The Quarterly Review of Economics and Finance 85 (2022) 200–207

Contents lists available at ScienceDirect

The Quarterly Review of Economics and Finance

journal homepage: www.elsevier.com/locate/qref

Cash, crime, and cryptocurrencies☆

Joshua R. Hendrickson[a], William J. Luther[b,*]

[a] University of Mississippi, Department of Economics, 306 Odom Hall, University, MS 38677, United States
[b] Department of Economics, Florida Atlantic University, Boca Raton, FL 33431, United States

ARTICLE INFO

Article history:
Received 9 February 2020
Received in revised form 12 January 2021
Accepted 16 January 2021
Available online 27 January 2021

JEL classification:
C78
E41
E42
E50

Keywords:
Bitcoin
Cash
Crime
Criminal activity
Cryptocurrency
Currency
Money
Money matching
Political economy
Tax
Taxation
Tax evasion

ABSTRACT

In *The Curse of Cash*, Kenneth Rogoff lists reductions in criminal activity and tax evasion among the primary benefits of eliminating cash. We maintain that, to the extent that individuals are interested in purchasing illicit goods and services or evading taxes, eliminating cash will encourage them to switch to close substitutes. Hence, governments intent on realizing the benefits cited by Rogoff would not merely need to eliminate cash. They would also need to ban alternatives. This is especially relevant given the proliferation of cryptocurrencies, which provide a fair degree of anonymity for users.

For criminals and criminal organizations, cash is king.[1] Relative to other payment technologies, like deposit accounts or even more cumbersome barter, physical currency lowers the cost of making (1) transactions that are not permitted by law and (2) otherwise legal transactions without paying the required taxes.[2] It is not surprising, then, that some have called for the elimination of cash. In the most-cited proposal, Rogoff (2016) lists the reduction in criminal activity and tax evasion among the primary benefits of eliminating cash.[3] And at least one study finds empirical support for the view that eliminating cash reduces criminal activity.[4]

Governmental efforts to eliminate cash have been fairly modest to date. Sweden seems to have gone the furthest (Heller, 2016). In 2010, the Swedish Tax Agency began requiring the use of certified cash registers to make evading taxes with cash payments more difficult (European Monitoring Centre on Change, 2013). Then, in 2013, the 1000 SEK note was phased out, leaving the 500 SEK—worth roughly $56—as the largest denomination note in

☆ George Selgin and seminar participants at the American Institute for Economic Research provided valuable comments on an earlier draft of this paper. Any remaining errors should be attributed to the authors.
* Corresponding author.
E-mail addresses: jrhendr1@olemiss.edu (J.R. Hendrickson), wluther@fau.edu (W.J. Luther).

1 Europol (2015) considers the motivations for using cash in criminal activities and the extent to which cash is employed by criminals.

2 We use the terms “cash” and “physical currency” interchangeably.

3 Rogoff’s proposal would see large denomination notes eliminated immediately in rich countries, with lower denomination notes phased out entirely or replaced with coins in time. Others, including Summers (2016), limit attention to large denomination notes “worth more than say $50 or $100.” See also: Chainey (2017).

4 Specifically, Wright et al. (2017) find that the transition from paper checks to an Electronic Benefit Transfer (EBT) system in the 1990s resulted in a 9.8 percent decrease in the overall crime rate.

https://doi.org/10.1016/j.qref.2021.01.004
1062-9769/

circulation. And, following a series of high-profile robberies, the Swedish bank tellers' union successfully lobbied to rid cash and ATMs from many bank branches (Magnusson & Gustafsson, 2013). These efforts, combined with the popularity of mobile payment apps like *Swish*, resulted in a gradual decline in the demand for cash. Currency outstanding fell by 47 percent, from 110 billion SEK in December 2009 to 58 billion SEK in December 2017 (The Riksbank, 2021).[5]

In May 2016, the European Central Bank announced it would discontinue producing and issuing its largest denomination note. The last 500 EUR note—worth roughly $534—was issued in April 2019, but "will always retain its value and can be exchanged at the national central banks of the Eurosystem for an unlimited period of time" (European Central Bank, 2016). Other denominations, which range from 5 to 200 EUR, will continue to be produced and issued.[6] Even in India and Venezuela, which launched demonetization schemes in late 2016, the efforts fell far short of eliminating cash.[7] Indeed, the largest denomination notes removed from circulation were ultimately replaced with *even larger* denomination notes in both cases.

Some jurisdictions prohibit cash transactions above a threshold or for a specific purpose. In Europe, Belgium (3000 EUR), Bulgaria (14,999 BGN), Croatia (15,000 EUR), Czech Republic (350,000 CZK), France (3000 EUR for fiscal residents and non-resident traders; 15,000 EUR for non-residents consumers), Greece (1500 EUR), Hungary (1,500,000 HUF per month for legal persons, unincorporated business associations and VAT registered private persons; no limit for consumers), Italy (999.99 EUR), Poland (15,000 euros), Portugal (1000 EUR), Romania (10,000 RON per person per day), Slovakia (5000 EUR; 15,000 EUR for natural person transacting outside his or her trade), and Spain (2500 EUR for residents; 15,000 EUR for non-residents) impose limits on cash transactions, as noted parenthetically (Dako, 2015).[8] In the United States, Louisiana passed House Bill 195 in 2011, which prohibited "any cash transactions in payment for the purchase of junk or used or secondhand property." In 2012, House Bill 1187 limited the prohibition to copper or aluminum-copper air conditioning coils, precious metals, or any other metals worth more than $300. In all of these cases, the efforts to restrict the use of cash have been quite limited. Nonetheless, these efforts suggest that governments are willing to consider eliminating cash if the corresponding reductions in crime or tax evasion are thought to be large enough.

We maintain that the mere elimination of cash is insufficient to realize the benefits of reduced crime and tax evasion cited by Rogoff and others. To the extent that individuals are interested in purchasing illicit goods and services or avoiding taxes, eliminating cash will encourage them to switch to close substitutes. Hence, governments intent on stamping out criminal activity or tax evasion would need to ban these alternative payment technologies as well.[9]

Our assertion, that one must consider alternative payment technologies when considering the effects of eliminating cash, is especially relevant given the proliferation of cryptocurrencies over the last decade. Cryptocurrencies like bitcoin are close substitutes to cash. They offer a greater degree of financial privacy and, hence, enable individuals to make transactions at a lower risk of detection than traditional digital payments. Consequently, efforts to eliminate cash will likely encourage adoption of cryptocurrencies.

In what follows, we consider the relationship between cash, crime, and cryptocurrencies.[10] In Section 1, we show that both cash and cryptocurrencies promote quasi-anonymous exchange (albeit to varying degrees) and should be considered close substitutes in markets where illicit goods and services are sold or taxes are evaded. In Section 2, we develop a model to demonstrate that banning cash might push users toward cryptocurrencies in such markets. Specifically, we extend the standard Lagos and Wright (2005) model to include two types of goods that can be traded in decentralized markets: one is a legal good, where digital dollars, currency, or cryptocurrencies might be used, and one is an illicit good, where physical dollars or cryptocurrencies might be used.[11] We show that, when individuals place sufficient value on exchanges taking place in the illicit market, banning cash leads them to adopt cryptocurrencies. We discuss the implications of the model in the context of Rogoff's proposal to ban cash in Section 3.

1. Cash and cryptocurrencies as close substitutes

Despite recent innovations in payment technologies, cash usage is still common. U.S. currency in circulation exceeded $2 trillion in December 2020, roughly 31 percent of M1. The number of notes in circulation grew at a compound annual growth rate of 4.55 percent from December 2009 to December 2019, while the value of notes in circulation grew at 6.84 percent. According to the Federal Reserve's Diary of Consumer Payment Choice, around 31 percent of all consumer transactions take place in cash. That makes cash the most frequently used payment technology in the United States, ahead of both debit (27 percent) and credit (18 percent) cards (O'Brien, 2017).[12]

The widespread use of cash is somewhat surprising given the obvious drawbacks of holding and transacting with physical currency. Cash does not bear interest. It is easier to lose and easier to steal than balances held at a bank—and less likely to be insured due to loss or theft. It is more cumbersome for high-valued transactions, since one must carry many notes, and odd-amount transactions, since one must provide the correct denominations or rely on another party to make change.[13] And it typically requires the sender and receiver be physically present in the same location when funds are transferred.

However, cash has several desirable characteristics that might make it superior to other, bank-offered payment technologies for some users or in some transactions despite the aforementioned drawbacks. For one, the start-up costs of using cash are low. One need not have a bank account or maintain a minimum balance beyond that being spent in order to make cash transactions. There are no bank or merchant terminal fees.[14] One need not have access to the Internet, telephone lines, or even electricity to spend

[5] It has rebounded slightly in the time since, but still remains well below peak. In December 2020, currency outstanding stood at 63 billion SEK (The Riksbank, 2021).

[6] Recent reports suggest Australia may soon follow by eliminating its largest denomination note, the 100 AUS, worth roughly $76 (Chung, 2016). But the Reserve Bank of Australia has pushed back, suggesting that "it is the $50 denomination—rather than the $100—that tends to be preferred by criminal elements" (Davies, Doyle, Fisher, & Nightingale, 2016).

[7] India pulled its 500 and 1000 INR notes, the larger worth just over $15 (Rajagopalan, 2016). Venezuela invalidated its 500 VEF note, which traded for a mere $0.34 on the black market at the time (Luther & Montenegro, 2017). Both demonetization schemes were conducted under the auspices of discouraging crime and corruption.

[8] Spain has recently proposed reducing the limit to 1000 EUR (Viaña, 2016).

[9] Some advocates of eliminating cash, like Rogoff, acknowledge this point.

[10] Our work complements that of Lastrapes (2018). See also: Alvarez and Lippi (2017), Hendrickson and Park (2020).

[11] Keister and Sanches (2019) use a similar model to analyze the demand for deposits, cash, and central bank-issued digital currency in separated markets.

[12] Cash is most frequently used in low-value transactions. Whereas 55 percent of transactions for amounts less than $10 were conducted in cash, smaller portions (35, 19, 15, and 8 percent) of larger-value transactions (between $10 and $24.99, $25 and $49.99, $50 and $99.99, add over $100, respectively) were conducted cash.

[13] Large payments by check or debit card, in contrast, require the mere writing or typing of a larger number. It is also possible to transfer the precise amount.

[14] Indeed, some merchants offer a cash discount.

or receive cash. And, perhaps most importantly, cash provides a greater degree of financial privacy than common bank-offered payment technologies.[15]

The degree of financial privacy afforded by a particular payment technology depends, at least in part, on the way in which transactions are processed (Luther & Smith, 2020). Bank-offered payment technologies, like checks or debit cards, are typically processed using a centralized mechanism, where a clearinghouse debits the paying party's account and credits the receiving party's account whenever a transaction is made. With the centralized mechanism, a transaction is observable not only to the parties of the transaction, but also to the financial intermediaries and the clearinghouse processing the transaction. It might also result in a record of the transaction (i.e., a paper trail).

Cash payments, in contrast, typically use a decentralized mechanism. The transaction alters no account balances as physical currency changes hands. Therefore, a cash transaction need not be observable to anyone other than the parties of the transaction and no record of the transaction, other than the parties' ending balances, remains after the transaction has been executed. In general, the non-account-based mechanism offers a greater degree of financial privacy than the account-based clearing mechanism.

The desirable characteristics discussed above suggest many situations where physical currency might be essential—that is, where it might enable a larger set of transactions than would otherwise be possible.[16] However, we focus exclusively on markets where illicit goods and services are sold or taxes are evaded.[17] Naturally, those participating in such markets are concerned with the risk of being detected by law enforcement officers and take steps to reduce that risk when it is cost-effective to do so. The choice of payment technology provides one such opportunity to reduce the risk of detection. To the extent that cash affords a greater degree of financial privacy than bank-offered payment technologies, like checks and debit cards, it will be more useful for those transacting in illicit markets.

It should be clear that cash does not enable *perfectly* anonymous exchange. Cash transactions do not rely on and, hence, are not visible to financial intermediaries. But they might be observed by others in close proximity if sufficient steps to hide the transaction are not taken. Cash transactions do not leave a paper trail. But the parties of the transaction are aware that it has occurred and might reveal this information to others at a later date. It is for these reasons, and potentially others, that we say cash affords a greater degree of financial privacy or, alternatively, promotes *quasi*-anonymous exchange.

Like cash, cryptocurrencies offer a greater degree of financial privacy than common bank-offered payment technologies and, hence, might promote quasi-anonymous exchange. Cryptocurrencies tend to employ neither a centralized ledger nor a non-ledger (cash-like) mechanism. Instead, transactions are processed over a distributed ledger. The typical distributed ledger enables physically distant transactions between pseudonymous users without the need for a trusted third-party to act as intermediary. However, it also produces a lasting public record of transactions. The net effect of these features, in terms of improving on the financial privacy afforded by cash, is ambiguous.

The bitcoin protocol provides a clear illustration.[18] To make a transaction, the sender encodes her payment with the receiver's public key and uses her own private key to authorize the transfer of funds.[19] The receiver decodes the payment with his private key. Both parties are pseudonymous, known only by their public keys. The transaction is announced to the network. In exchange for new bitcoin and any transaction fees offered by the sender, miners on the network race to add it to the blockchain, a public record of all past transactions. Once a sufficient number of miners confirm the transaction, it is recognized as valid. Hence, transactions are processed by the entire network, through distributed clearing, rather than the parties to the transaction or a trusted third-party.

Although the bitcoin protocol provides a fair degree of financial privacy, ancillary services and alternative protocols offer even more. For example, users might employ a tumbler, or mixing service, to obscure their transactions. Recall that all past transactions are publicly observable on the blockchain. Rather than sending funds directly to the receiver—and thereby revealing a connection between two public keys—a sender might instead opt to send the funds through a tumbler, where it is mixed with balances from other senders. The tumbler then sends an appropriate share of the mixed funds on to each of the intended recipients, retaining a small fee for the service. By using a tumbler, cryptocurrency users make it more difficult for others to trace their transactions on the blockchain.

The zerocoin protocol takes tumbling one step further. With the zerocoin protocol, senders first send bitcoin to an escrow account and mint a corresponding amount of a temporary currency called zerocoin. Then, the sender transfers the zerocoin balance to the receiver. Since this transaction is in zerocoin, it does not appear on the bitcoin blockchain. The receiver can then redeem the zerocoin using a zero-knowledge proof for the corresponding amount of bitcoin from the escrow account. The transactions between (1) sender and escrow and (2) escrow and receiver appear on the bitcoin blockchain, but there is no direct link between sender and receiver. Moreover, by implementing the mixing at the protocol level, zerocoin eliminates the need to trust a tumbling service. The zerocoin protocol was originally proposed as an extension for the bitcoin network, but has since been implemented by alternative cryptocurrencies.[20] The cryptocurrency Zcash employs a modified version of the protocol known as zerocash.

Several alternative cryptocurrencies, including Dash and Monero, are explicitly premised on the ability to facilitate quasianonymous transactions.[21] Each of these cryptocurrencies use their own unique processes to mask the identity of those engaged in a particular transaction.

There are many cryptocurrencies, each with its own unique features (Antonakakis, Chatziantoniou, & Gabauer, 2019; Ciaian, Rajcaniova, & Kancs, 2018; White, 2015). But some general observations can be made. Along some dimensions, some cryptocurrencies offer more financial privacy than cash. To the extent that agents place sufficiently more weight on these dimensions, they might prefer some cryptocurrency to both cash and traditional bank-offered payment technologies when making illicit transactions. If, instead, agents place relatively little weight on these dimensions, they might prefer cash to cryptocurrencies and traditional bank-

[15] Of course, private banknotes offer a degree of financial privacy similar to that of government-issued currency. However, few private banks issue such notes today. On the legality of private note issue, see: McBride and Schuler (2012), Schuler (2001).

[16] Luther (2016c) provides a brief review of the large literature considering the essentiality of money. See also: Lagos and Wright (2008).

[17] One should be careful not to ignore the more benign uses of cash when considering the welfare consequences of demonetization schemes. In general, the more cash is employed for benign transactions, the greater the welfare costs of baning cash will be. See the discussions in Luther, (2018b), White (2018).

[18] On bitcoin's initial launch, see Luther, (2018a, 2019).

[19] We focus on bitcoin's (potential) role as a medium of exchange. Others have maintained that, at least to date, bitcoin has functioned primarily as a speculative asset (Baur, Hong, & Lee, 2018; Yermack, 2013). See also: Hazlett and Luther (2020).

[20] Zcoin, Private Instant Verified Transaction (PIVX), and Zoin all employ the zerocoin protocol.

[21] Originally released as XCoin, Dash's name was changed to Darkcoin in February 2014 and, finally, to Dash in March 2015. Similarly, Monero was initially released as BitMonero in April 2014 and rebranded shortly thereafter.

offered payment technologies for illicit transactions. In any event, it seems reasonable to conclude that some cryptocurrencies and cash are relatively close substitutes for making illicit transactions since both offer more financial privacy than traditional bank-offered payment technologies. Hence, in the event of a ban on cash, some agents who had preferred to use cash when conducting illicit transactions prior to the ban might opt to use a cryptocurrency for such transactions following the ban.

2. The model

The model is a variation of Hendrickson and Salter (2016). Time is continuous and lasts forever. There is a continuum of agents with unit mass. There are three types of goods that can be traded in the economy: a centralized market good, a search good, and an illegal good. None of these goods are storable. People spend their time in a centralized market to trade. Everyone is capable of producing the centralized market good and all individuals consume this good. People also search for others to trade with in one-on-one transactions. As a result of this searching, people will randomly be matched pairwise to trade. A fraction of people, γ, do not want to engage in illegal trade and will only trade the search good in pairwise meetings. The remaining fraction of people, $1-\gamma$, do not want to consume the search good, but do want to consume the illegal good. Let $i \in \{L, I\}$ denote the individual's type, where L-types prefer legal trade in pairwise meetings and I-types prefer illegal trade.

In all pairwise trade, individuals lack access to the centralized market and therefore cannot produce the centralized market good. In addition, the interactions are anonymous and therefore credit is not feasible. Media of exchange are essential. We assume that there are three assets that can potentially be used as media of exchange: currency, electronic money, and bitcoin. Both currency and electronic money are provided by a central bank. The use of these media of exchange is complicated by the fact that when buyers and sellers meet, individuals must pay a proportional transaction cost. The size of the transaction cost varies by asset. These transactions costs can be motivated as follows. For electronic money, the transaction cost can be thought of as something akin to a "swipe fee." For bitcoin, the transaction cost can be thought of as a cost of verifying authenticity. For currency, this cost is akin to checking to see whether the currency is counterfeit. In addition, by default, electronic money leaves a record with the government authority. Thus, individuals who engage in illegal trades cannot use electronic money. Since bitcoin is pseudonymous, we also assume that that illegal traders have to pay an additional transaction cost to conceal these transactions.

The expected discounted utility of the agents who populate the model is given as

$$\mathcal{U} = \int_0^{\infty} e^{-\rho t}[x(t) - y(t)]dt + \sum_{n=1}^{\infty} e^{-\rho T_n}\{u[q_i^b(T_n)] - c[q_i^s(T_n)]\}$$

where q_i^b is the quantity consumed in pairwise meetings for individuals of type i, q_i^s is the quantity sold in pairwise meetings for individuals of type i, x is the quantity of consumption in the centralized market, T_n denotes the time period of the nth entry into the decentralized market, $y \leq \bar{y}$ is the quantity of production in the centralized market, where $\bar{y}$ is defined to be sufficiently large that this constraint never binds, ρ is the time discount rate, and $u', -u'', c' > 0$ and $c'' \geq 0$.[22]

[22] The assumption that $y > \bar{y}$ implies that production is unbounded and therefore asset balances can "jump." This ensures a degenerate distribution of asset balances across individuals.

Finally, there is a central bank that pays interest on the electronic money balances using seigniorage. The central bank's budget constraint can therefore be written as

$$rE = \mu Z \tag{1}$$

where E is the real aggregate supply of electronic money, Z is the real aggregate supply of currency, $r \leq \rho$ is the rate of return on electronic money, and μ is the growth rate of money.

2.1. The centralized market

Let $W(e, z, b)$ denote the value of entering the centralized market with real balances of electronic money, e_i, currency, z_i, and bitcoin, b_i. It follows that for individuals of type i,

$$W_i(e_i, z_i, b_i) = \int e^{-\rho t}\{[1 - F(t)](x_i - y_i) + f(t)V_i(e_i, z_i, b_i)\}dt$$

where $F(t)$ is the conditional distribution function that measures the probability that the individual has been matched pairwise at or before time t, $f(t)$ is the probability density function that the individual is matched during the interval $[t, t+dt)$, and V_i is the value of an individual of type i in a pairwise match. Suppose that the time it takes to enter a pairwise meeting is drawn from an exponential distribution. It follows that $F(t) = 1 - e^{-\alpha t}$ and $f(t) = \alpha e^{-\alpha t}$. Plugging this into the value function and simplifying yields

$$W_i(e_i, z_i, b_i) = \int e^{-(\rho+\alpha)t}\{x_i - y_i + \alpha V_i(e_i, z_i, b_i)\}dt$$

For simplicity, we assume that all trade in the CM is carried out using electronic money, but individuals can also use electronic money to reallocate their portfolio. Thus, the evolution of electronic money, currency, and bitcoin can be written, respectively, as

$$de_i = (r_e e_i + r_b b_i + y_i - x_i - \ell_{iz} - \ell_{ib})dt \tag{2}$$

$$dz_i = (\ell_{iz} - \pi z_i)dt \tag{3}$$

$$db = \ell_{ib}dt \tag{4}$$

where r_e is the rate of return paid on electronic money, r_b is the rate of return on bitcoin that is only realized when converted into electronic money, π is the rate of inflation, and ℓ_z and ℓ_b are net purchases of currency and bitcoin, respectively.

Let n denote net consumption in the CM. Given, W_i and Eqs. (2), (3), and (4), the Bellman equation can be written as

$$(\rho+\alpha)W_i(e_i, z_i, b_i) = \max_{n_i, \ell_{iz}, \ell_{ib}} n_i + \alpha V_i(e_i, z_i, b_i) + \frac{\partial W_i}{\partial e}(r_e e_i + r_b b_i - n_i - \ell_{iz} - \ell_{ib})$$

$$+ \frac{\partial W_i}{\partial z}(\ell_z - \pi z) + \frac{\partial W_i}{\partial b}\ell_b \tag{5}$$

The first-order conditions are:

$$\frac{\partial W_i}{\partial e_i} = 1 \tag{6}$$

$$\frac{\partial W_i}{\partial z_i} = 1 \tag{7}$$

$$\frac{\partial W_i}{\partial b_i} = 1 \tag{8}$$

Note that this implies that $\partial^2 W/\partial e = \partial^2 W/\partial z = \partial^2 W/\partial b = 0$. The Benveniste-Scheinkman conditions are therefore given as

$$\rho + \alpha - r_e = \alpha \frac{\partial V_i}{\partial e_i} \tag{9}$$

$$\rho+\alpha+\pi=\alpha\frac{\partial V_i}{\partial z_i} \quad (10)$$

$$\rho+\alpha-r_b=\alpha\frac{\partial V_i}{\partial b_i} \quad (11)$$

for electronic money, currency, and bitcoin, respectively.

2.2. Pairwise meetings

Once people are matched pairwise to trade, they receive a preference shock. With probability 1/2, a person wants to be a buyer and with probability 1/2, a person wants to be a seller. Let $d_{ie}\le e_i$, $d_{iz}\le z_i$, and $d_{ib}\le b_i$ denote the offers of real electronic money, currency, and bitcoin, respectively, offered by the buyer to the seller. It follows that the value function associated with pairwise meetings can be written:

$$V_i(e_i,z_i,b_i)=\frac{1}{2}[u(q_i^b)+W_i(e_i-d_{ie},z_i-d_{iz},b_i-d_{ib})]$$

$$+\frac{1}{2}[-c(q_i^s)+W_i(e_i+d_{ie},z_i+d_{iz},b_i+d_{ib})]$$

Once matched, the individuals negotiate the terms of trade. To avoid hold-up problems, we will assume that buyers simply make take-it-or-leave-it offers to sellers. Note that the buyer's offer to the seller must be incentive-feasible. In other words, the buyer must offer enough to the seller in order to induce the seller to produce. For the offer to be incentive feasible, it must be true that

$$(1-\chi_{i,e})d_{ie}+(1-\chi_z)d_{iz}+(1-\chi_{i,b})d_{ib}\ge c(q_i^s) \quad (12)$$

where $\chi_{i,e}$, χ_z and χ_b are the transaction cost associated with verifying the authenticity of the respective assets. Note that $\chi_{i,e}$ and $\chi_{i,b}$ depend on the type of trade. In a meeting to conduct illegal trade, $\chi_{I,e}=1$ and $\chi_{I,b}>\chi_{L,b}$.

Since buyers make take-it-or-leave-it offers, this constraint will always be binding. In addition, we will assume that the allocation of transaction asset is scarce such that $d_{ie}=e_i$, $d_{iz}=z_i$, and $d_{ib}=b_i$ if these assets are held in equilibrium. Finally, by definition the quantity traded by sellers must equal the quantity traded by buyers in pairwise meetings, $q_i=q_i^b=q_i^s$. The incentive compatibility constraint can therefore be written:

$$(1-\chi_{i,e})e_i+(1-\chi_z)z_i+(1-\chi_{i,b})b_i=c(q_i) \quad (13)$$

From the implicit function theorem, it follows that

$$\frac{\partial q_L}{\partial e}=\frac{1-\chi_{L,e}}{c'(q_L)}$$

$$\frac{\partial q_i}{\partial z_i}=\frac{1-\chi_z}{c'(q_i)}$$

$$\frac{\partial q_i}{\partial b_i}=\frac{1-\chi_{i,b}}{c'(q_i)}$$

Note that since $\chi_{I,e}=1$, the first condition only applies to legal traders. For illegal traders, $\partial q_I/\partial e=0$. Since the marginal effect of offering electronic money in illegal trade is zero, illegal traders have no incentive to offer (or accept) electronic money. Differentiating V_i with respect to e_i, z_i, and b_i, respectively, and using the above equations yields[23]

$$\frac{\partial V_L}{\partial e}=(1/2)(1-\chi_{L,e})\left[\frac{u'(q_L)-c'(q_L)}{c'(q_L)}\right]+1$$

$$\frac{\partial V_i}{\partial z}=(1/2)(1-\chi_z)\left[\frac{u'(q_i)-c'(q_i)}{c'(q)}\right]+1$$

$$\frac{\partial V_i}{\partial b}=(1/2)(1-\chi_{i,b})\left[\frac{u'(q_i)-c'(q_i)}{c'(q_i)}\right]+1$$

Plugging these conditions into Eqs. (9)–(11) yields,

$$\rho-r_e=\alpha(1/2)(1-\chi_{L,e})\left[\frac{u'(q_L)-c'(q_L)}{c'(q_L)}\right] \quad (14)$$

$$\rho+\pi=\alpha(1/2)(1-\chi_z)\left[\frac{u'(q_i)-c'(q_i)}{c'(q_i)}\right] \quad (15)$$

$$\rho-r_b=\alpha(1/2)(1-\chi_{i,b})\left[\frac{u'(q_i)-c'(q_i)}{c'(q_i)}\right] \quad (16)$$

The left-hand side of these equations represent the marginal cost of holding each asset and the right-hand side represents the expected marginal benefit.

2.3. Equilibrium

Let μ_b and μ_z denote the growth rate of supply bitcoin and currency, respectively. In a stationary equilibrium, it follows that $r_b=-\mu_b$ and $\pi=\mu_z$.

In the CM, the aggregate net consumption of legal buyers is γn_L and the aggregate net consumption of illegal buyers is $(1-\gamma)n_I$. Market clearing requires that $\gamma n_L+(1-\gamma)n_I=0$.

Using Eqs. (13)–(16), the equilibrium conditions for legal buyers and illegal buyers in the DM are given, respectively, as:

$$\frac{\rho-r_e}{\alpha(1-\chi_{L,e})}=(1/2)\left(\frac{u'(q_L)}{c'(q_L)}-1\right) \quad (17)$$

$$\frac{\rho+\mu_z}{\alpha(1-\chi_z)}=(1/2)\left(\frac{u'(q_L)}{c'(q_L)}-1\right) \quad (18)$$

$$\frac{\rho+\mu_b}{\alpha(1-\chi_{L,b})}=(1/2)\left(\frac{u'(q_L)}{c'(q_L)}-1\right) \quad (19)$$

$$(1-\chi_{L,e})e_L+(1-\chi_z)z_L+(1-\chi_{L,b})b_L=c(q_L) \quad (20)$$

$$\frac{\rho+\mu_z}{\alpha(1-\chi_z)}=(1/2)\left(\frac{u'(q_I)}{c'(q_I)}-1\right) \quad (21)$$

$$\frac{\rho+\mu_b}{\alpha(1-\chi_{I,b})}=(1/2)\left(\frac{u'(q_I)}{c'(q_I)}-1\right) \quad (22)$$

$$(1-\chi_z)z_I+(1-\chi_{I,b})b_I=c(q_I) \quad (23)$$

The aggregate quantity of electronic money in terms of the CM good is

$$E=e_L \quad (24)$$

The aggregate quantity of currency in terms of the CM good is

$$Z=z_L+z_I \quad (25)$$

The aggregate quantity of bitcoin in terms of the CM good is

$$B=b_L+b_I \quad (26)$$

Finally, recall that the central bank's budget constraint is

$$r_eE=\mu_zZ \quad (27)$$

Given (μ_z,μ_b), Eqs. (17)–(27) are sufficient to solve for the variables: $q_L, q_I, r_e, e_L, z_L, b_L, z_I, b_I, E, Z, B$.

[23] Again, note that the marginal value of electronic money in illegal trade would be equal to zero.

Table 1
Possible equilibria.

Legal traders	Illegal traders		
	Currency only	Currency &Bitcoin	Bitcoin only
Electronic money only	+	+	+
Currency only	+	X	X
Bitcoin only	+	+	+
Electronic money &currency	+	X	X
Electronic money &bitcoin	+	+	+
Currency &bitcoin	+	X	X
All assets	+	X	X

2.4. Types of equilibria

There is no guarantee that all assets will be held in equilibrium. As a result, we need to explain why an individual will choose to hold (or not hold) each of these assets. Table 1 lists all of the possible combinations of portfolios that could exist, given that illegal traders will never hold electronic money. However, not all of these combinations of portfolios are possible in equilibrium. The portfolios that are possible in equilibrium are denoted with a '+' whereas those that are not possible in equilibrium are denoted with an 'X.' As shown, there are 13 possible equilibria.

To see why this is the case, note that the left-hand side of the respective equilibrium condition rises when (1) the cost of holding an asset increases or (2) the transaction cost of using an asset increases. Therefore, the right-hand side must increase as well. And, for this to occur, the quantity of trade must decline. Individuals will want to hold the asset that gives them the largest possible quantity of trade. For example, a legal trader will hold all assets if and only if

$$\frac{\rho - r_e}{(1-\chi_{L,e})} = \frac{\rho + \mu_z}{(1-\chi_z)} = \frac{\rho + \mu_b}{(1-\chi_{L,b})}$$

However, since the transaction cost associated with using currency is constant across assets and $\chi_{L,b} < \chi_{I,b}$, this implies that

$$\frac{\rho + \mu_b}{(1-\chi_{I,b})} > \frac{\rho + \mu_z}{(1-\chi_z)}$$

Bitcoin would therefore provide a lower surplus to illegal traders than currency. As a result, illegal traders will not hold bitcoin and will instead choose to only hold currency. In fact, in any equilibrium in which legal traders are willing to hold currency, it must be true that

$$\frac{\rho + \mu}{(1-\chi_z)} \leq \frac{\rho + \mu_b}{(1-\chi_{L,b})}$$

If this is true, then it also must be true that

$$\frac{\rho + \mu}{(1-\chi_z)} < \frac{\rho + \mu_b}{(1-\chi_{I,b})}$$

Thus, illegal traders will never be willing to hold bitcoin in an equilibrium in which legal traders are willing to hold currency. This rules out 8 possible portfolio allocation combinations in Table 1 (those denoted with an 'X').

The government has two mechanisms for eliminating currency use in the model. It can increase the inflation rate or increase the transaction cost of using currency. Through these mechanisms, the government can increase the cost of holding currency to the point that no agent in the model will want to hold currency and the only feasible equilibria will be those in the final column of Table 1.

Let $\mathcal{W}$ denote societal welfare. The welfare function can be written as

$$\mathcal{W} = \gamma[u(q_L) - c(q_L)] + \kappa(1-\gamma)[u(q_I) - c(q_I)] \quad (28)$$

where $\kappa < 1$ is used as a parameter that captures the relative weight given the illegal trade in the social welfare function. If $\kappa \in (0, 1)$, then illegal trade is simply given less weight than legal trade. If $\kappa < 0$, then illegal trade actually reduces social welfare.

Let's denote the quantities of legal and illegal trade that maximize the surplus in the decentralized market as q_L^* and q_I^*, respectively. It is important to note that Eqs. (17)–(19), (21), and (22) imply that $q_L < q_L^*$ and $q_I < q_I^*$ if the left-hand side is greater than zero. Furthermore, note from Eqs. (20) and (23) that q_L and q_I are positively related to the aggregate real supply of assets. It therefore follows that welfare is strictly increasing in the real supply of cash if $\kappa \geq 0$. A necessary, but not sufficient condition for the elimination of cash to improve welfare is if $\kappa < 0$. Whether eliminating cash increases welfare depends on whether legal traders also use cash and, if so, the absolute magnitude of κ. In other words, when $\kappa < 0$, eliminating cash produces a social benefit by reducing illegal trade. However, if legal traders also use cash, there is a societal cost of the foregone legal trade from the elimination of cash. Whether society is better off or worse off depends on the magnitude of the reductions in trade and the absolute magnitude of κ.

There is also an additional complication. Recall that the central bank budget constraint is $rE = \pi Z$. If nobody in the economy is willing to hold currency, then in any equilibrium in which legal traders are willing to hold electronic money, the rate of return on electronic money must be zero. Eliminating currency therefore can therefore make legal traders worse off through an additional channel since those previously holding electronic money will see the cost of holding electronic money increase thereby reducing their electronic money balances and therefore the quantity of trade. In addition, those who were not previously holding electronic money cannot be made better off since they are either indifferent to the change (if they only held bitcoin) or are made worse off by the elimination of currency.[24]

What this suggests is that the only way in which society can possibly be made better off is if $\kappa < 0$ and if the reduction in the quantity of illegal trade sufficiently exceeds the reduction in legal trade.[25]

Regardless of the welfare consequences, the equilibrium conditions demonstrate that eliminating currency cannot eliminate illegal trade as long as illegal traders have a viable alternative payment technology. In this case, the illegal traders can (and will) switch to bitcoin in the event that policymakers commit to a policy to eliminate currency from circulation. Illegal traders will either continue using bitcoin, in the case where they were only using bitcoin before, or substitute bitcoin for currency, in the case where they were using both bitcoin and currency before. If they were not using bitcoin prior to the ban, then they will substitute bitcoin for currency following the ban. As long as bitcoin remains an alternative, eliminating currency can reduce—but not eliminate—illegal trade.

3. Discussion

The formal model presented in Section 2 confirms the intuitive view put forward in Section 1. If cash and cryptocurrencies are close

[24] It is important to note that this is a secondary effect of the elimination of cash. While we do not have privately issued money other than bitcoin in this model, eliminating cash would still reduce the quantity of trade of all who use currency in a model with privately-issued and interest-bearing bank deposits. Whether this results in an increase or decrease in welfare depends on whether legal traders use currency and the absolute magnitude of κ.

[25] Hendrickson and Park (2020) use a similar model to show that such policies are possible, but that the socially optimal policy is to induce a separating equilibrium in which only illegal traders use currency. Policymakers can then choose an inflation rate that provides a transfer from illegal traders to legal traders.

substitutes for conducting illicit transactions, a ban on cash might merely prompt those affected to use cryptocurrencies instead. With this in mind, we consider Rogoff's proposal to ban cash.

The case for improving social welfare by banning cash rests on a rather unlikely set of parameterizations. The social costs of illicit transactions must be sufficiently large to warrant the ban on cash. At the same time, however, the private benefits accruing to those transacting in the market for illicit goods and services must be sufficiently small. Otherwise, a ban on cash would prompt those making illicit transactions to switch to an alternative and a sizable portion of the gains from banning cash that Rogoff projects would go unrealized. We describe this as a rather unlikely set of parameterizations since many of the features that give rise to large social costs (e.g., a large market in illicit goods and services) would also tend to yield large private benefits to those in the market for illicit goods and services.

Rogoff (2016) seems to recognize the tenuous nature of his position, addressing the potential threat to his proposal from alternatives like bitcoin in two distinct ways. First, he argues that the available alternatives do not constitute a serious threat since "a strong central government has huge advantages in providing a safe guaranteed asset" (p. 16) and the Federal Reserve can "adopt a similar blockchain public ledger technology" (p. 213) should doing so prove useful. We do not deny that monies are subject to network effects and governments enjoy a large network of users at present.[26] The agents in our model take into account the extent to which a given money is likely to circulate, given all of its characteristics, when deciding which monies to accept.[27] Nor do we deny that governments might offer digital assets resembling cryptocurrencies. But one must keep in mind the situation under consideration. It would make little sense for a government to ban cash in an effort to eliminate criminal transactions while simultaneously offering a digital asset that enables quasi-anonymous exchange. Hence, such assets—if they exist at all—would almost certainly lack the financial privacy afforded by existing cryptocurrencies. And it is the greater degree of anonymity provided by alternatives like bitcoin that induces some users to switch in our model.

Second, Rogoff suggests that, if participants in illicit markets switch to alternatives like bitcoin, these alternatives can be banned as well. There is no denying that a sufficiently large and powerful government can prevent alternatives from circulating (Hendrickson, Hogan, & Luther, 2016; Hendrickson & Luther, 2017). However, in extending the ban on cash to include close substitutes, Rogoff fails to include the additional costs that such a broad ban would entail in the overall cost-benefit analysis. He also fails to acknowledge the philosophical difference between removing a government-issued currency from circulation and preventing privately-issued alternatives. The former amounts to arguing that the government should not be complicit in a given set of transactions. The latter amounts to arguing that the government should prevent others from being complicit in a given set of transactions. A reasonable person acting at the constitutional level *a la* Buchanan and Tullock (1962) might accept the former without accepting the latter.

Even if we restrict our analysis to the narrow consequentialist case, however, it is not obvious that banning close substitutes to cash is desirable. Two cases are worth considering. In the first case, the social gains from reducing illegal trade are sufficiently small such that banning alternatives like bitcoin reduces social welfare. Of course, such parameterizations imply that the initial ban on cash was either inconsequential (when bitcoin is at least as good as cash for illegal transactions) or welfare-reducing (when bitcoin is not as good as cash for illegal transactions). Since Rogoff intends to improve social welfare, these cannot be the parameterizations he has in mind. In the second case, the social losses from discouraging *legal* trade are sufficiently large such that banning alternatives like bitcoin reduces social welfare. Such parameterizations result when there are some legal transactions that can be made with bitcoin but cannot be made with electronic money. Hence, even if banning cash increases social welfare, it does not follow that banning alternatives like bitcoin is a good idea.

[26] It is far from obvious that governments have huge advantages in providing a safe guaranteed asset, however. Many governments manage their monies poorlyand even some of the best performers have mixed track records. See, for example, Selgin, Lastrapes, and White (2012).

[27] See also: Luther (2016a, b).

4. Conclusion

Concerns over the use of cash to purchase illegal goods and services and evade taxes have led Rogoff and others to call for removing large denomination notes from circulation and replacing small denomination notes with coins. Few demonetization schemes have been implemented to date—and those implemented have been limited in scope. But those limited efforts and the broader political discourse suggest that governments are taking such proposals seriously.

We have argued that the mere elimination of cash is insufficient. Since cryptocurrencies promote quasi-anonymous exchange, they should be considered close substitutes to cash in transactions where financial privacy is important. We have developed a model where banning cash prompts some users to switch to cryptocurrencies and discussed the welfare consequences to ban these alternatives in addition to cash. In particular, we note that banning alternatives like bitcoin might reduce social welfare, *even if banning cash is desirable*.

In addition to contributing to the ongoing policy debate concerning cash and cryptocurrencies, we also advance the theoretical literature on bitcoin. Whereas previous studies have merely assumed some demand for bitcoin, we have included a specific market where quasi-anonymous exchange is desirable. In doing so, we have offered an explicit friction that makes bitcoin essential.

Declarations of interest

None declared.

References

Alvarez, F., & Lippi, F. (2017). Cash burns: An inventory model with a cash-credit choice. *Journal of Monetary Economics*, *90*, 99–112.
Antonakakis, N., Chatziantoniou, I., & Gabauer, D. (2019). Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios. *Journal of International Financial Markets, Institutions and Money*, *61*, 37–51.
Baur, D. G., Hong, K., & Lee, A. D. (2018). Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money*, *54*, 177–189.
Buchanan, J. M., & Tullock, G. (1962). *The calculus of consent*. University of Michigan Press.
Chainey, R. (2017). *The US should get rid of cash and move to a digital currency, says this Nobel laureate economist*. World Economic Forum. January.
Chung, F. (2016). *Government floats $100 note removal.* , news.com.au, December.
Ciaian, P., Rajcaniova, M., & Kancs, A. (2018). Virtual relationships: Short-and long-run evidence from bitcoin and altcoin markets. *Journal of International Financial Markets, Institutions and Money*, *52*, 173–195.
Dako, A. (2015). *Cash payment limit in the European union*. Abroad. October.
Davies, C., Doyle, M.-A., Fisher, C., & Nightingale, S. (2016). *The future of cash*. pp. 43–52. Reserve Bank of Australia Bulletin. December.
European Central Bank. (2016). *ECB ends production and issuance of 500 banknote*. Press Release. May.
European Monitoring Centre on Change. (2013). *Cash register legislation, Sweden. European foundation for the improvement of living and working conditions*. June.
Europol. (2015). *Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering*. European Police Office. July.
Hazlett, P. K., & Luther, W. J. (2020). Is bitcoin money? And what that means. *Quarterly Review of Economics and Finance*, *77*, 144–149.

Heller, N. (2016). *Imagining a cashless world*. The New Yorker. October.
Hendrickson, J. R., & Luther, W. J. (2017). Banning bitcoin. *Journal of Economic Behavior & Organization*, *141*, 188–195.
Hendrickson, J. R., & Park, J. (2020). *The case against eliminating large denomination bills. Working paper*.
Hendrickson, J. R., & Salter, A. W. (2016). Money, liquidity, and the structure of production. *Journal of Economic Dynamics and Control*, *73*(C), 314–328.
Hendrickson, J. R., Hogan, T. L., & Luther, W. J. (2016a]). The political economy of bitcoin. *Economic Inquiry*, *54*(2), 925–939.
Keister, T., & Sanches, D. (2019). Should central banks issue digital currency? Working paper. *Federal Reserve Bank of Philadelphia Working Paper*.
Lagos, R., & Wright, R. (2005). A unified framework for monetary theory and policy analysis. *Journal of Political Economy*, *113*(3), 463–484.
Lagos, R., & Wright, R. (2008). *When is money essential? A comment on Aliprantis*. Camera and Puzzello. Working paper.
Lastrapes, W. D. (2018). The costs and benefits of eliminating currency. *Cato Journal*, *38*(2), 503–519.
Luther, W. J. (2016a]). Bitcoin and the future of digital payments. *The Independent Review*, *20*(3), 397–404.
Luther, W. J. (2016b]). Cryptocurrencies, network effects, and switching costs. *Contemporary Economic Policy*, *34*(3), 553–571.
Luther, W. J. (2016c]). Mises and the moderns on the inessentiality of money in equilibrium. *Review of Austrian Economics*, *29*(1), 1–13.
Luther, W. J. (2018a]). Is bitcoin intrinsically worthless? *Journal of Private Enterprise*, *33*(1), 31.
Luther, W. J. (2018b]). The curse of cash by Kenneth S. Rogoff. *Independent Review*, *22*(4), 619–622.
Luther, W. J. (2019). Getting off the ground: The case of bitcoin. *Journal of Institutional Economics*, *15*(2), 189–205.
Luther, W. J., & Montenegro, G. G. (2017). *The case for currency substitution in Venezuela*. Forbes. January.
Luther, W. J., & Smith, S. S. (2020). Is bitcoin a decentralized payment mechanism? *Journal of Institutional Economics*, *16*, 433–444.
Magnusson, N., & Gustafsson, K. (2013). *Swedish banks make money by saying no to cash*. Bloomberg Technology. April.
McBride, W., & Schuler, K. (2012). Where is private note issue legal? *Cato Journal*, *32*(2), 395–410.
O'Brien, S. (2017). *Understanding consumer cash use: Preliminary findings from the 2016 diary of consumer payment choice*. FedNotes. November.
Rajagopalan, S. (2016). *1. 25 billion people were shocked on November 8*. RealClearMarkets. November 2016.
The Riksbank. (2021). *Statistics on banknotes in circulation 1945–2020*. Data.
Rogoff, K. S. (2016). *The curse of cash*. Princeton University Press.
Schuler, K. (2001). Note issue by banks: A step toward free banking in the united states? *Cato Journal*, *20*(3), 453–465.
Selgin, G. A., Lastrapes, W. D., & White, L. H. (2012). Has the fed been a failure? *Journal of Macroeconomics*, *34*(3), 569–596.
Summers, L. H. (2016). *It's time to kill the $100 bill*. The Washington Post. February.
Viaña, D. (2016). *El gobierno limitará el pago en efectivo a 1. 000 euros*. El Mundo. November.
White, L. H. (2015). The market for cryptocurrencies. *Cato Journal*, *35*(2), 383–402.
White, L. H. (2018). The curse of the war on cash. *Cato Journal*, *38*(2), 477–487.
Wright, R., Tekin, E., Topalli, V., McClellan, C., Dickinson, T., & Rosenfeld, R. (2017). Less cash, less crime: Evidence from the electronic benefit transfer program. *The Journal of Law and Economics*, *60*(2), 361–383.
Yermack, D. (2013). *Is bitcoin a real currency? An economic appraisal*. National Bureau of Economic Research. Working Paper 19747.