BANK OF CANADA
BANQUE DU CANADA

Staff Working Paper/Document de travail du personnel—2025-18

Last updated: June 26, 2025

On the Programmability and Uniformity of Digital Currencies

Jonathan Chiu
Banking and Payments Department
Bank of Canada
jchiu@bankofcanada.ca

Cyril Monnet
Study Center Gerzensee
University of Bern
cyril.monnet@unibe.ch

DOI: https://doi.org/10.34989/swp-2025-18 | ISSN 1701-9397

Acknowledgements

We thank many friends and colleagues for many useful conversations. The views expressed here are those of the authors and do not necessarily reflect the position of the Bank of Canada.

Abstract

Central bankers argue that programmable digital currencies may compromise the uniformity of money. We explore this in a stylized model where programmable money arises endogenously, and differently programmed monies have varying liquidity. Programmability provides private value by easing commitment frictions but imposes social costs under informational frictions. Preserving uniformity is not necessarily socially beneficial. Banning programmable money lowers welfare when informational frictions are mild but improves it when commitment frictions are low. These insights suggest programmable money could be more beneficial on permissionless blockchains.

Topics: Digital currencies and fintech, payment clearing and settlement systems

JEL codes: E50, E58

Résumé

Les banquiers centraux affirment que les monnaies numériques programmables peuvent compromettre l'uniformité de la monnaie. Nous étudions cette question dans un modèle stylisé où la monnaie programmable apparaît de manière endogène et où les monnaies assujetties à différents programmes ont un niveau de liquidité variable. La programmabilité atténue les frictions liées à l'engagement et apporte ainsi une valeur privée, mais elle impose des coûts sociaux en raison de frictions informationnelles. En somme, il n'est pas nécessairement socialement bénéfique de préserver l'uniformité de la masse monétaire. Interdire la monnaie programmable réduit le bien-être lorsque les frictions informationnelles sont faibles ou que les frictions liées à l'engagement sont fortes, mais l'augmente dans le cas contraire. Ces observations donnent à penser que la monnaie programmable pourrait être plus bénéfique sur les chaînes de blocs sans permission.

Sujets : Monnaies numériques et technologies financières; Systèmes de compensation et de règlement des paiements

Codes JEL : E50, E58

"Should the lack of a uniform medium of exchange be a concern? Should Congress, as it did in the past, intervene to ensure a uniform medium of exchange? I do not think that economic history provides answers. To address these questions, economists need to develop models that can explain both why money is used and what form it should take."

– Arthur Rolnick (1999)

1 Introduction

Many researchers and practitioners believe that a key feature of digital money, compared to traditional money, is programmability. This characteristic allows software programs to be embedded into digital money, automatically enforcing pre-specified rules when certain conditions are met and eliminating the need for human intervention or intermediaries. Today, programmable money is often implemented via blockchain-based smart contracts that execute state-dependent transactions recorded on a distributed ledger. For example, a smart contract can execute or block a payment based on pre-defined conditions, without a trusted party. Kahn, van Oordt, and Zhu (2021) even argue that it may be optimal to program an expiry date, after which digital currency becomes non-transferable and loses its value. Proponents argue that programmable money can revolutionize financial transactions by addressing commitment problems, automating processes, and enhancing efficiency.[1] Some central banks also incorporate programmability into the design of their central bank digital currencies (CBDCs).[2]

However, money balances that are programmed differently may hold distinct market values, reflecting differences in transferability, maturity, contractibility, and risk. For instance, unlike traditional payment services (e.g., PayPal), blockchain-based cryptocurrencies bundle programmability with the digital representation of money (Lee, 2021). As a result, differently programmed cryptocurrencies cannot share a fungible digital representation.[3] This non-fungibility could undermine the uniformity (or singleness) of

[1]Very primitive forms of programmable paper money already exist—such as food stamps—but programmable digital money is easier to design and implement. For example, in initial coin offerings (ICOs), investors can use programmable money to restrict how start-ups spend raised funds. In daily life, parents can control when and how children spend pocket money. Stablecoin issuers can also pre-specify conditions for token redemption.

[2]For example, Banco Central do Brasil's Digital Real guidelines emphasize smart contracts and programmable money, while China's e-CNY project allows self-executing payments to support business model innovation. See Lee et al. (2021) for how tokenization and smart contracts address commitment problems.

[3]As highlighted in Kahn and van Oordt (2022), programmable money is fundamentally different from programmable payments, which apply pre-specified rules to otherwise fungible money balances. For instance, bank accounts allow users to arrange pre-authorized payments, but these still require intermediaries to move fungible balances on the account holder's

the money stock, where each unit of money should retain the same value and purchasing power as any other unit of the same denomination.

This is an important consideration for the design of digital money. Some central bankers have voiced concerns that programmable money could undermine the singleness of money. For example, Norges Bank Governor Ida Wolden Bache highlighted this risk in a recent speech (Bache 2023):[4]

> *"If programmability becomes a highly desired feature of money, and its supply is freely developed, it could jeopardize the singleness of money. This might lead to the use of multiple units of account in parallel within a country, or to a more fragile parity between different representations of the same unit of account."*

This concern stems from the historical experience that discounts in privately issued banknotes in the free banking era led to the loss of uniformity of money (e.g., Weber 2015; Fung, Hendry, and Weber 2017; Gorton and Zhang 2023). However, it is unclear how relevant this history is for future monetary systems because of new digital technologies. Given the innovative potential of programmability and its profound implications on the singleness of money, fundamental research is required to guide policy decisions, as suggested by Rolnick's comment cited in the epigraph to this paper, and to answer questions such as:

- Is programmable money beneficial?
- Is the singleness/uniformity of money desirable?
- When does programmability conflict with singleness?
- Should programmability be restricted to preserve singleness?

This paper addresses these questions by developing a microfounded model of programmable money. Our objective is to provide a simple framework that: i) captures the potential benefits of introducing programmable tokens and maintaining the singleness of money, and ii) allows us to understand how the desirability of programmability depends on the fundamental trade-off between underlying information and commitment frictions. To sharpen these economic insights, we develop a highly stylized model that

behalf (e.g., monthly rent payments). In contrast, programmable money relies on no trusted third party. Moreover, differently programmed tokens are intrinsically distinct from one another and therefore non-fungible. See Section 3 for further discussion.

[4] Relatedly, Carolyn A. Wilkins, external member of Bank of England Financial Policy Committee, argued that "programming could also undermine the uniformity of money which is required to provide a safe base to the financial system." The 2023 Consultation Paper by the Bank of England and HM Treasury reinforces this view. The BIS report by Garratt and Shin (2023) highlights the importance of singleness.

emphasizes transparency and clarity. The model features agents facing a lack of double coincidence of wants, creating demand for a means of payment. Smart contracts act as bankers, issuing money that can be programmed with varying degrees of liquidity. Agents cannot commit to certain future actions, which drives the endogenous creation of programmable money to restrict future choices. However, programmability also limits the flexibility of future holders. In equilibrium, programmed money has lower purchasing power than unprogrammed money, resulting in a loss of singleness. Nevertheless, banning programmable money is not necessarily optimal. When different monies are perfectly recognizable, prices adjust to reflect differences, enabling efficient outcomes. Indeed, from first principles, it is optimal to price distinct assets differently. However, when recognizability is imperfect, prices fail to fully adjust, which leads to welfare losses. As a result, the optimal policy governing programmability depends on the underlying balance between commitment frictions (which favor programmability) and information frictions (which favor uniformity).

Our model is the first to endogenize both the creation of programmable money and the liquidity values of differently programmed tokens (i.e., the degree of singleness). It highlights three key economic insights. First, singleness is neither necessary nor sufficient for maximum welfare—imposing par trading can trigger Gresham's Law. Second, programmability is more beneficial when commitment frictions are severe but recognizability is high, resembling a permissionless blockchain. Third, historical lessons from free banking may not apply directly, given evolving frictions and technologies.

Our paper contributes to the rapidly expanding literature on digital currencies, which can be divided into three main areas. The first area examines the design and operation of cryptocurrencies and utility tokens.[5] The second area focuses on stablecoins, particularly their price stability and regulatory issues.[6] The third area focuses on the macro and banking implications of central bank digital currencies.[7] Our paper uniquely examines the interaction between programmability and monetary singleness, filling an important gap in this literature. Our new insights can inform the design of digital currencies in all three areas.

This paper is organized as follows. Section 2 presents the model and defines programmability and singleness. Sections 3 analyzes equilibrium with perfect recognizability. Section 4 studies imperfect recognizability and the trade-off between commitment and information frictions. Section 5 examines

[5]Key studies include Biais et al. (2019), Choi and Rocheteau (2021), and Schilling and Uhlig (2019) for Bitcoin, and Cong et al. (2021) and Gans and Halaburda (2015) for utility tokens.

[6]See, for example, Li and Mayer (2021), Bertsch (2023), and Carapella (2024).

[7]Related studies include Andolfatto (2020), Chiu et al. (2023), Keister and Sanches (2023), Schilling et al. (2024), Tinn (2024), and Williamson (2022).

over-creation of tokens via Gresham's law. Section 6 concludes.

2 Environment

We consider a finite-horizon model with four consecutive periods.[8] Agents trade numeraire goods y in centralized markets (CM) in periods 1 and 4, and consumption goods q in decentralized markets (DM) in periods 2 and 3. These periods are denoted CM1, DM1, DM2, and CM2.

As shown in Figure 1, there are buyers, sellers, and bankers. Buyers and bankers enter in CM1; buyers exit after DM2, and bankers after CM2. Sellers enter in DM1 and DM2, exiting after CM2. The discount factor between CM1 and DM1 is β. The timing and the size of discounting do not matter.

Buyers

In CM1, buyers produce the numeraire good y y at a linear utility cost. Buyers are either type $i = L$ or type $i = H$ with $Pr(i = L) = f_L$ and $Pr(i = H) = f_H = 1 - f_L$. Each buyer receives a preference shock determining whether they value consumption in DM1 or DM2. Let q_1 be the consumption in DM1 and q_2 the consumption in DM2. Then the preferences of buyer i is

$$U_i(q_1, q_2) = \eta_i u(q_1) + (1 - \eta_i)u_i(q_2),$$

where $\eta_i \in \{0, 1\}$ is a stochastic variable that takes value 1 with probability σ_i and 0 otherwise, and where

$$\begin{aligned} u_L(q) &= \varepsilon q, \text{ with } \varepsilon \in (0,1), \\ u_H(q) &= u(q), \\ u'(q) > 0, u''(q) &< 0, u'(0) = \infty. \end{aligned}$$

Hence, L-buyers derive utility $u(q_1)$ from consumption in DM1 with probability σ_L, and derive utility εq_2 from consumption in DM2 with probability $1 - \sigma_L$. H-buyers derive utility $u(q_1)$ from consumption in DM1 with probability σ_H, and derive utility $u(q_2)$ from consumption in DM2 with probability $1 - \sigma_H$. Also, assume $\sigma_L > \sigma_H$. Therefore, L-buyers are more likely to consume early than H-buyers, but in case they consume late, their marginal utility is (arbitrarily) low. It will become clear later that assuming the special preference $u_L(q)$ is key for capturing the commitment problem, while having two types of buyers is key for generating the information problem.

[8] The model could easily be extended to a standard infinite-horizon framework (e.g., Lagos and Wright 2005).

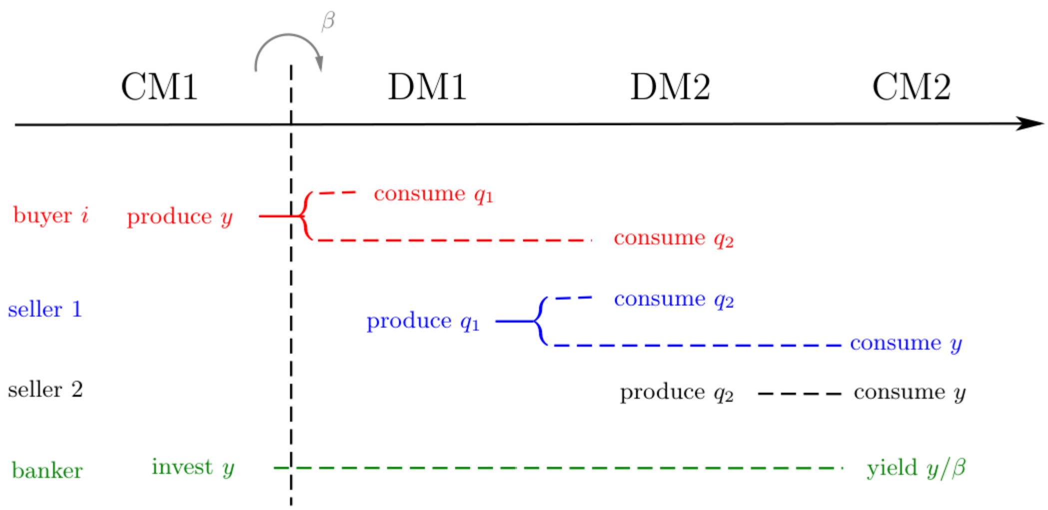

Figure 1: Model Setup

Sellers

There are two types of sellers: Type 1 sellers enter the economy in DM1, and Type 2 sellers enter in DM2. Type 1 sellers produce q_1 with a linear cost function and face a consumption shock. With probability α_e, they are early (e) sellers who want to consume in DM2; with probability $1 - \alpha_e$, they are late (ℓ) sellers who want to consume in CM2. All sellers have linear utility. The consumption shock, revealed *after* DM1, is crucial for generating the loss of singleness, as explained below. Type 2 sellers produce q_2 in DM2 with a linear cost function and want to consume in CM2. Sellers cannot observe the buyers' type. The terms-of-trade in both markets are determined by take-it-or-leave-it offers from the buyers.

Bankers

Transactions in DM1 and DM2 are subject to informational frictions, preventing the use of credit. Thus, buyers need a means of payment, giving rise to a token-in-advance constraint. Bankers create and sell tokens in CM1 for ϕ numeraire goods and have a storage technology to keep reserve of the numeraire good to redeem tokens in CM2. Reserves yields a return of $1/\beta$, so that the token-in-advance constraint does not distort consumption.[9] Tokens are programmable so that they are either transferable or not in DM2, denoted by $\mathfrak{p} \in \{0, 1\}$. The banker sells tokens at a price $\phi_{\mathfrak{p}}$, which depends on their

[9]We can easily relax this to make the token-in-advance constraint distortionary. We abstract from this as it is already well understood and is not the focus of the paper.

programmability. All tokens can be transferred in DM1. However, they are either programmed ($\mathfrak{p} = 1$) to be non-transferable in DM2, or unprogrammed ($\mathfrak{p} = 0$) and remain transferable in DM2. The banker commits to redeeming each token for one unit of numeraire goods in the next CM, subject to a balance-budget constraint ensuring sufficient reserves. This commitment is credible because bankers act as passive smart contracts, automatically issuing tokens when reserves are locked and releasing reserves upon redemption. As automated protocols, smart contracts face no incentive problems, similar to how stablecoins are issued in the crypto space. Buyers of type i purchase portfolios (m_{i0}, m_{i1}) constituted of $\mathfrak{p} = 0$ tokens and $\mathfrak{p} = 1$ tokens, respectively.

First best benchmark

It is straightforward to compute the first-best allocation. In DM1, all buyers should consume q^*, solving $u'(q^*) = 1$. In DM2, H-buyers should consume q^*, while L-buyers should not consume since their marginal utility is always below the marginal cost of production. All other consumption levels are indeterminate.

We define singleness and programmability as follows. Let $\mathcal{M}_i$ denote the set of tokens held by buyer i in equilibrium, where $\mathcal{M}_i \subset \{\{0,1\}, \{0\}, \{1\}\}$. For example, $\mathcal{M}_H = \{0,1\}$ means H-buyers hold both token types while $\mathcal{M}_L = \{1\}$ means L-buyers only hold $\mathfrak{p} = 1$ tokens.

Definition 1. The degree of singleness, $\mathcal{S}$, measures the fraction of DM meetings where all balances created in equilibrium, $\mathcal{M}_L \cup \mathcal{M}_H$, are valued the same.[10] The degree of programmability, $\mathcal{P}$, measures the fraction of balances created in equilibrium with $\mathfrak{p} = 1$:

$$\mathcal{P} = \frac{f_L m_{L1} + f_H m_{H1}}{\sum_{\mathfrak{p}=0,1} f_L m_{L\mathfrak{p}} + f_H m_{H\mathfrak{p}}}.$$

3 Equilibrium Characterization with Perfect Recognizability

We first examine the case where the sellers can perfectly recognize token types $\mathfrak{p}$. In DM1, with probability α_e, the seller wants to consume in DM2; with probability $1 - \alpha_e$, the seller wants to consume in CM2. The seller's type is only revealed ex-post, after the DM1 transaction. A portfolio $\mathbf{m}_i = (m_{i0}, m_{i1})$ induces the seller to sell $q_{i1} = m_{i1}(1 - \alpha_e) + m_{i0}$. We first derive exchange values of tokens in each market. In DM2, each token $\mathfrak{p}$ can buy $1 - \mathfrak{p}$ units of q_2. Since $\mathfrak{p} = 1$ tokens are not transferable, they cannot buy anything in DM2. In DM1, each token $\mathfrak{p}$ can buy $1 - \alpha_e + \alpha_e(1 - \mathfrak{p})$ units of q_1. This reflects the loss of singleness as tokens have different exchange values.

[10] Here, we follow Garratt and Shin (2023) to define the concept of singleness in terms of the purchasing power of tokens when they are used as a means of payment, that is, in DM1 and DM2 transactions.

The demand for $\mathfrak{p}$-tokens Let $v_i(\mathbf{m})$ denote the value function of type i buyers holding a portfolio $\mathbf{m}$. The marginal value of a token $\mathfrak{p}$ to a type L buyer in DM1 is

$$\frac{\partial v_L(\mathbf{m}_L)}{\partial m_{L\mathfrak{p}}} = \sigma_L u'(q_{1L})[1-\alpha_e+\alpha_e(1-\mathfrak{p})] + (1-\sigma_L)\varepsilon(1-\mathfrak{p}),$$

where the buyer buys $1-\alpha_e+\alpha_e(1-\mathfrak{p})$ units from a seller in DM1 with probability σ_L, and buys $(1-\mathfrak{p})$ units from a seller in DM2 with probability $1-\sigma_L$ to derive marginal utility ε. In CM1, given the token price $\phi_{\mathfrak{p}}$, a L-buyer's FOC with respect to the quantity $m_{L\mathfrak{p}}$ is

$$-\phi_{\mathfrak{p}} + \frac{\partial v_L(\mathbf{m}_L)}{\partial m_{L\mathfrak{p}}} \le 0.$$

Similarly, the marginal value of a token $\mathfrak{p}$ to a type H is

$$\frac{\partial v_H(\mathbf{m}_H)}{\partial m_{H\mathfrak{p}}} = \sigma_H u'(q_{1H})[1-\alpha_e+\alpha_e(1-\mathfrak{p})] + (1-\sigma_H)u'(q_{2H})(1-\mathfrak{p}).$$

In CM1, the H-buyer's FOC is

$$-\phi_{\mathfrak{p}} + \frac{\partial v_H(\mathbf{m}_H)}{\partial m_{H\mathfrak{p}}} \le 0.$$

The bank supply of $\mathfrak{p}$-tokens Being risk-neutral, competitive bankers supply any amount of p-tokens as long as they break even. The token price, $\phi_{\mathfrak{p}}$, represents the revenue from selling a $\mathfrak{p}$-token in numeraire goods. To back each token, the banker invests x units of numeraire, generating x/β units in CM2. This revenue must cover the banker's commitment to redeem tokens. The zero-profit condition then determines the price of each $\mathfrak{p}$-token as a function of expected redemptions. Then, the zero-profit condition of the banker gives

$$\phi_{\mathfrak{p}} = \beta[\sigma_i(1-\alpha_e+\alpha_e(1-\mathfrak{p})) + (1-\sigma_i)(1-\mathfrak{p})], \tag{1}$$

where the term in [.] is the expected redemption if a $\mathfrak{p}$-token is held solely by type i buyers. Otherwise, if a $\mathfrak{p}$-token is held by both types, then the zero-profit condition of the banker is given by

$$\phi_{\mathfrak{p}} = \beta\frac{1}{f_L m_{L\mathfrak{p}} + f_H m_{H\mathfrak{p}}}\sum_{i=L,H} f_i m_{i\mathfrak{p}}[\sigma_i(1-\alpha_e+\alpha_e(1-\mathfrak{p})) + (1-\sigma_i)(1-\mathfrak{p})]. \tag{2}$$

Proposition 1. *With $\varepsilon < 1$ and $\sigma_L > \sigma_H$, the unique equilibrium with perfect recognizability is such that L-buyers only hold $\mathfrak{p} = 1$-tokens and H-buyers only hold $\mathfrak{p} = 0$-tokens. The equilibrium allocation does not depend on the value of α_e.*

With perfect recognizability, sellers know which token type they are receiving. As a result, sellers produce more for $\mathfrak{p} = 0$-tokens than for $\mathfrak{p} = 1$-tokens. This would induce L-buyers to hold $\mathfrak{p} = 0$-tokens. However, when purchasing from the bank, $\mathfrak{p} = 0$-tokens are more expensive because they are redeemed more often. Since L-buyers derive low utility in DM2 ($\varepsilon < 1$) and rarely consume there ($\sigma_L > \sigma_H$), they prefer the cheaper $\mathfrak{p} = 1$-tokens, which better match their expected consumption needs. Interestingly, the equilibrium allocation does not depend on α_e. Each $\mathfrak{p} = 1$-token can buy $1 - \alpha_e$ units of DM1 goods. As α_e goes up, the $\mathfrak{p} = 1$-tokens are discounted more—but they are also cheaper to create, since they are redeemed less often. This encourages buyers to bring more $\mathfrak{p} = 1$-tokens to maintain their consumption.

Programmability mitigates commitment problems

Our model captures how token programmability helps mitigate commitment problems. For a L-buyer, consuming in DM2 is inefficient because their marginal utility is lower than the marginal production cost. However, without alternative uses, the buyer will spend all tokens in DM2, making it impossible to credibly commit to not spending them. This commitment problem raises the cost of acquiring tokens, as the banker needs to keep more reserves for redemption. Programmed tokens allow buyers to commit to not spending in DM2, lowering acquisition costs and improving welfare by enabling more efficient use of tokens in DM1.

Prohibition of programmable money

Next, motivated by the policy debate discussed in the introduction, we evaluate whether the regulator should prohibit programmable money. In that case, there are only tokens with $\mathfrak{p} = 0$, which function like traditional bank deposits that can be transferred at will. The equilibrium conditions for L- and H-buyers and the banker are given respectively by

$$\begin{aligned}
\phi_0 &= \beta\sigma_L u'(q_{1L}) + \beta(1 - \sigma_L)\varepsilon, \\
\phi_0 &= \beta u'(q_{1H}), \\
\phi_0 &= \beta.
\end{aligned}$$

Since $\varepsilon < 1$, these conditions then imply that $u'(q_{1H}) = 1 < u'(q_{1L})$. L-sellers find these $\mathfrak{p} = 0$-tokens too expensive. Hence, they do not acquire as many and, as a result, they reduce their consumption. Therefore the equilibrium allocation without programmability cannot be optimal. We summarize the results as follows.

Proposition 2. *With perfect recognizability,* $\mathcal{S} = 0$ and $\mathcal{P} = \frac{f_L}{f_L + f_H(1-\alpha_e)}$ *and the first-best allocation is supported. Prohibiting programmability makes* L*-buyers worse off, which reduces social welfare, even though it can fully restore the singleness of money. In this sense, programmability is essential.*

Prohibiting programmable money makes the tokens used by L-buyers more liquid. But they would not benefit from being able to spend it in DM2 (relative to programmed tokens). The reason is that they can no longer pre-commit to not consuming in DM2. Bankers anticipate that all their tokens will be redeemed and they respond by increasing the price (ϕ_0). As a consequence, L-buyers are worse off, since that price is too high relative to their marginal value of consumption in DM2. Hence, we have the following corollary.

Corollary 1. *Singleness is neither necessary nor sufficient for achieving efficiency.*

Discussion of various model features

Before proceeding, we briefly discuss key assumptions and features of the model to clarify their roles in generating the main results. The objective is to provide a simple model that: (i) captures the benefits of programmable tokens and monetary singleness, and (ii) highlights how the desirability of programmability depends on the trade-off between information and commitment frictions. To focus on these aspects, we use a stylized model that prioritizes transparency at the cost of abstracting from less essential considerations.

- Finite life: We study the commitment problem of L-buyers who, in DM2, do not care about their future. For simplicity, buyers have finite lives, but the model could be extended to infinite-lived agents facing exit shocks, which generate the same commitment problem.

- Buyers' preference shocks: The preference shock parameter σ_L captures the severity of the commitment problem. The problem is more acute when σ_L falls. We assume $\sigma_H < \sigma_L$ so that programmed tokens are cheaper for banks to create. This assumption underpins the welfare-improving role of programmability. The condition $\varepsilon < 1$ helps generate L-buyers' incentive to over-consume in DM2 in the simplest way possible.

- Sellers' linear preference: Assuming sellers have linear utility in DM2 leads to the result that the first-best allocation can be supported when tokens are perfectly recognizable. Without this, programmability can disrupt sellers' consumption smoothing. See an example in the Appendix where sellers have a trade surplus in DM2. Note that the main result of the paper is robust:

programmability remains welfare-improving, and there is still a trade-off between commitment and information frictions.

- Storage technology: We assume a return rate of $1/\beta$ to support first-best allocations. Without this, standard cash-in-advance distortions would appear, which we abstract from to focus on programmability and singleness.

- Programmable payments: The commitment-singleness trade-off could be avoided if buyers used programmable payments instead of programmable money. If transfer restrictions disappeared once balances reached sellers, sellers would not discount programmed tokens. However, buyers could exploit the system by first transferring funds to a secret wallet. This highlights that the trade-off arises only if programmability constrains not only the original users but also future users.

- Flexibility in modeling programmability: We capture programmability via time-dependent tokens, but similar results would hold under good-dependent, recipient-dependent, or state-dependent designs.

4 Imperfect Recognizability

In this section, we consider the case where tokens can be programmed, but a fraction π of DM1 sellers cannot observe the token type $\mathfrak{p}$. These uninformed sellers might want to infer buyer through contractual terms, but this is infeasible because all buyers active in DM1 derive the same marginal utility from consumption and have identical continuation values from holding tokens. For simplicity, we also assume that trade size cannot be used to separate types, as each buyer purchases a fixed quantity from many different sellers.[11] When sellers face unknown tokens, they naturally value them based on the population average. Specifically, a unit of unknown token can induce an uninformed seller to sell $q_1^\pi = (1-\alpha_e) + \alpha_e(1-\tilde{\mathfrak{p}})$ units of DM1 goods. This reflects the expected payoffs of consuming a unit in CM2 plus the expected payoff of consuming in DM2, given that the fraction of transferable tokens is

$$1-\tilde{\mathfrak{p}} = 1-\mathcal{P} = \frac{f_L m_{L0} + f_H m_{H0}}{\sum_{\mathfrak{p}=0,1} f_L m_{L\mathfrak{p}} + f_H m_{H\mathfrak{p}}}.$$

[11] In the Appendix, we relax this assumption and allow trade size to signal buyer types, introducing a signaling game between buyers and uninformed sellers. Under certain conditions, a separating equilibrium exists where H-buyers use unprogrammed money and over-consume, while L-buyers use programmed money and consume efficiently. As with the pooling equilibrium, imperfect recognizability leads to inefficiency.

Then, the marginal value of a token $\mathfrak{p}$ to a L-buyer in the DMs is

$$\begin{aligned}\frac{\partial v_L(\mathbf{m}_L)}{\partial m_{L\mathfrak{p}}} &= \sigma_L u'(q_{1L})(1-\pi)\left[1-\alpha_e+\alpha_e(1-\mathfrak{p})\right] \\ &\quad +\sigma_L u'(q_{1L}^{\pi})\pi\left[1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})\right]+(1-\sigma_L)\varepsilon(1-\mathfrak{p}).\end{aligned}$$

In CM1, given the price of token $\mathfrak{p}$, $\phi_{\mathfrak{p}}$, a L-buyer's FOC with respect to the quantity of $m_{L\mathfrak{p}}$ is

$$-\phi_{\mathfrak{p}}+\frac{\partial v_L(\mathbf{m}_L)}{\partial m_{L\mathfrak{p}}}\leq 0.$$

The marginal value of a token $\mathfrak{p}$ to a H-buyer in the DMs is

$$\begin{aligned}\frac{\partial v_H(\mathbf{m}_H)}{\partial m_{H\mathfrak{p}}} &= \sigma_H u'(q_{1H})(1-\pi)\left[1-\alpha_e+\alpha_e(1-\mathfrak{p})\right] \\ &\quad +\sigma_H u'(q_{1H}^{\pi})\pi\left[1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})\right]+(1-\sigma_H)u'(q_{2H})(1-\mathfrak{p}).\end{aligned}$$

In CM1, given the price of token $\mathfrak{p}$, $\phi_{\mathfrak{p}}$, a H-buyer's FOC with respect to the quantity of $m_{H\mathfrak{p}}$ is

$$-\phi_{\mathfrak{p}}+\frac{\partial v_H(\mathbf{m}_H)}{\partial m_{H\mathfrak{p}}}\leq 0.$$

Comparing these conditions with those in the previous section, we notice that the information problem tends to increase the marginal value of a programmed token and decrease the marginal value of an unprogrammed token. In other words, issuing an unprogrammed token "cross-subsidizes" the use of a programmed token when there are uninformed sellers who want to consume early. This effect distorts consumption in DM1 and token creation in CM1. Next, we show that it is still an equilibrium that L-buyers only hold $\mathfrak{p}=1$-tokens and H-buyers only hold $\mathfrak{p}=0$-tokens.

Proposition 3. *By continuity, for π not too big, $\mathcal{M}_H=\{0\}$, $\mathcal{M}_L=\{1\}$ is an equilibrium of the economy with imperfect recognizability.*

The result in Proposition 3 is intuitive. If the adverse selection problem in DM1 is not too severe (π is small), the expected price of a token will not differ too much from the price of the same token in the equilibrium with perfect recognizability. Therefore, the incentives of H- and L-buyers to only hold one type of token are preserved.

Given that the information problem distorts consumption in DM1, it may be socially optimal to restrict the use of programmed tokens under certain conditions. Focusing on this equilibrium, we examine how the welfare impacts of prohibiting programmability depends on the degree of information frictions (captured by π) and commitment frictions (captured by σ_L).

Proposition 4. *In the equilibrium with $\mathcal{M}_H=\{0\}$ and $\mathcal{M}_L=\{1\}$, prohibiting programmability reduces welfare for π small enough, but increases welfare for σ_L large enough.*

Intuitively, it is optimal to allow programming when tokens are easy to recognize and when users cannot easily commit to future actions. One may argue that this is the case for a permissionless blockchain where digital tokens can be readily verified and priced on chain while anonymous users can hardly make binding promises.

5 Gresham's Law: Over-creation of Programmed Tokens

In Section 4, we focus on the case where buyers' equilibrium token sets remain unchanged. In this section, we examine the general case and further explore how informational frictions can distort buyers' incentives and induce them to over-create programmed tokens. We focus on the case of log utility in order to obtain analytical results. We show in the Appendix that the equilibrium portfolio choices must be characterized by one of the following two cases:

- separating equilibrium: $\mathcal{M}_{\mathrm{H}} = \{0\}$, $\mathcal{M}_{\mathrm{L}} = \{1\}$
- mixing equilibrium: $\mathcal{M}_{\mathrm{H}} = \{0, 1\}$, $\mathcal{M}_{\mathrm{L}} = \{1\}$

In the separating case, buyers specialize in their token holdings as before, while in the mixing case, H-buyers choose to hold both programmed and unprogrammed tokens. This shows the following result.

Proposition 5. *When*

$$\pi \leq \bar{\pi} \equiv \frac{(\sigma_L - \sigma_H)(1 - \alpha_e)}{\alpha_e \sigma_H},$$

the unique equilibrium is "separating": $\mathcal{M}_{\mathrm{H}} = \{0\}$, $\mathcal{M}_{\mathrm{L}} = \{1\}$. *When* $\pi > \bar{\pi}$, *the unique equilibrium is "mixing":* $\mathcal{M}_{\mathrm{H}} = \{0, 1\}$, $\mathcal{M}_{\mathrm{L}} = \{1\}$.

Interestingly, when information frictions are sufficiently severe, H-buyers are induced to hold programmed tokens even though they have no commitment problems. They do so to exploit the lack of information and pool their tokens with others. This mechanism resembles a version of Gresham's law, where agents over-create tokens with inflated value. With imperfect recognizability, the degree of singleness, $\mathcal{S}$, is given by π, while programmability is given by $\tilde{\mathfrak{p}}$.

To illustrate the equilibrium effects of changing π, Figure 2 presents a numerical example. For $\pi \in (0, 0.1)$, a separating equilibrium emerges where token prices remain constant as π rises (plots i and ii). Here, H-buyers cross-subsidize L-buyers in uninformed meetings, leading to H-buyers' under-consumption and L-buyers' over-consumption (plots vii and xi), which reduces overall welfare (plot iv).

For $\pi \in (0.1, 1)$, a mixing equilibrium occurs, where H-buyers shift their portfolios towards more programmed tokens, consistent with Gresham's law (plots viii and ix). This results in under-consumption by H-sellers in DM2 meetings (plot xii). As $\sigma_H < \sigma_L$, the portfolio change reduces ϕ_1 (plot i), inducing L-buyers to acquire more programmed tokens and over-consume in informed DM1 meetings (plot vi). Welfare eventually falls below the level without programmability (plot iv, dash line).

This example highlights that prohibiting programmability to preserve monetary singleness is not always optimal. Such policy improves welfare only when information frictions dominate commitment frictions.

6 Conclusion

This paper studies an economy where programmable tokens arise endogenously to mitigate commitment problems. While programmability may threaten monetary singleness, its social desirability depends on the trade-off between commitment and information frictions. We show that singleness is neither necessary nor sufficient for efficiency. Programmability is optimal when tokens are easily recognized and users cannot commit to future actions—a setting resembling permissionless blockchains. More broadly, our findings caution policymakers against relying on lessons from the free banking era when designing future monetary systems, given the fundamentally different technologies and frictions involved.

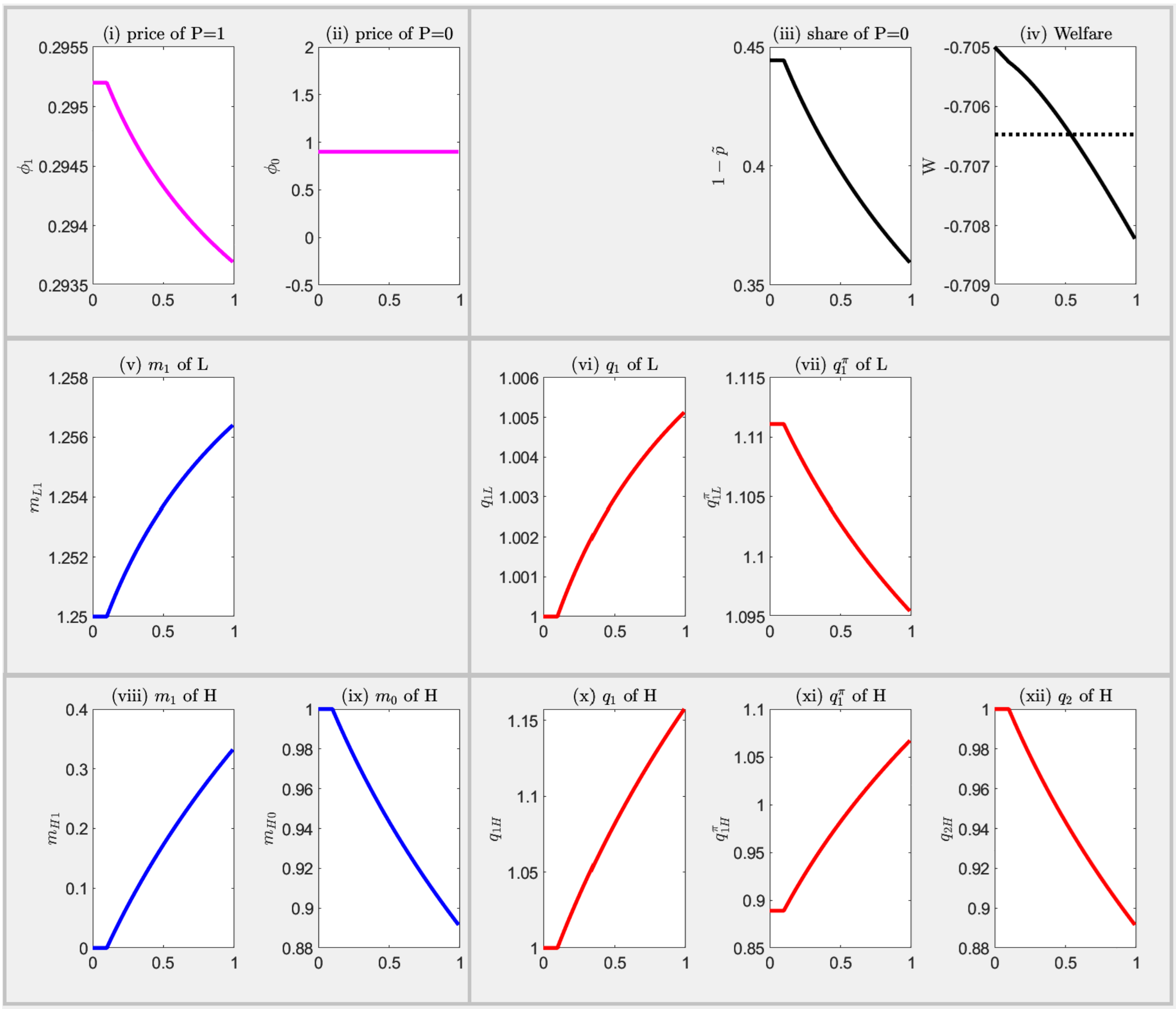

Figure 2: Equilibrium Effects of π ($\alpha_e = 0.2, \sigma_L = 0.41, \sigma_H = 0.4, \beta = 0.9, f_L = 0.5, \varepsilon = 0.995$)

Appendix

A. Proof of Proposition 1:

Proof. Since $\mathcal{M}_{\mathrm{i}} = \{0\}$,$\{1\}$, or $\{0,1\}$ for $i = H, L$, there are potentially nine equilibrium outcomes. Obviously, H-buyers holding only $\mathfrak{p}_1$ is not an equilibrium because $q_{2H} = 0$ and, for any finite ϕ_0, H-buyers have an incentive to hold some $\mathfrak{p}_0$. If there are initially no $\mathfrak{p}_0$ tokens, bankers can make a profit by creating some. Hence, we only need to consider six remaining cases.

Case (i): $\mathcal{M}_{\mathrm{H}} = \{0\}$, $\mathcal{M}_{\mathrm{L}} = \{1\}$

The equilibrium conditions for L- and H- buyers and the banker are given by

$$\begin{aligned}
\phi_1 &= \beta\sigma_L u'(q_{1L})(1-\alpha_e) \\
\phi_0 &= \beta\sigma_H u'(q_{1H}) + \beta(1-\sigma_H)u'(q_{2H}) \\
\phi_0 &= \beta \\
\phi_1 &= \beta\sigma_L(1-\alpha_e).
\end{aligned}$$

Since $q_{1H} = q_{2H} \equiv q_H$, we have $\phi_0 = \beta u'(q_H)$ or $u'(q_H) = 1$. H-buyers do not hold $\mathfrak{p}_1$ if $\sigma_L > \sigma_H$. Also, L-buyers do not hold $\mathfrak{p}_0$if $1 > \varepsilon$.

$$\phi_0 > \beta\sigma_L u'(q_{1L}) + \beta(1-\sigma_L)\varepsilon$$

Hence, this is an equilibrium.

Case (ii): $\mathcal{M}_{\mathrm{H}} = \{0\}$, $\mathcal{M}_{\mathrm{L}} = \{0\}$

The equilibrium conditions are

$$\begin{aligned}
\phi_0 &= \beta\sigma_L u'(q_{1L}) + \beta(1-\sigma_L)\varepsilon \\
\phi_0 &= \beta\sigma_H u'(q_{1H}) + \beta(1-\sigma_H)u'(q_{2H}) \\
\phi_0 &= \beta \\
q_{1H} &= q_{2H} \equiv q_H.
\end{aligned}$$

Hence we have

$$1 = u'(q_H) = \sigma_L u'(q_{1L}) + (1-\sigma_L)\varepsilon.$$

We now check the incentives to offer $\mathfrak{p}_1$ to serve type L only. L-buyers hold it if

$$\phi_1 \leq \beta(1-(1-\sigma_L)\varepsilon)(1-\alpha_e).$$

H-buyers do not hold it if

$$\phi_1 > \beta \sigma_H u'(q_H)(1-\alpha_e) = \beta \sigma_H (1-\alpha_e).$$

And the banker makes non-zero profit if

$$\phi_1 > \beta \sigma_L (1-\alpha_e).$$

Since $\sigma_L > \sigma_H$, it is profitable to introduce $\mathfrak{p}_1$ iff $1 > \varepsilon$. Since the proposed equilibrium can be disturbed, this is not an equilibrium.

Case (iii): $\mathcal{M}_{\mathrm{H}} = \{0\}$, $\mathcal{M}_{\mathrm{L}} = \{0,1\}$

The equilibrium conditions are

$$\begin{aligned}
\phi_1 &= \beta \sigma_L u'(q_{1L})(1-\alpha_e) \\
\phi_0 &= \beta \sigma_L u'(q_{1L}) + \beta(1-\sigma_L)\varepsilon \\
\phi_0 &= \beta \sigma_H u'(q_{1H}) + \beta(1-\sigma_H) u'(q_{2H}) \\
\phi_0 &= \beta \\
\phi_1 &= \beta \sigma_L (1-\alpha_e).
\end{aligned}$$

These conditions imply that

$$1 = \sigma_L + (1-\sigma_L)\varepsilon,$$

which contracts with the assumption that $\varepsilon < 1$. So this is not an equilibrium.

Case (iv): $\mathcal{M}_{\mathrm{H}} = \{0,1\}$, $\mathcal{M}_{\mathrm{L}} = \{1\}$

The equilibrium conditions are

$$\begin{aligned}
\phi_1 &= \beta \sigma_L u'(q_{1L})(1-\alpha_e) \\
\phi_1 &= \beta \sigma_H u'(q_{1H})(1-\alpha_e) \\
\phi_0 &= \beta \sigma_H u'(q_{1H}) + \beta(1-\sigma_H) u'(q_{2H}) = \frac{\phi_1}{(1-\alpha_e)} + \beta(1-\sigma_H) u'(q_{2H}) \\
\phi_0 &= \beta \\
\phi_1 &= \beta \frac{f_L m_L \sigma_L + f_H m_H \sigma_H}{f_L m_L + f_H m_H}(1-\alpha_e).
\end{aligned}$$

Note that the last condition implies that

$$\phi_1 > \beta \sigma_H (1-\alpha_e),$$

which, together with the second FOC above, imply that

$$u'(q_{1H}) > 1.$$

But the third FOC above also implies that

$$u'(q_{2H}) < 1.$$

This contradicts with the fact that

$$q_{1H} \geq q_{2H}.$$

So this is not an equilibrium.

Case (v): $\mathcal{M}_{\mathrm{H}} = \{0, 1\}$, $\mathcal{M}_{\mathrm{L}} = \{0\}$

The equilibrium conditions are

$$\begin{aligned}
\phi_0 &= \beta\sigma_L u'(q_{1L}) + \beta(1-\sigma_L)\varepsilon \\
\phi_1 &= \beta\sigma_H u'(q_{1H})(1-\alpha_e) \\
\phi_0 &= \beta\sigma_H u'(q_{1H}) + \beta(1-\sigma_H)u'(q_{2H}) = \frac{\phi_1}{(1-\alpha_e)} + \beta(1-\sigma_H)u'(q_{2H}) \\
\phi_0 &= \beta \\
\phi_1 &= \beta\sigma_H(1-\alpha_e).
\end{aligned}$$

The last three conditions imply that

$$u'(q_{2H}) = 1.$$

The first FOC implies that

$$u'(q_{1L}) > 1.$$

Finally, the fact that L-buyers do not hold $\mathfrak{p}_1$ requires that

$$1 > \frac{\sigma_H}{\sigma_L} > u'(q_{1L}),$$

but this contradicts with the condition above. So this is not an equilibrium.

Case (vi): $\mathcal{M}_{\mathrm{H}} = \{0, 1\}$, $\mathcal{M}_{\mathrm{L}} = \{0, 1\}$

The equilibrium conditions are

$$\begin{aligned}
\phi_1 &= \beta\sigma_L u'(q_{1L})(1-\alpha_e) \\
\phi_0 &= \beta\sigma_L u'(q_{1L}) + \beta(1-\sigma_L)\varepsilon \\
\phi_1 &= \beta\sigma_H u'(q_{1H})(1-\alpha_e) \\
\phi_0 &= \beta\sigma_H u'(q_{1H}) + \beta(1-\sigma_H)u'(q_{2H}) \\
\phi_0 &= \beta \\
\phi_1 &= \beta\frac{f_L m_L \sigma_L + f_H m_H \sigma_H}{f_L m_L + f_H m_H}(1-\alpha_e).
\end{aligned}$$

The first four conditions imply that

$$1 > u'(q_{2H}) \geq u'(q_{1H}),$$

but this contradicts with the condition that

$$\beta = \phi_0 = \beta\sigma_H u'(q_{1H}) + \beta(1-\sigma_H)u'(q_{2H}).$$

So this is not an equilibrium.

In conclusion, the unique equilibrium portfolio is Case (i): $\mathcal{M}_{\mathrm{H}} = \{0\}$, $\mathcal{M}_{\mathrm{L}} = \{1\}$. Since $u'(q_{1H}) = u'(q_{1L}) = u'(q_{2H}) = 1$ and $q_{2L} = 0$, the first-best allocation is achieved. □

B. Proof of Proposition 3

Proof. Consider an equilibrium with $\mathcal{M}_{\rm H} = \{0\}$, $\mathcal{M}_{\rm L} = \{1\}$. The equilibrium conditions are

$$\begin{aligned}
\phi_1 &= \beta\sigma_L u'(q_{1L})(1-\pi)(1-\alpha_e) + \beta\sigma_L u'(q_{1L}^{\pi})\pi\left[1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})\right],\\
\phi_0 &= \beta\sigma_H u'(q_{1H})(1-\pi) + \beta\sigma_H u'(q_{1H}^{\pi})\pi\left[1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})\right] + \beta(1-\sigma_H)u'(q_{2H}),\\
\phi_0 &= \beta,\\
\phi_1 &= \beta\sigma_L(1-\alpha_e),\\
1-\tilde{\mathfrak{p}} &= \frac{f_H m_{H0}}{f_L m_{L1} + f_H m_{H0}}.
\end{aligned}$$

Since H-buyers only hold $\mathfrak{p} = 0$-tokens, $q_{1H} = q_{2H} \equiv q_H$. Since they hold m_{H0} units of $\mathfrak{p} = 0$-tokens, $q_H = m_{H0}$. However, when they meet an uninformed seller in DM1, they can only obtain $m_{H0}\left[1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})\right]$ units of consumption. Therefore,

$$q_{1H} = q_{2H} = \frac{q_{1H}^{\pi}}{1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})} > q_{1H}^{\pi}.$$

In contrast, L-buyers only hold $\mathfrak{p} = 1$-tokens. Their consumption in DM1 is higher when they meet an uninformed seller (relative to when they meet an informed one) because the uninformed seller values the token at the average value. Therefore,

$$q_{1L} = m_{L1}(1-\alpha_e) < m_{L1}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) = q_{1L}^{\pi}.$$

To verify that this is an equilibrium, we need to check that the FOCs are satisfied. First, L-buyers do not hold $\mathfrak{p} = 0$-tokens:

$$1 > \sigma_L u'(q_{1L})(1-\pi) + \sigma_L u'(q_{1L}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + (1-\sigma_L)\varepsilon. \tag{3}$$

Note that the FOC of L-buyers given ϕ_1 implies that

$$\begin{aligned}
&\sigma_L u'(q_{1L})(1-\pi) + \sigma_L u'(q_{1L}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\\
=&\sigma_L(1-\alpha_e) + \alpha_e\sigma_L u'(q_{1L})(1-\pi).
\end{aligned}$$

Using this result, inequality (3) becomes

$$1 > \sigma_L(1-\alpha_e) + \alpha_e\sigma_L u'(q_{1L})(1-\pi) + (1-\sigma_L)\varepsilon. \tag{4}$$

Also, from the low type's FOC, we know that

$$1 > u'(q_{1L})(1-\pi).$$

Therefore we can bound the RHS of(4),

$$\begin{aligned}
&\sigma_L(1-\alpha_e)+\alpha_e\sigma_L u'(q_{1L})(1-\pi)+(1-\sigma_L)\varepsilon\\
<&\sigma_L(1-\alpha_e)+\alpha_e\sigma_L+(1-\sigma_L)\varepsilon\\
=&\sigma_L+(1-\sigma_L)\varepsilon\\
<&1.
\end{aligned}$$

This shows that (4) and therefore (3) always hold. Hence L-buyers have no incentives to hold $\mathfrak{p}=0$-tokens. Next, we also need to show that H-buyers have no incentive to hold $\mathfrak{p}=1$-tokens. This is the case if π is low enough so that

$$\phi_1>\beta\sigma_H u'(q_{1H})(1-\pi)(1-\alpha_e)+\beta\sigma_H u'(q_{1H}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})).$$

$\square$

C. Proof of Proposition 4

Proof. When $\pi = 0$, the first-best allocation is supported with programmability and is not supported without it. By the continuing existence of $\mathcal{M}_{\mathrm{H}} = \{0\}$, $\mathcal{M}_{\mathrm{L}} = \{1\}$ equilibrium with imperfect recognizability when π is not too large, welfare with programmability is close to the first best welfare with $\pi = 0$. In particular, prohibiting programmability would create a first order loss in informed meetings by moving away from the first allocations in those meetings. It would generate only a second order gain by shifting the allocation in uninformed meetings, because there are few uninformed meetings when π is small. We now examine the effect of σ_L in this equilibrium. When there is no programmability, the social welfare is

$$\tilde{W} = f_L[\sigma_L W_{1L} + (1-\sigma_L)W_{2L}] + f_H[\sigma_H W_{1H} + (1-\sigma_H)W_{2H}],$$

where

$$\begin{aligned}
W_{1L} &= u(q_{1L}) - q_{1L}, \\
W_{2L} &= q_{2L}(\varepsilon - 1), \\
W_{1H} &= u(q_{1H}) - q_{1H}, \\
W_{2H} &= u(q_{2H}) - q_{2H}.
\end{aligned}$$

The equilibrium conditions imply

$$\begin{aligned}
\phi_0 &= \beta\sigma_L u'(q_{1L}) + \beta(1-\sigma_L)\varepsilon, \\
\phi_0 &= \beta\sigma_H u'(q_{1H}) + \beta(1-\sigma_H)u'(q_{2H}), \\
\phi_0 &= \beta.
\end{aligned}$$

Hence, we have

$$1 = u'(q_{1H}) = u'(q_{2H}) = \sigma_L u'(q_{1L}) + (1-\sigma_L)\varepsilon,$$

implying that $q_{1H} = q_H^*$ and q_{1L} is arbitrarily close to q_{1L}^* as $\sigma_L \to 1$. As a result, $\tilde{W}$ approaches its first-best level as $\sigma_L \to 1$. $\square$

When $\sigma_L = 1$, the welfare with programmability is

$$\bar{W} = f_L[(1-\pi)W_{1L} + \pi W_{1L}^{\pi}] + f_H[\sigma_H(1-\pi)W_{1H} + \sigma_H \pi W_{1H}^{\pi} + (1-\sigma_H)W_{2H}],$$

with

$$
\begin{aligned}
W_{1L} &= u(q_{1L}) - q_{1L}, \\
W_{1L}^{\pi} &= u(q_{1L}^{\pi}) - q_{1L}^{\pi}, \\
W_{1H} &= u(q_{1H}) - q_{1H}, \\
W_{1H}^{\pi} &= u(q_{1H}^{\pi}) - (q_{1H}^{\pi}), \\
W_{2H} &= u(q_{2H}) - q_{2H}.
\end{aligned}
$$

Note that

$$
\begin{aligned}
q_{1L} &= m_{L1}(1 - \alpha_e) \\
q_{1L}^{\pi} &= m_{L1}(1 - \alpha_e + \alpha_e(1 - \tilde{\mathfrak{p}})) \\
q_{1H} &= m_{H0} \\
q_{2H} &= m_{H0} \\
q_{1H}^{\pi} &= m_{H0}(1 - \alpha_e + \alpha_e(1 - \tilde{\mathfrak{p}})),
\end{aligned}
$$

implying that

$$
\begin{aligned}
q_{1L}^{\pi} &= q_{1L}\frac{1 - \alpha_e + \alpha_e(1 - \tilde{\mathfrak{p}})}{1 - \alpha_e} \\
q_{1H}^{\pi} &= q_{1H}(1 - \alpha_e + \alpha_e(1 - \tilde{\mathfrak{p}})) = q_{2H}(1 - \alpha_e + \alpha_e(1 - \tilde{\mathfrak{p}})).
\end{aligned}
$$

Hence, whenever $\tilde{\mathfrak{p}} < 1$, some quantities are not at their first-best levels. Therefore, $\bar{W}$ is lower than its first-best level when $\sigma_L = 1$. By continuity, this is true for $\sigma_L$close to 1.

D. Proof of Proposition 5

Proof. **Step 1: We first show that, with imperfect recognizability and CRRA preferences, Cases (i) and (iv) are equilibrium portfolio choices.**

CASE (i) : Consider an equilibrium with $\mathcal{M}_{\mathbf{H}} = \{0\}$, $\mathcal{M}_{\mathbf{L}} = \{1\}$

The consumption levels are then

$$
\begin{aligned}
q_{1H} &= m_{H0} \\
q_{1H}^{\pi} &= m_{H0}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
q_{2H} &= m_{H0} \\
q_{1L} &= m_{L1}(1-\alpha_e) \\
q_{1L}^{\pi} &= m_{L1}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
q_{2L} &= 0.
\end{aligned}
$$

The equilibrium conditions for L- and H-buyers and the banker are given by

$$
\begin{aligned}
\phi_1 &= \beta\sigma_L u'(q_{1L})(1-\pi)(1-\alpha_e) + \beta\sigma_L u'(q_{1L}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
\phi_0 &= \beta\sigma_H u'(q_{1H})(1-\pi) + \beta\sigma_H u'(q_{1H}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_H)u'(q_{2H}) \\
\phi_0 &= \beta \\
\phi_1 &= \beta\sigma_L(1-\alpha_e) \\
1-\tilde{\mathfrak{p}} &= \frac{f_H m_{H0}}{f_L m_{L1} + f_H m_{H0}}.
\end{aligned}
$$

Since $m_{H0} = q_{1H}$ and $(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\, m_{H0} = q_{1H}^{\pi}$, we have

$$
q_{1H} = \frac{q_{1H}^{\pi}}{1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})}.
$$

Since $q_{1H} = q_{2H} \equiv q_H$, we have

$$
q_{1H} = q_{2H} = \frac{q_{1H}^{\pi}}{1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})}.
$$

First, L-buyers have no incentives to hold $\mathfrak{p}_0$:

$$
\phi_0 > \beta\sigma_L u'(q_{1L})(1-\pi) + \beta\sigma_L u'(q_{1L}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_L)\varepsilon
$$

or

$$
1 > \sigma_L u'(q_{1L})(1-\pi) + \sigma_L u'(q_{1L}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + (1-\sigma_L)\varepsilon
$$

Note that the FOC of the low type given ϕ_1 implies that (setting $\mathfrak{p} = 0$):

$$\begin{aligned} -\phi_{\mathfrak{p}} + \beta\sigma_L u'(q_{1L})(1-\pi)(1-\alpha_e) + \beta\sigma_L u'(q_{1L}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) &= 0 \\ -\sigma_L(1-\alpha_e) + \sigma_L u'(q_{1L})(1-\pi)(1-\alpha_e) + \sigma_L u'(q_{1L}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) &= 0, \end{aligned}$$

so

$$\sigma_L u'(q_{1L})(1-\pi)(1-\alpha_e) + \sigma_L u'(q_{1L}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) = \sigma_L(1-\alpha_e)$$

$$\begin{aligned} &\sigma_L u'(q_{1L})(1-\pi) + \sigma_L u'(q_{1L}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\ =&\sigma_L(1-\alpha_e) + \alpha_e\sigma_L u'(q_{1L})(1-\pi). \end{aligned}$$

Using this result, the above condition becomes

$$1 > \sigma_L(1-\alpha_e) + \alpha_e\sigma_L u'(q_{1L})(1-\pi) + (1-\sigma_L)\varepsilon.$$

Also, from the low type's FOC, we know that

$$\begin{aligned} \beta\sigma_L(1-\alpha_e) &> \beta\sigma_L u'(q_{1L})(1-\pi)(1-\alpha_e) \\ \Rightarrow 1 &> u'(q_{1L})(1-\pi). \end{aligned}$$

Therefore, the RHS of the above condition is

$$\begin{aligned} &\sigma_L(1-\alpha_e) + \alpha_e\sigma_L u'(q_{1L})(1-\pi) + (1-\sigma_L)\varepsilon \\ <&\sigma_L(1-\alpha_e) + \alpha_e\sigma_L + (1-\sigma_L)\varepsilon \\ =&\sigma_L + (1-\sigma_L)\varepsilon \\ <&1. \end{aligned}$$

Hence, the low type has no incentives to hold $\mathfrak{p}_0$.

Next, H-buyers have no incentives to hold $\mathfrak{p}_1$ if

$$\phi_1 > \beta\sigma_H u'(q_{1H})(1-\pi)(1-\alpha_e) + \beta\sigma_H u'(q_{1H}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})).$$

This requires

$$\begin{aligned} \beta\sigma_L(1-\alpha_e) &> \underbrace{\beta\sigma_H u'(q_{1H})(1-\pi)(1-\alpha_e) + \beta\sigma_H u'(q_{1H}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))}_{=\phi_0-\beta(1-\sigma_H)u'(q_{2H})} \\ \sigma_L(1-\alpha_e) + (1-\sigma_H)u'(q_{2H}) &> 1 \end{aligned}$$

Notice that (FOC H):

$$
\begin{aligned}
1 &= u'(q_{2H}) - \pi\sigma_H \left[u'(q_{2H}) - u'(q_{1H}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\right] \\
1 &= u'(q_{2H}) - \pi\sigma_H \left[u'(q_{2H}) - u'(q_{2H}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})))(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\right] \\
1 &= u'(q_{2H}) - \frac{\pi\sigma_H}{q_{2H}} \left[u'(q_{2H})q_{2H} - u'(q_{2H}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})))q_{2H}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\right]
\end{aligned}
$$

$$
\begin{aligned}
1 &= u'(q_{1H}) - \pi\sigma_H \left[u'(q_{2H}) - u'(q_{1H}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\right] \\
1 &= u'(q_{1H}) \left[1 - \pi\sigma_H + \pi\sigma_H(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]
\end{aligned}
$$

Since u is concave, $u''(q) < 0$ for all q. Suppose the coefficient of relative risk aversion is less than 1. Then, $u'(x)x$ is increasing. Therefore, $u'(\alpha q)\alpha q < u'(q)q$ for all $\alpha < 1$. In this case (or in the homothetic case),

$$u'(q_{2H}) \geq 1.$$

Hence H has no incentive to hold $\mathfrak{p}_1$ whenever

$$
\begin{aligned}
\beta\sigma_L(1-\alpha_e) &> \beta\sigma_H u'(q_{1H}) \left[(1-\pi)(1-\alpha_e) + \pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right] \\
\frac{\sigma_L(1-\alpha_e)}{\sigma_H} &> \frac{\left[(1-\pi)(1-\alpha_e) + \pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]}{\left[1-\pi\sigma_H+\pi\sigma_H(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]}
\end{aligned}
$$

Since $\tilde{\mathfrak{p}} < 1$ and does not go to 1 as $\alpha_e \to 1$ (if anything $\tilde{\mathfrak{p}} \to 0$ in that case), the inequality above shows the conjecture that for α_e sufficiently high, this equilibrium no longer exists because ϕ_1 becomes so low that H-buyers choose to hold some $\mathfrak{p}_1$ tokens.

CASE (ii) : Consider an equilibrium with $\mathcal{M}_{\mathbf{H}} = \{0\}$, $\mathcal{M}_{\mathbf{L}} = \{0\}$

The consumption levels are then

$$
\begin{aligned}
q_{1H} &= q_{1H}^{\pi} = q_{2H} = m_{H0} \\
q_{1L} &= q_{1L}^{\pi} = q_{2L} = m_{L0}.
\end{aligned}
$$

The equilibrium conditions for L- and H-buyers and the banker are given by

$$\phi_0 = \beta\sigma_L u'(q_{1L}) + \beta(1-\sigma_L)\varepsilon$$

$$\phi_0 = \beta u'(q_{1H})$$

$$\phi_0 = \beta$$

$$\tilde{\mathfrak{p}} = 0.$$

We now check the incentives to offer $\mathfrak{p}_1$ to serve L-buyers. They have an incentive to hold if

$$\phi_1 \leq \beta\sigma_L u'(q_{1L})(1-\pi)(1-\alpha_e) + \beta\sigma_L u'(q_{1L})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})).$$

So,

$$\begin{aligned}
\phi_1 &\leq \beta\sigma_L u'(q_{1L})\left[(1-\alpha_e)+\pi\alpha_e(1-\tilde{\mathfrak{p}})\right] \\
\Rightarrow \phi_1 &\leq \beta(1-(1-\sigma_L)\varepsilon)\left[(1-\alpha_e)+\pi\alpha_e(1-\tilde{\mathfrak{p}})\right].
\end{aligned}$$

H-buyers have no incentives to hold if

$$\begin{aligned}
\phi_1 &> \beta\sigma_H u'(q_{1H})(1-\pi)(1-\alpha_e) + \beta\sigma_H u'(q_{1H})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
&> \beta\sigma_H u'(q_{1H})\left[(1-\alpha_e)+\pi\alpha_e(1-\tilde{\mathfrak{p}}))\right].
\end{aligned}$$

And the banker makes non-zero profit if

$$\phi_1 > \beta\sigma_L(1-\alpha_e).$$

It is profitable to introduce $\mathfrak{p}_1$ iff

$$\begin{aligned}
\beta(1-(1-\sigma_L)\varepsilon)\left[(1-\alpha_e)+\pi\alpha_e(1-\tilde{\mathfrak{p}})\right] &> \beta\sigma_L(1-\alpha_e) \\
(1-\varepsilon+\sigma_L\varepsilon)\left[(1-\alpha_e)+\pi\alpha_e(1-\tilde{\mathfrak{p}})\right] &> \sigma_L(1-\alpha_e).
\end{aligned}$$

In the worst case scenario $\tilde{\mathfrak{p}}=1$, then it is profitable to introduce $\mathfrak{p}_1$ whenever

$$1 \geq \varepsilon,$$

which is always the case. So $\mathcal{M}_H=\{0\}$, $\mathcal{M}_L=\{0\}$ cannot be an equilibrium.

CASE (iii): Consider an equilibrium with $\mathcal{M}_{\mathbf{H}}=\{0\}$, $\mathcal{M}_{\mathbf{L}}=\{0,1\}$

The consumption levels are then

$$\begin{aligned}
q_{1H} &= m_{H0} \\
q_{1H}^{\pi} &= m_{H0}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
q_{2H} &= m_{H0} \\
q_{1L} &= m_{L0}+m_{L1}(1-\alpha_e) \\
q_{1L}^{\pi} &= (m_{L0}+m_{L1})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
q_{2L} &= m_{L0}.
\end{aligned}$$

The equilibrium conditions for L- and H- buyers and the banker are given by

$$\phi_0 = \beta\sigma_L(1-\pi)u'(q_{1L}) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_L)\varepsilon$$
$$\phi_1 = \beta\sigma_L(1-\pi)u'(q_{1L})(1-\alpha_e) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))$$
$$\phi_0 = \beta\sigma_H(1-\pi)u'(q_{1H}) + \beta\sigma_H u'(q_{1H}^{\pi})\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_H)u'(q_{2H})$$
$$\phi_0 = \beta$$
$$\phi_1 = \beta\sigma_L(1-\alpha_e)$$
$$1-\tilde{\mathfrak{p}} = \frac{f_H m_{H0} + f_L m_{L0}}{f_L m_{L1} + f_L m_{L0} + f_H m_{H0}} > 0.$$

Notice (important for below) that the second FOC implies

$$1 > (1-\pi)u'(q_{1L}).$$

This implies

$$\begin{aligned} 1 &= \sigma_L\left[(1-\pi)u'(q_{1L}) + \pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\right] + (1-\sigma_L)\varepsilon \\ \sigma_L(1-\alpha_e) &= \sigma_L\left[(1-\pi)u'(q_{1L}) + \pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\right] - \sigma_L(1-\pi)u'(q_{1L})\alpha_e, \end{aligned}$$

and subtracting both equations,

$$\begin{aligned} 1-\sigma_L(1-\alpha_e) &= (1-\sigma_L)\varepsilon + \sigma_L(1-\pi)u'(q_{1L})\alpha_e \\ 1-\sigma_L+\sigma_L\alpha_e &= (1-\sigma_L)\varepsilon + \sigma_L(1-\pi)u'(q_{1L})\alpha_e. \end{aligned}$$

Since $1 > (1-\pi)u'(q_{1L})$, this contradicts $\varepsilon < 1$. So, $\mathcal{M}_H = \{0\}$, $\mathcal{M}_L = \{0,1\}$ cannot be an equilibrium.

CASE (iv): Consider an equilibrium with $\mathcal{M}_H = \{0,1\}$, $\mathcal{M}_L = \{1\}$

In this case, the consumption levels are

$$\begin{aligned} q_{1L} &= m_{L1}(1-\alpha_e) \\ q_{1L}^{\pi} &= m_{L1}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\ q_{2L} &= 0 \end{aligned}$$

and

$$\begin{aligned} q_{1H} &= m_{H0} + m_{H1}(1-\alpha_e) \geq (m_{H0}+m_{H1})(1-\alpha_e) \equiv \tilde{q}_H \\ q_{1H}^{\pi} &= (m_{H0}+m_{H1})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\ q_{2H} &= m_{H0} \leq q_{1H}. \end{aligned}$$

The equilibrium conditions are

$$\phi_1 = \beta\sigma_L(1-\pi)u'(q_{1L})(1-\alpha_e) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))$$
$$\phi_1 = \beta\sigma_H(1-\pi)u'(q_{1H})(1-\alpha_e) + \beta\sigma_H\pi u'(q_{1H}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))$$
$$\phi_0 > \beta\sigma_L(1-\pi)u'(q_{1L}) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_L)\varepsilon$$
$$\phi_0 = \beta\sigma_H(1-\pi)u'(q_{1H}) + \beta\sigma_H\pi u'(q_{1H}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_H)u'(q_{2H})$$
$$\phi_0 = \beta$$
$$\phi_1 = \beta\frac{\sigma_L(f_L m_{L1}) + \sigma_H(f_H m_{H1})}{f_L m_{L1} + f_H m_{H1}}(1-\alpha_e) = \beta\tilde{\phi}(1-\alpha_e)$$
$$1-\tilde{\mathfrak{p}} = \frac{f_H m_{H0}}{f_L m_{L1} + f_H m_{H0} + f_H m_{H1}} < 1.$$

This is an equilibrium condition whenever at $m_{H1} = 0$, the H-buyer wants to purchase $\mathfrak{p}_1$. Define

$$\begin{aligned}
\tilde{q}_{1H} &= m_{H0} \\
\tilde{q}_{1H}^{\pi} &= m_{H0}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
q_{2H} &= m_{H0}
\end{aligned}$$

Then H-buyer wants to buy $\mathfrak{p}_1$ iff

$$\begin{aligned}
\phi_1 &< \beta\sigma_H(1-\pi)u'(\tilde{q}_{1H})(1-\alpha_e) + \beta\sigma_H\pi u'(\tilde{q}_{1H}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
\phi_1 &< \beta\sigma_H(1-\pi)u'(q_{2H})(1-\alpha_e) + \beta\sigma_H\pi u'(q_{2H})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k \\
\phi_1 &< \left[\beta\sigma_H(1-\pi)(1-\alpha_e) + \beta\sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]u'(q_{2H}),
\end{aligned}$$

and we also have

$$\begin{aligned}
\phi_0 &\leq \beta\sigma_H(1-\pi)u'(q_{2H}) + \beta\sigma_H\pi u'(q_{2H})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k + \beta(1-\sigma_H)u'(q_{2H}) \\
1 &\leq \left[1-\sigma_H\pi + \sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]u'(q_{2H}).
\end{aligned}$$

Hence a necessary condition is

$$\begin{aligned}
\phi_1 &< \frac{\left[\beta\sigma_H(1-\pi)(1-\alpha_e) + \beta\sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]}{[1-\sigma_H\pi + \sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k]} \\
\tilde{\phi}(1-\alpha_e) &< \frac{\sigma_H(1-\pi)(1-\alpha_e) + \sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}{[1-\sigma_H\pi + \sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k]}.
\end{aligned}$$

At the same time, it must be that L-buyers do not want to purchase $\mathfrak{p}_0$. Use the FOC with respect to $\mathfrak{p}_1$, since

$$u'(q_{1L}) = \frac{\tilde{\phi}(1-\alpha_e)}{\sigma_L(1-\pi)(1-\alpha_e) + \sigma_L\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}.$$

The FOC with respect to $\mathfrak{p}_0$ implies,

$$1 \quad > \quad \frac{(1-\pi)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}{(1-\pi)(1-\alpha_e)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}\tilde{\phi}(1-\alpha_e)+(1-\sigma_L)\varepsilon.$$

Hence, $\mathcal{M}_H=\{0,1\}$, $\mathcal{M}_L=\{1\}$ is an equilibrium whenever

$$\tilde{\phi}(1-\alpha_e)<[1-(1-\sigma_L)\varepsilon]\,\frac{(1-\pi)(1-\alpha_e)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}{(1-\pi)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k},$$

and

$$\tilde{\phi}(1-\alpha_e)<\sigma_H\frac{(1-\pi)(1-\alpha_e)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}{[1-\sigma_H\pi+\sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k]}.$$

Which is the tighter upper-bound on $\tilde{\phi}(1-\alpha_e)$?

$$\begin{aligned}
[1-(1-\sigma_L)\varepsilon]\,\frac{(1-\pi)(1-\alpha_e)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}{(1-\pi)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k} \quad &< \quad \sigma_H\frac{(1-\pi)(1-\alpha_e)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}{[1-\sigma_H\pi+\sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k]}\\
[1-(1-\sigma_L)\varepsilon]\left[1-\sigma_H\pi+\sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right] \quad &< \quad \sigma_H\left[(1-\pi)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]\\
1-\sigma_H-(1-\sigma_L)\varepsilon\left[1-\sigma_H\pi+\sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right] \quad &< \quad 0
\end{aligned}$$

or

$$\frac{1-\sigma_H}{1-\sigma_L}<\varepsilon\left[1-\sigma_H\pi+\sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right],$$

which cannot be. So the tighter constraint is

$$\tilde{\phi}(1-\alpha_e)<\sigma_H\frac{(1-\pi)(1-\alpha_e)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}{[1-\sigma_H\pi+\sigma_H\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k]}.$$

Therefore, that bounds is separating case (i) and (iv).

CASE (v) : Next, consider the equilibrium with $\mathcal{M}_H=\{0,1\}$, $\mathcal{M}_L=\{0\}$

In this case, the consumption levels are

$$\begin{aligned}
q_{1L} \quad &= \quad m_{L0}\\
q_{1L}^{\pi} \quad &= \quad m_{L0}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\leq q_{1L}\\
q_{2L} \quad &= \quad m_{L0}
\end{aligned}$$

and

$$\begin{aligned}
q_{1H} \quad &= \quad m_{H0}+m_{H1}(1-\alpha_e)\\
q_{1H}^{\pi} \quad &= \quad (m_{H0}+m_{H1})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))\\
q_{2H} \quad &= \quad m_{H0}\leq q_{1H}.
\end{aligned}$$

We want to show that this cannot be an equilibrium because L-buyers would want to purchase $\mathfrak{p}_1$.

The equilibrium conditions are

$$\phi_0 = \beta\sigma_L(1-\pi)u'(q_{1L}) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_L)\varepsilon$$

$$\phi_1 > \beta\sigma_L(1-\pi)u'(q_{1L})(1-\alpha_e) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))$$

$$\phi_0 = \beta\sigma_H(1-\pi)u'(q_{1H}) + \beta\sigma_H\pi u'(q_{1H}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_H)u'(q_{2H})$$

$$\phi_1 = \beta\sigma_H(1-\pi)u'(q_{1H})(1-\alpha_e) + \beta\sigma_H\pi u'(q_{1H}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))$$

$$\phi_0 = \beta$$

$$\phi_1 = \beta\sigma_H(1-\alpha_e)$$

$$1-\tilde{\mathfrak{p}} = \frac{\sigma_L f_L m_{L0} + \sigma_H f_H m_{H0}}{f_L m_{L0} + f_H m_{H0} + f_H m_{H1}} < 1.$$

We have from the FOC of the L-buyer with respect to $\mathfrak{p}_0$,

$$\begin{aligned}
\phi_0 &= \beta\sigma_L(1-\pi)u'(q_{1L}) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_L)\varepsilon \\
1 &= \left[(1-\pi) + \pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]\sigma_L u'(q_{1L}) + (1-\sigma_L)\varepsilon
\end{aligned}$$

$$\frac{1-(1-\sigma_L)\varepsilon}{\sigma_L\left[(1-\pi)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]} = u'(q_{1L})$$

and we need

$$\begin{aligned}
\phi_1 &> \beta\sigma_L(1-\pi)u'(q_{1L})(1-\alpha_e) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
\sigma_H(1-\alpha_e) &> \left[\sigma_L(1-\pi)(1-\alpha_e) + \sigma_L\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]u'(q_{1L}) \\
\sigma_H(1-\alpha_e) &> \left[\frac{(1-\pi)(1-\alpha_e)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}{(1-\pi)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k}\right](1-(1-\sigma_L)\varepsilon)
\end{aligned}$$

or

$$\sigma_H\frac{(1-\alpha_e)\left[(1-\pi)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]}{\left[(1-\pi)(1-\alpha_e)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]} > (1-(1-\sigma_L)\varepsilon).$$

Or rearranging,

$$(1-\sigma_L)\varepsilon > 1-\sigma_H\frac{(1-\alpha_e)\left[(1-\pi)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]}{\left[(1-\pi)(1-\alpha_e)+\pi(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))^k\right]} = 1-A\sigma_H,$$

since $A<1$ and

$$A\sigma_H < \sigma_H < \sigma_L.$$

While $\varepsilon < 1$, the inequality above can never be satisfied.

Hence $\mathcal{M}_H = \{0,1\}$, $\mathcal{M}_L = \{1\}$ cannot be an equilibrium.

CASE (vi): Consider an equilibrium with $\mathcal{M}_H = \{0,1\}$, $\mathcal{M}_L = \{0,1\}$

In this case, the consumption levels are

$$\begin{aligned}
q_{1L} &= m_{L0} + m_{L1}(1-\alpha_e) \\
q_{1L}^{\pi} &= (m_{L0} + m_{L1})\,(1-\alpha_e + \alpha_e(1-\tilde{\mathfrak{p}})) \\
q_{2L} &= m_{L0}
\end{aligned}$$

and

$$\begin{aligned}
q_{1H} &= m_{H0} + m_{H1}(1-\alpha_e) \\
q_{1H}^{\pi} &= (m_{H0} + m_{H1})(1-\alpha_e + \alpha_e(1-\tilde{\mathfrak{p}})) \\
q_{2H} &= m_{H0} \leq q_{1H}.
\end{aligned}$$

The equilibrium conditions are

$$\begin{aligned}
\phi_0 &= \beta\sigma_L(1-\pi)u'(q_{1L}) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_L)\varepsilon \\
\phi_1 &= \beta\sigma_L(1-\pi)u'(q_{1L})(1-\alpha_e) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
\phi_0 &= \beta\sigma_H(1-\pi)u'(q_{1H}) + \beta\sigma_H\pi u'(q_{1H}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_H)u'(q_{2H}) \\
\phi_1 &= \beta\sigma_H(1-\pi)u'(q_{1H})(1-\alpha_e) + \beta\sigma_H\pi u'(q_{1H}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
\phi_0 &= \beta \\
\phi_1 &= \beta\frac{\sigma_L\,(f_L m_{L1}) + \sigma_H\,(f_H m_{H1})}{f_L m_{L1} + f_H m_{H1}}(1-\alpha_e) = \beta\tilde{\phi}(1-\alpha_e) \\
1-\tilde{\mathfrak{p}} &= \frac{f_H m_{H0} + f_L m_{L0}}{f_L m_{L1} + f_L m_{L0} + f_H m_{H0} + f_H m_{H1}} < 1.
\end{aligned}$$

Hence,

$$1 = \sigma_L(1-\pi)u'(q_{1L}) + \beta\sigma_L\pi u'(q_{1L}^{\pi})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + (1-\sigma_L)\varepsilon$$

and using that expression to get rid of $u'(q_{1L}^{\pi})$ in the FOC with respect to $\mathfrak{p}_1$,

$$\begin{aligned}
\tilde{\phi}(1-\alpha_e) &= \sigma_L(1-\pi)u'(q_{1L})(1-\alpha_e) + [1-\sigma_L(1-\pi)u'(q_{1L}) - (1-\sigma_L)\varepsilon] \\
\tilde{\phi}(1-\alpha_e) &= 1-(1-\sigma_L)\varepsilon - \alpha_e\sigma_L(1-\pi)u'(q_{1L}) \\
u'(q_{1L}) &= \frac{\left[1-\tilde{\phi}(1-\alpha_e) - (1-\sigma_L)\varepsilon\right]}{\alpha_e\sigma_L(1-\pi)}.
\end{aligned}$$

Now solve for $u'(q^{\pi}_{1L})$ using FOC with respect to $\mathfrak{p}_0$,

$$\begin{aligned}
1 &= \sigma_L(1-\pi)u'(q_{1L}) + \beta\sigma_L\pi u'(q^{\pi}_{1L})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + (1-\sigma_L)\varepsilon \\
1 &= \sigma_L(1-\pi)\frac{\left[1-\tilde{\phi}(1-\alpha_e)-(1-\sigma_L)\varepsilon\right]}{\alpha_e\sigma_L(1-\pi)} + \beta\sigma_L\pi u'(q^{\pi}_{1L})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + (1-\sigma_L)\varepsilon \\
1 &= \frac{\left[1-\tilde{\phi}(1-\alpha_e)-(1-\sigma_L)\varepsilon\right]}{\alpha_e} + \beta\sigma_L\pi u'(q^{\pi}_{1L})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + (1-\sigma_L)\varepsilon \\
\alpha_e &= \left[1-\tilde{\phi}(1-\alpha_e)-(1-\alpha_e)(1-\sigma_L)\varepsilon\right] + \alpha_e\beta\sigma_L\pi u'(q^{\pi}_{1L})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
\left[\tilde{\phi}+(1-\sigma_L)\varepsilon-1\right](1-\alpha_e) &= \alpha_e\beta\sigma_L\pi u'(q^{\pi}_{1L})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) > 0.
\end{aligned}$$

This requires

$$1 < \tilde{\phi} + (1-\sigma_L)\varepsilon,$$

however, since $\tilde{\phi} < \sigma_L$ this contradicts $\varepsilon < 1$.

Therefore, $\mathcal{M}_H = \{0,1\}, \mathcal{M}_L = \{0,1\}$ cannot be an equilibrium.

Step 2: We now derive the threshold value $\bar{\pi}$ for the log-utility case.

Case (i) $\mathcal{M}_H = \{0\}$**,** $\mathcal{M}_L = \{1\}$

The equilibrium conditions for L- and H-buyers and the banker are given by

$$\begin{aligned}
\phi_1 &= \beta\sigma_L\frac{(1-\pi)}{q_{1L}}(1-\alpha_e) + \beta\sigma_L\frac{\pi}{q^{\pi}_{1L}}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
\phi_0 &= \beta\sigma_H\frac{(1-\pi)}{q_{1H}} + \beta\sigma_H\frac{\pi}{q^{\pi}_{1H}}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta\frac{(1-\sigma_H)}{q_{2H}} \\
\phi_0 &= \beta \\
\phi_1 &= \beta\sigma_L(1-\alpha_e) \\
1-\tilde{\mathfrak{p}} &= \frac{f_H m_{H0}}{f_L m_{L1} + f_H m_{H0}}.
\end{aligned}$$

Equilibrium quantities and prices are given by

$$\begin{aligned}
q_{1L} &= m_{L1}(1-\alpha_e) \\
q^{\pi}_{1L} &= m_{L1}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \\
q_{1H} &= m_{H0} \\
q_{2H} &= m_{H0} \\
q^{\pi}_{1H} &= m_{H0}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))
\end{aligned}$$

$$m_{L1} = \frac{1}{1-\alpha_e}$$

$$m_{H0} = 1$$

$$1 - \tilde{\mathfrak{p}} = \frac{f_H}{\frac{f_L}{1-\alpha_e} + f_H}$$

$$\phi_0 = \beta$$

$$\phi_1 = \beta\sigma_L(1-\alpha_e).$$

Type H has no incentives to hold $\mathfrak{p} = 1$-tokens if

$$\sigma_L(1-\alpha_e) > \sigma_H(1-\pi)(1-\alpha_e) + \sigma_H\pi.$$

$$\sigma_L(1-\alpha_e) > \sigma_H(1-\alpha_e) + \sigma_H\pi(1-(1-\alpha_e)).$$

$$\frac{(\sigma_L - \sigma_H)(1-\alpha_e)}{\sigma_H\alpha_e} > \pi.$$

Case (iv) $\mathcal{M}_H = \{0,1\}$**,** $\mathcal{M}_L = \{1\}$

The equilibrium conditions for L- and H-buyers and the bank are given by

$$\phi_1 = \beta\sigma_L\frac{(1-\pi)}{q_{1L}}(1-\alpha_e) + \beta\sigma_L\frac{\pi}{q_{1L}^{\pi}}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))$$

$$\phi_1 = \beta\sigma_H\frac{(1-\pi)}{q_{1H}}(1-\alpha_e) + \beta\sigma_H\frac{\pi}{q_{1H}^{\pi}}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))$$

$$\phi_0 = \beta\sigma_H\frac{(1-\pi)}{q_{1H}} + \beta\sigma_H\frac{\pi}{q_{1H}^{\pi}}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta\frac{(1-\sigma_H)}{q_{2H}}$$

$$\phi_0 = \beta$$

$$\phi_1 = \beta\frac{\sigma_L f_L m_{L1} + \sigma_H f_H m_{H1}}{f_L m_{L1} + f_H m_{H1}}(1-\alpha_e)$$

$$1 - \tilde{\mathfrak{p}} = \frac{f_H m_{H0}}{f_L m_{L1} + f_H m_{H0} + f_H m_{H1}}.$$

Equilibrium quantities are given by

$$q_{1L} = m_{L1}(1-\alpha_e)$$

$$q_{1L}^{\pi} = m_{L1}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) = \frac{q_{1L}}{1-\alpha_e}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))$$

$$q_{1H} = m_{H0} + m_{H1}(1-\alpha_e)$$

$$q_{2H} = m_{H0}$$

$$q_{1H}^{\pi} = (m_{H0}+m_{H1})(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}}))$$

$$\phi_0 = \beta$$
$$\phi_1 = \beta\sigma_L \frac{(1-\alpha_e)}{q_{1L}}.$$

L-buyers have no incentives to hold $\mathfrak{p} = 0$-tokens whenever

$$\phi_0 > \beta\sigma_L \frac{(1-\pi)}{q_{1L}}(1-\alpha_e) + \beta\sigma_L \frac{\pi}{q_{1L}^{\pi}}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) + \beta(1-\sigma_L)\varepsilon$$

$$1 > \frac{\sigma_L f_L m_{L1} + \sigma_H f_H m_{H1}}{f_L m_{L1} + f_H m_{H1}}(1-\alpha_e) + (1-\sigma_L)\varepsilon.$$

Since $\frac{\sigma_L f_L m_{L1} + \sigma_H f_H m_{H1}}{f_L m_{L1} + f_H m_{H1}} \in (\sigma_H, \sigma_L)$, this condition holds whenever

$$1 > \sigma_L(1-\alpha_e) + (1-\sigma_L)\varepsilon,$$

which is always satisfied since $\alpha_e > 0$ and $\varepsilon < 1$. We now verify conditions such that, at the given prices, H-buyers want to acquire type $\mathfrak{p} = 1$-tokens. Suppose a H-buyer does not acquire $\mathfrak{p} = 1$-tokens, but only $\mathfrak{p} = 0$-tokens. Then they consume

$$q_{1H} = m_{H0}$$
$$q_{2H} = m_{H0}$$
$$q_{1H}^{\pi} = m_{H0}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})),$$

where m_{H0} is given by

$$\phi_0 \quad = \quad \beta\sigma_H \frac{(1-\pi)}{m_{H0}} + \beta\sigma_H \frac{\pi}{m_{H0}} + \beta \frac{(1-\sigma_H)}{m_{H0}}$$

and so $m_{H0} = 1$. Then $q_{1H} = q_{2H} = 1$ and $q_{1H}^{\pi} = 1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})$. The first order condition with respect to $\mathfrak{p} = 1$-tokens is

$$\begin{aligned} -\phi_1 + \beta\sigma_H \frac{(1-\pi)}{q_{1H}}(1-\alpha_e) + \beta\sigma_H \frac{\pi}{q_{1H}^{\pi}}(1-\alpha_e+\alpha_e(1-\tilde{\mathfrak{p}})) \quad &= \\ -\phi_1 + \beta\sigma_H(1-\pi)(1-\alpha_e) + \beta\sigma_H\pi & \end{aligned}$$

and since

$$\phi_1 \in (\beta(1-\alpha_e)\sigma_H, \beta(1-\alpha_e)\sigma_L),$$

the H-buyer will prefer to acquire $\mathfrak{p} = 1$-tokens if

$$\beta(1-\alpha_e)\sigma_L \quad < \quad \beta\sigma_H(1-\pi)(1-\alpha_e) + \beta\sigma_H\pi$$

or

$$\frac{(1-\alpha_e)(\sigma_L-\sigma_H)}{\sigma_H\alpha_e} \quad < \quad \pi.$$

$\square$

E. An Example Where Buyers Play a Signaling Game When Tokens Are Imperfectly Recognizable

Below, we consider a signaling game and show that for low α and high σ_H, a separating equilibrium exists: H-buyers hold M unprogrammed tokens and consume too much, while L-buyers hold $1/(1-\alpha) < M$ programmed tokens and consume efficiently.

Suppose in CM1, a fraction π of buyers learn in advance that, if they trade in the DM1, the sellers will be uninformed. When an uninformed seller is offered m tokens in a match, the seller's belief is that all the m tokens offered are NOT programmed whenever

$$m \geq M,$$

otherwise the belief is that they are all programmed. Suppose $u(q) = \log q$. We conjecture that in equilibrium, $p_0 = 1$ and $p_1 = \sigma_L(1-\alpha)$. That is, buyers separate in their portfolio choice. L-buyers hold less than M $\mathfrak{p} = 1$-tokens and H-buyers hold more than M $\mathfrak{p} = 0$-tokens. We will verify that these are the equilibrium prices.

Define

$$\mathbf{1_M} = 1 \text{ iff } m_0 + m_1 \geq M.$$

The problem of a type i buyer is

$$\max_{m_{i0}, m_{i1}} \sigma_i u(q_{i1}^{\pi}) + (1-\sigma_i) u_i(q_{i2}) - p_0 m_0 - p_1 m_1,$$

where

$$\begin{aligned}
q_{i1}^{\pi} &= (m_{i0} + m_{i1})(1-\alpha) + \mathbf{1_M}(m_{i0} + m_{i1})\alpha \\
q_{i2} &= m_{i0} \\
u_L(q_2) &= \varepsilon q_2 \\
u_H(q_2) &= u(q_2).
\end{aligned}$$

First, consider L-buyers: Suppose $\mathbf{1_M} = 0$, then

$$\max_{m_{L0}, m_{L1}} \sigma_L u((m_{L0} + m_{L1})(1-\alpha)) + (1-\sigma_L)\varepsilon m_{L0} - m_{L0} - \sigma_L(1-\alpha) m_{L1} + \lambda_M \left[M - (m_{L0} + m_{L1})\right]$$

The FOCs are

$$\begin{aligned}
m_{L0}: \quad & \sigma_L \frac{1}{(m_{L0} + m_{L1})} + (1-\sigma_L)\varepsilon - 1 - \lambda_M && \leq \quad 0 \\
m_{L1}: \quad & \sigma_L \frac{1}{(m_{L0} + m_{L1})} - \sigma_L(1-\alpha) - \lambda_M && \leq \quad 0
\end{aligned}$$

with ε small enough, $m_{L0} = 0$. Then either $m_{L0} = 1/(1-\alpha) < M$ or $m_{L0} = M$.

Hence, the solution is

$$m_{L1} = \min\{\frac{1}{1-\alpha}, M\},$$
$$m_{L0} = 0.$$

Suppose $\mathbf{1_M} = 1$, then:

$$\max_{m_{L0}+m_{L1}\geq M} \sigma_L u((m_{L0}+m_{L1})) + (1-\sigma_L)\varepsilon m_{L0} - m_{L0} - \sigma_L(1-\alpha)m_{L1}$$

Hence, the solution is

$$m_{L1} = \max\{\frac{1}{1-\alpha}, M\}$$
$$m_{L0} = 0.$$

Then the buyer chooses between (i) revealing the true token type

$$m_{L1} = \min\{\frac{1}{1-\alpha}, M\},$$

with a payoff

$$\sigma_L \log((1-\alpha)\min\{\frac{1}{1-\alpha}, M\}) - \sigma_L(1-\alpha)\min\{\frac{1}{1-\alpha}, M\}$$

or (ii) pretending to hold programmed tokens by choosing

$$m_{L1} = m_{H0} \geq M$$

with a payoff

$$\sigma_L\{\log m_{H0} - (1-\alpha)m_{H0}\}.$$

Option (i) is better if

$$\log((1-\alpha)\min\{\frac{1}{1-\alpha}, M\}) - \sigma_L(1-\alpha)\min\{\frac{1}{1-\alpha}, M\} > \log m_{H0} - (1-\alpha)m_{H0}. \tag{5}$$

Second, consider H-buyers: suppose $\mathbf{1_M} = 0$, then

$$\max_{m_{H0}+m_{H1}<M} \sigma_H u((m_{H0}+m_{H1})(1-\alpha)) + (1-\sigma_H)u(m_{H0}) - m_{H0} - \sigma_L(1-\alpha)m_{H1} + \lambda_M\left[M - (m_{H0}+m_{H1})\right]$$

FOC:

$$m_{H0} : \sigma_H \frac{1}{m_{H0}+m_{H1}} + (1-\sigma_H)\frac{1}{m_{H0}} - 1 - \lambda_M = 0$$
$$m_{H1} : \sigma_H \frac{1}{m_{H0}+m_{H1}} - \sigma_L(1-\alpha) - \lambda_M \leq 0$$

If $m_{H1} > 0$ and $\lambda_M = 0$, then we have

$$\frac{\sigma_H}{\sigma_L(1-\alpha)} = m_{H0} + m_{H1} < M$$

and

$$m_{H0} = \frac{1-\sigma_H}{1-\sigma_L(1-\alpha)}.$$

Otherwise, $m_{H1} = 0$ and $\lambda_M = 0$, then

$$m_{H0} = 1 < M,$$

which is consistent with $m_{H1} = 0$ iff $\sigma_H < \sigma_L(1-\alpha)$.

If $\lambda_M > 0$, then $m_{H0} + m_{H1} = M$ and if $m_{H1} > 0$, then

$$\begin{aligned} \sigma_H \frac{1}{m_{H0}+m_{H1}} + (1-\sigma_H)\frac{1}{m_{H0}} - 1 - \left(\sigma_H \frac{1}{m_{H0}+m_{H1}} - \sigma_L(1-\alpha)\right) &= 0 \\ (1-\sigma_H)\frac{1}{m_{H0}} - 1 + \sigma_L(1-\alpha) &= 0, \end{aligned}$$

so that

$$m_{H0} = \frac{(1-\sigma_H)}{1-\sigma_L(1-\alpha)}.$$

If $m_{H1} = 0$, then $m_{H0} = M$, which is consistent with $m_{H1} = 0$ iff

$$\begin{aligned} \sigma_H \frac{1}{M} - \sigma_L(1-\alpha) - \lambda_M &\leq 0 \\ \sigma_H \frac{1}{M} - \sigma_L(1-\alpha) - \left[\sigma_H \frac{1}{M} + (1-\sigma_H)\frac{1}{M} - 1\right] &\leq 0 \\ -\sigma_L(1-\alpha) - (1-\sigma_H)\frac{1}{M} + 1 &\leq 0 \end{aligned}$$

or

$$M < \frac{(1-\sigma_H)}{1-\sigma_L(1-\alpha)}.$$

Notice that none of this is not consistent with the seller's beliefs that all payment below M is done with programmed money. Suppose $\mathbf{1_M} = 1$, then

$$\max_{m_{H0}+m_{H1}>M} \sigma_H u((m_{H0}+m_{H1})) + (1-\sigma_H)u(m_{H0}) - m_{H0} - \sigma_L(1-\alpha)m_{H1} + \lambda_M \left[m_{H0}+m_{H1}-M\right]$$

FOC:

$$\begin{aligned} m_{H0} :& \sigma_H \frac{1}{m_{H0}+m_{H1}} + (1-\sigma_H)\frac{1}{m_{H0}} - 1 + \lambda_M = 0 \\ m_{H1} :& \sigma_H \frac{1}{m_{H0}+m_{H1}} - \sigma_L(1-\alpha) + \lambda_M \leq 0 \end{aligned}$$

If $m_{H1} > 0$, then we have

$$m_{H0} + m_{H1} = \frac{\sigma_H}{\sigma_L(1-\alpha)} > M$$

or

$$m_{H0} + m_{H1} = M > \frac{\sigma_H}{\sigma_L(1-\alpha)}$$

and

$$m_{H0} = \frac{1-\sigma_H}{1-\sigma_L(1-\alpha)}.$$

Otherwise, $m_{H1} = 0$ and (with $M > 1$),

$$m_{H0} = M > 1,$$

which is consistent with $m_{H1} = 0$ iff

$$\begin{aligned} \sigma_H \frac{1}{m_{H0}} - \sigma_L(1-\alpha) &\leq 0 \\ \frac{\sigma_H}{\sigma_L(1-\alpha)} &\leq M. \end{aligned}$$

Overall, if

$$M > \max\left\{1, \frac{\sigma_H}{\sigma_L(1-\alpha)}\right\}, \tag{6}$$

then conditional on $\mathbf{1}_{\boldsymbol{M}} = 1$, it is optimal to choose

$$m_{H1} = 0, m_{H0} = M$$

with a payoff

$$\sigma_H \log M - M$$

and conditional on $\mathbf{1}_{\boldsymbol{M}} = 0$, if $\frac{\sigma_H}{\sigma_L(1-\alpha)} < 1$,

$$m_{H1} = 0, m_{H0} = 1$$

with a payoff

$$\sigma_H \log(1-\alpha) - 1.$$

Hence, H-buyers choose $m_{H0} = M$ to reveal the true type of tokens iff

$$\sigma_H \log M - M \geq \sigma_H \log(1-\alpha) - 1.$$

Under this condition, $m_{H0} = M$ and going back to the choice of L-buyers, option (i) is better if

$$\begin{aligned}
\log((1-\alpha)\min\{\frac{1}{1-\alpha}, M\}) - \sigma_L(1-\alpha)\min\{\frac{1}{1-\alpha}, M\} &> \log m_{H0} - (1-\alpha)m_{H0} \qquad (7)\\
\log((1-\alpha)\min\{\frac{1}{1-\alpha}, M\}) - \sigma_L(1-\alpha)\min\{\frac{1}{1-\alpha}, M\} &> \log M - (1-\alpha)M \qquad (8)
\end{aligned}$$

We require $M > 1/(1-\alpha)$ so that L-buyers choose $m_{L1} = 1/(1-\alpha)$ and H-buyers choose $m_{H0} = M$. So this signaling equilibrium exists iff $\sigma_H < \sigma_L(1-\alpha)$ and

$$M > \max\left\{1, \frac{\sigma_H}{\sigma_L(1-\alpha)}\right\} = 1$$

$$\sigma_H \log M - M \geq \sigma_H \log(1-\alpha) - 1$$

$$-\sigma_L > \log M - (1-\alpha)M.$$

F. An Example Where Sellers Have Trade Surplus in DM2

Suppose the utility function of sellers in DM2 is given as

$$u_s(q_{2s}) = (1+\gamma)\min\{1, q_{2s}\}.$$

The first-best allocation requires the consumption of sellers in DM2 to be $q_{2s} = 1$. Then the marginal value of a token to a L-buyer is

$$\sigma_L u'(q_{1L})[1 - \alpha_e + \alpha_e(1-\mathfrak{p})(1+\gamma))] + (1-\sigma_L)\varepsilon(1-\mathfrak{p}),$$

and the marginal value to a H-buyer is

$$\sigma_H u'(q_{1H})[1 - \alpha_e + \alpha_e(1-\mathfrak{p})(1+\gamma))] + (1-\sigma_H)u'(q_{2H}).$$

When $\mathcal{M}_H = \{0\}$, $\mathcal{M}_L = \{1\}$, the equilibrium conditions for L- and H-buyers and the banker are given by

$$\begin{aligned}
\phi_1 &= \beta\sigma_L u'(q_{1L})(1-\alpha_e) \\
\phi_1 &= \beta\sigma_L(1-\alpha_e) \\
\phi_0 &= \beta\sigma_H u'(q_{1H})(1+\alpha_e\gamma) + \beta(1-\sigma_H)u'(q_{2H}) \\
\phi_0 &= \beta.
\end{aligned}$$

Assume $u(q) = \log(q)$. Then, the first two conditions imply that

$$q_{1L} = 1 = m_L(1-\alpha_e).$$

The last two conditions above imply that

$$\begin{aligned}
m_H &= 1 \\
q_{1H} &= 1 + \alpha_e\gamma > 1 = q_{2H}.
\end{aligned}$$

H-buyers have no incentive to hold $\mathfrak{p}_1$ if

$$\phi_1 > \beta\sigma_H u'(q_H)(1-\alpha_e)$$

or

$$\sigma_L > \frac{\sigma_H}{1+\alpha_e\gamma},$$

which is satisfied. Finally, L-buyers have no incentive to hold $\mathfrak{p}_0$ if

$$\phi_0 > \beta\sigma_L u'(q_{1L})(1+\alpha_e\gamma) + \beta(1-\sigma_L)\varepsilon$$

or

$$1 > \frac{\alpha_e\gamma}{1-\sigma_L} + \varepsilon.$$

So, for γ not too big, this is an equilibrium. However, the allocation is

$$\begin{aligned} q_{1L} &= 1, q_{2L} = 0 \\ q_{1H} &= 1+\alpha_e\gamma > 1, q_{2H} = 1, \\ q_{2s} &= \frac{f_H\sigma_H}{f_H\sigma_H + f_L\sigma_L} < 1. \end{aligned}$$

Hence, the sellers under-consume in DM2 while H-buyers over-consume in DM1.

References

Andolfatto, D. (2020). Assessing the impact of central bank digital currency on private banks. *The Economic Journal*, 131(634): 525-540.

Bache, I. W. (2023). Central bank digital currency and the singleness of money. Speech at the 22nd BIS Annual Conference, Basel, Switzerland, 23 June 2023. Published by Norges Bank. Available at: `https://www.norges-bank.no/en/news-events/news/Speeches/2023/2023-10-27-bis/`.

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

Bertsch, C. (2023). Stablecoins: Adoption and fragility. *Sveriges Riksbank*.

Carapella, F. (2024). Stablecoin self-regulation. *Federal Reserve Board of Governors*, manuscript.

Chiu, J., Davoodalhosseini, S. M., Jiang, J., and Zhu, Y. (2023). Bank market power and central bank digital currency: Theory and quantitative assessment. *Journal of Political Economy*, 131(5): 1213-1248.

Choi, M., and Rocheteau, G. (2021). Money mining and price dynamics. *American Economic Journal: Macroeconomics*, 13(4): 246-294.

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

Fung, B. S. C., Hendry, S., and Weber, W. E. (2017). Canadian bank notes and Dominion notes: Lessons for digital currencies. *Bank of Canada Staff Working Paper No. 2017-5*.

Gans, J. S., and Halaburda, H. (2015). Some economics of private digital currency. In *Economic analysis of the digital economy*, 257-276.

Garratt, R., and Shin, H. S. (2023). Stablecoins versus tokenised deposits: Implications for the singleness of money. *BIS Bulletin*, 73.

Gorton, G. B., and Zhang, J. Y. (2023). Taming wildcat stablecoins. *University of Chicago Law Review*, 90: 909.

Kahn, C. M., and van Oordt, M. R. C. (2022). The demand for programmable payments. *Tinbergen Institute Discussion Paper No. 22-076/IV*.

Kahn, C. M., van Oordt, M. R. C., and Zhu, Y. (2021). Best before? Expiring central bank digital currency and loss recovery. *Bank of Canada Staff Working Paper No. 2021-67*.

Keister, T., and Sanches, D. (2023). Should central banks issue digital currency? *The Review of Economic Studies*, 90(1): 404-431.

Lagos, R., and Wright, R. (2005). A unified framework for monetary theory and policy analysis. *Journal of Political Economy*, 113(3): 463-484.

Lee, A. (2021). What is programmable money? *FEDS Notes*.

Lee, M., Martin, A., and Townsend, R. M. (2021). Optimal design of tokenized markets. Available at SSRN: `https://ssrn.com/abstract=3820973`.

Li, Y., and Mayer, S. (2021). Money creation in decentralized finance: A dynamic model of stablecoin and crypto shadow banking. Available at: `https://dx.doi.org/10.2139/ssrn.3757083`.

Rolnick, A. J. (1999). Maintaining a uniform (electronic) currency. *Journal of Money, Credit and Banking*, 31(3): 674-676.

Schilling, L., and Uhlig, H. (2019). Some simple bitcoin economics. *Journal of Monetary Economics*, 106: 16-26.

Tinn, K. (2024). A theory model of digital currency with asymmetric privacy. Available at SSRN: `https://ssrn.com/abstract=4891933` or `http://dx.doi.org/10.2139/ssrn.4891933`.

Weber, W. E. (2015). The efficiency of private e-money-like systems: The U.S. experience with national bank notes. *Bank of Canada Staff Working Papers*, 15-3.

Williamson, S. (2022). Central bank digital currency: Welfare and policy implications. *Journal of Political Economy*, 130(11): 2829-2861.