = 0$. While there is a lot of effort being put into developing technology to better secure private keys, there will always be a possibility of losing

access to tokens.

This highlights a big issues for money provided privately. During some periods a deflationary path for money may be appropriate, but other times it could be extremely harmful. For instance, during the financial crisis in 2008, the increase in demand for money called for an increase in growth of the money supply. A shrinking money supply would have extended the time necessary for the economy to recover.

Corrollary 1. *If the government issues money, a stable price equilibrium is possible for a cryptocurrency with a cap on total production.*

With a central bank money, it is possible to get the same results as the economy without currency loss. The government could declare their digital currency must be accepted on par with the cryptocurrency. Define $\Delta^g \in \mathbb{R}_+$ as the real value of government token production and $M^{+g} \in \mathbb{R}_+$ as the real value of private plus government money. With a government digital money susceptible to loss, the central bank can follow a simple rule to maintain a stable price. The rule for the the government can be defined by

$$\Delta_t^g = \omega M_{t-1}^{+g}, \quad \forall t > T$$

with the money growth rate $\omega = \psi$. This would allow the number of tokens to remain constant, and the proposition would be valid.

However, a different rule will need to be followed for a government issued digital currency held directly with the central bank. Token holders would lose their anonymity, but would no longer deal with the issue of token loss. With no token loss with government money's, the growth rate of money would no longer be one for one with the rate of token loss. Starting with the time period after the cap, the growth rate can be defined by

$$\Sigma_{t=1}^{\infty} \omega_t = \Sigma_{t=1}^{\infty} \psi \cdot (1-\psi)^{T+t-1}.$$

As the government fraction of the total money stock grows, the percentage of tokens that needs replacing shrinks.

IV. Welfare Properties

Following the welfare analysis in FVS, there is a strictly positive amount of tokens in the initial period. This is done to allow for record-keeping without having the government engage in the costly process of minting tokens. A solution to the social planner's problem is characterized by the surplus maximizing quantity q^* in the DM. With the ability to implement lump-sum taxes in the CM, Rocheteau (2012) shows that a social planner can achieve the efficient level of production in the DM by removing tokens in the DM. After the initial date, the economy will be in the first-best allocation since there will be no more costs for token production.

In order to simplify the analysis, we continue to impose that buyers are able to make take-it-or-leave-it offers to sellers. This will eliminate the inefficiencies associated with the hold-up problem, and allow the focus to be on issues related to token loss.

Recall the definition of money demand from the proof of proposition 1

$$z(\gamma) \equiv \frac{1}{\gamma} L_1^{-1}\left(\frac{1}{\beta\gamma}\right).$$

Real money demand is defined as a function of the real return on currency. Due to consumer preferences, $\frac{u'(q_t)}{w'(q_t)}$ is strictly decreasing in q_t. We assume preferences that imply the demand for real balances decreases in the inflation rate. As a result, $z_1 : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly increasing.

In this equilibrium, the quantity traded in the DM $\hat{q}$ satisfies

$$\sigma(1-\psi)\frac{u'(\hat{q_{cl}})}{w'(\hat{q_{cl}})} + 1 - \sigma(1-\psi) - \psi = \frac{1}{\beta},$$

We know production with the stable price equilibrium is below the socially efficient quantity of $q*$. A comparison can now be made to an environment without token loss. Here, we can contrast production in the DM to the FVS model with a cap on total production. In order to represent the FVS model, assume $\psi = 0$ due to the lack of token loss.

Proposition 4: *Suppose we have 2 economies with an equilibrium with a stable price. Now, suppose for both economies buyers have the same bargaining power, ($\theta = \hat{\theta}$). In addition for both economies, consider the following functions for utility from consumption, $u(q) = \hat{u(q)}$, the cost of producing DM goods $w(q) = \hat{w(q)}$, and the costs of producing new tokens $c(\Delta) = \hat{c(\Delta)}$. One economy has currency loss while the other has none. If we let $\sigma = \hat{\sigma}$ and $\beta = \hat{\beta}$ for both economies and $\psi > 0$ for the economy that has currency loss, the DM good production with a stable price equilibrium is less than an economy without currency loss, $\hat{q_{cl}} < \hat{q}$.*

With a digital currency suffering token loss, there will be less allocation of the DM good in comparison to the FVS model. The intuition behind this is self-evident. Agents take into account the possiblity of losing money in the DM and as a result are less willing to carry money into the DM. This lowers the tokens worth in exchange and as a store of value. In addition, there will be less tokens available for trade due to agents misplacing tokens. Both of these factors lead to decrease in production in the decentralized market. Furthermore, the result illustrates the impact on welfare from this feature of a private digital currency. Next, we look at another feature of digital currency that impacts this result.

Cap on each Period's Token Production

As mentioned previously, Bitcoin and most cryptocurrencies have an algorithm that places an upper bound on total token creation. In addition, the algorithm adjusts mining difficulty to maintain a determinant trend in the long run. In the short run, once the algorithm adjusts, the production of tokens is guided by profit and loss. In order to emulate this, we will introduce a cap on each period's production $\overline{\Delta}_t = \alpha M_t$ for all $t \geq 0$.

In equilibrium, a necessary condition for efficiency is to have the real rate of return on money equal to the rate of time preference. This usually ensures that there is no opportunity cost of holding money balances in the DM. Since this involves a strictly positive real return on money in equilibrium, it cannot normally be achieved with purely private token creation. However, with an algorithm limiting each periods token production, we can show a positive real return for private

currency that suffers loss in a steady state.

Proposition 5: *Suppose that $\psi > 0$ and there is a set of caps $\{\overline{\Delta}_{t=0}^{\infty}\}$ on token creation. These caps are such that $\overline{\Delta}_t \in (0, \psi\overline{M})$ for all $t \geq 0$. Then there exists a stationary monetary equilibrium with a strictly positive real return on money.*

With a positive real return on currency, the price of tokens will rise to a level that induces entrepreneurs to produce more tokens than are lost. At this point, it becomes unsustainable for tokens to continue to increase in value permanently. The maximum demand for money will be met and tokens must be removed to enable market clearing. In order to prevent this, a cap must be in place to prevent entrepreneurs from increasing the level of token production. Moreover, the cap must be set to a level lower than the amount of tokens misplaced each period. Otherwise, the economy converges to a stable price steady state.

In comparison to FVS, a purely private arrangement can provide a positive real return on money. This holds for FVS even after a finite date where currency production no longer occurs. Without currency loss, the money stock will remain constant at this point. However, while currency loss does make a positive return possible, this is not enough to get efficient production in the DM. Normally, a currency with a rate of return equal to time preference provides efficiency in the DM. However, there will still be a cost to holding money with $\gamma = \frac{1}{\beta}$. The potential to lose currency makes it costly to hold money at this rate of return. Recall the money demand function

$$\phi_t = \beta\phi_{t+1}\Big(\sigma(1-\psi)\frac{u'(m^{-1}(\beta A))}{w'(m^{-1}(\beta A))} + (1-\sigma)(1-\psi)\Big)$$

To get efficient production we must have $u^{'}(q^*) = w^{'}(q^*)$. This will give us

$$\phi_t = \beta\phi_{t+1}\Big(\sigma(1-\psi)\frac{1}{1} + (1-\sigma)(1-\psi)\Big)$$
$$\phi_t = \beta\phi_{t+1}(1-\psi)$$
$$\frac{1}{\beta(1-\psi)} = \frac{\phi_{t+1}}{\phi_t} = \gamma_{t+1}.$$

Thus, efficient production in the DM is only possible with a return $\gamma_{t+1} = \frac{1}{\beta(1-\psi)}$. This illustrates how the Friedman rule, $\gamma = \frac{1}{\beta}$, will not obtain the efficient allocation. Similar to results in He et al., the consumer takes into account the potential to lose access to their currency. As a result, the return on currency needs to compensate for that loss in order to achieve the optimal allocation.

Proposition 6: *There is no purely private arrangement that can deliver optimal production in the DM.*

Similar to FVS, entrepreneurs would need to take tokens out of circulation for a steady state with efficient production to be possible. This is not possible since it is not consistent with profit seeking behavior. Even after the upper bound on token creation has been reached, a private currency cannot maximize the surplus in the DM. A state actor needs to step in and remove tokens from circulation.

Let's say the government implements a lump sum tax $\tau \geq 0$ in the CM on consumers. Due to linear costs in the CM, the tax will be neutral and not lead to distributional effects. With the government taxing money out of the money supply, there will be an increase in the return of money. With an increase in the real value of tokens, entrepreneurs have an incentive to create more tokens each period. However, with a cap on token production, entrepreneurs will face an upper bound on token production.

Proposition 7: *With a cap on token production each period $\overline{\Delta} = \alpha M$, there can be an efficient return with a tax $\tau = (\alpha + (1-\beta)(1-\psi))M_t$.*

In this case, a shrinking money supply that achieves an efficient return is still socially wastful. The economy would still incur welfare loss each period in the CM. The loss comes from the cost of producing tokens as compared to a central bank creating money at almost no cost. The welfare loss from Bitcoin mining bears a resemblance to the extraction of gold under the gold standard. Milton Friedman (1951) estimated the resource costs associated with running a gold standard were around one and half percent of national income. This would have been about half of the increase in income each year. [9] Current estimates of Bitcoin mining put the cost around $1.2 billion annually. Even the upper bound on token creation from Bitcoin's algorithm cannot address this issue. After all the tokens are created, the miner's activity is still necessary for the network to remain active. Instead of a reward of new Bitcoin and transaction fees, the miners receive transaction fees only.

Another factor to consider is the negative externality from Bitcoin mining energy usage. Vries (2018) estimates the Bitcoin network consumes around 2.55 gigawatts of electricity, and could eventually consume 7.67 gigawatts. This would put Bitcoin's energy use in the range of developed nations such as Austria (8.2 gigawatts).[10] Currently, the limited number of transactions on the network make this a poor substitute for most fiat regimes.

V. Monetary Policy

We now examine the proper role for monetary policy in the presence of privately-issued currencies. We now extend to the government the ability to introduce its own brand of currency. Recall, that an efficient equilibrium is not possible with an economy with a purely private arrangement. The authors investigate if is possible to achieve a socially optimal outcome with the introduction of government money and monetary policy.

The government creates a brand of tokens that is referred to as currency g, and we will refer to tokens created by entrepreneurs as currency p. The government budget constraint becomes

$$\phi_t^g \Delta_t^g + \tau_t = c(\Delta_t^g), \tag{14}$$

where $\tau_t \in \mathbb{R}$ is the real value of lump-sum taxes, $\phi_t^g \in \mathbb{R}_+$ is the real value of government-issued currency, and $\Delta_t^g \in \mathbb{R}$ is the amount of the government brand issued at date t.

Two features set the government issuer apart from its private counterpart. First, the ability to tax consumers and withdraw money from circulation. We demonstrate this in corollary 1 and proposition 8. We will now focus on the other property that differentiates government tokens. That

[9] Allan Meltzer (1983) did a more recent estimate with the current income money ratio and it was lower. Yet, it would still amount to 16% of the increase in income per year.

[10] In an attempt to put this in perspective, Saad Imran (2018) makes the point that Bitcoin mining uses around 2.22% of the electricity of the world's data centers.

is, similar to the second part of corollary 1, the government could issue a digital currency that is held directly at the Federal Reserve. This type of currency would not suffer from token loss that occurs from a decentralized ledger. Thus, the law of motion for government money is given by

$$\overline{M}_t^g = \Delta_t^g + \overline{M}_{t-1}^g \tag{15}$$

at all dates, given an initial condition $M_{-1}^g \in \mathbb{R}_+$.

Definition 2. *A perfect-foresight monetary equilibrium is an array* $\{M_t, M_t^c, \phi_t, \phi_t^g, \Delta_t^*, \Delta_t^{*,g}, \tau_t\}_{t=0}^{\infty}$ *satisfying (9)-(15) at all dates* $t \geq 0$.

Unlike FVS, consumers will consider the private money inferior due to token loss. For an equilibrium, the government money would have a lower rate of return then the private money in the economy. We can define the government return on money $\gamma_{t+1} = \frac{\phi_{t+1}^g}{\phi_t^g}$ and find equilibrium conditions for it to be valued.

Proposition 8: *Suppose* $\psi = 0$ *for money issued by the government* M^g*. The condition* $\gamma_t^p = \frac{\gamma_t^g}{(1-\psi)}$ *must hold in order for both currencies to be valued in equilibrium.*

Agents will take into account the possibility of losing private tokens in their decision for money holdings. As a result, the return on the private digital currency must compensate for this possibility. With $\gamma_t^g = (1-\psi)\gamma_t^p$, the government digital currency allows for the same level of consumption in the DM. This leads us to the following corollary.

Corollary 2. *With a government rule that ensures* $\gamma_t^g > (1-\psi)\gamma_t^p$*, there is no equilibrium where agents value private money.*

The government can drive out private money by guaranteeing a return lower than private money. Agents will consider the fact government money is not susceptible to loss and adjust accordingly. As long as government compensates for the expected token loss, agents will prefer to hold the government issued tokens. In FVS, agents do not naturally discriminate between government and private money. As a result, the government must peg the real value of government money to a high enough level to drive out private money. Entrepreneurs will not shrink their supply of currency to match the positive return of government money. This will drive private money out as agents prefer the money with a higher return. In contrast, with the addition of token loss to private currency, agents will naturally discriminate and prefer government money as long as the return compensates for token loss.

FVS point out how a private currency can help discipline the central bank by ensuring that it provides a good money. With the addition of token loss, the government will have more room for discretion. As the private money will be discriminated against due to the token loss arising from its security properties. This does allow the government more flexibility in dealing with economic downturns, but still provides an incentive to keep inflation under control. However, there is a caveat to go along with this result. Namely, we ignore the benefits of anonymity that a private digital currency can provide.

Conclusion

In recent years, there has been increased enthusiasm regarding the viability of cryptocurrencies. Consequently, an academic literature studying cryptocurrency has also emerged. In terms of thinking about the viability of cryptocurrency, there has also been increasing awareness of the costs of producing such forms of money. In this sense, the costs of producing digitally issued money can be significantly higher than pieces of paper issued by sovereign governments. Yet, in addition to the relatively unique features of the costs of producing digital money, cryptocurrencies are also embedded with unique security features. Notably, a unique feature of cryptocurrency is that such forms of private outside money are based on cryptography — holders of coins store their currencies such as Bitcoin at an address on a decentralized ledger that is linked to both a private and public key. If a private key is lost or damaged, the coins are permanently missing. This aspect of many cryptocurrencies is typically omitted from previous that study whether privately issued outside money would circulate over time. Consequently, failing to account for permanent coin loss may fundamentally alter the conditions where private money circulates. It is also likely to impact whether the supply of private money over time would be socially efficient. In light of this gap in the existing literature, the objective of this paper is to study how exogenous token loss affects the conditions where privately produced money circulates. In particular, we discuss how the relationship between the price of coins and the degree of token loss also depends on the shape of the cost function.

References

[1] Fernandez-Villaverde, Jesus and Sanches, Daniel, 2019. Can Currency Competition Work? Journal of Monetary Economics, 106 1–15

[2] Friedman, M., 1951. Commodity-Reserve Currency. Journal of Political Economy Vol. 59, No. 3 , pp. 203-232

[3] Hayek, F. , 1999. The denationalization of money: an analysis of the theory and practice of concurrent currencies. In: Kresge, S. (Ed.), The Collected Works of F.A. Hayek, Good Money, Part 2. The University of Chicago Press .

[4] Imran, S., 2018. The Positive Externalities of Bitcoin Mining. Node Blockchain

[5] Kahn, C. M., F. Rivadeneyra, and T.-N. Wong (2020). Eggs in One Basket: Security and Convenience of Digital Currencies, Bank of Canada Staff Working Paper (2021-6)

[6] Lagos, R. and Wright, R., 2005. A Unified Framework for Monetary Theory and Policy Analysis. Journal of Political Economy Vol. 113, No. 3, pp. 463-484

[7] R. Lagos, G. Rocheteau, 2005. Inflation, output and welfare. International Economic Review 46 495–522.

[8] Martin, A. , Schreft, S.L. , 2006. Currency competition: a partial vindication of Hayek. Journal of Monetary Economics 53 (8), 2085–2111 .

[9] Meltzer A., 1983. Monetary Reform in an Uncertain Environment. Cato Journal, vol. 3, No. 1, pp. 93-112

[10] He, P., Huang, L and Wright, Randall, 2008. Money, Banking and Monetary Policy. Journal of Monetary Economics, 55(2008) 1013-1024

[11] Rocheteau, G. , 2012. The cost of inflation: a mechanism design approach. J. Econ. Theory 147 (3), 1261–1279

[12] Vries, A., 2018. Bitcoin's Growing Energy Problem. Joule , vol. 2, issue 5, pp. 801-805

Appendix

Nash Bargaining over a trade between Consumers in a DM meetup:

Next, we have the FOC for q :

$$\theta\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big]^{\theta-1}\big[u'(q)\big]\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]^{1-\theta}+$$
$$\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big]^{\theta}\big(1-\theta\big)\big[-w(q)+\beta\cdot\phi^{1}_{t+1}\cdot d\big]^{-\theta}(-w'(q))=0,$$

$$\theta\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big]^{\theta-1}\big[u'(q)\big]\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]^{1-\theta}=$$

$$\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big]^{\theta}\big(1-\theta\big)\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]^{-\theta}(w'(q))$$

$$\theta\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big]^{-1}\cdot u'(q)\cdot\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]=(1-\theta)w'(q)$$

$$\theta u'(q)\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]=(1-\theta)w'(q)\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big] \tag{16}$$

Next, we determine the first-order condition for d :

$$\theta\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big]^{\theta-1}\big[-\beta\phi_{t+1}\big]\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]^{1-\theta}+$$
$$\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big]^{\theta}\big(1-\theta\big)\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]^{-\theta}\cdot(\beta\phi_{t+1})=0,$$

$$\theta\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big]^{-1}\cdot\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]=(1-\theta)$$

$$\theta\big[-w(q)+\beta\cdot\phi_{t+1}\cdot d\big]=(1-\theta)\big[u(q)-\beta\cdot\phi_{t+1}\cdot d\big] \tag{17}$$

$$[-w(q)+\beta\cdot\phi_{t+1}\cdot d]=\frac{(1-\theta)}{\theta}[u(q)-\beta\cdot\phi_{t+1}\cdot d] \tag{18}$$

We can now substitute from (18) into (16) to find q^* when the liquidity constraint is not binding:

$$\theta u'(q)[-w(q)+\beta\cdot\phi_{t+1}\cdot d]=(1-\theta)w'(q)[u(q)-\beta\cdot\phi_{t+1}\cdot d]$$

$$\theta u'(q)\frac{(1-\theta)}{\theta}\left[u(q)-\beta\cdot\phi_{t+1}\cdot d\right]=(1-\theta)w'(q)\left[u(q)-\beta\cdot\phi_{t+1}\cdot d\right]$$

$$u'(q)=w'(q) \tag{19}$$

$q^*\in\mathbb{R}_+$ satisfies $u'(q^*)=w'(q^*)$, so that there is a socially efficient level of production in DM if the liquidity constraint does not bind.

Next, substitute $q_t=q^*$ into (18) to find d when the liquidity constraint is not binding:

$$\theta\left[-w(q^*)+\beta\cdot\phi_{t+1}\cdot d\right]=(1-\theta)\left[u(q^*)-\beta\cdot\phi_{t+1}\cdot d\right]$$

$$(1-\theta)u(q^*)-(1-\theta)\left[\beta\cdot\phi_{t+1}\cdot d\right]=-\theta w(q^*)+\theta\left[\beta\cdot\phi_{t+1}\cdot d\right]$$

$$(1-\theta)u(q^*)+\theta w(q^*)=\beta\phi_{t+1}\cdot d \tag{20}$$

■

Proof of Real Money Holdings:

$$-\theta u'(q)w(q) + \theta u'(q)\beta \cdot \phi_{t+1} \cdot d = (1-\theta)w'(q)u(q) - (1-\theta)w'(q)\beta \cdot \phi_{t+1} \cdot d$$

$$\theta u'(q)\beta \cdot \phi_{t+1} \cdot d + (1-\theta)w'(q)\beta \cdot \phi_{t+1} \cdot d = (1-\theta)w'(q)u(q) + \theta u'(q)w(q)$$

$$\beta \cdot \phi_{t+1} \cdot d = \frac{\theta w(q)u'(q) + (1-\theta)u(q)w'(q)}{\theta u'(q) + (1-\theta)w'(q)} \tag{21}$$

■

Proof of Special Case. Set $\theta = 1$ when d is not binding

$$(1-1)u(q^*) + 1 \cdot w(q^*) = \beta\phi_{t+1} \cdot d$$

$$w(q^*) = \beta\phi_{t+1} \cdot d$$

In the case when d is binding:

$$\phi_{t+1} \cdot d = \phi_{t+1}M_t^c$$

If the buyer has full bargaining power:

$$m(q) \equiv \frac{(1)w(q)u'(q) + (1-1)u(q)w'(q)}{(1)u'(q) + (1-1)w'(q)}$$

simplify

$$m(q) \equiv \frac{w(q)u'(q)}{u'(q)}$$

simplify

$$m(q) \equiv w(q)$$

and so

$$w(q) = \beta\phi_{t+1}M_t^c$$

Upon solving to get the quantity of the DM good produced in terms of the real value of tokens:

$$\beta\phi_{t+1}M_t^c = w^{-1}(\beta\phi_{t+1}M_t^c)$$

■

Consumer's Portfolio Choice before entering DM:

$$-\phi_t M_t^c+(1-\psi)\Big\{\sigma[u(q)+\beta\phi_{t+1}M_t^c-\beta\phi_{t+1}d]+\sigma[(1-\psi)(-w(\overline{q})+\beta\phi_{t+1}M_t^c+\beta\phi_{t+1}\overline{M_t^c})+\psi\beta\phi_{t+1}M_t^c]$$
$$+(1-2\sigma)\beta\phi_{t+1}M_t^c\Big\}$$

Now, we can sum up all the terms with $\phi_{t+1}M_t^c$ inside the $(1-\psi)$ bracket.

$$\sigma[\beta\phi_{t+1}M_t^c]+\sigma[(1-\psi)(\beta\phi_{t+1}M_t^c)+\psi\beta\phi_{t+1}M_t^c]+(1-2\sigma)\beta\phi_{t+1}M_t^c$$

$$\sigma\beta\phi_{t+1}M_t^c+\sigma[\beta\phi_{t+1}M_t^c]+(1-2\sigma)\beta\phi_{t+1}M_t^c$$

$$\beta\phi_{t+1}M_t^c$$

Simplify further by eliminating the work function and tokens received. Remember, we are only concerned with optimizing the amount of tokens for a purchase in the DM.

$$-\phi_t M_t^c+(1-\psi)\Big\{\sigma[u(q)-\beta\phi_{t+1}d]+\beta\phi_{t+1}M_t^c\Big\}$$

Proof of Money Demand:

The first-order condition for money balances is:

$$-\phi_t+(1-\psi)\Big\{\sigma(u'(q)\frac{\partial q_t}{\partial M_t^c}-\beta\phi_{t+1})+\beta\phi_{t+1}\Big\}=0$$

To solve for $\frac{\partial q(M_t^c,t)}{\partial M_t^c}$, remember that $m\left(q(M_t^c,t)\right)=\beta\cdot\phi_{t+1}\cdot M_t^c$

Upon taking the derivative with respect to M_t^c:

$$m'\left(q(M_t^c,t)\right)\frac{\partial q(M_t^c,t)}{\partial M_t^c}=\beta\phi_{t+1}$$

$$\frac{\partial q(M_t^c,t)}{\partial M_t^c}=\frac{\beta\phi_{t+1}}{m'\left(q(M_t^c,t)\right)}$$

We let $A=\phi_{t+1}\cdot M_t^c$ and substitute into the first-order condition:

$$\phi_t=\sigma(1-\psi)u'\left(m^{-1}(\beta A)\right)\frac{\beta\phi_{t+1}}{m'\left(q(M_t^c,t)\right)}-\sigma(1-\psi)\beta\phi_{t+1}+(1-\psi)\beta\phi_{t+1}$$

$$\phi_t=\beta\phi_{t+1}\Big(\sigma(1-\psi)\frac{u'(m^{-1}(\beta A))}{m'(m^{-1}(\beta A))}-\sigma(1-\psi)+(1-\psi)\Big)$$

$$\phi_t = \beta\phi_{t+1}\Big(\sigma(1-\psi)\frac{u'(m^{-1}(\beta A))}{m'(m^{-1}(\beta A))} + (1-\sigma)(1-\psi)\Big)$$

If the buyer's liquidity constraint no longer binds, $\sigma(1-\psi)[u(q) - \beta\phi_{t+1}d]$ remains constant with any change in M_t^c. The first-order condition for money balances will now become:

$$-\phi_t + \Big(1-\psi\Big)\beta\phi_{t+1} = 0$$

$$\phi_t = \beta\phi_{t+1}\Big(1-\psi\Big)$$

■

Proof of Money Demand for special case with functional forms:
Let's say the utility from consumption can be defined as $u(q) = 2q^{1/2}$, and $w(q) = q$ represents the cost of producing DM goods. Therefore, if the buyer has full bargaining power:

$$w(q) = q = \beta\phi_{t+1}M_t^c$$

Solve for the inverse to get the quantity of the DM good produced in terms of the real value of tokens:

$$q = \beta\phi_{t+1}M_t^c = w^{-1}(\beta\phi_{t+1}M_t^c)$$

and so

$$w(w^{-1}(\beta\phi_{t+1}M_t^c)) = \beta\phi_{t+1}M_t^c$$

Now, we use $u(q) = 2q^{1/2}$ to get

$$u(w^{-1}(\beta\phi_{t+1}M_t^c)) = 2(\beta\phi_{t+1}M_t^c)^{1/2}$$

Now, we solve for $\frac{u'(w^{-1}(\beta A))}{w'(w^{-1}(\beta A))}$

$$\frac{u'(w^{-1}(\beta A))}{w'(w^{-1}(\beta A))} = \frac{\beta\phi_{t+1}}{\beta\phi_{t+1}\sqrt{\beta\phi_{t+1}M_t^c}}$$

simplify

$$\frac{u'(w^{-1}(\beta A))}{w'(w^{-1}(\beta A))} = \frac{1}{\sqrt{\beta\phi_{t+1}M_t^c}}$$

now substitute into L_1 to get

$$L_1(\phi_{t+1}M_t^c) = \sigma(1-\psi)\frac{1}{\sqrt{\beta\phi_{t+1}M_t^c}} + (1-\sigma)(1-\psi)$$

We can also use the first-order condition for the portfolio choice:

$$\phi_t = \sigma(1-\psi)u'(w^{-1}(\beta\phi_{t+1}M_t^c)) + \beta\phi_{t+1}\Big((1-\sigma)(1-\psi)\Big)$$

Substituting $w^{-1}(\beta\phi_{t+1}M_t^c) = q = \beta\phi_{t+1}M_t^c$, and solving for $u'(q)$.

$$u(q) = \frac{q^{\frac{1}{2}}}{\frac{1}{2}} = \frac{[\beta\phi_{t+1}M_t^c]^{\frac{1}{2}}}{\frac{1}{2}}$$

$$u'(w^{-1}(\beta\phi_{t+1}M_t^c)) = \frac{1}{2}\frac{\beta\phi_{t+1}[\beta\phi_{t+1}M_t^c]^{-\frac{1}{2}}}{\frac{1}{2}}$$

$$u'(w^{-1}(\beta\phi_{t+1}M_t^c)) =$$

$$\phi_t = \sigma(1-\psi)\frac{\beta\phi_{t+1}}{[\beta\phi_{t+1}M_t^c]^{\frac{1}{2}}} + \beta\phi_{t+1}\Big((1-\sigma)(1-\psi)\Big)$$

The first-order condition for portfolio problem becomes

$$\phi_t = \beta\phi_{t+1}\Big(\frac{\sigma(1-\psi)}{[\beta\phi_{t+1}M_t^c]^{\frac{1}{2}}} + (1-\sigma)(1-\psi)\Big)$$

giving us the same condition for L_1

$$L_1(\phi_{t+1}M_t^c) = \sigma(1-\psi)\frac{1}{\sqrt{\beta\phi_{t+1}M_t^c}} + (1-\sigma)(1-\psi)$$

■

Proof of Proposition 1: First, by condition iii, the first order condition to the entrepreneur's problem in the steady-state is:

$$\overline{\phi} = c'(\Delta^*)$$

Thus, token creation each period will satisfy $\Delta^* = (c')^{-1}(\overline{\phi})$. In turn, we have the following law of motion $\overline{M} = (c')^{-1}(\overline{\phi}) + (1-\psi)\overline{M}$. Moreover, it is easy to see that $\overline{M} = \frac{1}{\psi}(c')^{-1}(\overline{\phi})$ in the steady state.

Under the above cost function, the entrepreneur will create $\frac{1}{2}\overline{\phi}$ tokens each period.

Given that token creation is $\frac{1}{2}\overline{\phi}$ each period, we can easily show the steady-state level of the money supply to be $\overline{M} = \frac{1}{2\psi}\overline{\phi}$.

Next, define the value of tokens in the steady-state as $\overline{b} \equiv \overline{\phi M}$:

$$1 = \beta\overline{\gamma} L_1\left(\overline{\gamma}\overline{b}\right)$$

Rearrange to get a consumer's money demand

$$\overline{b} = \frac{1}{\overline{\gamma}} L_1^{-1}(\frac{1}{\beta\overline{\gamma}})$$

define as $z_1(\gamma)$

$$\overline{b} = \frac{1}{\overline{\gamma}} L_1^{-1}(\frac{1}{\beta\overline{\gamma}}) \equiv z_1(\overline{\gamma}).$$

Because $\overline{\gamma} = 1$, the above equation becomes

$$\overline{b} = L_1^{-1}(\frac{1}{\beta}) \equiv z_1(1).$$

Now, impose the steady state on the first-order condition for portfolio problem

$$\overline{\phi} = \beta\overline{\phi}\Big(\frac{\sigma(1-\psi)}{[\beta\overline{b}]^{\frac{1}{2}}} + (1-\sigma)(1-\psi)\Big)$$

$$1 = \beta\Big(\frac{\sigma(1-\psi)}{[\beta\overline{b}]^{\frac{1}{2}}} + (1-\sigma)(1-\psi)\Big)$$

$$\frac{1}{\beta} = L_1 = \frac{\sigma(1-\psi)}{[\beta\overline{b}]^{\frac{1}{2}}} + (1-\sigma)(1-\psi)$$

Now solve for $\overline{b}$ to get real money demand:

$$\overline{b} = L_1^{-1}(\frac{1}{\beta}) = \frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$$

The real money demand in the steady-state can be shown by:

$$z_1(1) = \frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$$

To allow a stable price, the real money demand must satisfy $\overline{b} < \beta^{-1}w(q^*)$. Otherwise, the rate of return on currency must be greater than 1. The liquidity constraint no longer binds when the real value of money holding becomes

$$\frac{u'(q*)}{m'(q*)} = 1 = \frac{1}{\sqrt{\beta \cdot \overline{\phi} \cdot \overline{M}}} \rightarrow \sqrt{\beta \cdot \overline{\phi} \cdot \overline{M}} = 1 \rightarrow \overline{\phi} \cdot \overline{M} = \frac{1}{\beta}$$

In order to show $\overline{b} < \beta^{-1} w(q^*)$, we take $\frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2} < \frac{1}{\beta}$ and multiply by β on both sides

$$\frac{\beta^2(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2} < 1$$

$$\beta^2(\sigma(1-\psi))^2 < (1-\beta(1-\psi)+\beta\sigma(1-\psi))^2$$

$$\beta(\sigma(1-\psi)) < 1-\beta(1-\psi)+\beta\sigma(1-\psi)$$

$$0 < 1-\beta(1-\psi)$$

Since $\beta < 1$, it will be the case that $0 < 1-\beta(1-\psi)$.

The market clearing condition in the steady-state implies

$$\overline{\phi M} = z_1(1)$$

Setting the real value of money in the steady-state equal to real money demand, we solve for the price of tokens needed in the steady-state.

$$z_1(1) = \frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2} = \frac{1}{2\psi}\overline{\phi}^2 = \overline{\phi M}$$

$$\frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2} = \frac{1}{2\psi}\overline{\phi}^2$$

$$\frac{2\psi\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2} = \overline{\phi}^2$$

The price of tokens in the steady-state becomes:

$$\overline{\phi} = \frac{\sigma(1-\psi)\sqrt{2\beta\psi}}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))}$$

To see what effect having an increase in likelihood of a trade in the DM on the steady-state price, take the partial derivative of $\overline{\phi}$ with respect to σ:

$$\frac{\partial\overline{\phi}}{\partial\sigma} = \frac{\sqrt{2\beta\psi}(1-\psi)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))} + \frac{\sqrt{2\beta\psi}\sigma(1-\psi)(-1)\beta(1-\psi)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$$

$$\frac{\partial\overline{\phi}}{\partial\sigma} = \underbrace{\frac{\sqrt{2\beta\psi}(1-\psi)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))}}_{\oplus} - \underbrace{\frac{\sqrt{2\beta\psi}\beta\sigma(1-\psi)^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}}_{\oplus}$$

Assume first term is greater than second term

$$\frac{\sqrt{2\beta\psi}(1-\psi)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))} > \frac{\sqrt{2\beta\psi}\beta\sigma(1-\psi)^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$$

$$\frac{1}{1} > \frac{\beta\sigma(1-\psi)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))}$$

$$1-\beta(1-\psi)+\beta\sigma(1-\psi) > \beta\sigma(1-\psi)$$

$$1-\beta(1-\psi) > 0$$

Since $\beta \in (0,1)$, we know the above is true. Thus, $\frac{\partial\overline{\phi}}{\partial\sigma} > 0$.

To see the effect of currency loss on the steady-state price, take the partial derivative of $\overline{\phi}$ with respect to ψ:

$$\frac{\partial\overline{\phi}}{\partial\psi} = \frac{2\beta\psi}{2\sqrt{2\beta\psi}}\frac{\sigma(1-\psi)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))}$$

$$+\sqrt{2\beta\psi}\Big(\frac{-\sigma}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))} + \frac{\sigma(1-\psi)(-1)(\beta-\beta\sigma)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}\Big)$$

$$\frac{\partial\overline{\phi}}{\partial\psi} = \underbrace{\frac{\beta\psi\sigma(1-\psi)}{\sqrt{2\beta\psi}(1-\beta(1-\psi)+\beta\sigma(1-\psi))}}_{\oplus} - \underbrace{\frac{\sigma\sqrt{2\beta\psi}}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))}}_{\oplus} - \underbrace{\frac{\sqrt{2\psi}\beta^{\frac{3}{2}}\sigma(1-\psi)(1-\sigma)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}}_{\oplus}$$

Assume first term smaller than second plus the third term:

$$\frac{\beta\psi\sigma(1-\psi)}{\sqrt{2\beta\psi}(1-\beta(1-\psi)+\beta\sigma(1-\psi))} < \frac{\sigma\sqrt{2\beta\psi}}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))} + \frac{\sqrt{2\psi}\beta^{\frac{3}{2}}\sigma(1-\psi)(1-\sigma)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$$

simplify

$$\frac{\beta\psi(1-\psi)}{\sqrt{2\beta\psi}} < \sqrt{2\beta\psi} + \frac{\sqrt{2\psi}\beta^{\frac{3}{2}}(1-\psi)(1-\sigma)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))}$$

We know the last term is positive so if we show 2nd term larger than 1st term will still hold true

$$\frac{\sqrt{\beta\psi}(1-\psi)}{\sqrt{2}} < \sqrt{2\beta\psi}$$

$$\frac{\sqrt{\psi}(1-\psi)}{\sqrt{2}} < \sqrt{2\psi}$$

$$\sqrt{\psi}(1-\psi) < 2\sqrt{\psi}$$

$$(1-\psi) < 2$$

Which gives us $\frac{\partial\overline{\phi}}{\partial\psi} < 0$.

Substitute $\overline{\phi} = \frac{\sigma(1-\psi)\sqrt{2\beta\psi}}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))}$ into the steady-state money supply to get

$$\overline{M} = \frac{1}{2\psi}\overline{\phi} = \frac{1}{2\psi}\cdot\frac{\sigma(1-\psi)\sqrt{2\beta\psi}}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))} = \frac{\sqrt{\beta}\sigma(1-\psi)}{\sqrt{2\psi}(1-\beta(1-\psi)+\beta\sigma(1-\psi))}$$

To find the effect of an increase in currency loss on the steady-state level of tokens, take the partial derivative of $\overline{M}$ with respect to ψ:

$$\frac{\partial \overline{M}}{\partial \psi} = -\frac{\overline{\phi}}{2\psi^2} + \frac{1}{2\psi}\frac{\partial \overline{\phi}}{\partial \psi} = -\frac{\overline{\phi}}{2\psi^2} + \ominus$$

Thus, $\frac{\partial \overline{M}}{\partial \psi} < 0$.

In order to find the effect of successful trades on the steady-state money supply, take the partial derivative of $\overline{M}$ with respect to σ:

$$\frac{\partial \overline{M}}{\partial \sigma} = \frac{1}{2\psi}\Big(\frac{\partial \overline{\phi}}{\partial \sigma}\Big) = \frac{1}{2\psi}\Big(\oplus\Big)$$

Therefore, $\frac{\partial \overline{M}}{\partial \sigma} < 0$. ■

Proof of Proposition 2. First by condition (iii) in the steady-state equilibrium would imply that the first order condition to the entrepreneur's problem in the steady-state be represented by:

$$\overline{\phi} = c_0$$

The amount of tokens produced at this price is indeterminate. With entrepreneurs producing tokens in the range $\Delta^* \in [0, \infty]$ each period. In the steady-state condition (v) must hold:

$$\overline{\phi M} = z_1(1)$$

From the previous proof, we substitute $z_1(1) = \frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$ and for the steady-state price $\overline{\phi} = c_0$ to get

$$c_0\overline{M} = \frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$$

Which will give the steady-state supply of tokens

$$\overline{M} = \frac{1}{c_0}\frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$$

Next, by condition iv we get the law of motion for tokens represented by

$$\overline{M} = \Delta^* + (1-\psi)\overline{M}$$

It is easy to show that $\Delta^* = \psi\overline{M} = \frac{\psi}{c_0}\frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}$.

To find the effect of an increase in currency loss on the steady-state level of tokens, take the partial derivative of $\overline{M}$ with respect to ψ:

$$\frac{\partial \overline{M}}{\partial \psi} = \frac{\partial}{\partial \psi}\Big\{\frac{1}{c_0}\frac{\beta(\sigma(1-\psi))^2}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2}\Big\}$$

$$\frac{\partial \overline{M}}{\partial \psi} = \frac{1}{c_0}\Big\{\frac{2\beta(\sigma(1-\psi))(-\beta\sigma)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^2} + \frac{\beta(\sigma(1-\psi))^2(-2)(\beta-\beta\sigma)}{(1-\beta(1-\psi)+\beta\sigma(1-\psi))^3}\Big\}$$

$$\frac{\partial \overline{M}}{\partial \psi} = \frac{-2\beta^2\sigma^2(1-\psi)(1-\beta(1-\psi)+\beta\sigma(1-\psi)) - 2\beta^2\sigma^2(1-\sigma)(1-\psi)}{c_0(1-\beta(1-\psi)+\beta\sigma(1-\psi))^3}$$

$$\frac{\partial \overline{M}}{\partial \psi} = \frac{\overbrace{-2\beta^2\sigma^2(1-\psi)}^{\ominus}\overbrace{(1-\beta(1-\psi)+\beta\sigma(1-\psi)+(1-\sigma)(1-\psi))}^{\oplus}}{\underbrace{c_0(1-\beta(1-\psi)+\beta\sigma(1-\psi))^3}_{\oplus}}$$

Which gives us $\frac{\partial \overline{M}}{\partial \psi} < 0$.

A change in the rate of currency loss will have no effect on the steady-state price, $\frac{\partial \overline{\phi}}{\partial \psi} = 0$.

Set Ω, then compare the $\frac{\partial \overline{M}}{\partial \psi}$ from proposition 1 to proposition 2.

$$\frac{\partial \overline{M}^{p2}}{\partial \psi} = \frac{-2\beta^2\sigma^2(1-\psi)(\Omega+(1-\sigma)(1-\psi))}{c_0\Omega^3}$$

$$\frac{\partial \overline{M}^{p1}}{\partial \psi} = \frac{-\sqrt{\frac{\beta}{2}}\frac{\sigma}{\psi^{\frac{3}{2}}}(1-\psi)}{\Omega} + \frac{\sqrt{\frac{\beta\psi}{2}}\sigma(1-\psi)}{\Omega} - \frac{\sigma\sqrt{2\beta\psi}}{\Omega} - \frac{\sqrt{2\psi}\beta^{\frac{3}{2}}\sigma(1-\psi)(1-\sigma)}{\Omega^2}$$

$$\frac{\partial \overline{M}^{p1}}{\partial \psi} = \frac{-\sqrt{\frac{\beta}{2}}\frac{\sigma}{\psi^{\frac{3}{2}}}(1-\psi)\Omega^2}{\Omega^3} + \frac{\sqrt{\frac{\beta\psi}{2}}\sigma(1-\psi)\Omega^2}{\Omega^3} - \frac{\sigma\sqrt{2\beta\psi}\Omega^2}{\Omega^3} - \frac{\sqrt{2\psi}\beta^{\frac{3}{2}}\sigma(1-\psi)(1-\sigma)\Omega}{\Omega^3}$$

Multiply through by Ω^3 and combine terms and assume $\frac{\partial \overline{M}^{p2}}{\partial \psi} < \frac{\partial \overline{M}^{p1}}{\partial \psi}$

$$\frac{-2}{c_0}\beta^2\sigma^2(1-\psi)(\Omega+(1-\sigma)(1-\psi)) < \Omega^2\Big(-\sqrt{\frac{\beta}{2}}\sigma(1-\psi)(\frac{1}{\psi^{\frac{3}{2}}}-\psi^{\frac{1}{2}})-\sigma\sqrt{2\beta\psi}\Big)-\sqrt{2\psi}\beta^{\frac{3}{2}}\sigma(1-\psi)(1-\sigma)\Omega$$

$$\frac{-2\beta^2\sigma^2(1-\psi)(\Omega+(1-\sigma)(1-\psi))}{\Omega^2\Big(-\sqrt{\frac{\beta}{2}}\sigma(1-\psi)(\frac{1}{\psi^{\frac{3}{2}}}-\psi^{\frac{1}{2}})-\sigma\sqrt{2\beta\psi}\Big)-\sqrt{2\psi}\beta^{\frac{3}{2}}\sigma(1-\psi)(1-\sigma)\Omega} > c_0$$

As c_0 gets larger the adjustment to a change in ψ to maintain a steady-state is smaller. ■

Proof of Proposition 3. Consider a set of caps with the property that $\overline{\Delta}_t > 0$ at dates $0 \le t \le T$ and $\overline{\Delta}_t = 0$ at all subsequent dates $t \ge T+1$, given a finite date $T > 0$. Set $\phi_t = \overline{\phi}$ at all dates $t \ge T+1$, with the constant $\overline{\phi} > 0$ satisfying

$$1 = \beta L_1(\overline{\phi}\Sigma_{\tau=0}^{T}\overline{\Delta}_\tau).$$

This comes from

$$\phi_t = \beta\phi_{t+1}L_1(\phi_{t+1}M_t)$$

$\phi_t = \phi_{t+1} = \overline{\phi}$ because $t \ge T+1$. So you have

$$\overline{\phi} = \beta\overline{\phi}L_1(\overline{\phi}M_t)$$

cancel out $\overline{\phi}$ on both sides

$$1 = \beta L_1(\overline{\phi} M_t)$$

Since no more tokens are created at this point, at all future dates $\overline{\phi}\Sigma_{\tau=0}^{T}\overline{\Delta}_{\tau}$=$M_t$

$$1 = \beta L_1(\overline{\phi}\Sigma_{\tau=0}^{T}\overline{\Delta}_{\tau}).$$

The above equation is not possible with currency loss. Let's assume that we have price stability and all the tokens have been created. We will now introduce currency loss for each period into the above equation.

$$1 = \beta L_1(\overline{\phi}\Sigma_{m=T+j}^{\infty}(1-\psi)_m\Sigma_{\tau=0}^{T}\overline{\Delta}_{\tau}).$$

One of two things needs to happen for this equation to remain true. Entrepreneurs would need to create more tokens or the price would need to increase. The first possibility is not possible because token creation has been capped. The second causes a contradiction. It would no longer be the case that $\phi_t = \phi_{t+1}$.

Therefore, a sequence with price stability does not exist with currency loss and a cap on total token creation. ■

Proof of Proposition 4.

$$\frac{1}{\beta} = \sigma(1-\psi)\frac{u'(\hat{q_{cl}})}{w'(\hat{q_{cl}})} + 1 - \sigma(1-\psi) - \psi = \sigma\frac{u'(\hat{q})}{w'(\hat{q})} + 1 - \sigma = \frac{1}{\beta}$$

$$\sigma(1-\psi)\frac{u'(\hat{q_{cl}})}{w'(\hat{q_{cl}})} + 1 - \sigma(1-\psi) - \psi = \sigma\frac{u'(\hat{q})}{w'(\hat{q})} + 1 - \sigma$$

$$\sigma(1-\psi)\frac{u'(\hat{q_{cl}})}{w'(\hat{q_{cl}})} + \sigma\psi - \psi = \sigma\frac{u'(\hat{q})}{w'(\hat{q})}$$

As you can see $\frac{u'(\hat{q_{cl}})}{w'(\hat{q_{cl}})} > \frac{u'(\hat{q})}{w'(\hat{q})}$ and since $\frac{u'(q)}{w'(q)}$ is decreasing in q then $\hat{q_{cl}} < \hat{q}$. ■

Proof of Proposition 5. Suppose $\phi < \overline{\phi}$, then token production is less than what is needed for a stable price $\Delta^* < \overline{\Delta}^* = \frac{1}{2}\overline{\phi}$. There will be less new tokens created than tokens lost from the money supply in the previous period $\Delta^* < \psi M_{-1}$. Since token production will be less than the amount of tokens lost it will be the case that $\gamma < 1$ and thus deflation is observed. The price of tokens will be greater than the previous period $\phi_{+1} > \phi$. This will lead to more tokens being created than the previous period since token production is increasing in price $\Delta^*_{+1} > \Delta^*$.

This process will continue for n periods until $\phi_{+n} = \overline{\phi}$. Token production for each period equals token loss $\Delta^*_{+n} = \overline{\Delta}^* = \psi\overline{M}$. At this point $\gamma = 1$ for the remaining periods. Thus, it is not possible to have a steady state with deflation in this economy with no cap.

With a cap $\overline{\Delta}^* = \alpha\overline{M} < \psi\overline{M}$, the number of tokens will decrease in the steady state and allow for a positive real return on currency. ■

Proof of Proposition 6. In equilibrium the real value of tokens must remain the same. In order to have a steady state with $\overline{\gamma} = \frac{1}{\beta(1-\psi)}$, the amount of tokens must evolve according to

$$\phi_{t+1}M_{t+1} = \frac{1}{\beta(1-\psi)}M_{t+1} = 1 \cdot M_t = \phi_t M_t$$

Now substitute $\phi_{t+1} = \frac{1}{\beta(1-\psi)}, \phi_t = 1$ and $M_{t+1} = \beta(1-\psi)M_t$ into $\phi_{t+1}M_{t+1} = \phi_{t+1}\Delta_t^* + \phi_{t+1}(1-\psi)M_t$ to get

$$\begin{gathered}\beta(1-\psi)M_t = \Delta_{t+1}^* + (1-\psi)M_t \\ (\beta(1-\psi) - (1-\psi))M_t = \Delta_{t+1}^* \\ (\beta-1)(1-\psi)M_t = \Delta_{t+1}^* \\ \underbrace{(\beta-1)}_{(-)}\underbrace{(1-\psi)}_{(+)}\overline{M} = \overline{\Delta}^* < 0\end{gathered}$$

■

Proof of Proposition 7. Similar to the proof of proposition 6, the amount of tokens must evolve according to

$$\phi_{t+1}M_{t+1} = \frac{1}{\beta(1-\psi)}M_{t+1} = 1 \cdot M_t = \phi_t M_t$$

Now substitute $\phi_{t+1} = \frac{1}{\beta(1-\psi)}, \phi_t = 1$ and $M_{t+1} = \beta(1-\psi)M_t$ into $\phi_{t+1}M_{t+1} = \phi_{t+1}\Delta_t^* + \phi_{t+1}(1-\psi)M_t$ to get

$$\beta(1-\psi)M_t = \Delta_{t+1}^* + (1-\psi)M_t$$

Now, we place a cap on token production $\overline{\Delta} = \alpha M$ and there is a tax τ each period.

$$\beta(1-\psi)M_t = \alpha M_{t+1} + (1-\psi)M_t - \tau$$

$$\begin{gathered}\tau = (\alpha + (1-\psi) - \beta(1-\psi))M_t \\ \tau = (\alpha + (1-\beta)(1-\psi))M_t > 0\end{gathered}$$

■

Proof of Proposition 8. We must have $q^g = q^p$ in order for agents to hold both currencies. The returns must yield the same amount of production in the DM. Recall the money demand function for tokens with currency loss.

$$\phi_t^p = \beta\phi_{t+1}^p\Big(\sigma(1-\psi)\frac{u'(q^p)}{w'(q^p)} + (1-\sigma)(1-\psi)\Big)$$

$$\frac{1}{\gamma_{t+1}^p} = \frac{\phi_t^p}{\phi_{t+1}^p} = \beta\Big(\sigma(1-\psi)\frac{u'(q^p)}{w'(q^p)} + (1-\sigma)(1-\psi)\Big)$$

Now if you divide both sides by $(1-\psi)$ you get

$$\frac{1}{(1-\psi)\gamma_{t+1}^p} = \beta\Big(\sigma\frac{u'(q^p)}{w'(q^p)} + (1-\sigma)\Big)$$

Since $q^p = q^g$ we have

$$\frac{1}{(1-\psi)\gamma_{t+1}^p} = \beta\Big(\sigma\frac{u'(q^p)}{w'(q^p)} + (1-\sigma)\Big) = \beta\Big(\sigma\frac{u'(q^g)}{w'(q^g)} + (1-\sigma)\Big) = \frac{1}{\gamma_{t+1}^g}$$

which gives us $\gamma_{t+1}^g = (1-\psi)\gamma_{t+1}^p$. ■