FEDERAL RESERVE BANK *of* ATLANTA

Money Is Privacy

Charles M. Kahn, James McAndrews, and William Roberds

Working Paper 2004-18
August 2004

WORKING PAPER SERIES

FEDERAL RESERVE BANK *of* ATLANTA | WORKING PAPER SERIES

Money Is Privacy

Charles M. Kahn, James McAndrews, and William Roberds

Working Paper 2004-18
August 2004

Abstract: An extensive literature in monetary theory has emphasized the role of money as a record-keeping device. Money assumes this role in situations where using credit would be too costly, and some might argue that this role will diminish as the cost of information, and thus the cost of credit-based transactions, continues to fall.

In this paper we investigate another use for money: the provision of privacy. That is, a money purchase does not identify the purchaser while a credit purchase does. In a simple trading economy with moral hazard, the efficiency of money is compared with that of credit, and we find that money may be useful even when information is free.

JEL classification: D830, E420, G280

Key words: money, privacy, memory, search.

The authors gratefully acknowledge the helpful comments of Akihiko Matsui. They also thank participants in conferences held at the University of Minnesota and the University of Iowa for helpful comments. The views expressed here are the authors' and not necessarily those of the Federal Reserve Bank of Atlanta or the Federal Reserve System. Any remaining errors are the authors' responsibility.

Please address questions regarding content to Charles M. Kahn, Department of Finance, University of Illinois, c-kahn@uiuc.edu; James McAndrews, Research Department, Federal Reserve Bank of New York, jamie.mcandrews@ny.frb.org; or William Roberds, Research Department, Federal Reserve Bank of Atlanta, 1000 Peachtree Street, NE, Atlanta, Georgia, 404-498-8970, william.roberds@atl.frb.org.

1 Introduction

In this paper we investigate the role of money in providing transactions privacy. Our interest in this topic stems in part from the ongoing development of e-commerce, and in particular, consumer transactions on the Internet. From the perspective of monetary theory, Internet-based or "virtual" transactions differ fundamentally from ordinary transactions because there is currently no widely accepted form of e-cash, or "virtual money."[1] Without cash, purely anonymous transactions are not possible.

Is this lack of anonymity desirable? Some of the literature on money versus credit (e.g., Townsend 1989, Taub 1994, Kocherlakota 1998, Kocherlakota and Wallace 1998, Aiyagari and Williamson 2000) suggests that the value of money as a transactions medium stems largely from its role as a proxy or "sufficient statistic" for more complicated, credit-based systems of individual accounts. The more costly and the more imperfect the available credit-based system, the greater the need for money. With the development of the Internet, however, the costs of maintaining and transmitting vast amounts of information are falling dramatically. Some might therefore argue that the low cost of Web-based information processing means that there will be no role for e-money as a medium of exchange.

Our counter-argument is that in addition to its value as a possibly imperfect proxy for credit, the value of money also derives from its use in anonymous exchanges, facilitating certain otherwise-infeasible transactions. This property of money is most often associated with various types of shady deals,[2] but we will argue that it is of potential social value in economic situations where the parties in the transaction cannot trust each other not to take subsequent opportunistic actions.[3]

In a simple trading economy with moral hazard,[4] we compare the efficiency of using as a transactions technology a non-anonymous record-keeping

[1] See Kuttner and McAndrews (2001) and Schreft (2002) for surveys of the various technologies available for online payment.

[2] Camera (2001) explores the role of money as a facilitator of illicit activity. He, Huang, and Wright (2003) note that currency is more subject to theft than bank money. In the present paper we ignore these disadvantages associated with the anonymity of money, in order to concentrate on its role in preventing identity theft.

[3] The increasing incidence of identity theft and related frauds suggests that this is more than a theoretical possibility. A recent survey by the Federal Trade Commision (2003) found that over 12 percent of Americans have been victims of identity theft within the past five years. See Kahn, McAndrews, and Roberds (2000) for a treatment of privacy issues in a law and economics context.

[4] In particular we consider an economy where theft may be prevalent. Theft is merely an example of ex post opportunistic behavior that may arise under limited enforcement.

device or anonymous money. We then consider the more realistic case of anonymous money supplemented by a voluntary record-keeping device, and in particular the effects of improvements in monitoring technologies (or equivalently, privacy protection) on the demand for money.

In the case of Internet trading, for example, virtual money can increase efficiency of transactions. We also investigate an alternative arrangement which may appear on the Internet, the use of intermediaries to provide anonymity. We show that such an arrangement supplements non-anonymous trade, but does not always act as a perfect substitute for anonymous money. In cases where the legal structure cannot provide perfect enforcement, the use of virtual money may dominate alternative arrangements.

2 The model

There are N ex ante identical, infinitely-lived agents, where N is large.[5] All agents are risk neutral, and have a common discount factor δ. It will be convenient to think of agents as each having a unique "identity," corresponding to a distinct "location," where the list of agents' locations is public information. A unique, indivisible, nonstorable consumption good can be produced at each location. In every period, one agent randomly wakes up "hungry" for the consumption good of another agent, also randomly selected. Hungry agents then journey to the location of their preferred supplier. The identity of the hungry agent may or may not be revealed at this point, according to the information structure of the economy and the transactions technology available.[6]

When hungry, an agent desires exactly one unit of the particular supplier's good, which provides a utility of u. If not hungry, or if faced with a different supplier's good, the agent receives no utility. It costs the supplier s utils to make a unit of the good, where $0 < s < u$.

After receiving the preferred supplier's good, the hungry agent takes it back to his dwelling in order to consume it. Once he has returned home, the hungry agent may be "robbed" by another agent. For simplicity in calculations, only one agent per period will be able to attempt a robbery, where the would-be robber is randomly chosen. A robbery attempt costs the robber c utils and will be successful only a fraction α of the time. If

[5] For purposes of computing equilibria, it is convenient to have N finite. Later on, we will let N approach infinity in order to facilitate welfare comparisons.

[6] In the terminology of money search models, "single coincidences" of wants are possible under this setup, while "double coincidences" are not.

successful, the robbery carries a cost to the victim of f utils, so that the net utility to the consumer after a robbery is $u - f$, which may be positive or negative. Successful theft imparts a benefit to the thief of εf utils, where $0 < \varepsilon < 1$. The timing of events within a period is displayed in Table 1.

Table 1: Events within a period
a. Consumer, supplier randomly chosen
b. Consumer journeys to supplier's location
c. Trade occurs
d. Theft occurs with probability α
e. Consumer and possibly thief consume

In this environment, information on transactions carries both costs and benefits. No one automatically knows who is hungry on a particular day, so if a would-be thief waits around another agent's location, there will be only an $\alpha / (N-1)$ chance of committing a successful robbery. In what follows, we assume that

$$\frac{\alpha \varepsilon f}{N-1} < c \qquad (1)$$

which assures that no thief will attempt to steal from an individual at random. However, a supplier always knows that he has provided someone a good, and so if the consuming agent reveals his identity to his supplier, the consumer makes it more likely he will be a victim. On the other hand, if the consumer remains anonymous, the supplier may be unwilling to give him the good, since there may be no way to obtain reciprocity in the future.

In the absence of theft, fully efficient exchange would allow the hungry agent in every period to purchase a good from his supplier. We let V^* be the expected symmetric utility established by a fully informed social planner. Since each agent has a $1/N$ chance of consuming or supplying each period, and since theft is socially wasteful, an agent's discounted expected utility under fully efficient exchange would be

$$V^* = \frac{u - s}{\delta N} \qquad (2)$$

2.1 Information and exchange structures

We will compare outcomes in this model under a variety of information structures. Initially we consider *bilaterally observable gift exchanges.* In this arrangement, both suppliers and consumers keep track of a history of exchanges with each other agent, but no one knows about trades made by an agent with other agents. The history available in such arrangements, while restricted, serves as both an incentive to exchange and an incentive to theft.

Next, we consider *publicly observable gift exchanges*—what Kocherlakota (1998) refers to as "memory." In these there is a perfect record of all trades made by all participants. In the record, in every transaction, each agent's identity is revealed to all other agents.

We then consider the effect of introducing money. Money is an imperfect record of the history of trades by an individual. But it is a record which maintains the anonymity of consumers, and is therefore of value in supplementing exchange. In particular, it allows the achievement of outcomes which cannot be obtained without money.

We will also consider an environment of *semi-anonymous gift exchange.* In this case the identity of the consuming agent is never revealed, limiting the possibilities for both trade and theft. Nonetheless, trade can sometimes be sustained under "social norms" (Araujo (2004)).

Finally we will consider a semi-anonymous record-keeping technology, and examine its advantages and disadvantages compared to money.

2.2 Bilateral information on goods exchanged

In this environment, each supplier in an exchange is informed of the identity of the recipient. Each potential supplier must decide whether the disutility of production is worth the gain of "reciprocal privileges" with a given consumer. Absent theft, the supplier's expected benefit from future (next period onwards) exchange opportunities with a given counterparty are

$$\left[\frac{1}{\delta N(N-1)}\right](u-s) \tag{3}$$

Exchange can be sustained as long as s, the cost of supplying a good, does not exceed the quantity (3), the expected benefits from reciprocal privileges. In this case the expected discounted utility for each consumer (from trades with all other agents) is simply given by V^*.

For a given transaction, the only potential thief in this environment is the supplier of the good. Were the supplier to steal the good, the buyer would infer that the seller was the thief, and could punish the seller by not engaging in trade with the seller in any future meetings.

The instantaneous expected benefit to the supplier from theft is $\alpha\varepsilon f - c$. If $\alpha\varepsilon f < c$, then theft will not be attempted and trade will proceed as in the previous case. If $\alpha\varepsilon f \geq c$, then theft may occur. An equilibrium without theft is sustainable as long as

$$\left[\frac{1}{\delta N(N-1)}\right](u-s) \geq \max\{s, \alpha\varepsilon f - c\} \tag{4}$$

Exchange will still occur even with theft, however, if the expected net benefit from continued future exchanges is large enough, i.e., if $\alpha\varepsilon f \geq c$ and

$$\frac{u - s - N^{-1}\left(\alpha(1-\varepsilon)f + c\right)}{\delta N(N-1)} \geq \max\{s, \alpha f - u\} \tag{5}$$

In other words, the expected net benefit from future exchanges must outweigh the expected disutility from production. It must also exceed the disutility from acquiring a good and subsequently being robbed; otherwise hungry agents will refuse to acquire goods. In this case the expected discounted utility for each consumer is given by

$$\frac{u - s - N^{-1}\left(\alpha(1-\varepsilon)f + c\right)}{\delta N} \tag{6}$$

Note that (6) includes both the expected benefit of being a thief and the expected cost of being a victim of theft.

If neither (4) nor (5) holds, then autarky is the only equilibrium.

2.3 Full information on goods exchanged

We next consider an environment in which there is full information about the identity of recipients of goods in any exchange that occurs. Consider the incentives for theft. After each exchange, the designated thief knows where his potential victim lives. The identity of a thief and the presence of stolen goods are not observable. The instantaneous expected benefit to theft is $\alpha\varepsilon f - c$, and theft will occur as long as this is nonnegative.[7]

Exchange occurs if agents are willing to supply goods to other agents who have supplied goods in the past; a failure to supply results in the supplier being relegated to autarky. Hence exchange will be sustained if the

[7] In this section we simply assume that a victim has no way of announcing that he has been robbed, and makes no response to a theft. In a later section we consider an environment in which a victim's behavior changes as a result of the theft.

cost of supplying a good does not exceed the expected future net benefit of exchange. If $\alpha\varepsilon f < c$, this condition is equivalent to

$$\frac{u-s}{\delta N} \geq s \tag{7}$$

If on the other hand, $\alpha\varepsilon f \geq c$, either autarky can result, or exchange will occur subject to attempted theft after each exchange and a consequent loss of value by recipients of goods. Exchange can still occur so long as

$$\frac{u-s-\alpha\left(1-\varepsilon\right)f-c}{\delta N} \geq \max\left\{s, \alpha f-u\right\} \tag{8}$$

Comparing (8) with (5) we note that the RHS of each condition is the same because defection has the same benefit under either arrangement. The LHS is different since an attempt at theft is certain under full information, but penalties for defection are enforced by more agents. Under full information agents' expected discounted utility is

$$\frac{u-s-\alpha(1-\varepsilon)f-c}{\delta N} \tag{9}$$

3 The effects of introducing money

We now consider the effects of introducing fiat money into the environments described above. Here, the construct analyzed in Kiyotaki and Wright (1989) comprises a unit of money: an indivisible, inherently valueless, non-counterfeitable object, where each agent can hold a maximum of one such object. There is a fixed supply of money and not all agents possess money at any given time. Money confers anonymity–a consumer making a purchase with money does not reveal his identity to his supplier, or to others. The quantity of money circulating in the economy is known to all agents, however.

3.1 Money under semi-anonymity

Suppose that would-be consumers cannot (or prefer not to) reveal their identity to would-be suppliers. Trade in this case is "semi-anonymous," since the supplier's identity is always known. Money offers opportunities for exchange in this environment. Let M be the fraction of agents in the economy with money, and let $\underline{V}(n)$ be the value function of an agent n units of money, where $n \in \{0, 1\}$. Absent theft, the flow Bellman equations for each type of agent are[8]

$$\delta \underline{V}(0) = \frac{M}{N} \left(-s(1+\delta) + \underline{V}(1) - \underline{V}(0)\right) \tag{10}$$

$$\delta \underline{V}(1) = \frac{1-M}{N} \left(u\,(1+\delta) + \underline{V}(0) - \underline{V}(1)\right) \tag{11}$$

Algebraic manipulation of (10) and (11) yields

$$\underline{V}(0) = \frac{M}{N} \left(\frac{1+\delta}{\delta}\right) \left[\frac{(1-M)(u-s) - \delta N s}{1+\delta N}\right] \tag{12}$$

$$\underline{V}(1) = \left(\frac{1-M}{N}\right) \left(\frac{1+\delta}{\delta}\right) \left[\frac{M(u-s) + \delta N u}{1+\delta N}\right] \tag{13}$$

If exchange occurs, it remains anonymous; hence the instantaneous expected return to theft is $(\alpha\varepsilon f)/(N-1) - c$, which is assumed to be negative. The existence of monetary equilibrium requires that obtaining money is a sufficient incentive to supply a good, i.e., that

$$\underline{V}(1) - \underline{V}(0) \geq (1+\delta)s \tag{14}$$

which is equivalent to

$$(1-M)u \geq s(1-M+\delta N) \tag{15}$$

As is common in search models of money, a monetary equilibrium obtains if agents are patient enough (for sufficiently small $\delta > 0$).

In monetary equilibrium, an agent's expected utility is given by

$$\frac{M(1-M)(u-s)}{\delta N} \tag{16}$$

and the welfare-maximizing quantity of money is given by $M = 1/2$. Expected utility is less than V^* because trade can only occur if money holdings are exactly right.

[8] For computational simplicity these and other Bellman equations involving money are written as if the fraction of agents holding money does not depend on whether the agent himself holds money. This approximation holds precisely as $N \to \infty$.

3.2 Money as an alternative to bilateral information

Now we consider allowing consuming agents to choose between transactions technologies. In this section we allow them the following two choices: they may anonymously purchase goods with money, or they may choose to reveal their identity to their suppliers (and no one else) with the intent of obtaining "credit" for future reciprocal actions. Agents purchasing on credit are expected to make repayment by supplying goods to counterparties with whom they have previously engaged in credit transactions, who choose to purchase on credit and not with cash. Agents failing to make these required payments lose their credit with that counterparty and subsequent transactions between the two are limited to cash. As was the case in the previous section, a credit purchase exposes the purchaser to the possibility of theft from the supplier.

Depending on the model parameters, money, credit, or both may be used in equilibrium. Credit alone will be used, for example, if there is no theft and if agents are patient enough. Money will used exclusively if the likelihood and cost of theft is high enough. We can also show that there are equilibria where both money and credit exist.

For there to be an equilibrium with both money and credit, it must be the case that theft sometimes occurs in credit transactions, so that holders of money will always prefer to transact with money when they wish to consume. This will only be possible when their potential supplier does not have money; otherwise the transaction will proceed on a credit basis. Likewise, it must be the case that potential suppliers without money must prefer transacting with money, when it is available, to transacting with credit.

Taking the above considerations into account, we can write the Bellman equations for agents without and with money as

$$\begin{aligned} V(0) &= \frac{1}{N}\left(u - \frac{\alpha f}{N} + \frac{V(0)}{1+\delta}\right) + \frac{M}{N}\left(-s + \frac{V(1)}{1+\delta}\right) + \\ &\quad \frac{1-M}{N}\left(-s + \frac{\alpha\varepsilon f - c}{N} + \frac{V(0)}{1+\delta}\right) + \left(1 - \frac{2}{N}\right)\frac{V(0)}{1+\delta} \qquad (17) \\ V(1) &= \frac{1-M}{N}\left(u + \frac{V(0)}{1+\delta}\right) + \frac{M}{N}\left(u - \frac{\alpha f}{N} + \frac{V(1)}{1+\delta}\right) + \\ &\quad \frac{1}{N}\left(-s + \frac{\alpha\varepsilon f - c}{N} + \frac{V(1)}{1+\delta}\right) + \left(1 - \frac{2}{N}\right)\frac{V(0)}{1+\delta} \qquad (18) \end{aligned}$$

where $V(n)$ is the value functions for agents with n units of money, when agents have a choice between the use of money and "bilateral credit." Equation (17) says that the value function of an agent without money equals the weighted sum of the continuation values of being a consumer in a credit transaction, a supplier in a cash transaction, a supplier in a credit transaction, and not transacting at all. Equation (18) says that the value function of an agent with money equals the weighted sum of the continuation value of being a consumer in a cash transaction, a consumer in a credit transaction, a supplier in a credit transaction, and not transacting. Equations (17) and (18) can be rewritten in standard flow form as

$$\begin{aligned} \delta V(0) &= \frac{1+\delta}{N}\left[u - s - N^{-1}\left(\alpha f - (1-M)\left(\alpha \varepsilon f - c\right)\right)\right] + \\ &\quad \frac{M}{N}\left(V(1) - V(0)\right) \qquad (19) \\ \delta V(1) &= \frac{1+\delta}{N}\left[u - s - N^{-1}\left(M \alpha f - \alpha \varepsilon f - c\right)\right] - \\ &\quad \frac{1-M}{N}\left(V\left(1\right) - V\left(0\right)\right) \qquad (20) \end{aligned}$$

Solving for $V(0)$ and $V(1)$ we obtain

$$\begin{aligned} V(0) &= \frac{1+\delta}{\delta N}\{u - s \\ &\quad + \frac{1}{N(1+\delta N)}[(M(1-M) - (1+N\delta))\alpha f \qquad (21) \\ &\quad - \left(M^2 + (1-M)\left(1+N\delta\right)\right)\left(\alpha \varepsilon f - c\right)]\} \end{aligned}$$

$$\begin{aligned} V(1) &= \frac{1+\delta}{\delta N}\{u - s \\ &\quad + \frac{1}{N(1+\delta N)}[-\left(M(1+N\delta) + (1-M)^2\right)\alpha f \qquad (22) \\ &\quad - ((1+N\delta) - (1-M)M)\left(\alpha \varepsilon f - c\right)]\} \end{aligned}$$

To sustain this behavior as an equilibrium, it must be the case that agents are willing to "repay debts," i.e., agents must have an incentive to supply a consumption good in credit transactions. The agent's alternative would be to carry out future transactions with that counterparty solely in cash. Hence this equilibrium requires

$$-s + \frac{V(0)}{1+\delta} \geq \left(\frac{N-1}{N}\right)\frac{V\left(0\right)}{1+\delta} + \left(\frac{1}{N}\right)\frac{\underline{V}(0)}{1+\delta} \qquad (23)$$

which tends to

$$u - s - N^{-1}\left(\alpha\left(1-\varepsilon\right)f + c\right) \geq 0 \qquad (24)$$

as δ tends to zero. Condition (24) will be satisfied if $\alpha(1-\varepsilon)f+c$ is not too large, i.e., if the problem with theft is not too severe. Agents with money will prefer to buy with money rather than credit as long as

$$u+\frac{V(0)}{1+\delta}\geq u-\alpha f+\frac{V(1)}{1+\delta} \tag{25}$$

which is equivalent to

$$(\delta N)\,\alpha f\geq M\,(\alpha\,(\varepsilon-1)\,f-c) \tag{26}$$

which is satisfied as long theft is socially costly ($\alpha\varepsilon f<\alpha f+c$). Finally it must be the case that suppliers prefer cash to credit, i.e., that

$$-s+\frac{V(1)}{1+\delta}\geq -s+N^{-1}\,(\alpha\varepsilon f-c)+\frac{V(0)}{1+\delta} \tag{27}$$

which reduces to

$$\frac{1}{1+\delta N}\,(\alpha f\,(1-M)+(\alpha\varepsilon f-c)\,M)\geq\alpha\varepsilon f-c \tag{28}$$

which holds $M>0$ for $\delta>0$ sufficiently small. Two points should be noted. First, once cash exists the requirements for maintaining willingness to repay debts are stricter than they otherwise would be: the threat is not to revert to autarky but to revert to monetary transactions. Thus, the existence of money to a certain extent drives out debt.[9] Second, it is the nonobservability of an individuals money holdings which necessitates imposing two of the constraints in the money-credit equilibrium (conditions (25) and (27)). Note in particular if sellers could not hide their money holdings then (27) could be relaxed.

3.3 Money as an alternative to full information

As in the previous section, consumers have a choice between using money or revealing their identity in credit transactions. In the latter case their identity is revealed not only to their counterparty but all other agents in the economy.

As under bilateral information, equilibria exist with only money or only credit transactions. Sufficiently patient agents will prefer to transact with credit as long as there is no theft. If theft is sufficiently likely and costly,

[9] For other examples of interactions between different forms of payments media see He, Huang, and Wright (2003).

agents will only want to use money. There are also equilibria where both money and credit are used. In such an equilibrium holders of money always transact in money if this is possible. In the money-credit equilibrium, the flow Bellman equations can be written as

$$\delta\overline{V}(0) = \frac{1+\delta}{N}(u-s-\alpha f) + \frac{M}{N}\left(\overline{V}(1) - \overline{V}(0)\right) \tag{29}$$

$$\delta\overline{V}(1) = \frac{1+\delta}{N}(u-s-M\alpha f) - \frac{1-M}{N}\left(\overline{V}(1) - \overline{V}(0)\right) \tag{30}$$

where $\overline{V}$ denotes the value function of agents who have a choice between money and multilateral credit. Solving for $\overline{V}(0)$ and $\overline{V}(1)$ we obtain

$$\overline{V}(0) = \frac{1+\delta}{\delta N}\left\{u+s-\alpha f + \frac{M}{1+\delta N}\left[(1-M)\alpha f\right]\right\} \tag{31}$$

$$\overline{V}(1) = \frac{1+\delta}{\delta N}\left\{u-s-M\alpha f - \frac{1-M}{1+\delta N}\left[(1-M)\alpha f\right]\right\} \tag{32}$$

To sustain this equilibrium, it must be the case that agents are willing to "repay debts," i.e., agents must have an incentive to supply a consumption good in credit transactions. The agent's alternative would be to carry out subsequent transactions solely in cash. Hence this equilibrium requires

$$-s + \frac{\overline{V}(0)}{1+\delta} \geq \frac{\underline{V}(0)}{1+\delta} \tag{33}$$

which is equivalent to

$$\left[\delta N + 1 - M(1-M)\right](u-\alpha f) \geq \left[1 - M(1-M)\right]s \tag{34}$$

which is satisfied, for example, if M is sufficiently small, or the likelihood of theft α is sufficiently low. This equilibrium also requires that agents with money prefer to buy with money rather than credit, i.e., that

$$u + \frac{\overline{V}(0)}{1+\delta} \geq u - \alpha f + \frac{\overline{V}(1)}{1+\delta} \tag{35}$$

which is equivalent to

$$\delta N + M \geq 0 \tag{36}$$

which is automatically satisfied for $\delta N, M > 0$. Suppliers prefer receiving money to credit so long as

$$s + \frac{\overline{V}(1)}{1+\delta} \geq -s + N^{-1}(\alpha\varepsilon f - c) + \frac{\overline{V}(0)}{1+\delta} \tag{37}$$

which reduces to

$$\frac{(1-M)\,\alpha f}{1+\delta N} \geq \frac{\alpha\varepsilon f - c}{N} \tag{38}$$

which holds for $\delta > 0$ sufficiently small.

4 Some welfare comparisons

We can use the analysis above to make welfare comparisons among different economies, using expected aggregate instantaneous steady-state utility as a criterion, where the expectation is taken over the success or failure of theft. We begin by comparing an economy where semi-anonymous transactions take place only with money (the economy of section 3.1), to an economy where bilateral information is available on all transactions (section 2.2), and one where full information is available on all transactions and "multilateral credit" arises (section 2.3). In the absence of theft (when $\alpha\varepsilon f < c$), such a comparison is quite simple and is displayed in Table 2.

Table 2: money versus credit without theft

	Money	Credit	
		Bilateral	Multilateral
$\sum U$	$M(1-M)(u-s)$	$u-s$	$u-s$
Feas.	$(u-s)(1-M) \geq s\delta N$	$u-s \geq s\delta N(N-1)$	$u-s \geq s\delta N$

From Table 2 it is clear that credit dominates money where both are feasible. Bilateral credit is the most delicate arrangement and depends on there being a relatively small number of agents in the economy. As we drive N to infinity while allowing the interval between time periods and δ to shrink as $1/N$, we obtain the limiting results (where $r > 0$ is the limit of δN) displayed in Table 3.[10]

Table 3: money vs. credit w/o theft as $N \to \infty$

	Money	Multilateral Credit
Steady-state $\sum U$	$M(1-M)(u-s)$	$u-s$
Feasibility	$(u-s)(1-M) \geq sr$	$u \geq sr$

[10] Technically this last step is necessary to make the environment of Section 2.4 compatible with Kocherlakota's (1998) concept of "memory." Essentially this requires that all matches be between agents without any previous contact.

Bilateral credit becomes infeasible in this case as the chance of a repeated match goes to zero. Multilateral credit remains feasible, however, and absent theft we have the standard results of the money literature that credit is feasible whenever money is, and delivers higher welfare.

When theft can occur, these comparisons are less straightforward. Table 4 offers steady-state comparisons of economies under the threat of theft (for which $\alpha\varepsilon f \geq c$) with only money (section 3.1), bilateral credit (section 2.2), or multilateral credit (section 2.3).

Table 4: $E\left(\sum U\right)$ with theft for various environments

Money Only	Bilateral Credit	Money and Credit
$M(1-M)(u-s)$	$u-s$ $-N^{-1}\left(\alpha(1-\varepsilon)f+c\right)$	$u-s-$ $\alpha(1-\varepsilon)f-c$

Feasibility for monetary equilibrium is the same as before, i.e., condition (15); feasibility for bilateral credit is given by (5), and feasibility for multilateral credit is given by (8). From the table it is clear that under the threat of theft, money can dominate credit. Bilateral credit, where feasible, dominates multilateral credit, as it affords fewer opportunities for socially costly theft. Bilateral credit may dominate money if problems with theft are not too severe.

Finally, Table 5 offers a welfare comparison of the economies with money only, multilateral credit only, and a combination of multilateral credit and money (section 3.3).

Table 5: $E\left(\sum U\right)$ with theft for various environments

Money Only	Multilateral Credit Only	Money and Credit
$M(1-M)(u-s)$	$u-s$ $-\alpha(1-\varepsilon)f-c$	$u-s-$ $(1-M(1-M))$ $\times\left(\alpha(1-\varepsilon)f+c\right)$

For the equilibrium with both money and credit, feasibility is given by condition (34) in addition to (15). A combination of both money and credit necessarily dominates credit by itself, and will dominate money as long as feasibility condition (34) is met, and the surplus created in trade exceeds the social cost of theft, i.e., as long as $u-s>\alpha(1-\varepsilon)f+c$. If the cost and likelihood of theft are too high, then only exchange with money is possible.

In short, in an economy without theft and with a frictionless system of credit, money would be superfluous. When theft is present, it would be welfare-improving to introduce money into a world with frictionless credit, as money introduces the possibility of anonymous, theft-free transactions. Not all potential consumers will have access to money, however, meaning that money does not completely supplant credit.

5 Robustness

Money is not the only mechanism for sustaining exchange without theft. In this section, we consider two other possible"social norms": gift-giving, and retaliation by the victims of theft.

5.1 Gift-giving

To analyze gift-giving, consider a version of this environment under semi-anonymity. Each potential supplier's identity is known to the consuming agent, but the identity of the potential consumer is unknown to the supplier. Then, following Araujo (2004), we can show that exchange can sometimes be sustained under a "social norm," whereby each potential supplier agrees to supply a good to an unknown consumer, in anticipation of reciprocity when the supplier wishes to consume.

For gift-giving to be a Nash equilibrium, it must be the case that the anticipated net future benefit of adhering to the social norm of gift-giving exceeds the anticipated future benefits of defecting from the social norm. Defection is contagious in the sense that as a defector refuses to supply his good, this results in additional defections. To rule out defections it must be true that

$$-s + V^* \geq V_d \tag{39}$$

where V_d is the expected value of defecting, which may be written as

$$V_d = u \sum_{t=1}^{\infty} \left(\frac{1}{1+\delta} \right)^t \frac{N - E(D_t)}{N(N-1)} \tag{40}$$

where D_t is the number of defectors as of time t and E denotes expectation as of period 0. Given that there are i defectors at time t, then

$$\Pr\{D_{t+1} = j | D_t = i\} = \begin{cases} \left(\frac{i}{N}\right)\left(\frac{N-i}{N-1}\right) & \text{if } j = i+1 \\ 1 - \left(\frac{i}{N}\right)\left(\frac{N-i}{N-1}\right) & \text{if } j = i \\ 0 & \text{if } j \neq i, i+1 \end{cases}$$

Let the N-dimensional vector π_t, represent the probability distribution of D_t. It follows that $\pi_t = A^{t-1}\pi_1$ where A is the $N \times N$ transition matrix

$$A = \begin{bmatrix} 1-\frac{N-1}{N(N-1)} & \frac{N-1}{N(N-1)} & 0 & \cdots & 0 \\ 0 & 1-\frac{2(N-2)}{N(N-1)} & \frac{2(N-2)}{N(N-1)} & \ddots & \vdots \\ \vdots & \ddots & \ddots & & 0 \\ \vdots & & \ddots & 1-\frac{N-1}{N(N-1)} & \frac{N-1}{N(N-1)} \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix} \quad (41)$$

Furthermore,

$$\pi_1' = (0, 1, 0, \ldots, 0) \quad (42)$$

since there are two defectors in period 1–the initial defector and his victim at time 0. Define Δ as the N-dimensional row vector whose ith element is $(N-i)/(N-1)$. We can then rewrite V_d as

$$\begin{aligned} V_d &= u \sum_{t=1}^{\infty} \sum_{i=1}^{N} \left(\frac{1}{1+\delta} \right)^t \pi_t(i) \left(\frac{N-i}{N(N-1)} \right) \\ &= \frac{u}{(1+\delta) N} \Delta \sum_{t=1}^{\infty} \left(\frac{A}{1+\delta} \right)^t \pi_1 \\ &= \frac{u}{N} \Delta \left((1+\delta) I - A \right)^{-1} \pi_1 \end{aligned} \quad (43)$$

where I is the N-dimensional identity matrix.[11]

Then, as agents become more patient and δ goes to zero, it is evident from (43) that the value of defecting tends to a finite limit, whereas the value of adhering to the gift-giving norm (the LHS of (39)) grows without bound. Hence, exchange can be sustained under gift-giving for sufficiently patient agents.

Gift-giving becomes increasingly fragile as the number of agents grows, however. We can bound the value of defecting from below as

$$V_d \geq u \left(\frac{1}{\delta N} - \frac{(1+\delta)}{N(N-1)\delta^2} + \frac{(1+\delta)^{-N+2}}{N(N-1)\delta^2} \right) \quad (44)$$

[11] These calculations closely follow those of Araujo (2004, 246). Following Ellison (1994) and Kandori (1992), Araujo also examines social norms sustained by sequential equilibria. In this paper we confine our attention to Nash equilibrium; extensions to sequential equilibrium in the context of money and theft would be an interesting, though involved, extension.

This inequality can be understood as follows: since there is one meeting per period, the number of defections can increase at most by one per period. The worst case scenario is

$$D_t = \min\{t+1, N\} \tag{45}$$

Actual contagion must proceed more slowly than this worst-case scenario. Let

$$\underline{V}_d = u \sum_{t=1}^{N-1} \left(\frac{1}{1+\delta}\right)^t \left(\frac{N-t-1}{N(N-1)}\right) \tag{46}$$

$\underline{V}_d$ gives the value of defecting if a further defection would occur every period following the initial defection, until the entire population were exhausted; simplifying (46) we obtain the RHS of (44). Driving N to infinity and taking limits as in the previous section, we obtain a limiting lower bound for V_d

$$\underline{V}_d^{\infty} = \frac{u}{r^2}\left(r - 1 + e^{-r}\right) \tag{47}$$

where r is the limit of δN. Comparing $\underline{V}_d^{\infty}$ to the analogous limiting expression for V^*, we obtain a sufficient condition for gift-giving to be infeasible

$$\underline{V}_d^{\infty} > -s + V^{*\infty} \tag{48}$$

or equivalently,

$$\frac{r(1+r)}{1-e^{-r}} > \frac{u}{s} \tag{49}$$

From (49) it is clear that gift-giving is not feasible for N and r sufficiently large. Comparing (15) and (49) it is also clear that for large N, there will be a range of values of r for which monetary exchange is feasible while gift-giving is not.

5.2 Retaliation by victims

In describing the public information regime of section 2.3, we assumed that victims of theft had no way to retaliate. In fact, retaliation could take many forms. In the opposite extreme, suppose that a victim of theft could make a public announcement that a theft had occurred. In an equilibrium with trade and without theft, such an announcement would signal a "defection" from the social norm of no theft, leading all agents to revert to autarky in subsequent periods. An equilibrium without theft is sustainable as long as the expected net benefits to future exchange exceed both the disutility of supplying and the private return to theft:

$$\frac{u-s}{\delta N} \geq \max\{s, \alpha\varepsilon f - c\} \tag{50}$$

The ability to make such announcements is welfare-improving in that it reduces opportunities for theft. Condition (50) is also less stringent that condition (4), meaning that if such announcements are possible, theft-free trade is easier to achieve in an environment of full information than under bilateral information. If condition (50) is violated, however, trade with money may still dominate trade with credit. Note also that public announcements are the most forceful form of retaliation, and other forms of retaliation would be expected to have more limited effects. In addition, (49) may hold and (50) may fail simultaneously, while money is still feasible. In other words, there are parameter values where money succeeds while both memory and gift-giving fail.

6 Intermediation

Intermediaries can also be in the business of providing privacy. One possibility is "inside money"—a reputable agent issues a limited number of non-counterfeitable notes which circulate.[12] However there are also ways an intermediary can provide privacy with a setup which does not resemble money. On the Internet, for example, there are sites which serve as "anonymizers." These serve as gateways to other sites, scrambling the Web surfer's information so his identity cannot be traced.

In this section we consider both an anonymizing institution which takes the form of intermediated credit, and an institution providing inside money.

6.1 Intermediated credit

We start with the economy of section 2.3 in which transactions are public information. In addition, we assume that $\alpha\varepsilon f > c$ so that theft will occur (in the absence of retaliation by victims).

Let us now suppose that a bank charter is given to one agent. All other agents have the option of opening an "account" with the banker. When agents with a bank account wish to consume, they go to the banker and

[12] For example, Cavalcanti and Wallace (1999) or Kiyotaki and Moore (2000) present models of inside money based on this idea.

give him the location of their desired supplier. If the supplier has a bank account, the banker goes to the supplier, purchases the good with bank credit, and immediately and privately passes on the good to the consuming agent. Would-be thieves (other than the banker) are stymied because they do not know the location of the agent with the good. The banker is, in effect, "anonymizing" agents' transactions.

This arrangement is sustainable as an equilibrium as long as (1) all agents have a bank account, (2) all agents believe that if they "defect" from this arrangement, all other agents will likewise defect, and the economy will return to autarky, and (3) there can be public announcements of defections by the counterparty of the defector.

Note there are two opportunities for defection, the first being that a potential supplier can refuse to provide a good to the banker, and the second being that the banker, who knows the identities of consuming agents, can rob them after delivering their consumption good. The supplier will supply his good to the banker as long as the expected net benefit of (theft-free) future transactions exceeds the disutility of supplying the good, i.e., as long as (7) holds. The banker will refrain from robbing his "depositors" only if the expected net benefit of being theft-free in future transactions exceeds the short-term gain from theft, i.e., if

$$\frac{u-s}{\delta N} \geq \alpha \varepsilon f - c \tag{51}$$

which is satisfied for $\delta N > 0$ sufficiently small. Thus, this arrangement is sustainable if the banker is patient enough. Note also that the combination of the two conditions (7) and (51) is simply the condition (50). In other words, the intermediated credit arrangement succeeds precisely in cases where public announcements of theft are effective.

Thus, a "banking" type of arrangement can in some cases deliver a first-best outcome (credit transactions without theft).[13] Intermediation is superior to both unintermediated trade under full information (without retaliation) because it reduces the scope for theft, and to trade under bilateral information because it does not require such a high degree of patience on the part of suppliers. On the other hand, if agents are too impatient, or if

[13] Given the level of abstraction of our model, we can regard this arrangement as an idealization of a money order or of a cashier's check—in each case the transaction can be kept anonymous from the seller but not from the bank. While it may seem farfetched for the purchaser to worry about needing privacy to protect him from his own banker, exactly the analogous problem arises on the Internet, as purchasers worry about the security of databases that underlie their online payments arrangements.

the temptation to steal is too great, money or a combination of money and unintermediated credit will be feasible, while intermediated credit will not.

6.2 Private banknotes

Suppose that the information structure only allows for semi-anonymous gift exchange. One agent is allowed to issue private bearer notes. Technologically, the notes are the same as fiat money described above: non-counterfeitable, discrete, and subject to the restriction that each individual may hold at most one note. In addition, there is no requirement that notes be redeemed. Thus, notes circulate indefinitely and their use in a purchase preserves the anonymity of the purchaser. The quantity of notes outstanding is known by all agents.

In the long run, the same set of monetary equilibria would obtain under private money as under fiat money. While private money would offer an improvement over autarky, a private issuer would have an incentive to issue as many notes as possible, i.e., until the incentive constraint (15) binds. If (15) binds for a per-capita money stock $M > 1/2$, then the use of private money would result in an oversupply of notes.

Likewise, we could introduce private money into an economy in which all transactions are public information. Then the private money issuer would issue notes until either (15) or (34) were binding. From the discussion above, this would necessarily lead to an improvement over either autarky or credit-only transactions. If the money issuer chooses a per-capita money stock $M > 1/2$, it would again lead to an oversupply of banknotes.[14]

In terms of privacy, the important distinction between circulating media and accounts is that as the money passes from hand to hand, even the initial issuer no longer knows who currently holds it.

7 Conclusion

Somewhat paradoxically, recent advances in monetary theory have shed doubt on the value of money in technologically sophisticated economies.

[14] We have glossed over the technically interesting but (for our purposes) inessential issue of how such an equilibrium starts up. The banker enjoys seignorage in initial periods by issuing money for purchases. In those initial periods, the banker also bears an additional cost as being the most likely victim: potential thieves in period 1 will regard the banker's location as being the one most likely to contain goods. Given the long run benefits it may still be worthwhile for the banker to issue notes; if not he may choose a randomizing strategy in which he sometimes gives out money in early periods without obtaining goods.

Money has been portrayed as at best, an imperfect proxy for memory (Kocherlakota 1998 and related papers), or at worst, an enabler of illicit, welfare-reducing activities (Camera 2001). In this paper, we have argued that the "demotion" of money to a poor cousin of credit-based arrangements may have been premature. In an economy with less-than-perfect enforcement, we have shown that the value of money may derive from its supposed imperfection, from the anonymity that it confers.

This is not to argue that arrangements other than money cannot also provide purchasers with anonymity. Above we have considered several such arrangements, including private intermediation and reciprocal gift-giving. Yet we have also shown that there are some circumstances where trade with money is feasible while trade under these alternative arrangements is not. This suggests to us that the classic solution to the problem of transactions privacy—money—will persist well into the foreseeable future.

References

[1] Aiyagari, S. Rao and Stephen D. Williamson, "Money and Dynamic Credit Arrangements with Private Information." *Journal of Economic Theory*, 91 (2), April 2000, 248-79.

[2] Araujo, Luis, "Social Norms and Money." *Journal of Monetary Economics*, 51, 2004, 241-256.

[3] Camera, Gabriele. "Dirty Money." *Journal of Monetary Economics* 47, 2001, 377-415.

[4] Cavalcanti, Ricardo and Neil Wallace. "A Model of Private Banknote Issue." *Review of Economic Dynamics 2, 1999, 104-136.*

[5] Ellison, Glenn. "Cooperation in the Prisoner's Dilemma with Anonymous Random Matching." *Review of Economic Studies* 61, 1994, 567-588.

[6] Federal Trade Commission. *Identity Theft Survey Report*, 2003.

[7] He, Ping, Lixin Huang, and Randall Wright. "Money and Banking in Search Equilibrium." Manuscript, August 2003.

[8] Kahn, Charles M., James McAndrews, and William Roberds. "A Theory of Transactions Privacy." Federal Reserve Bank of Atlanta Working Paper 2000-22, November 2000.

[9] Kandori, Michihiro. "Social Norms and Community Enforcement," *Review of Economic Studies 59, 63-80.*

[10] Kiyotaki, Nobuhiro and John Moore. "Inside Money and Liquidity." Mimeo, 2000.

[11] Kiyotaki, Nobuhiro and Randall Wright, "On Money as a Medium of Exchange." *Journal of Political Economy* 97 (4), August 1989, 927-954.

[12] Kocherlakota, Narayana R. "Money is Memory." *Journal of Economic Theory,* 81(2), August 1998, 232-51.

[13] Kocherlakota, Narayana R. and Neil Wallace. "Incomplete Record-Keeping and Optimal Payment Arrangements." *Journal of Economic Theory*, 81(2), August 1998, 272-89.

[14] Kuttner, Kenneth N., and James J. McAndrews. "Personal On-line Payments." *Federal Reserve Bank of New York Economic Policy Review* 7, December 2001, 35–50.

[15] Schreft, Stacey. "Clicking with Dollars: How Consumers Can Pay for Purchases from E-tailers." *Federal Reserve Bank of Kansas City Economic Review*, First Quarter 2002, 37-64.

[16] Taub, Bart. "Currency and Credit Are Equivalent Mechanisms." *International Economic Review*, 35(4), November 1994, 921-56.

[17] Townsend, Robert M. "Currency and Credit in a Private Information Economy." *Journal of Political Economy*, 97(6), December 1989, 1323-44.