# CRYPTOCURRENCY, SECURITY, AND FINANCIAL INTERMEDIATION

**Nicholas Glenn**
Department of Economics
University of Akron
Akron, OH 44325
nglenn@akron.edu

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

August 13, 2022

**ABSTRACT**

In recent years, the use of cryptocurrencies has increased. As these currencies continue to play a larger role, they eventually will be an important component of banking system activity. Moreover, in addition to the standard role of financial intermediaries to facilitate lending, intermediaries can be valuable firms that help provide safe-keeping of tokens. The objective of this paper is to demonstrate these important functions in a micro-founded model of monetary exchange. Furthermore, we also consider the possibility that central banks issue their own digital currencies which may affect the level of intermediation in the private banking system.

## I. Introduction

Satashi Nakamoto created the cryptocurrency known as bitcoin in 2008. Since then, many other cryptocurrencies have been introduced and have been circulating in the global financial system. Notably, recent estimates of the total market capitalization of the over 7,000 different cryptocurrencies are almost $350 billion. In particular, the total capitalization of bitcoin is about $200 billion followed by ethereum at around $40 billion.[2]

Why have cryptocurrencies become increasingly more accepted? Some value the privacy that they derive from conducting transactions in cryptocurrency. However, many also value that alternatives to the centralized financial system are important as central banks continue printing money and devaluing fiat monies issued by sovereign governments. That is, one of the initial motivations for establishing cryptocurrencies such as bitcoin was to avoid inflation risk coming out of the recent Great Financial Crisis. This has further been magnified due to central bank responses to the current public health crisis across the globe. Consequently, some economists argue that physical cash could eventually be eliminated. In this way, cryptocurrency could prove valuable as a means to conduct private trustless transactions.[3]

A unique feature of cryptocurrency is that such forms of money make use of cryptography where coin holders store their bitcoin at a public address on a decentralized ledger that is linked

*Corresponding Author

[2]Data from https://coinmarketcap.com.

[3]Kahn et al. (2005) demonstrate the importance of anonymity in dealing with identity theft from transactions. A consumer using cash or a digital replacement is not at risk of financial loss associated with identity theft.

to both a private and public key.[4] As the identity of the individual behind the public address is unknown, public key cryptography is necessary for network verification. The public address is similar to a pen name in that it's a pseudonym. When a transfer request from the address is made to the Bitcoin network, the crypto holder uses the private key to digitally sign the message containing the request. In order to complete the transfer, the Bitcoin network verifies the digital signature with the public key. The verification process illustrates the importance of the security of the private key. The person in possession of the private key is in control of the funds at the address.

In order to prevent hackers from gaining access to their private keys, crypto owners often store their private key on a hardware wallet offline in "cold storage". 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. However, 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]

Yet, as shown by He et al. (2005, 2008), one of the essential roles of banks in the financial system is to provide safekeeping of different assets.[8] Consequently, the OCC recently extended to banks the same authority over cryptocurrency: "Because national banks are authorized to perform safekeeping and custody services for physical assets, national banks are likewise permitted to provide those same services via electronic means (i.e., custody of cryptocurrency.)" Further, they stress that these services could be extended and intertwined with other important functions of intermediaries such as the extension of credit: "By providing such services, banks can continue to fulfill the intermediation function they have historically played in providing payment, loan, and deposit services."[9]

Consequently, as economists continue to think about the larger impact of cryptocurrency in the global financial system, they cannot ignore the role that they will eventually play in the traditional, deposit-based banking system. That is, economists need to develop frameworks where institutions bank in terms of cryptocurrencies such as bitcoin. In particular, recently crypto credit markets such as Bitfinex and Bitbond have been established in which borrowing and lending in terms of bitcoin has emerged. It is not hard to envision that deposit-based intermediaries which have long played an essential function in terms of the extension of credit will begin to do the same. That is, economists need to develop frameworks in which individuals do not engage in borrowing and lending in outside money issued by sovereign governments but instead by profit-maximizing issuers of digital fiat money. Such loans are not subject to an "inflation tax" where revenues may be redistributed back into the economy — rather they are in terms of assets that are subject to permanent loss due to

[4]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.

[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 additional discussion, see "Lost Passwords Lock Millionaires Out of Their Bitcoin." (Popper, New York Times, January 12, 2021).

[8]In contrast to He et al., we study a framework where the money supply is produced by profit-maximizing agents. Thus, it is endogenous rather than following simple exogenous growth rate. Further, the money stock is subject to permanent loss over time.

[9]Office of the Comptroller of the Currency (Interpretative Letter #1170: July 2020). For additional discussion, see "Banks can now hold Bitcoin: Behind the OCC's big decision and why it matters." (Roberts, Fortune, July 22, 2020).

separation of holders from their private keys. For this reason, central banks also need to begin to consider how borrowing and lending in terms of cryptocurrency may be offered by traditional intermediaries. Moreover, how would the issuance of central bank digital currency (hereafter, CBDC) affect economic activity in the private banking system?

Under what conditions will individuals choose to participate in the private banking system? How would the issuance of private tokens affect the circulation of physical cash? Would the issuance of CBDC drive private digital monies out of circulation? How would the different levels of safekeeping services provided by private banks affect not only the level of intermediation in the overall financial system, but also the conditions under which different types of currencies circulate?

To study these important issues, we extend the framework of Berentsen, Camera, and Waller (2007) with microfounded financial intermediaries by replacing central bank fiat currency with digital money that is subject to permanent loss as in the case of cryptocurrency. In particular, in order to consider the circulation of cryptocurrency as in Fernandez-Villaverde & Sanches (2019), we introduce tokens that are produced by profit-maximizing issuers of money rather than outside money issued by a sovereign government. Yet, in contrast to Fernandez-Villaverde & Sanches, we consider that a percentage of the stock of tokens will be lost over time in the absence of safe-keeping services. Furthermore, we also investigate how the issuance of CBDC affects the circulation of different forms of money and the level of intermediation in the overall banking system.

We refer to the private intermediaries in the framework as private "banks." As in Berentsen, Camera, and Waller (BCW), such banks have access to a record keeping technology that keeps track of the financial histories of agents. As banks may provide different levels of credit extension, safekeeping, and payments processing, we consider that there are three different types of banks in the model.[10] To begin, we start the analysis in a way that is close to BCW in that type I banks only intermediate between borrowers and lenders – they do not provide safekeeping services. Importantly, since type I banks do not provide safekeeping, individuals would obtain the highest level of privacy in transactions. However, the borrower is responsible for the security of the cryptocurrency. We proceed to look at type II banks who provide safekeeping over tokens that are borrowed, but not over an individual's other money holdings. In this manner, since such banks provide some level of transactions services on the part of borrowers, borrowers sacrifice some privacy in exchange for additional security of their holdings of tokens. Finally, we look at type III banks who process all transactions between buyers and sellers. Consequently, in this setup, token loss would never occur. It is this part of our analysis that most closely matches up with BCW. Notably, as type III banks provide transactions services through all of an individual's holdings, borrowers completely sacrifice their level of privacy.[11] Yet, we also show that a steady-state would

[10] As discussed by BCW, credit functions like illiquid bonds in Kocherlakota (2003). Yet, in our framework, we look at the transfer of money produced by profit-maximizing agents and central banks.

[11] Our position is that the only way for an individual to obtain complete anonymity is by maintaining sole possession of the individual's tokens. Notably, commercial banks and other types of banking institutions are subject to Know Your Customer (KYC) laws which require banks to verify an account holder's identity. For example, in the United States, this policy was first established through the Bank Secrecy Act of 1970. Moreover, anonymity in payments is also limited as banks must also monitor transactions, report suspicious activity, report transfers of currency over $10,000 to the FinCen (a department within the office of the U.S. Treasury) and record transactions of over $3,000 as part of Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) regulations. Moreover, in 2019, these policies were extended to Converible Virtual Currency and "money service businesses" such as on-line crypto exchange platforms like CoinBase. (See "Public Statements & Remarks: Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets." October 11, 2019) Furthermore, recent proposals would require intermediaries to verify a counterparty's identity prior to conducting transactions with unhosted wallets. For example, see "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," Department of the Treasury (RIN 1506-AB47, December 23, 2020). All of these restrictions limit the ability of individuals to transfer funds anonymously. Thus, the only way to insure anonymity is by conducting peer to peer transactions in which both participants use unhosted wallets. This would only be possible in our framework with Type I banks.

not exist unless there is a hard cap on token production.

In terms of CBDC, one of the concerns is that the issuance of CBDC would lead to disintermediation of the private banking system. In thinking about this issue, we also consider the more general question as to why individuals choose to be "unbanked" and disintermediation across the overall banking system occurs. In particular, one of the suggested potential benefits of a CBDC would be to promote financial inclusion so we also want to study the decisions of individuals to participate in the banking system. For example, a recent FDIC survey found that individuals choose to be unbanked because the minimum account balances and/or fees administered by banks were "too high." Moreover, in a recent speech on the merits and costs of issuing a CBDC in the United States, Governor Waller (August 5, 2021) also cites that the fees associated with commercial banking drive non-participation in the banking system. Notably, Waller along with other economists have argued that in order for the issuance of a CBDC to promote financial inclusion, the costs of offering banking services directly by the central bank would need to dominate those among commercial banks. He argues that there is no reason to believe that central banks have any technological advantages in this regard. However, our revised framework includes costs of intermediation which potentially vary between commercial banks and the central bank.[12] Some of these costs from intermediation would also involve the costs of providing safekeeping services.

The complications from establishing private keys and providing security over cryptocurrency have also been studied in other work but in slightly different contexts. For example, Kahn et al (2020) delve deeper into security protocols and look at various tradeoffs in dealing with theft of the private key. On the one hand, lowering the number of addresses that hold funds attacts hackers because each address is worth more. To avoid this possibility, holders can increase password strength. However, the password is susceptible to theft each time it is used during a transaction.[13] As a result, customers need to follow a strict security protocol to ensure thieves do not gain access to their password. Moreover, a difficult password and protocol require effort from the customer. With the bank and customer sharing liability, the bank faces a moral hazard problem. That is, the bank cannot control the customers actions and the customer will not fully internalize the costs of theft and underprovide the level of care in regards to security. Consequently, there is an important role for the government to regulate security protocols. Nevertheless, our framework diverges by looking at microfoundations for monetary exchange and financial intermediaries. As a result, we focus our attention on the issues related to loss of currency on the money supply. Not withstanding, Kahn et al raise an important issue that has relavance to our paper. That is, the ability to scale with the technology used leaves the holder of the currencies susceptible to losses not possible with physical cash.[14]

In terms of existing work on the implications of CBDC, there have been a number of important contributions in the past couple of years. Among a number of insights, Williamson (forthcoming) shows that the issuance of CBDC can lead to disintermediation, but this may be socially valuable since it helps avoid over-accumulation of capital as described by Aiyagari (1994) and Diamond

[12]There are, of course, incentive problems in the private banking system. See Keister and Sanches (forthcoming) and Williamson (forthcoming) which incorporates this concern.

[13]Kahn & Roberds (2008) investigate identity theft and find two types of equilibria can exist that are relevant for the circulation of cryptocurrency. To begin, one equilibrium involves "existing account fraud" which includes theft of an existing card. The second type of equilibrium involves "new account fraud" which means that the data is stolen and used to create a new credit card account. Cryptocurrency users do not have to worry about the latter more costly type of fraud. However, existing account fraud is a significant issue. If an individual's "identity" is stolen by obtaining a holder's private key, they are limited to spending the balance at the address. Consequently, an account used frequently for transactions should be maintained with a low balance. Further, accounts should be maintained in separate wallets to avoid potential contagion resulting from a wallet's stolen password.

[14]For example, from "Lost Passwords Lock Millionaires Out of Their Bitcoin." 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. This amount of cash would be too bulky to carry around and lose at one time.

(1965). In related work, Keister and Sanches (forthcoming) study a model where the circulation of CBDC causes disintermediation to occur and bank deposits which circulate as a medium of exchange are displaced. While there can be positive social benefits in terms of promoting the level of exchange, there are also other negative macroeconomic consequences from higher costs of bank funding which lower investment in the economy. In comparison to the previous work, Andolfatto (2021) studies the impact of CBDC in a monopolistic banking sector. Due to the competitive pressure imposed on the monopolist, the amount of loans issued by the bank may increase if CBDC is introduced in the economy. Similar to our approach, Davoodalhosseini (2021) considers how the introduction of CBDC may displace physical cash a means of payment. The primary difference from our work compared to the existing literature is that we consider how financial intermediaries are important firms that can provide safekeeping. Depending on the level of safekeeping, participation in the private banking system is determined. The different levels of safekeeping also play a role in determining the conditions in which physical cash, private digital money, or CBDC circulate.

The remainder of the paper is organized as follows. Section II describes the benchmark physical environment. Section III looks at type I banks, type II banks, and type III banks. Section IV offers concluding comments.

## II. Environment

There is a [0,1] set of infinitely-lived consumers who consume and produce goods at different points in discrete time. Consumers first meet in a decentralized market (First Market or DM) and then in a centralized market (Second Market or CM). In addition to consumers, following Fernandez-Villaverde & Sanches (2019), there are also entrepreneurs (miners) who create tokens. Hereafter, we simply refer to their paper as 'FS'. In the second market, both types of agents interact and consume. In the first sub-period, consumers meet in pairs but entrepreneurs are idle. Consumers receive a preference shock to whether they can produce or consume at the beginning of the period. This friction along with the absence of record keeping creates a role for a medium of exchange. In contrast to BCW, profit-driven entrepreneurs provide one of the potential forms of a medium of exchange through producing electronic tokens. In addition, the central bank issues its own form of money which we call "government" money. This may take the form of an electronic token or as physical cash. If it is of the electronic version, we often describe this form of government money as "Central Bank Digital Currency (CBDC)". A consumer can produce but not consume with a probability of $n$ and can consume but not produce with a probability $1-n$. We will call a consumer who wants to consume a buyer and a consumer who can produce a seller.

Buyers get utility $u(q_b, q_b^g)$ from $q_b$ and $q_b^g$ consumption bought with private and government money respectively in the first market. However, the goods purchased with either type of money are identical. Hence, as we write $u(q_b, q_b^g)$, it is just a function of total consumption. Additionally, we have $u_{q_b}(q_b, q_b^g) > 0$, $u_{q_b^g}(q_b, q_b^g) > 0$, $u_{q_b q_b}(q_b, q_b^g) < 0$, $u_{q_b^g q_b^g}(q_b, q_b^g) < 0$, $u_{q_b}(0, q_b^g) = +\infty$, $u_{q_b^g}(q_b, 0) = +\infty$, $u_{q_b}(\infty, q_b^g) = 0$, and $u_{q_b^g}(q_b, \infty) = 0$. Sellers incur utility loss $c_{1,q_s}(q_s, q_s^g)$ from production of $q_s$ and $q_s^g$ units of goods in exchange for private money and government money respectively in the first market. Similar to utility, we can represent the disutility associated with total production. Lastly, the functional form of the cost function follows $c_{1,q_s}(q_s, q_s^g) \geq 0$, $c_{1,q_s^g}(q_s, q_s^g) \geq 0$, $c_{1,q_s q_s}(q_s, q_s^g) \geq 0$ and $c_{1,q_s^g q_s^g}(q_s, q_s^g) \geq 0$.

In addition to consumers, private banks and a central bank may also be active. In particular, private banks compete to offer their services in a perfectly competitive environment. In the DM, after the preference shock, sellers have no need for their money holdings in the DM and buyers would like to increase their money holdings for purchases. To attract deposits from sellers, banks

will offer interest on deposits and loan out this money to buyers in exchange for interest on the loan. In the CM, banks and consumers will settle their debt. Banks will be given a technology to force repayment at zero cost. However, they do incur costs for banking activity in general which are passed on to consumers in the amount $f$ for each unit of deposits. In contrast, the central bank only offers a safekeeping service to prevent token loss. Thus, we think about these costs as costs incurred in various banking activities such as safekeeping of money. Similarly, the central bank charges a fee $f_g$ that can vary from the fee of private banks. As we will explain below, introducing such costs makes the deposit decision non-trivial. In this manner, there will be conditions where individuals choose to "non-banked". Alternatively, central bank digital currency (the electronic form of government money in our model) may lead to disintermediation of the private banking system. See Keister and Sanches (forthcoming) and Williamson (forthcoming) who discuss these issues in detail.

By comparison, entrepreneurs have access to an additional technology that creates tokens. These tokens come in digital form.[15] 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 in the second sub-period $c_2 : \mathbb{R}_+ \to \mathbb{R}_+$ for minting tokens. We refer to the entrepreneurs as miners since 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. We denote the cost function of producing tokes as $c_2(\Delta)$ where $\Delta$ denotes the number of tokens produced since the process takes place in the second sub-period. To capture these costs, the cost function is strictly increasing and weakly convex: $c_2'(\Delta) > 0$, $c_2''(\Delta) \geq 0$, and $c_2(0) = 0$. Entrepreneurs create these tokens in exchange for the centralized market good produced by consumers. The entrepreneur's profit motive determines the supply of tokens which enable trade between buyers and sellers in the decentralized market. In contrast to private money production, the central bank mints government money at no cost. If the government money is of the electronic form, a centralized ledger is used. Thus, the central bank does not make use of a cost-intensive proof of work algorithm to verify the ledger.

By comparison, $x^e$ denotes an entrepreneur's consumption of the good produced in the second market. Entrepreneurs are only active in the second market with their preferences denoted by $U^e(x^e, \Delta) = x^e - c_2(\Delta)$.

For the most part, meetings in the first market are anonymous, precluding any chance of credit. This friction, along with the fact that goods are perishable, makes a medium of exchange necessary to facilitate trade. Although a token is intrinsically worthless, it obtains its value from use as a medium of exchange. Since entrepreneurs' only motivation is to maximize profits, their behavior can be predicted by other agents. This allows agents to form expectations about the future private money supply and use this to determine the relative price level over time. Additionally, the agents are aware of the growth rate of central bank currency and can correctly predict the price level in terms of government money.

In the second market all consumers consume and produce with utility $U(x)$ from $x$ consumption, $U'(x) > 0, U'(0) = \infty, U'(+\infty) = 0$ and $U''(x) \leq 0$. In addition, consumers have the ability to transform labor into a perishable good through the use of a linear technology. The consumers either consume the good or use it to exchange with entrepreneurs and consumers for tokens. By introducing differences in preferences among consumers across both sub-periods, money

[15] While some people may use paper wallets that resemble paper bills, this is only to store the private key and address of their bitcoins – miners play no part in producing them. Paper wallets are only one way among many of personally safekeeping a private key.

holdings are degenerate at the beginning of a period.[16] The discount factor across dates is $\beta \in (0, 1)$.

## Banks, Record keeping, and Storage

Following BCW, financial intermediation occurs through perfectly competitive private firms who accept nominal deposits and make nominal loans. In contrast to BCW, private banks facilitate borrowing and lending in terms of both forms of money. Moreover, the unique security features of cryptocurrency that lead to token loss give rise to the need of provision of security. However, with banks providing security, the consumer will lose the privacy of his transactions that comes with anonymity. Due to these potential concerns, the banking system around cryptocurrency could develop in a variety of ways. In order to address this, we will consider private "banks" that provide three different levels of security in our analysis. Consequently, we can analyze how the provision of different levels of banking affects the equilibrium allocation and welfare. The central bank may also offer to provide safekeeping of electronic government money (i.e., CBDC). However, it does not issue loans to private individuals.

All private banks make use of a technology at zero cost that allows record keeping of financial histories of individuals. In particular, all private banks will have a record of anyone who defaults on their one-period loan. Due to linear production costs in the CM, consumers have no need to smooth out the repayment of loans to the bank. Similar to BCW, banks do not have a record of trading histories in the first market. However, in our framework, type II and type III banks will have a partial record of trading histories due to processing transactions for consumers. Similar to BCW, there is no inside money issued that will influence the money supply. Moreover, in contrast to models with theft such as Kahn et al, He et al, and Sanches & Williamson (2010), the security features from banks have a direct influence on the supply of money. Specifically, money holdings are not shuffled from honest agents to thieves as in prior work, but lost from the money supply permanently. However, as previously mentioned, private banks charge a fee $f$ for accepting deposits. We view these costs as reflecting efforts towards safekeeping or other costs of banking activity. In a similar manner, individuals can also deposit their government money at the CB if it is electronic. The price of depositing funds with the CB may be different and is denoted as $f_g$.

As mentioned previously, consumers receive a preference shock upon entering the first market. After the preference shock, consumers will have the opportunity to conduct business with banks. No longer in need of a medium of exchange, sellers choose whether to deposit their money holdings at either private banks or the central bank. Buyers looking to supplement their money holdings can borrow either private money or government money that is deposited at private banks. In contrast, the CB only provides safekeeping. After dealing with the banks, buyers and sellers will meet up to trade. The timing described will be the same in each of the different bank type's environment. However, with each change of bank type, there will be variations in provision of security of money balances.

There will be three different cases concerning the banking setup. The first case will only have type I banks available. In this scenario, the bank will transfer the digital tokens to the borrowers from depositors, but does not provide safekeeping of tokens. As a result, the tokens will be susceptible to currency loss since the borrower is responsible for the security of the tokens. However, the seller will be shielded from token loss as the buyer is liable for any borrowed tokens lost in the DM. From this perspective, our framework differs in a significant way from BCW. Some users of digital currency may prefer this arrangement due to the anonymity that can still be retained. Moreover, we can analyze the benefits specifically from financial intermediation in terms of a digital currency subject to token loss. as previously mentioned, individuals may choose to be

[16] In this manner, our framework follows Lagos and Wright (2005).

"non-banked" due to the costs of transacting with banks.

We consider two additional scenarios in order to analyze the benefits of banks providing safekeeping. The second case will look at only type II banks. In this scenario, banks hold onto borrowed tokens to provide safekeeping for the buyer and will transfer tokens to the seller during the meetup between buyer and seller. The buyer retains tokens brought into the DM and supplements the transaction with the tokens left after token loss. In this case, banks ensure that tokens borrowed from the bank will not be susceptible to token loss. However, the buyer will lose anonymity with purchases made by the bank, but retain privacy with any remaining purchases. Lastly, in the third case, type III banks provide safekeeping for *both* buyers and sellers as they are able to process transactions in the DM between buyers and sellers. That is, a buyer will deposit all of his tokens with the type III bank at the beginning of the first sub-period. In this manner, token loss will be eliminated, but a buyer loses all anonymity with transactions processed by banks in the first market. Under most conditions for cryptocurrency, the elimination of token loss precludes the existence of a steady state. We will begin by looking at type I banks after we describe details of the central bank.

In part, central banks fund their activities by collecting a neutral lump-sum tax $\Lambda$ in the CM and they also do this through seigniorage. The central bank pays interest $i^g$ on money holdings in the CM each period. With the special case of physical currency, the interest paid out will be $i^g = 0$. Additionally, the central bank injects currency into the CM each period. The government's budget constraint is $\phi_t^g \tau M_t^g + \Lambda_t = \phi_t^g i^g M_t^g$ where $\Lambda$ represents a lump-sum tax collected by the government in the CM. The real price of private and government money is denoted by $\phi$ and $\phi^g$ respectively. Additionally, we have $M$ and $M^g$ representing the average stock of private and government money. The government will use the tax along with monetary injections to cover interest paid out to agents holding government money.

## III. Equilibrium Banking Activity

### Welfare

We now solve for the planner's first best allocation. The expected steady state lifetime utility of a consumer at the beginning of the period is given by:

$$(1-\beta)\mathcal{W} = (1-n)u(q_b, q_b^g) - nc_1(q_s, q_s^g) + U(x) - x, \tag{1}$$

where $q_b$ is consumption and $q_s$ is production in the first market. Agents are treated symmetrically by a planner who maximizes (1) subject to the feasibility constraint $(1-n)q_b = nq_s$. Optimal consumption of the good in the second market will satisfy $U'(x^*) = 1$. In addition, optimal consumption and production of the good in the first market are such that $u_{q_b}(q_b, q_b^g) = c_{1,q_s}(\frac{1-n}{n}q_b, \frac{1-n}{n}q_b^g)$. We let $q^* \equiv q_b^* = \frac{n}{(1-n)}q_s^*$ to yield $u_{q_b}(q_b^*, q_b^g) = c_{1,q_s}(\frac{1-n}{n}q_b^*, \frac{1-n}{n}q_b^g)$.

The following is a description of one time period in chronological order. To begin, the first market starts with consumers observing their production and consumption shocks. Again, consumers become either a buyer with a probability $(1-n)$ or seller with a probability $n$. After the shock, the banking sector opens and agents can borrow or deposit money. The banking sector then closes and trade takes place. This leads into the second market where they also trade goods, but in addition settle financial claims with a bank.

All consumers and entrepreneurs follow identical strategies and real allocations are constant over time in a stationary and symmetrical equilibrium. We define $M$ and $M^g$ as the average stock of private and government money held by consumers. In contrast, $m$ and $m_g$ denote an individual's holdings of money balances in terms of private and government money respectively. In a stationary

equilibrium, real money balances of private money at the end of the period are time-invariant $\phi M = \phi_{+1} M_{+1}$. Real money balances consisting of government money are invariant as well $\phi^g M^g = \phi^g_{+1} M^g_{+1}$. In terms of the money supply over time, $\gamma$ is the growth rate of private money. Thus, in the steady state

$$\frac{\phi}{\phi_{+1}} = \frac{P_{+1}}{P} = \frac{M_{+1}}{M} = \gamma.$$

Finally, in a steady-state where government money also circulates

$$\frac{\phi^g}{\phi^g_{+1}} = \frac{P^g_{+1}}{P^g} = \frac{M^g_{+1}}{M^g} = \gamma^g.$$

Let $V(m, m_g)$ denote the expected value from trading in market 1 with private money balances $m$ and goverment money balances $m_g$ at time $t$. In addition, $W(m, m_g, l, l_g, d, d_g, d_{c,g})$ denotes the value function of a consumer entering the second market with $m$ units of private money, $m_g$ units of government money, $l$ loans with private currency, $l_g$ loans with government currency, $d$ deposits with private money, and $d_g$ and $d_{c,g}$ deposits with government money at a private bank or the central bank respectively at time $t$.

## Type I Banks

We begin our analysis of equilibrium activity by studying an economy with Type I banks and a CB.

### Money Supply with Government Money and the Entrepreneur's Problem

The central bank and entrepreneurs determine the quantity of money in the economy. For the entrepreneur's problem, we first denote $M \in \mathbb{R}_+$ and $M^g \in \mathbb{R}_+$ as the per capita supply of private and government currency respectively in the current period and $M_{-1} \in \mathbb{R}_+$ and $M^g_{-1} \in \mathbb{R}_+$ as the supply of digital and government currency in the previous period. Next, we denote $\Delta \in \mathbb{R}_+$ as the entrepreneur's net circulation of newly minted tokens in the current period (or mined).

In addition to the government money injected by the central bank $\tau M^g_{-1}$, the evolution of the money supply depends on the rate of currency loss. Along with the probability of currency loss for private currency $\psi$ and government currency $\psi^g$, the law of motion for tokens depends on the type of bank available and consumer behavior.[17]

With type I banks, we can denote the law of motion for the total amount of private currency at the beginning of the DM in the current period by $M = \Delta + (1 - \psi)M_{-1}$. with $\psi M_{-1}$ representing the currency loss from the First Market. Next, regardless of the type of bank available, we can denote the law of motion for the total amount of government money at the beginning of the DM in the current period by $M^g = (1 + \tau - \rho\psi^g)M^g_{-1}$ with $\tau M^g_{-1}$ representing central bank injections. Additionally, with CBDC, token loss will impact the money supply each period. With a private bank, $\rho = 1$ and the bank will not impact the rate of token loss. However, with a deposit at the CB, $\rho = (1 - n)$ and the token loss will only affect money holdings brought in by buyers. This occurs because the CB only offers safekeeping of CBDC and therefore tokens will not be lent out to buyers who are susceptible to token loss.

[17] While many different types of CBDC are being considered across central banks, we consider that the CB introduces a token-based CBDC that uses a similar technology as cryptocurrency. For an introduction to the different types of CBDCs that are currently under consideration, see https://101blockchains.com/retail-cbdc-architecture/. The token-based form of CBDC is sometimes referred to as "token-based retail CBDC."

The entrepreneur's money holdings with $M \in \mathbb{R}_+$ for private digital tokens and $M^g \in \mathbb{R}_+$ for government currency. If we assume that $\Delta \geq 0$, then the the entrepreneur's budget constraint can be shown as

$$x + \phi M + \phi^g M^g = \phi\Delta + \phi M_{-1} + \phi^g M^g_{-1} \quad \forall t \geq 0$$

The entrepreneur will not participate in the First Market. Further, unless $\beta(1-\psi)\phi \geq \phi_{-1}$, the entrepreneur will choose not to hold currency across time periods. Thus, $M_{-1} + M^g_{-1} = M + M^g = 0$, and the budget constraint can be rewritten as $x = \phi\Delta$. The entrepreneur will consume an amount of the CM good equal to the amount of new tokens created. Since $\Delta \geq 0$, then $x \geq 0$.

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

$$\Delta^* \in arg \max_{\Delta \in \mathbb{R}_+} \big[\phi\Delta - c_2(\Delta)\big].$$

The amount of new token creation will adjust accordingly to any price change in tokens. Therefore, the solution to the entrepreneur's profit maximization problem satisfies $\phi = c_2'(\Delta^*)$. The entrepreneur will create additional tokens until the disutility from the work needed to create an additional token is equivalent to the real value of the token. For each period, the optimal amount of tokens for the entrepreneur to produce is $\Delta^* = (c_2')^{-1}(\phi)$.

Next, we determine the steady state stock of tokens for a given price $\overline{\phi}$. We consider three different initial values for tokens: $\phi = \overline{\phi}$, $\phi > \overline{\phi}$ and $\phi < \overline{\phi}$.

**Lemma 1**: *Suppose that the cost of producing tokens is $c_2(\Delta)$ and there is no cap on token production. Under these conditions, entrepeneurs after n periods will produce just enough currency to replace what is lost each period $\Delta^*_{+n} = \overline{\Delta}^* = \psi\overline{M}$.*

In summary, a stable price is the only possibility when there is no cap on total token production. By comparison, in FS, there is always an incentive for entrepreneurs to produce additional tokens and the supply of money will grow unbounded without token loss if the cost of producing tokens is strictly convex.[18] However, in our framework, entrepreneurs must have sufficient incentive to continually produce tokens over time to make up for token loss each period.

## A Consumer's Problem in the Second Market

Following BCW, in the second market, consumers produce $h$ goods and consume $x$, redeem interest payments on government money if the money is CBDC, and adjust their money balances. Entrepreneurs produce digital tokens for the Second Market good. The Central Bank injects government currency into the second market $\tau^e M^g$ and pays interest on money holdings $i^g$. The central bank can issue either CBDC or a physical currency. When holding government money, a consumer has the choice of depositing his funds in either a private bank or the central bank. A consumer who deposits $d_g$ units of the government currency at the private bank will receive $(1 + i^g_d)d_g$ units of government money, with $i^g_d$ as the interest the private bank pays out. Additionally, a consumer also has the option to deposit $d_{c,g}$ units of his CBDC tokens with the central bank. However, since the CB does not lend to individuals, it does not pay out any interest on deposits. As previously discussed, private banks and the CB charge different fees for accepting deposits. However, the CB does not provide safekeeping for physical currency. Thus, in the case of physical

[18] In order to achieve a stationary money supply, the FS environment needs a cap on total token production similar to Bitcoin. In Martin and Shreft (2006), agents are given what is known as L-beliefs. That is, agents do not value currency minted after a specified threshold. This will ensure agents stop minting currency at some point and the money supply is bounded.

cash, $f_g = 1$. The consumer will receive $(1 + i_d)d$ units of the private digital currency for a deposit $d$ minus a fee identical to a deposit made with government money. A consumer with an outstanding loan pays back $(1 + i_l^g)l_g$ units of the government money and $(1 + i)l$ units of private currency in the second market. Additionally, the bank does not protect the borrower from token loss.

In the second market, the consumer's problem is:

$$W(m^g, m, l_g, l, d_g, d_{c,g}, d) = \max_{x,h,m_{+1},m_{+1}^g} \left[U(x) - h + \beta V_{+1}(m_{+1}^g, m_{+1})\right]$$

$$\begin{aligned} s.t. \quad x + \phi^g m_{+1}^g + \phi m_{+1} = h + \phi^g(1+i^g)m^g + \phi m + \phi^g(1+i^g)(1+i_d^g)(1-f)d_g + \phi(1+i_d)(1-f)d \\ + \phi^g(1+i^g)(1-f_g)d_{c,g} - \phi^g(1+i_l^g)l_g - \phi(1+i)l - \Lambda \end{aligned} \tag{2}$$

where $m_{+1}$ and $m_{+1}^g$ is the amount of private and government money taken into period $t + 1$. The consumer will have $\phi^g(1 + i^g)(1 + i_d^g)(1 - f)d_g$ available from deposits with the private bank. This is a result of earning interest from the deposit as well as interest paid out by the central bank. Upon substituting for $h$, the consumer's problem becomes

$$\begin{aligned} W(m^g, m, l_g, l, d_g, d_{c,g}, d) = \phi^g\left[(1+i^g)m^g + (1+i^g)(1+i_d^g)(1-f)d_g + (1+i^g)(1-f_g)d_{c,g} - (1+i_l^g)l_g\right] \\ \phi\left[m + (1 + i_d)(1 - f)d - (1 + i)l\right] - \Lambda \\ + \max_{x,m_{+1}^g} \left[U(x) - x - \phi^g m_{+1}^g - \phi m_{+1} + \beta V_{+1}(m_{+1}^g, m_{+1})\right] \end{aligned}$$

The first order condition for the second market good is $U'(x) = 1$. Notably, the consumer's wealth does not influence the optimal choice for $x$. This is a result of the consumer's quasi-linear preferences. Moreover, consumption of the second market good is always the same. The consumer will adjust his production of the second market good to ensure money is leftover to bring into the first market. The consumer's demand for government money satisfies:

$$\phi^g \geq \beta(1 + i^g)V_{m^g,+1}(m_{+1}, m_{+1}^g)$$

where $V_{m^g,+1}(m_{+1}, m_{+1}^g)$ is the marginal value of an additional unit of government money taken into period $t + 1$. The price of a unit of government money is a function of its store of value and the goods it can buy in the following period's first market. In a similar manner, the consumer's demand for private tokens satisfies:

$$\phi \geq \beta V_{m,+1}(m_{+1}, m_{+1}^g)$$

where $V_{m,+1}(m_{+1}, m_{+1}^g)$ is the marginal value of an additional unit of digital money taken into period $t + 1$.

The seller must consider the benefit of the government money in the next period when deciding how much of the first market good to produce. In particular, the benefit of producing goods to acquire government currency is reflected in the following envelope condition:

$$W_{m,g}(m^g, m, l_g, l, d_g, d_{e,g}, d) = (1 + i^g)\phi^g.$$

The value of a marginal increase in government money held is reflected by the decrease in the disutility of labor in the second market by being able to sell the government money. Similarly, the benefit of producing goods to acquire private digital tokens is reflected in the following envelope condition:

$$W_m(m^g, m, l_g, l, d_g, d_{c,g}, d) = \phi.$$

When choosing how much to borrow, the consumer faces the marginal cost of paying back the loan in the following second market. The envelope condition for loans made with the sovereign currency is

$$W_{l^g}(m^g, m, l_g, l, d_g, d_{c,g}, d) = -\phi(1 + i_l^g).$$

That is, they will incur $\phi(1 + i_l^g)$ units of disutility as they will need to work more to repay their loans.

By comparison, the envelope condition for loans made with private money is

$$W_l(m^g, m, l_g, l, d_g, d_{c,g}, d) = -\phi(1 + i).$$

When making deposits of private money at private banks, the envelope condition for deposits is

$$W_d(m^g, m, l_g, l, d_g, d_{c,g}, d) = \phi(1 + i_d)(1 - f).$$

The envelope condition for deposits made with the government money is

$$W_{d,g}(m^g, m, l_g, l, d_g, d_{c,g}, d) = \phi^g(1 + i^g)(1 + i_d^g)(1 - f).$$

The benefit of depositing funds comes from the labor savings in the second market. Finally, the envelope condition for holding government money with the central bank is

$$W_{d,cg}(m^g, m, l_g, l, d_g, d_{c,g}, d) = \phi^g(1 + i^g)(1 - f_g).$$

The government will only charge the marginal cost of holding deposits. Thus, the fees it charges on net do not enter the government budget constraint.

## A Consumer's Problem in the First Market

Consumers are subject to token loss with both types of currency. Private digital money is subject to loss with a probability $\psi$, and government currency will be lost at a rate of $\psi^g$. However, we view that in practice the rate of token loss would essentially be the same. In the special case of physical currency, losses do not occur since there is no private key involved. We want to emphasize here that token loss is different than inflation. First with inflation, there is the potential for seignorage revenues to be rebated back into the economy. Second, only buyers who do not deposit funds are susceptible to token loss. Also, $p$ denotes the nominal price of goods in terms of private digital money and $p^g$ in terms of government money. In order to determine $p$ and $p^g$, we will use competitive pricing instead of bargaining. Buyers will never deposit funds and sellers will never take out loans, $l_s = l_{g,s} = d_b = d_{g,b} = 0$.

An agent with $m$ units of private money and $m^g$ units of government money at the beginning of the first market has expected lifetime utility

$$V(m, m_g) = (1-n)[u(q_b, q_b^g) + W((1-\psi)m + (1-\psi^g)m^g + (1-\psi)l + (1-\psi^g)l_g - pq_b - p^g q_b^g, l, l_g)] +$$
$$n[-c_1(q_s, q_s^g) + W((1-\psi)(m-d) + (1-\psi^g)(m^g - d_g - d_{c,g}) + pq_s + p^g q_s^g, d, d_g, d_{c,g})], \quad (3)$$

where $pq_b$ and $p^g q_b^g$ is the amount of money spent as a buyer with a private digital currency and government currency respectively. Additionally, $pq_s$ and $p^g q_s^g$ reflect the private digital and government money received by a seller. If a buyer, money will be brought into the second market if what is retained of the loan and money brought into the first period exceeds $pq_b + p^g q_b^g$. However, this will not ever be the case since the buyer decides on the loan amount in the first market. The buyer will not borrow more money then he plans on spending due to the interest costs of the loan. For the seller, he will hold on to all of the money received in the first market for producing goods for a buyer. Since type I banks do not provide safekeeping, individuals would obtain the highest level of privacy in transactions.

## Sellers' decisions

A seller can deposit his money holdings in either a private bank or with the central bank. In doing so, his deposits will be shielded from token loss. Though private banks pay interest on deposits that they hold, the central bank does not because it does not engage in lending like private banks do.

We will now cover potential scenarios for a seller in the DM. First, they will need to make a decision on whether or not they will accept government money, private money, or potentially both. In doing so, the sellers' only concern is whether or not a currency is valued in the following CM. As long as the currency is valued, they will adjust their level of production according to its expected value next period. The seller may be willing to accept both currencies simultaneously as well. Next, we look at the deposit decision of the seller. The seller must first make a decision on whether they will deposit or not. If so, he will then decide if the deposit will be made at a private bank or the central bank.

In looking at sellers' decisions, we note that there are eight different possible scenarios. The first case is only relevant for sellers holding private money while the other scenarios consider sellers holding government money. Under case 1, we find conditions where individuals deposit private money at private banks. This is the only decision for a seller holding private money to consider because the CB will not accept deposits of private money. In case 2, we find conditions in which individuals deposit physical cash if that is the form of government money that is supplied. Under case 3, we look at the potential for disintermediation at the CB to occur. That is, we find conditions in which sellers do not deposit government money at the CB. Further, in case 4, we find conditions where sellers also do not deposit government money at private banks. Thus, if both (3) and (4) apply, sellers holding government money choose to be "non-banked".

Under case 5, we look at where sellers will choose to bank if they choose to deposit government money. In 5A, individuals deposit government money at private banks, but not the CB due to central bank fees being greater than the rate of token loss. In this case, government money does not lead to disintermediation of the private banking system. This is equivalent to central banks issuing their own digital tokens, but outsourcing the safekeeping functions to private banks. Such an approach seems to be favored among central banks contemplating issuing CBDC. For example, in a report issued by the European Central Bank on the possibility of a digital euro, Lagarde and Panetta (2020) argue: "While the Eurosystem would always retain control over the issuance of a digital euro, supervised private intermediaries would be best placed to provide ancillary, user-facing services and to build new business models on its core back-end functionality. A model whereby access to the digital euro is intermediated by the private sector is therefore preferable."[19] Under 5B, disintermediation does occur as sellers choose to deposit at the CB but not at private banks. Under 6A, sellers are willing to use both types of banks, but ultimately choose to deposit at private banks. With 6B, the seller would rather use both banks than go unbanked, but will choose to use the CB. Lastly, under condition 6C, the seller is indifferent between making a deposit at each type of bank. As a result, there may be partial disintermediation due to some of the funds ending up at the CB.

The problem of a seller is

$$\max_{q_s^g, q_s, d_g, d_{c,g}, d} [-c_1(q_s^g, q_s) + W((1-\psi^g)(m^g - d_g - d_{c,g}) + (1-\psi)(m-d) + p^g q_s^g + pq_s, d_g, d_{c,g}, d)]$$

$$s.t. \quad d_{c,g} \leq \alpha m^g, d_g \leq (1-\alpha)m^g, d \leq m$$

[19] Further, in a speech about the potential issuance of a digital euro, Panetta (February 10, 2021) argues: "...the ECB does not plan to interact directly with potentially hundreds of millions of users of a digital euro. We simply do not have the capacity or the resources to do so. Financial intermediaries – in particular banks – would provide the front-end services, as they do today for cash-related operations. We would provide safe money, while financial intermediaries would continue to offer additional services to users."

where $\alpha$ and 1-$\alpha$ represent the proportion of the seller's money holdings that may be deposited at either the CB or at private banks.

We begin by looking at the amount that sellers are willing to produce in exchange for private tokens. In this decision, the seller's first order condition for $q_s$ is

$$-c_{1,q_s}(q_s^g, q_s) + W_m(m^g, m, l_g, l, d_g, d_{e,g}, d)(p) = 0$$

In choosing how much to produce, the seller looks at tradeoffs over disutility to be incurred in the DM and CM. From the envelope condition for private money balances $c_{1,q_s}(q_s^g, q_s) = p\phi$. The amount sellers produce is independent of $m$ and $d$ due to linear preferences. The seller trades off the level of disutility between production in the DM and CM.

Next, we find the first order condition for producing goods in exchange for government money $q_s^g$

$$-c_{1,q_s^g}(q_s^g, q_s) + W_{m,g}(m^g, m, l_g, l, d_g, d_{e,g}, d)(p^g) = 0.$$

By the envelope condition for government money balances $c_{1,q_s^g}(q_s^g, q_s) = p^g\phi^g(1 + i^g)$. When making his production decision, the seller takes into consideration the interest paid on the government currency. In the special case of physical currency, the decision becomes $c_{1,q_s^g}(q_s^g, q_s) = p^g\phi^g$. Production is once again independent of $m^g$ and $d_g$.

Next, we take a look at the seller's decision of how much money to deposit with banks. The seller's deposit decision becomes

$$\mathscr{L} \max_{d,d_g,d_{c,g}} = -c_1(q_s^g, q_s) + W((1-\psi^g)(m^g - d_g - d_{c,g}) + (1-\psi)(m-d) + p^g q_s^g + pq_s, d_g, d_{c,g}, d)$$
$$-\lambda_d(d-m) - \lambda_d^{c,g}(d_{c,g} - \alpha m^g) - \lambda_d^g(d_g - (1-\alpha)m^g)$$

where $\lambda_d$, $\lambda_d^{c,g}$ and $\lambda_d^g$ are the Lagrange multipliers on the deposit constraint with private money, government money with the central bank, and government money at a private bank.

The first order condition with respect to $d$ is:

$$-(1-\psi)W_m + W_d - \lambda_d = 0$$

Substitute the envelope conditions $W_m = \phi$ and $W_d = \phi(1 + i_d)(1 - f)$ to obtain $\lambda_d = \phi((1-f)i_d - f + \psi)$. With $i_d > \frac{f-\psi}{1-f}$, the constraint binds and $d = m$. Under this scenario, the conditions for case 1 will be satisfied. The consumer would choose to deposit private money if the interest rate on deposits exceeds the bank's fee for accepting deposits. The required rate of return would be lower however if there is a greater role for safekeeping (i.e., $\psi$ is higher).

We now turn to look at the decision to deposit government money at private banks through the first-order condition with respect to $d_g$:

$$-(1-\psi^g)W_{m,g} + W_{d,g} - \lambda_d^g = 0$$

From the envelope conditions $W_{m,g} = \phi^g(1 + i^g)$ and $W_{d,g} = \phi^g(1 + i^g)(1 + i_d^g)(1 - f)$, we have:

$$\lambda_d^g = \phi^g(1 + i^g)((1 + i_d^g)(1 - f) - (1 - \psi^g))$$

With physical currency, this reduces down to $\lambda_d^g = \phi^g(1-f)i_d^g - f$. The government does not provide safekeeping and payment services with physical currency. If the interest from a deposit is positive $i_d^g > \frac{f}{1-f}$, then conditions for case 2 will be met with the seller depositing all of the physical currency. Next, we look at the decision when agents are holding CBDC and may choose to deposit with a CB.

The first order condition for deposits of government money at the CB is

$$-(1-\psi^g)W_{m,g} + W_{d,eg} - \lambda_d^{e,g} = 0$$

Substitute the envelope conditions $W_{m,g} = \phi^g(1+i^g)$ and $W_{d,eg} = \phi^g(1+i^g)(1-f_g)$ to obtain

$$\lambda_d^{c,g} = \phi^g\big((1+i^g)\big((1-f_g) - (1-\psi^g)\big)$$

If $\psi^g < f_g$, the service fees exceed the cost of potential loss of tokens. In which case, conditions for case 3 are met and the seller will not deposit funds at the central bank.

We next consider case 4 in which sellers also choose not to deposit CBDC at private banks. With CBDC, the multiplier is shown by

$$\lambda_d^g = \phi^g(1+i^g)((1+i_d^g)(1-f) - (1-\psi^g))$$

If $i_d^g < \frac{f-\psi^g}{1-f}$, condition 4 will be met and the seller is not willing to deposit at a private bank. The benefit from interest on deposits does not exceed the possibility of loss after service fees are deducted. Thus, if both case 3 and case 4 hold, individuals holding government money are "non-banked".

When do individuals holding government money choose to use either type of bank? We can find conditions where sellers use one bank or the other. First, if $\psi_g < f_g$ and $i_d^g > \frac{f-\psi^g}{1-f}$, the conditions for case 5a are met and the seller deposits his holdings of government money with the private bank but not the CB. In this case, the returns from using the private bank exceed the cost from potential token loss. In contrast, the service costs from depositing at the CB are greater than token loss. Next, if $f_g < \psi^g$ and $i_d^g < \frac{f-\psi^g}{1-f}$, the conditions for 5B are met. Thus, the individual will deposit CBDC at the CB, but not at private banks even though depositing at private banks dominates holding tokens individually.

We proceed by considering that even though depositing funds at the CB is better than holding the government money individually, the returns from depositing funds at private banks dominate the returns from depositing funds at the CB. In this case, the derivative of the seller's utility with respect to $\alpha$ is less than zero if the following holds $\lambda_d^{c,g} < \lambda_d^g$. Upon substituting $\lambda_d^{cg}$ and $\lambda_d^g$, the seller would deposit all of his funds at private banks as long as $i_d^g > \frac{f-f_g}{1-f}$. If $f_g < \psi_g$, and $i_d^g > max\Big\{\frac{f-\psi^g}{1-f}, \frac{f-f_g}{1-f}\Big\}$, the conditions for case 6A hold and the seller ultimately would deposit all of his funds at private banks. On the other hand, if $f_g < \psi_g$, and $i_d^g > \frac{f-\psi^g}{1-f}$, but $i_d^g < \frac{f-f_g}{1-f}$, the seller would ultimately deposit all of his funds at the CB even though depositing funds at private banks dominates holding tokens individually. Lastly, condition 6C is met if $i_d^g = \frac{f-f_g}{1-f}$, and the seller is indifferent to depositing with the two banks.

## Buyers' decisions

After the consumer receives his shock to become a buyer, he may take out a loan from a private bank. With private Type I banks, such banks will not provide safekeeping for buyers and will not process transactions with the loan. Buyers are willing to borrow any type of currency that they carry into the DM. If they carry both government and private currency, they will be willing to borrow both types of currency. Additionally, in regards to a physical currency or CBDC, consumers will self-insure for consumption shocks and not borrow money if the return to currency is high enough. Lastly, when buyers choose to carry only private money with $\psi > 0$, the buyers will always take out a loan.

When we previously discussed the seller's problem, we noted that there will be conditions where banks do not hold deposits of a particular type of currency. However, for brevity, our analysis of the buyer's problem assumes that either case 1, case 2, case 5A, or 6A hold. As a result, banks hold all types of deposits and can thereby make loans in any type of currency. Thus, we start by determining how much of any currency that buyers will want to borrow.

If an agent is a buyer in the first market, his problem becomes

$$\max_{q_b^g, q_b, l_g, l} [u(q_b^g, q_b) + W((1-\psi^g)m^g + (1-\psi)m + (1-\psi^g)l_g + (1-\psi)l - p^g q_b^g - pq_b)]$$

$$s.t. \quad p^g q_b^g \leq (1-\psi^g)m^g + (1-\psi^g)l_g, pq_b \leq (1-\psi)m + (1-\psi)l$$

In contrast to BCW, money brought into the DM is subject to currency loss. Due to the degree of currency loss, the buyer can only spend a portion of money he brings into the market, $(1-\psi)m$ and $(1-\psi^g)m^g$. However, with physical currency, the liquidity constraint is $p^g q_b^g \leq m^g + l_g$ because physical currency is not associated with a private key.

Additionally, as we previously discussed, if sellers do not deposit with the private bank, the buyer cannot take out a loan of any size. The buyer takes the constraint as given but it is determined endogenously in equilibrium. The buyer's problem becomes

$$\mathscr{L} \max_{q_b, q_b^g, l, l_g} = u(q_b, q_b^g) + W((1-\psi)m + (1-\psi^g)m^g + (1-\psi)l + (1-\psi)l_g - pq_b - p^g q_b^g, l + l_g)$$

$$-\lambda(pq_b - (1-\psi)m - (1-\psi)l)) - \lambda^g(p^g q_b^g - (1-\psi^g)m^g - (1-\psi^g)l_g) - \lambda_l(l - \bar{l}) - \lambda_l^g(l_g - \bar{l}_g)$$

where $\lambda$ is the multiplier on the buyer's private digital cash constraint, $\lambda^g$ is the multiplier on the buyer's government currency constraint, $\lambda_l$ on the borrowing constraint with private digital tokens and $\lambda_l^g$ is the borrowing constraint with government money.

We will look at the buyer's choice of quantity of the first market good $q_b$ bought with a private digital currency first. The buyer's first order condition is

$$u_{q_b}(q_b, q_b^g) = pW_m + p\lambda.$$

The buyer's desired amount of consumption depends on the cost of working to repay the loan and whether the liquidity constraint binds. Upon substituting $W_m = \phi$ and $\frac{c_{1,q_s}(q_s, q_s^g)}{\phi} = p$

$$u_{q_b}(q_b, q_b^g) = c_{1,q_s}(q_s, q_s^g)\Big(1 + \frac{\lambda}{\phi}\Big)$$

After the substitutions, we compare the buyer's gain in value from an additional unit of consumption versus the seller's disutility from producing the additional amount of goods. Notably, the cash

constraint drives a wedge between the buyer's and seller's marginal returns. Thus, this inefficiency drives down the value of trade between the buyer and the seller.

Next, we will look at the buyer's choice of quantity of the first market good $q_b^g$ to buy with government currency. The buyer's first order condition for choosing how much to purchase with government money is

$$u_{q_b^g}(q_b, q_b^g) = p^g W_{m^g} + p^g \lambda^g.$$

Akin to the use of private digital tokens, the buyer's desired amount of consumption depends on the cost of working to repay the loan and whether the liquidity constraint binds.

From $W_{m,g} = \phi^g(1 + i^g)$ and $\frac{c_{1,q_s^g}(q_s,q_s^g)}{\phi^g} = p^g(1 + i^g)$ we obtain

$$u_{q_b^g}(q_b, q_b^g) = c_{1,q_s^g}(q_s, q_s^g)\Big(1 + \frac{\lambda^g}{\phi^g(1 + i^g)}\Big)$$

Similar to when private digital tokens are in use, the last equation compares the gains from additional consumption at the cost of producing goods. However, the seller will consider the interest paid by the central bank when making their production decision. In particular, if the interest rate on CBDC is higher, buyers will be able to obtain more consumption.

The buyer's first order condition for $l$ is

$$(1 - \psi)W_m + (1 - \psi)\lambda = -W_l + \lambda_l$$

Each unit of funding from digital currency provides the buyer with more cash that he values at rate $W_m$. It also helps relieve the constraint on money holdings which he values at rate $\lambda$. However, the buyer will be held back by his debt brought into the second market.

From the previous envelope conditions: $W_m = \phi$ and $W_l = -\phi(1 + i)$

$$\lambda = \frac{\phi(i + \psi) + \lambda_l}{(1 - \psi)}$$

If $\lambda = 0$, then $u_{q_b}(q^*, q_b^g) = c_{1,q_s}(q^*, q_s^g)$ and trades are efficient. However, for this to occur, deflation must be at a rate $\gamma = \beta$ and currency loss must be zero and the loan constraint must not bind. Upon substituting for $\lambda$, the quantity traded in the first market satisfies:

$$\frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, q_s^g)} = 1 + \frac{(i + \psi)}{(1 - \psi)} + \frac{\lambda_l}{\phi(1 - \psi)}$$

If the borrowing constraint does not bind,

$$\frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, q_s^g)} = 1 + \frac{(i + \psi)}{(1 - \psi)} = \frac{1 + i}{1 - \psi}$$

which provides banks with the ability to fund loans of private tokens where the buyer borrows up to the point the marginal benefit of borrowing equals the marginal cost. In comparison to BCW, he will not borrow as much because loans in terms of digital money are subject to loss of the private key. He then spends all his private digital money and consumes $q_b = (1 - \psi)(m + l)/p$. Here, we also see the costs of currency loss. Additionally, trades are inefficient as long as $i > -\psi$.

All buyers enter the period with the same amount of private digital money and therefore face the same problem. The same is true for the seller and so $q_b$ and $q_s$ is the same for all buyers and sellers respectively $q_s = \frac{1-n}{n} q_b$.

The buyer's first order condition for $l_g$ is

$$(1-\psi^g)W_{m,g} + (1-\psi^g)\lambda^g \leq -W_{l^g} + \lambda_l^g$$

Each unit of funding from government money provides the buyer with more cash that he values at rate $W_{m,g}$. It also helps relieve the constraint on money holdings which he values at rate $\lambda^g$. However, the buyer will be held back by his debt which must be paid in units of the sovereign currency.

From the previous envelope conditions: $W_{m,g} = \phi^g(1+i^g)$ and $W_{l^g} = -\phi^g(1+i_l^g)$

$$\lambda^g \leq \frac{\phi^g(1+i_l^g - (1-\psi^g)(1+i^g)) + \lambda_l^g}{1-\psi^g}$$

Upon substituting for $\lambda^g$, the quantity traded in the first market satisfies:

$$\frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, q_s^g)} = \frac{(1+i_l^g)}{(1+i^g)(1-\psi^g)} + \frac{\lambda_l^g}{\phi^g(1+i^g)}$$

If the borrowing constraint does not bind,

$$\frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, q_s^g)} = \frac{(1+i_l^g)}{(1+i^g)(1-\psi^g)}$$

The buyer borrows up to the point where the marginal benefit of borrowing equals the marginal cost. The buyer takes into account the rate of token loss and the interest that can be earned from the CBDC. Under the special case of physical cash, this condition becomes to $\frac{u_{q_b}(q_b,q_b^g)}{c_{1,q_s}(q_s,q_s^g)} = 1 + i_l^g$. He then spends all his government money and consumes $q_b^g = \big((1-\psi^g)(m^g+l)\big)/p^g$.

All the buyers enter the period with the same amount of government money and therefore face the same problem. The same is true for the seller and so $q_b^g$ and $q_s^g$ is the same for all buyers and sellers respectively $q_s^g = \frac{1-n}{n} q_b^g$.

## A Bank's Problem

As was previously stated, we begin by focusing on type I banks with private tokens in use. The details of the bank's problem under type II and type III banks are available in the appendix. For such banks, the only function they serve is to intermediate between borrowers and lenders. Banks will compete with one another by offering better deposit rates. As a result of perfect competition, the interest rates will be driven to parity: $i = (1-f)i_d - f$. The representative bank solves the following problem per borrower:

$$\max_l (i + f - (1-f)i_d)l$$

$$s.t. \quad l \leq \bar{l}, \quad u(q_b, q_b^g) - (1+i)l\phi \geq \Gamma,$$

where $\Gamma$ is the reservation value of the borrower. The reservation value represents the surplus a borrower would receive from taking out a loan from another bank.

Since the bank will receive no profits due to free entry, it reduces down to:

$$\frac{(1-\psi)u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, q_s^g)} = 1 + i + \frac{\lambda_L}{\phi\lambda_\Gamma}$$

With $\bar{l} = \infty$, $\lambda_L = 0$ and the loan amount satisfies $\frac{u_{q_b}(q_b,q_b^g)}{c_{1,q_s}(q_s,q_s^g)} = \frac{(1+i)}{(1-\psi)}$. This is the same amount that satisfies the buyer's desired demand since the loan constraint does not bind. However, if enforcement of loan contracts is not costless or banks are unable simply to enforce contracts, then the lending constraint may bind so that $\lambda_L > 0$. In this case, trade in the DM will be even more inefficient with $\frac{u_{q_b}(q_b,q_b^g)}{c_{1,q_s}(q_s,q_s^g)} > \frac{(1+i)}{(1-\psi)}$. In comparison to BCW, the degree of inefficiency is stronger because of the rate of token loss.

We now show the condition with government money in use and refer to the appendix for how it is derived. With $\bar{l} = \infty$, $\lambda_L = 0$ and the loan amount for CBDC satisfies $\frac{u_{q_b^g}(q_b,q_b^g)}{c_{1,q_s^g}(q_s,q_s^g)} = \frac{(1+i_l^g)}{(1+i^g)(1-\psi^g)}$. If a physical currency is in use, this becomes identical to BCW $\frac{u_{q_b^g}(q_b,q_b^g)}{c_{1,q_s^g}(q_s,q_s^g)} = 1 + i_l^g$. Both of these amounts that satisfies the buyer's desired demand since the loan constraint does not bind.

## Marginal Value of Private and Government Money

Consumers can carry either government or a private digital currency into the DM. We will start by looking at the choice of private digital money holdings. In choosing the amount of private money balances to acquire in the CM, consumers need to consider the probability of being a buyer $(1-n)$ and being a seller $(n)$ in the following DM. A buyer values their tokens for the first market good they can purchase. Also, if a buyer, they need to consider the amount of private digital money that can be borrowed from banks. This will reduce the amount of private digital tokens they carry into the first market. If a seller, the tokens derive worth from the store of value function. However, with digital tokens, they also take the probability of token loss into account.

As in the previous section, we initially consider that buyers will be able to borrow any type of currency. Upon determining the amount of money an individual will want to carry into the DM, we will conclude by looking at the different conditions where intermediation in terms of each type of currency occurs. The marginal value of private money starts with:

$$V_m(m,m^g) = (1-n)\left[u_{q_b}(q_b,q_b^g)\frac{\partial q_b}{\partial m} + W_m\Big((1-\psi) - p\frac{\partial q_b}{\partial m} + (1-\psi)\frac{\partial l}{\partial m}\Big) + W_l\frac{\partial l}{\partial m}\right]$$

$$+n\left[-c_{1,q_s}(q_s,q_s^g)\frac{\partial q_s}{\partial m} + W_m\left((1-\psi) + p\frac{\partial q_s}{\partial m} - (1-\psi)\frac{\partial d}{\partial m}\right) + W_d\frac{\partial d}{\partial m}\right]$$

Money brought into the DM by a seller will not affect his production of the DM good. Therefore, we can substitute $\partial q_s/\partial m = 0$ for the consumer's decision on money holdings. Also, since sellers deposit all of their holdings of private money, $\partial d/\partial m = 1$.

Lastly, use the envelope conditions for cash, loans, and deposits to get

$$V_m(m,m^g) = (1-n)\left[u_{q_b}(q_b,q_b^g)\frac{\partial q_b}{\partial m} + \phi\Big((1-\psi) - p\frac{\partial q_b}{\partial m} + (1-\psi)\frac{\partial l}{\partial m}\Big) - \phi(1+i)\frac{\partial l}{\partial m}\right] + n\phi(1+i_d)(1-f)$$

If a buyer in the first market, the consumer must weigh the additional utility provided from consumption of the first market good bought with an additional unit of private money. Additionally, the buyer considers the gain in utility from borrowing less funds from banks. If a seller, an

additional unit of money will reduce his labor in the second market. In particular, this will depend on the interest rate paid by banks on deposits of tokens.

All of the tokens held by a buyer will be spent in the first market. Consequently, $p(\partial q_b/\partial m) = (1-\psi) + (1-\psi)\partial l/\partial m$ and the first order condition becomes:

$$V_m(m, m^g) = (1-n)\left[u_{q_b}(q_b, q_b^g)\frac{\partial q_b}{\partial m} - \phi(1+i)\frac{\partial l}{\partial m}\right] + n\phi(1+i_d)(1-f)$$

As a buyer, the net role of money demand is to purchase more goods and reduce borrowing costs. Next, substitute $\frac{\partial l}{\partial m} = \frac{p}{(1-\psi)}\frac{\partial q_b}{\partial m} - 1$

$$V_m(m, m^g) = (1-n)\left[\frac{\partial q_b}{\partial m}(u_{q_b}(q_b, q_b^g) - \frac{\phi(1+i)p}{(1-\psi)}) + \phi(1+i)\right] + n\phi(1+i_d)(1-f)$$

Recall the equilibrium conditions from the credit market, $\frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s)} = \frac{(1+i)}{(1-\psi)}$. Next, substitute $c_{1,q_s}(q_s, q_s^g) = p\phi$. Then, we apply $u_{q_b}(q_b, q_b^g) = p\phi\frac{(1+i)}{(1-\psi)}$ to obtain

$$V_m(m, m^g) = (1-n)\frac{(1-\psi)u_{q_b}(q_b, q_b^g)}{p} + n\phi(1+i_d)(1-f) \tag{4}$$

which is similar to BCW, but the marginal value of tokens is lower in our setup due to token loss. In regards to the first term, an extra unit of money allows consumers to buy more goods depending on the rate of token loss and prices in the DM. The second term reflects the store of value which is enhanced by depositing tokens with banks. These funds are not susceptible to token loss because buyers are responsible for all tokens that are borrowed from banks. In a symmetric equilibrium $q_s = \frac{1-n}{n}q_b$. If $m < m^*$ then $0 < q_b < q^*$ and so $\partial q_b/\partial m > 0$. Thus, $V_{mm}(m, m^g) < 0$. When $m \geq m^*$ then $q_b = q^*$ implying $\partial q_b/\partial m = 0$. Thus, $V_{mm}(m, m^g) = 0$. Hence, $V(m, m^g)$ is concave in $m$.

From $c_{1,q_s}(q_s, q_s^g) = p\phi$ in (4)

$$V_m(m, m^g) = \phi\left[(1-n)\frac{(1-\psi)u_{q_b}(q_b, q_b^g)}{c_{q_s}(q_s, q_s^g)} + n(1+i_d)(1-f)\right] \tag{5}$$

Equation (5) reflects the dual role of money. When a buyer, he receives $(1-\psi)u_{q_b}(q_b, q_b^g)/c_{1,q_s}(q_s, q_s^g)$ due to the medium of exchange role. If the agent is a seller, he lends money and receives $(1+i_d)(1-f)$ from the return on deposits of tokens. In particular, the extent of token loss reduces the value of money.

Now we look at the marginal value of government money. As the derivation of the government money version of equation (5) above is similar to the case of private money, we omit much of the algebra in the text. Details, however, are available in a separate appendix. Government money potentially earns interest which increases its store of value and purchasing power.

$$V_m^g(m, m^g) = (1-n)\left[\frac{(1-\psi^g)u_{q_b^g}(q_b, q_b^g)}{p^g}\right] + n\phi^g(1+i^g)(1+i_d^g)(1-f)$$

In regards to the first term, an extra unit of money allows consumers to buy more goods depending on the rate of token loss and prices in the DM. The second term reflects the store of value which is

enhanced by depositing tokens with banks. These funds are not susceptible to token loss, but a service fee is deducted for this service in addition to the interest earned.

From $c_{1,q_s^g}(q_s, q_s^g) = p^g \phi^g (1 + i^g)$ in (4)

$$V_m^g(m, m^g) = \phi^g \left[ (1-n) \frac{(1-\psi^g)(1+i^g) u_{q_b^g}(q_b, q_b^g)}{c_{q_s^g}(q_s, q_s^g)} + n(1+i^g)(1+i_d^g)(1-f) \right] \tag{6}$$

Equation (6) reflects the dual role of money. When a buyer, he receives $(1-\psi^g)(1+i^g)u_{q_b^g}(q_b, q_b^g)/c_{1,q_s^g}(q_s, q_s^g)$ due to the medium of exchange role. If the agent is a seller, he lends money and receives $(1+i_d^g)(1-f)$ from the net return on deposits of tokens. In particular, the extent of token loss reduces the value of money, where as the interest from the central bank increases it.

In comparison to FS, we establish that a monetary equilibrium with price stability exists if the costs of producing new private tokens are strictly convex where $c_2'(0) = 0$. To do so, we find the nominal interest rate that will clear the market. From $\phi = \beta V_{+1,m}(m_{+1}, m_{+1}^g)$, substitute into (5) to get:

$$\frac{\phi_{-1}}{\beta} = \phi \left[ (1-n) \frac{(1-\psi) u_{q_b}(q_b, q_b^g)}{c_{q_s}(q_s, q_s^g)} + n(1+i_d)(1-f) \right]$$

Now use $q_s = \frac{1-n}{n} q_b$ and $\frac{\phi_{-1}}{\phi} = \gamma$ and subtract both sides by the real value of a token $\phi$:

$$\frac{\gamma - \beta}{\beta} = (1-n) \left[ \frac{(1-\psi) u_{q_b}(q_b, q_b^g)}{c_{q_s}(q_s, q_s^g)} - 1 \right] + n((1-f)i_d - f) \tag{7}$$

The right-hand side measures the value of bringing a marginal unit of money into the first market. The first term is the net benefit (marginal benefit minus marginal cost) of spending the unit of money on goods when a buyer and the second term is the net benefit from depositing a unit of idle balances when a seller. The first term is lowered by the potential to lose currency in the first market.

Since banks can enforce repayment, they will be unconstrained and $\bar{l} = \infty$. Consequently, $\lambda_l = 0$ and $\frac{u_{q_b}(q_b, q_b^g)}{c_{q_s}(q_s, q_s^g)} = \frac{1+i}{1-\psi}$ in (6) yields

$$\frac{\gamma - \beta}{\beta} = (1-n)i + n[(1-f)i_d - f]$$

The first term now represents the interest saving from borrowing one less unit of money when a buyer.

Zero profits for banks implies $i = (1-f)i_d - f$. Therefore, we have

$$\frac{\gamma - \beta}{\beta} = i \tag{8}$$

In terms of $q_b$:

$$\frac{\gamma - \beta}{\beta} = \frac{(1-\psi) u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, q_s^g)} - 1 \tag{9}$$

The rate of token loss impacts the quantity of goods traded. This is due to only sellers being shielded from token loss.

We now find the monetary equilibrium with credit using government money. Akin to the derivation for private money, the derivation can be found in the appendix. Ultimately, in regards to the interest on deposit, we obtain

$$\frac{\gamma^g - \beta(1+ni^g)}{\beta(1+ni^g)(1-f)} + \frac{f}{1-f} = i_d^g \tag{10}$$

The interest rate that clears the market is decreasing in the interest rate on CBDC. Obviously, the store of value motive for holding CBDC is increasing in the rate of interest paid by the CB. As a result, the bank can offer a lower interest rate to the seller and still ensure enough money is brought into the DM for an equilibrium to exist. The rate of token loss has no effect on the interest rate with type I banks. Without safekeeping for loans, the consumer will not discriminate between money carried into the DM and money that is borrowed. Therefore, the banks cannot charge a higher rate of interest on loans with a change in the rate of token loss.

Next, $q_b^g$ is pinned down through the following condition:

$$\frac{\gamma^g - \beta(1+ni^g)}{\beta(1+ni^g)} = \frac{(1+i^g)(1-\psi^g)u_{q_b^g}(q_b, q_b^g)}{c_{q_s^g}(q_s, q_s^g)} - 1 \tag{11}$$

Now that we have determined the equilibrium interest rates on deposits, we can pin down the conditions for sellers to deposit funds at the different banks. In particular, we will focus on conditions in which intermediation in terms of each form of money will take place. We begin by studying the conditions where case 1 holds and sellers deposit their private tokens at private banks. In order for private tokens to be deposited, we need $i_d > \frac{f-\psi}{1-f}$. Upon substituting for $i_d$, the condition for case 1 is satisifed as long as individuals discount the future and some amount of token loss occurs. In particular, this holds if $1 > \beta(1-\psi)$. As long as the seller discounts the future and there is token loss, he will deposit his funds.

Next, we look at the conditions where case 2 applies. Notably, in this case we require $i_d^g > \frac{f}{1-f}$. Upon substituting the deposit rate, case 2 applies as long as the gross growth rate of cash is positive. That is, $\sigma^g > -1$. We proceed by studying the conditions where case 5A holds and sellers deposit their CBDC at private banks. Sellers will choose to deposit their funds as long as $\psi^g < f^g$ and $i_d^g > \frac{f-\psi^g}{1-f}$. Notably, this occurs as long as $\sigma^g > (1-\psi^g)\beta(1+ni^g)-1$.

Finally, we turn to look at case 6A. If $f_g < \psi_g$, and $i_d^g > max\left\{\frac{f-\psi^g}{1-f}, \frac{f-f_g}{1-f}\right\}$, sellers will choose to deposit with the private bank even though it's better to deposit with the CB than go unbanked. After substituting for the deposit rate, case 6A holds as long as $\gamma^g > (1-f_g)\beta(1+ni^g)$. This takes place if $\sigma^g > (1-f_g)\beta(1+ni^g) - 1$. Thus, in all of these cases, the creation of CBDC does not lead to disintermediation of the private sector. In summary, we argue that issuing CBDC does not lead to disintermediation of the private banking system for two reasons. First, there is no reason to believe that the CB possesses any technological advantages over private banks. Second, the CB does not engage in lending which limits its ability to pay interest on deposits, unlike private banks which can augment the interest that they pay on deposits with income earned from lending to buyers.

### Consumer's Choice of Currency Type

We will first look at a consumer's choice between using physical government currency and private currency. We start by finding conditions where the private currency dominates. To do so, we compare condition (11) to (9). The consumer will choose the private currency when it leads to more trade in the DM.

After we set $\psi^g = 0$ and $i^g = 0$ for (11), we can compare (11) and (9). In order for private money to dominate

$$\frac{\gamma^g}{\beta} = \frac{u_{q_b^g}(q_b, q_b^g)}{c_{1,q_s^g}(q_s, \frac{1-n}{n}q_b^g)} > \frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, \frac{1-n}{n}q_b^g)} = \frac{\gamma}{\beta(1-\psi)}$$

which eventually becomes $\gamma^g > \frac{\gamma}{(1-\psi)}$. We can substitute $\gamma^g = 1 + \sigma^g$ and set the private growth rate with no cap at 1. In order for private tokens to drive physical money out of circulation, the growth rate of physical cash must be sufficiently high $\sigma^g > \frac{\psi}{(1-\psi)}$. This along with $1 > \beta(1-\psi)$ ensures that there will be intermediation in terms of private money. On the one hand, there is an implicit tax on holding private tokens due to the potential for token loss. If the explicit inflation tax is above a certain threshold, private currency will drive physical cash out of circulation. However, the threshold rate of growth of cash is higher if the rate of token loss is higher. Yet, higher rates of money growth can be sustained if the effective rate of return to holding private tokens is lower because of token loss. However, if $-1 < \sigma^g < \frac{\psi}{(1-\psi)}$, consumers will prefer to hold physical cash and sellers will deposit their cash at private banks. Lastly, if $\sigma^g = \frac{\psi}{(1-\psi)}$, the two currencies will circulate alongside each other.

Next, in order for CBDC to drive out private money,

$$\frac{\gamma^g}{\beta(1+ni^g)(1-\psi^g)(1+i^g)} = \frac{u_{q_b^g}(q_b, q_b^g)}{c_{1,q_s^g}(q_s, \frac{1-n}{n}q_b^g)} < \frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, \frac{1-n}{n}q_b^g)} = \frac{\gamma}{\beta(1-\psi)}$$

which reduces to

$$\frac{\gamma^g}{(1+ni^g)(1-\psi^g)(1+i^g)} < \frac{\gamma}{(1-\psi)}$$

Notably, we impose that $\gamma = 1$ and we can assume $\psi = \psi^g$ since the security technology is the same for both types of currency. As a result, the inequality becomes $\gamma^g < (1+ni^g)(1+i^g)$. If we substitute $\gamma^g = 1 + \sigma^g$, CBDC will circulate and sellers will deposit their tokens at private banks as long as

$$n(i^g)^2 + (1+n)i^g > \sigma^g > max\Big\{(1-\psi^g)\beta(1+ni^g) - 1, \sigma^g > (1-f_g)\beta(1+ni^g) - 1\Big\}$$

If the rate of growth of CBDC is low enough in comparison to interest payments, it raises the real returns enough to where only CBDC circulates. In contrast, if $\sigma^g > n(i^g)^2 + (1+n)i^g$, only private money will circulate. Lastly, both currencies will circulate if $\sigma^g = n(i^g)^2 + (1+n)i^g$

**Type II Banks**

In this section, type II private banks will be available to consumers in the DM. In contrast to type I banks, these banks are in charge of the private key for private tokens that are borrowed. Thus, private tokens will not be subject to loss as they are held by the bank until the requested transfer for the borrower during exchange in the DM occurs. However, tokens brought in the DM by buyers will be subject to token loss prior to their transactions. From this perspective, the role of intermediaries is more important because of their actions in the economy's payments system and the additional safekeeping function. Since banks provide some level of transactions services on the part of borrowers, borrowers sacrifice some privacy in exchange for additional security of their holdings of tokens. As the structure of the derivations with Type II banks largely follows our previous work for type I banks, we only present the conditions which are different from the previous section. Details, however, are available in the separate appendix.

The consumer's problem in the second market will be the same as when type I banks are available. However, for the first market, we need to take into account the fact that the loan will not be susceptible to loss because these tokens are protected by banks who process payments on behalf of buyers. An agent with $m$ units of private money and $m^g$ units of government money at the beginning of the first market has expected lifetime utility

$$V(m) = (1-n)[u(q_b, q_b^g) + W((1-\psi)m + (1-\psi^g)m^g + l + l_g - pq_b - p^g q_b^g, l, l_g)] +$$
$$n[-c_1(q_s, q_s^g) + W((1-\psi)(m-d) + (1-\psi^g)(m^g - d_g) + pq_s + p^g q_s^g, d, d_g)], \quad (12)$$

where the buyer does not incur any loss from his loan. There is no need to look at the seller's decision since the rest of the problem is identical to our previous case. Additionally, similar to the case with type I banks, a stable price with private tokens is the only possibility when there is no cap on total token production. Will just provide the proof in the appendix since it is almost identical to the case with type I banks.

## Buyers' decisions

After the consumer receives his shock to become a buyer, he must determine the size of the loan to take out from the bank. Type II banks have a safe-keeping function, but the buyer may still lose some of his tokens prior to exchange in the DM. If an agent is a buyer in the first market, his problem becomes

$$\max_{q_b^g, q_b, l_g, l} [u(q_b^g, q_b) + W((1-\psi^g)m^g + (1-\psi)m + l_g + l - p^g q_b^g - pq_b)]$$
$$s.t. \quad p^g q_b^g \leq (1-\psi^g)m^g + l_g, pq_b \leq (1-\psi)m + l$$

The buyer also faces a constraint on the loan size that is bounded above by $\bar{l}$ and $\bar{l}_g$. The buyer takes the constraint as given but it is determined endogenously in equilibrium. We will look at the buyer's choice of the first market good $q_b$ to be acquired via purchases with private money first. The buyer's first order condition for the quantity of the first market good $q_b$ is the same as our case with only type I banks.

$$u_{q_b}(q_b, q_b^g) = pW_m + p\lambda.$$

The buyer's desired amount of consumption depends on the cost of working to repay the loan and whether the liquidity constraint binds. From, $W_m = \phi$ and $\frac{c_{1,q_s}(q_s, q_s^g)}{\phi} = p$ we obtain

$$u_{q_b}(q_b, q_b^g) = c_{1,q_s}(q_s, q_s^g)\Big(1 + \frac{\lambda}{\phi}\Big)$$

Since all of the loan is retained for spending, the buyer's choice for a loan will be different. Without token loss, the loan will buy more of the DM good than under type I banks.

Next, we will look at the buyer's choice of quantity of the first market good $q_b^g$ to be purchased with government money. The buyer's first order condition for choosing how much of goods to purchase through government money is

$$u_{q_b^g}(q_b, q_b^g) = p^g W_{m^g} + p^g \lambda^g.$$

Akin to the use of digital tokens, the buyer's desired amount of consumption depends on the cost of working to repay the loan and whether the liquidity constraint binds. Upon substituting

$W_{m,g} = \phi^g(1+i^g)$ and $\frac{c_{1,q_s^g}(q_s,q_s^g)}{\phi^g} = p^g(1+i^g)$

$$u_{q_b^g}(q_b,q_b^g) = c_{1,q_s^g}(q_s,q_s^g)\Big(1+\frac{\lambda^g}{\phi^g(1+i^g)}\Big)$$

Similar to when private digital tokens are in use, the last equation compares the gains from additional consumption at the cost of producing goods. However, the seller will consider the interest paid by the central bank when making their production decision. Additionally, the cash constraint will cause an inefficiency in trade.

Since the steps to obtaining the solution to loans are similar to type I banks, we refer to the appendix for most of the work. The buyer's condition for $l$ reduces to

$$\frac{u_{q_b}(q_b,q_b^g)}{c_{1,q_s}(q_s,q_s^g)} = 1+i+\frac{\lambda_l}{\phi}$$

In contrast to the setting with only type I banks, the rate of currency loss will play no direct role in the loan decision. That is, through type II banks, the buyer will take out a larger loan at similar interest rates. From this perspective, the additional safe-keeping function of such intermediaries promotes credit market activity. If the borrowing constraint does not bind,

$$\frac{u_{q_b}(q_b,q_b^g)}{c_{1,q_s}(q_s,q_s^g)} = 1+i$$

In this case the buyer will borrow up to the point where the marginal benefit of borrowing equals the marginal cost. He then spends all his money and consumes $q_b = ((1-\psi)m+l)/p$. However, trades are inefficient as long as $i > 0$. Unlike the case with type I banks, interest rates will never be negative.

The buyer's first order condition for $l_g$ reduces to

$$\frac{u_{q_b}(q_b,q_b^g)}{c_{1,q_s}(q_s,q_s^g)} = \frac{\phi^g(1+i_l^g)}{\phi^g(1+i^g)} + \frac{\lambda_l^g}{\phi^g(1+i^g)}$$

If the borrowing constraint does not bind, $\frac{u_{q_b}(q_b,q_b^g)}{c_{1,q_s}(q_s,q_s^g)} = \frac{(1+i_l^g)}{(1+i^g)}$. The buyer borrows up to the point where the marginal benefit of borrowing equals the marginal cost. He then spends all his government money and consumes $q_b^g = \big((1-\psi^g)m^g+l\big)/p^g$.

Under certain conditions, the consumer will carry enough government money in the DM where borrowing is no longer needed. To find the threshold, we need to find conditions where the multiplier on the government money constraint is negative $\lambda^g \leq \phi^g(i_l^g - i^g)$. If $i^g > i_l^g$, then $\lambda^g = 0$. We then get the following condition and have efficient production, $\frac{u_{q_b}(q_b,q_b^g)}{c_{1,q_s}(q_s,q_s^g)} = 1$.

## Marginal Value of Private and Government Money

We now look at the role that the safekeeping function provided to borrowers has on activity in the DM. Yet, the condition regarding the marginal value of private tokens and government money brought in the DM is the same as an economy with only type I banks. Identical to an economy with type I banks, the seller does not suffer currency loss for the money deposited. However, as we show below, the consumer will borrow a larger amount for a given interest rate because of safekeeping provided by banks.

We first consider the effect of safekeeping of private token deposits on nominal interest rates. Zero profits for the banks implies $i = i_d$, therefore:

$$\frac{\gamma - \beta(1-(1-n)\psi)}{\beta(1-(1-n)\psi)} = i \tag{13}$$

In terms of $q_b$:

$$\frac{\gamma - \beta}{\beta} = \frac{(1-(1-n)\psi)u_{q_b}(q_b, q_b^g)}{c_{q_s}(q_s, q_s^g)} - 1 \tag{14}$$

Of note, the rate of token loss impacts the market clearing interest rate. The interest rate is increasing in the rate of token loss. Also, (14) reflects the fact that borrowed tokens will not be subject to loss and will be available for trade.

We now find the monetary equilibrium with credit using government money. Zero profits for the banks implies $i = i_d$ therefore:

$$\frac{\gamma^g - \beta(1 + ni^g - (1-n)\psi^g)}{\beta((1-n)(1-\psi^g) + n(1+i^g))(1-f)} + \frac{f}{1-f} = i_d^g$$

In terms of $q_b$

$$\frac{\big((1-n)(1-\psi^g)(1+i^g) + n(1+i^g)^2\big)u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, q_s^g)} - 1 = \frac{\gamma^g - \beta}{\beta} \tag{15}$$

Similar to type I banks, the interest rate decreases with an increase in the interest rate on CBDC. Now though, the buyer is willing to pay a premium for the safekeeping to avoid token loss. At higher rates of token loss, the safekeeping service becomes more valuable, and the buyer is willing to pay more for the service. In turn, the bank can pay out a higher interest on deposits. In particular, this ensures that paying higher interest on deposits is critical to clear the credit market. Without the higher interest rate, consumers would have a stronger preference for borrowing tokens and there would be a shortage of money in the DM. However, with the higher interest rate on deposits, consumers are willing to carry enough tokens into the DM to ensure an equilibrium in the credit market exists.

Next, based upon the equilibrium interest rates on deposits, we can look at the conditions where sellers deposit currency at private banks. We begin by studying when case 1 holds. In order for private tokens to be deposited, we need $i_d > \frac{f-\psi}{1-f}$. Based on the interest rate on deposits, private tokens will be deposited as long as $1 > \beta(1-\psi)(1-(1-n)\psi)$. Similar to the result with type I banks, if the seller discounts the future or there is token loss, sellers deposit their funds. The condition does reflect the fact that only a portion of tokens are lost due to safekeeping.

We now turn to case 2. In order for physical currency to be deposited, we need $i_d^g > \frac{f}{1-f}$. After substituting for the deposit rate, sellers will choose to deposit physical currency as long as the growth rate of money is positive. This is the same as the condition under type I banks. We proceed by considering case 5A where sellers deposit their CBDC at private banks. If $\psi^g < f^g$ and $i_d^g > \frac{f-\psi^g}{1-f}$, the seller will deposit his government money with the private bank. After substituting for the deposit rate, sellers will choose to deposit physical currency as long as the growth rate of money satisfies

$$\gamma^g > \beta\big(1 + ni^g + (\psi^g)^2(1-n) - \psi^g n(1+i^g) - 2(1-n)\psi^g\big)$$

Finally, we look at case 6A. If $f_g < \psi_g$, and $i_d^g > max\Big\{\frac{f-\psi^g}{1-f}, \frac{f-f_g}{1-f}\Big\}$, sellers will choose to deposit with the private bank even though it's better to deposit with the CB than go unbanked. Upon substituting for the interest rate on deposits, the condition holds as long as

$$\frac{(1+ni^g-(1-n)\psi^g)}{((1-n)(1-\psi^g)+n(1+i^g))} < f_g$$

If the costs of depositing funds at the CB are high enough, sellers will always deposit with private banks at a positive money growth rate.

**Consumer's Choice of Currency Type**

We will first look at a consumer's choice between using physical government currency and private currency. We start by finding conditions where the private currency dominates. To do so, we compare condition (14) to the condition for physical currency. In order for private money to circulate

$$\frac{\gamma^g}{\beta} = \frac{u_{q_b^g}(q_b, q_b^g)}{c_{1,q_s^g}(q_s, \frac{1-n}{n}q_b^g)} > \frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, \frac{1-n}{n}q_b^g)} = \frac{\gamma}{\beta(1-(1-n)\psi)}$$

which reduces to $\gamma^g > \frac{\gamma}{(1-(1-n)\psi)}$.

Private currency will circulate, and banks provide intermediation when $1 > \beta(1-\psi)(1-(1-n)\psi)$. As before, we set the gross growth rate for goverment money $\gamma^g = 1+\sigma^g$ and the private growth rate so that $\gamma = 1$. We can then solve for growth rate of government money where private money dominates $\sigma^g > \frac{(1-n)\psi}{(1-(1-n)\psi)}$ If this condition is met along with $1 > \beta(1-\psi)(1-(1-n)\psi)$, private money will circulate and sellers will deposit funds. Consumers take into account the potential for token loss with private tokens. However, as type II banks provide safekeeping for tokens that are borrowed, the effective rate of token loss is lower.

We can now compare the thresholds for when private money drives cash out between type I and type II banks. Notably, it can be shown that the threshold rate of money growth in which private tokens drive cash out of circulation is lower with type II banks. Due to the additional safekeeping functions of type II banks relative to type I banks, the effective rate of token loss for private tokens is lower. Consequently, the rate of money growth in which cash circulates must be lower under Type II banks.

In order for private money to drive out CBDC

$$\gamma^g > \frac{\gamma\big((1-n)(1-\psi^g)(1+i^g)+n(1+i^g)^2\big)}{(1-(1-n)\psi)}$$

Substituting $\gamma_g$ and $\gamma$, we set private gross growth rate so that $\gamma = 1$. If we substitute $\gamma^g = 1+\sigma^g$, CBDC will circulate and sellers will deposit their tokens at private banks as long as

$$\frac{\big((1-n)(1-\psi^g)(1+i^g)+n(1+i^g)^2\big)-(1-(1-n)\psi)}{(1-(1-n)\psi)} > \sigma^g$$

Additionally, we require $\sigma^g > max\Big\{\beta(1+ni^g-(1-n)\psi^g) - f_g\beta((1-n)(1-\psi^g)+n(1+i^g))-1, \beta\big(1+ni^g+(\psi^g)^2(1-n)-\psi^g n(1+i^g)-2(1-n)\psi^g\big)-1\Big\}$ in order for sellers to

deposit their funds. In particular, as long as there is some token loss and the CB pays interest on CBDC, the threshold rate of growth of CBDC in which CBDC circulates is higher under Type II banks than under Type I banks. Notably, due to the additional safekeeping offered by type II banks, the effective rate of token loss will be lower. Consequently, CBDC can circulate at higher inflation rates since the returns from holding CBDC improve with type II banks.

### Type III Banks

We now look at an environment where type III banks are introduced. In addition to providing safekeeping for borrowed currency, type III banks offer a service where borrowers can deposit their money holdings brought from the DM. The bank will keep track of the private keys and process payments to sellers at the time of transaction. As a result, token loss is eliminated with type III banks. The downside to this arrangement is the total loss of privacy.

### Cap on Total Token Production

By establishing zero token loss, type III banks limit the potential equilibria in the economy. With $c_2'(0) = 0$, entrepreneurs have an incentive to create private tokens as long as the price is greater than zero. This will lead to an unbounded money supply and an equilibrium with runaway inflation. If a cap on private token production each period $\hat{\Delta}_t = \alpha M_t > 0$ is introduced, the money supply will grow at a slower pace, but it will be unbounded. Moreover, the economy will still be in an equilibrium with runaway inflation. Similar to FS, the unbounded money supply restricts the existence of a steady state. That is, a steady state only exist when token production at time period $T$ is capped at zero every period $\hat{\Delta}_{t\geq T} = 0$. With a cap on total production, the money supply becomes constant and there is a stable price steady state. This would preclude some of the cryptocurrencies that are currently available.[20]

## Buyers' decisions

After the consumer receives his shock to become a buyer, he will take out a loan from the bank. The banks will provide safekeeping and process transactions with the loan. In addition, the buyer can deposit his initial money holdings with the bank for safekeeping. As a result, the buyer will no longer be subject to currency loss for any of his money holdings. However, as banks provide the highest level of transactions services through all of an individual's holdings, borrowers completely sacrifice their level of privacy. Since the structure of the analysis largely follows our previous arguments, we begin by simply presenting the buyer's decision problem and then move directly to the equilibrium conditions. Details are available in the separate appendix.

If an agent is a buyer in the first market, his problem becomes

$$\max_{q_b^g, q_b, l_g, l} [u(q_b^g, q_b) + W(m^g + m + l_g + l - p^g q_b^g - pq_b)]$$

$$s.t. \quad p^g q_b^g \leq m^g + l_g, pq_b \leq m + l$$

Similar to BCW, both government and private money are no longer susceptible to currency loss. The buyer can spend all of the money he brings into the market, $m$ and $m^g$.

If the borrowing constraint does not bind,

[20] While Bitcoin has a cap of 21 million bitcoins, cryptocurrencies such as Ethereum and Monero have no cap on total token production.

$$\frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, q_s^g)} = \frac{(1 + i_l^g)}{(1 + i^g)}$$

The condition is similar to when type II banks are in use. The buyer takes into account the rate of token loss and the interest that can be earned from holding CBDC. With physical currency, this condition becomes to $\frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, q_s^g)} = 1 + i_l^g$. He then spends all his government money and consumes $q_b^g = (m^g + l)/p^g$. If the borrowing constraint binds, the borrower borrows $\bar{l}$, spends all of his government money and consumes $q_b^g = (m^g + \bar{l}_g)/p^g$.

## Marginal Value of Digital and Government Money

The marginal value of money is identical to BCW and when physical currency is in use.

$$V_m(m, m^g) = \phi \left[ (1 - n) \frac{u_{q_b}(q_b, q_b^g)}{c_{q_s}(q_s, q_s^g)} + n(1 + i_d) \right] \tag{16}$$

Importantly, there is no token loss under type III banks. We proceed by looking at the marginal value of government money. In particular, government money earns interest which increases its store of value and purchasing power.

$$V_m^g(m, m^g) = \phi^g \left[ (1 - n) \frac{(1 + i^g) u_{q_b^g}(q_b, q_b^g)}{c_{q_s^g}(q_s, q_s^g)} + n(1 + i^g)(1 + i_d^g)(1 - f) \right] \tag{17}$$

Of note, there is no longer any token loss due to complete safekeeping.

The equilibrium conditions for private tokens are identical to BCW and the case with physical currency.

$$\frac{\gamma - \beta}{\beta} = i \tag{18}$$

In terms of $q_b$:

$$\frac{\gamma - \beta}{\beta} = \frac{u_{q_b}(q_b, q_b^g)}{c_{q_s}(q_s, q_s^g)} - 1 \tag{19}$$

Since none of the tokens will be subject to loss, they will all be available for trade.

We now find the monetary equilibrium with credit using government money. The interest rate behaves identically to when type I banks are in use.

$$\frac{\gamma^g - \beta(1 + ni^g)}{\beta(1 + ni^g)(1 - f)} + \frac{f}{1 - f} = i_d^g$$

In terms of consumption

$$\frac{\gamma - \beta(1 + ni^g)}{\beta(1 + ni^g)} = \frac{(1 + i^g) u_{q_b}(q_b, q_b^g)}{c_{q_s}(q_s, q_s^g)} - 1 \tag{20}$$

The interest rate behaves the same as with type I banks. This is due to the fact that the interest rate does not have to increase with token loss. Consequently, the buyer will not have a preference for borrowed money over money brought directly into the DM. Consequently, he does not need higher

returns on deposits to entice him to bring enough money to the DM for an equilibrium. Since the interest rates under type III banks are the same as type I banks, the conditions where sellers deposit their funds are the same as under type I banks.

We will first look at a consumer's choice between using physical government currency and private currency. We start by finding conditions where the private currency dominates. With $\psi = 0$, we need $\gamma^g > \gamma$. Additionally, we need private token creation capped at zero each period. As before, we set the gross growth rate for government money $\gamma^g = 1 + \sigma^g$ and set private growth rate so that $\gamma = 1$. We can then solve for growth rate of government money where private money dominates to get $\sigma^g > 0$. If there is positive growth of physical cash, it will not circulate. As a result of token loss being eliminated, private tokens will be valued identically with physical currency at the same rate of money growth. Since private tokens have zero money growth, physical tokens must have no growth or deflation to be valued.

Next, along with token creation capped at zero, in order for private money to drive out CBDC

$$\frac{\gamma^g}{\beta(1+ni^g)(1+i^g)} = \frac{u_{q_b^g}(q_b, q_b^g)}{c_{1,q_s^g}(q_s, \frac{1-n}{n}q_b^g)} > \frac{u_{q_b}(q_b, q_b^g)}{c_{1,q_s}(q_s, \frac{1-n}{n}q_b^g)} = \frac{\gamma}{\beta}$$

which reduces to

$$\gamma^g > (1+ni^g)(1+i^g)$$

As before, we set the gross growth rate for government money $\gamma^g = 1 + \sigma^g$ and set private growth rate so that $\gamma = 1$. The condition for private money to circulate becomes $n(i^g)^2 + (1+n)i^g < \sigma^g$. In contrast, with a cap on total private token production, CBDC will circulate and sellers will deposit their tokens at private banks as long as

$$n(i^g)^2 + (1+n)i^g > \sigma^g > max\Big\{(1-\psi^g)\beta(1+ni^g) - 1, \sigma^g > (1-f_g)\beta(1+ni^g) - 1\Big\}$$

With a cap on total private token production, the condition in which private money dominates CBDC is the same as with type I banks. However, if there is no upper bound on private token creation, government money is the only currency with an equilibrium. Simply put, with type III banks, there is not any potential for token loss. As a result, the real return is all that matters for the circulation of private tokens. If the rate of growth of CBDC is sufficiently high, the net rate of return would be relatively low and CBDC will be dominated by private tokens.

## IV. Conclusion

In recent years, the use of cryptocurrencies has increased in significant ways. As these currencies continue to evolve and play a larger role in economies, they eventually will be an important component of banking system activity. Moreover, in addition to the standard role of financial intermediaries to facilitate loans between borrowers and lenders, intermediaries can be valuable firms that help individuals avoid uncertainty from holding cryptocurrency because of the potential to lose their private keys. That is, intermediaries can help provide safe-keeping of tokens. The objective of this paper is to rigorously demonstrate these valuable functions of intermediaries in a micro-founded model of monetary exchange. We consider that there may be different types of intermediaries who offer different services including safe-keeping and providing transactions services. Furthermore, we also consider the possibility that central banks issue their own digital currencies. While this may lead to disintermediation, we contend that central banks do not possess any technological advantages over private banks who also issue loans and therefore can pay interest on deposits. Yet, the conditions where the issuance of central bank digital currencies may lead to disintermediation or drive privately produced digital money out of circulation depends on the different levels of safekeeping that private banks can provide.

## References


[1] Aiyagari, S., Williamson, S., 2000. Money and dynamic credit arrangements with private information. J. Econ. Theory, 91, 248–279.

[2] Andolfatto, D., 2021. Assessing the impact of central bank digital currency on private banks. The Economic Journal, 131, 525-540.

[3] Aruoba, S.B., Waller, C., Wright, R., 2011. Money and capital, Journal of Monetary Economics. 58, 98-116.

[4] Berentsen, A., Camera, G., Waller, C., 2005. The distribution of money balances and the non-neutrality of money. International Economic Review, 46, 465–487.

[5] Berensten, A., Camera, G. and Waller, C., 2007. Money, Credit and Banking. Journal of Economic Theory, 135, 171–195.

[6] Davoodalhosseini, S.M., 2021. Central bank digital currency and monetary policy. Journal of Economic Dynamics and Control, 104, 1-50.

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

[8] He, P., Huang, L. and Wright, R., 2005. Money and Banking in Search Equilibrium. International Economic Review, 46, 637-670.

[9] He, P., Huang, L and Wright, R., 2008. Money, Banking and Monetary Policy. Journal of Monetary Economics, 55, 1013-1024.

[10] Kahn, C. M., J. McAndrews, and Roberds, W., 2005. Money is privacy. International Economic Review, 46(2), 377-399.

[11] Kahn, C. M., and Roberds, W., 2008. Credit and Identity Theft. Journal of Monetary Economics, 55, 251–264.

[12] 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).

[13] Keister, T., and Sanches, D., 2022. Should central banks issue digital currency? Forthcoming Review of Economic Studies.

[14] Kocherlakota, N., 2003. Societal benefits of illiquid bonds. Journal of Economic Theory, 108, 179–193.

[15] Lagarde, C. and Panetta, F. 2020. Report on a Digital Euro. European Central Bank Paper. October.

[16] Lagos, R. and Wright, R., 2005. A Unified Framework for Monetary Theory and Policy Analysis. Journal of Political Economy, 113(3), 463-484.

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

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

[19] Sanches, D., Williamson S., 2010. Money and credit with limited commitment and theft. Journal of Economic Theory, 145, 1525–1549.

[20] Waller, C. CBDC: A Solution in Search of a Problem? August 5, 2021.

[21] Williamson, S., 2021. Central Bank Digital Currency: Welfare and Policy Implications. Forthcoming. Journal of Political Economy.