How do Private Digital Currencies Affect Government Policy?[*]

Max Raskin Fahad Saleh David Yermack

NYU School of Law *McGill University* *NYU Stern*

August 14, 2019

Abstract

This paper provides a systematic evaluation of the different types of digital currencies. We express skepticism regarding centralized digital currencies and therefore focus our economic analysis on private digital currencies. Specifically, we highlight the potential for private digital currencies to improve welfare within an emerging market with a selfish government. In that setting, we demonstrate that a private digital currency not only improves citizen welfare but also encourages local investment and enhances government welfare. The fact that a private digital currency enhances government welfare implies a permissive regulatory policy which enables citizens to realize the previously referenced welfare gains.

Keywords: Cryptocurrency, Digital Currency, Bitcoin, Blockchain

JEL Classification: E42, F30, G18, O38

[*] We thank Franz Hinzen, Gur Huberman, Gloria Yu and conference participants at the ABFER/ NUS/ MAS Workshop on Digital Currency Economics for comments. Part of this paper was written while David Yermack was a visiting professor at Erasmus University Rotterdam.

1 Introduction

Currency crises are nothing new. As long as governments have maintained monopoly power over the printing presses, there has existed a temptation to devalue a country's sovereign currency. From the ancient Roman Empire to Robert Mugabe's Zimbabwe, a citizenry's loss of faith in its government's money often portends economic collapse. In order to mitigate or at least function through such a collapse, individuals throughout history have turned to alternatives to state-backed money. These alternatives have included more stable sovereign currencies like the U.S. dollar and commodities like gold and silver. This paper explores a new alternative to state-backed money: private digital currencies.

Bitcoin, the first and most successful of the private cryptocurrencies, was self-consciously birthed in response to the Financial Crisis of 2007-2008. Text containing The Times of London's headline, "Chancellor on brink of second bailout for banks," was encoded in the first block of the Bitcoin blockchain, mined on January 3, 2009. This text gave a hint of the creator's skepticism of the government-run banking system. The pseudonymous creator of bitcoin, Satoshi Nakamoto, was very explicit in his belief that, "[t]he central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."[1] Nakamoto's vision for bitcoin was as an "e-currency based on cryptographic proof, without the need to trust a third party middleman" making money "secure and transactions effortless."[2] In other words, the idea was to decentralize and privatize the issuance of digital money.

Nakamoto's analogy of the decentralization of money was to the decentralization of data security. Before strong encryption, users had to rely on central third parties to store and secure their data.[3] The use of encryption has allowed individuals to store their data securely without the need of a trusted third party. This is analogous to the Bitcoin blockchain by

[1] http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

[2] Id.

[3] Id.

which individuals can transfer value without the need of a centralized party, but instead in reliance on a network that is trust-minimized.

The analogy is instructive because while it is now technically possible for individuals to secure their data themselves, the growth and success of social media companies has shown that this is a decision many choose not to make. Extending the analogy, in the developed world, the overwhelming majority choose to continue to participate in the government-run banking system and to use government-backed money. Individuals did not rush to bitcoin or another digital currency in the wake of the Financial Crisis of 2007-2008, and the dollar strengthened.

At first blush, Nakamoto's vision did not pan out, except insofar as a new option was created that a majority of people choose not to use. When one investigates the developing world, however, the story is a little different. Following the financial crisis, a number of developing countries have experienced significant declines in the value of their sovereign currencies, bordering on crisis levels. Two examples are the Turkish lira and the Argentine peso. The lira lost about a third of its value in 2018 amid Turkey's high current account deficit and massive amounts of U.S. dollar-denominated debt. The Argentine peso lost about half of its value in 2018 as that country struggled with fiscal and trade deficits.[4]

These are the first currency crises since the creation of bitcoin, and therefore they offer an opportunity to investigate the impact that alternative digital currencies have on unstable sovereign currencies. Extrapolating out, this may show that Nakamoto's vision has come to fruition. Although private digital currencies have not replaced the dollar, their mere existence may have a counterfactual impact in that they exist as a check on both fiscal and regulatory policy. This paper formalizes that assertion.

This paper highlights that a private digital currency has significant implications for a corrupt emerging market. We define a corrupt emerging market as an economy with high volatility and a government that sets policy based on selfish interests rather than considering the welfare of citizens. We model the interaction of the government and citizenry within that

[4] https://ftalphaville.ft.com/2019/05/14/1557806416000/Currency-crisis-redux-/

setting. We allow for endogenous fiscal, monetary and regulatory policy. We establish three main findings.

Our first finding establishes that citizens gain from the existence of the private digital currency. Citizens accrue those gains through two channels. First, as documented by Dyhrberg (2016), private digital currencies offer diversification. We demonstrate that this diversification generates welfare gains for citizens. Second, the private digital currency serves as competition for local investment so that the existence of the private digital currency restrains monetary policy, thereby generating lower inflation.

Our second finding highlights that private digital currencies encourage local investment. This finding also operates through two channels. First, we show that a private digital currency generally serves as a complement rather than as a substitute for local investment so that citizens, when given access to a private digital currency, not only invest in that currency but also expand investment in the local economy. Second, the existence of the private digital currency disciplines monetary policy by creating an alternative to local fiat. That monetary policy discipline reduces inflation and results in higher returns from investment which in turn encourages higher local investment.

Our third finding demonstrates that the government may gain from permitting the private digital currency within the local economy. This finding arises because the government extracts revenue gains from citizens through taxation. Higher local investment generates higher tax revenues for the government. The government permits the private digital currency because of the additional revenue without regard to citizen welfare. This finding is particularly important because it implies that the previously discussed citizen welfare gains arise in equilibrium.

Our paper contributes to a growing literature that studies blockchain economics and cryptocurrencies. That literature dates back to Yermack (2015) which provides the first study of bitcoin's return properties. Since then, the literature has exploded into several rich sub-fields. Harvey (2016) and Yermack (2017) provide overviews of blockchain as it relates to finance. Biais, Bisière, Bouvard, and Casamatta (2019) and Saleh (2019a) analyze the game-theoretic aspects of prominent consensus protocols. Easley, O'Hara, and Basu (2019) and Huberman, Leshno, and Moallemi (2019) investigate the role that fees play within Bitcoin. Biais, Bisière, Bouvard, Casamatta, and Menkveld (2018) study cryptocurrency pricing. Hinzen, John, and Saleh (2019) study and explain the limited adoption of some cryptocurrencies. Makarov and Schoar (2019) study arbitrage and price formation within cryptocurrency markets. Cong and He (2019) and Cong, Li, and Wang (2018) examine economic implications of smart contracts. Howell, Niessner, and Yermack (2019) empirically analyze ICOs whereas Chod and Lyandres (2018) and Li and Mann (2018) develop underlying economic theory to understand ICOs. Griffin and Shams (2018) and Li, Shin, and Wang (2019) highlight price manipulation within cryptocurrency markets. Foley, Karlsen, and Putnins (2019) establish that a significant proportion of Bitcoin transactions pertain to illegal activity.

Our paper relates most closely to Dyhrberg (2016), Yu and Zhang (2018) and Saleh (2019b). Dyhrberg (2016) empirically establishes the hedging value of a cryptocurrency. We theoretically highlight that such value has important welfare implications within emerging markets. Yu and Zhang (2018) empirically document demand shifts towards cryptocurrencies during times of local economic distress. Our theory provides an explanation for such shifts. Saleh (2019b) examines welfare implications of cryptocurrencies in a different setting but also finds evidence that cryptocurrencies may enhance welfare. Our paper also relates closely to Raskin and Yermack (2016), which discusses digital currencies in the context of central banking.

The remainder of this paper is organized as follows. Section 2 provides a typology for classifying the various digital currencies that exist. There is no systematic evaluation of the different types of digital currencies and such a typology will be helpful not only for the purposes of this paper but also for future research. This paper's focus is on private decentralized digital currencies. These are the unique innovation that has sprung forth from the creation of bitcoin and blockchain. There will be a brief discussion of centralized public digital currencies, also known as central bank digital currencies. The paper expresses skepticism over the novelty of central bank digital currencies, which in many ways simply mimic the existing financial structure of many governments. Section 3 provides a formal economic analysis of the effect of a private digital currency on a corrupt emerging market. We find that a private digital currency enhances citizen welfare, encourages local investment, and induces a permissive regulatory policy. Section 4 concludes.

2 Typology

Before analyzing the impact digital currencies have in unstable monetary regimes, it is necessary to lay out a classification of these instruments. This paper offers a typology of digital currency along two axes: state-sponsorship and centralization.

With respect to state-sponsorship, digital currencies can be either public or private. Public digital currencies have some relationship to a sovereign state. Private digital currencies do not have a relationship to a sovereign state, but are instead governed by private individuals or entities. The key distinction here, which will be discussed later, comes with respect to legal enforcement. State-sponsored currencies have the backing of an entity that is able to enforce laws that privilege the currency. There are a number of ways to privilege the sovereign's money, such as legal tender laws or taxation of competing currency. Whatever the method, public currencies possess some legal privilege relative to other currencies.

The second factor in our typology is centralization. A digital currency can either be centralized or decentralized. A number of definitions exist for centralization. For instance, some make a mathematical calculation of centralization based on the number of market participants, nodes, miners, or other metrics. This paper adopts a different definition.

A digital currency is centralized if it has formal barriers to entry that prevent participation in the software writing and validation process of the network. This definition asks whether the code can be changed through some kind of consensus mechanism. If a party is not prevented from participating in the network or there is no one there to prevent that party from participating, then the network is decentralized. This is a qualitative understanding of centralization that has a parallel in antitrust theory. In evaluating barriers to entry to a given industry, there are both formal and economic barriers to entry. A formal barrier would be legal prohibitions or requirements that prevent a new entrant from challenging an incumbent. An economic barrier would be phenomena like economies of scale or upfront capital investments that create costs for a new entrant who wishes to challenge an incumbent.

This analysis equally applies to digital currencies. Formal barriers to entry indicate a centralized currency. Such barriers may prevent a node from validating a transaction or prevent an individual from accessing and proposing alterations to the codebase. This paper focuses on formal barriers because in the context of emerging markets with unstable monetary regimes, what is relevant is the ability to offer competing alternatives. Whether those alternatives are economically viable – especially as compared with the domestic fiat currency – is one of the topics of this paper.

Finally, it is worth noting that these distinctions are confirmed by the Securities and Exchange Commission's ("SEC") "Framework for 'Investment Contract' Analysis of Digital Assets." The jurisdiction of the SEC is bounded by statutory language that gives it the ability to take enforcement actions against securities and the catchall "investment contracts." In defining which digital assets are securities and which are currencies, the SEC had to articulate some principles. Hinman (2018) and Henderson and Raskin (2019) have pointed to decentralization as one of the important principles for classifying digital assets as digital currencies and this decentralization is a formal, not an economic one.

2.1 Application of Typology

In applying this typology, the first category that exists is private decentralized digital currencies. The canonical example is bitcoin. Bitcoin has no privileges or legal protections granted to it by the government. It is decentralized because it is written and maintained in an open source manner and there are no formal barriers to participation in the Bitcoin blockchain network. Anyone with computing power is able to act as both a node and a miner.[5] Litecoin and ether are other examples of private decentralized digital currencies. This category has an analog in precious metals used as currency. Gold and silver are no longer backed or privileged by any government, and anyone can mine these precious metals.

The second category is private centralized digital currencies. These are currencies that are typically run by a closely held company or consortium that exercises control over the protocol that issues and maintains the currency. The networks that create and manage these currencies give formal privileges to certain participants and not others. Those who participate in the currency place trust in a third party for a number of features, including supply, security, and fungibility. Examples of this kind of currency include custodial stablecoins, Libra, and e-gold.

The third category is public centralized digital currencies. A number of sovereign states have announced plans to issue their own digital currencies. These proposals are discussed in-depth below, but the common feature is that the sovereign itself controls the protocol, codebase, and interactions with the network. Essentially all sovereign currencies today are public centralized digital currencies. They are digital because most of the money that exists in the world does not exist in physical form. Their backing and management is achieved by sovereign states with legal protections and privileges. For instance, only the U.S. federal government through its instrumentalities like the Federal Reserve can issue U.S. dollars; no other entities are able to participate formally in monetary policy.

The fourth are public decentralized digital currencies. These are currencies that have the backing of a sovereign, but the sovereign does not seek to exercise control over the currency. In the digital realm, such a currency does not currently exist. The closest analog would be gold, silver, or commodity standards that governments have adopted at certain points in history. One of the rationales behind the gold standard, for instance, is that the state would give primacy to a currency that was out of its control, which was another way of saying that they would commit themselves to a non-discretionary monetary policy. The amount of gold

[5] Indeed, it is technically possible, although practically not feasible, to validate transactions without computing power.

in circulation and its features could not be controlled by a central authority. That the central authority still gave privileges to gold is akin to a developing country adopting the U.S. dollar as its standard. A gold standard or any public decentralized currency is the government accepting the position that the market or some external entity can produce a better money than it can.

This article focuses on public centralized and private decentralized currencies for our economic analyses. We will begin with a discussion of various central banks' proposals for digital currencies.

2.2 Central Bank Digital Currencies

At first glance, the idea of a central bank digital currency sounds antithetical to the motivating political force behind the creation of bitcoin and other digital currencies, namely, to compete with sovereign-backed banking systems. As mentioned above, the genesis block of the Bitcoin blockchain makes reference to the instability of the fractional reserve banking system and the state-sponsorship of banking institutions.

A number of countries have announced plans to issue or investigate the use of digital currencies. Some examples include Sweden, China, Russia, Venezuela, and the Marshall Islands.[6]

It is clear that the proposals for central bank digital currencies are public, centralized proposals. These proposals very closely resemble the "Chicago Plan" of narrowing the banking system by allowing individuals and smaller institutions to hold deposits directly at the central bank. Such a plan is currently being revived by the Federal Reserve.[7] There are both advantages and disadvantages of this proposal, but they are not the advantages that undergird the rationale of decentralized private digital currencies. A blockchain is almost certainly

[6] See https://www.riksbank.se/en-gb/payments--cash/e-krona/, https://www.npr.org/2019/07/31/742223881/facebooks-digital-money-plan-raises-stakes-for-china-s-cryptocurrency-ambitions, https://www.nytimes.com/2018/01/03/technology/russia-venezuela-virtual-currencies.html and http://time.com/money/5186316/this-is-the-first-country-to-adopt-a-cryptocurrency-as-its-official-curr

[7] https://www.federalreserve.gov/newsevents/pressreleases/files/other20190805a2.pdf

not needed to have such a narrowing of the banking system. More traditional databases and technical solutions can be used by the government to keep track of its digital money. This could be similar to the technology used by existing centralized financial services companies like PayPal and Visa.

For a particular case study, in 2016 Sweden's Riksbansk said that research would be done towards launching an e-krona, which would be issued by the central bank. As with all of these programs, details were scarce, but the thrust of the proposal was to hasten Sweden's move away from cash. According to the Riksbank, "[s]ix out of ten people in Sweden have used cash as a means of payment in the last month. The corresponding figure for 2016 was eight out of ten."[8] There are a number of reasons that governments wish to move away from cash, including combating tax evasion, as well as monitoring the financial activity of their citizenry. Privacy advocates are skeptical of such an enforced move away from cash and think such transitions should happen naturally if there is a market demand for it.[9]

The innovation of cryptocurrencies has never been their digital nature – digital money has existed almost as long as computers have. The innovation of this new crop of private currencies is the fact that they do not need a central party to verify transactions and maintain the security and reliability of the system. The key question that must be asked when looking at central bank digital currencies is who maintains the codebase that undergirds central bank's digital currency. If it is the central bank itself, then issuance is no different from the existing system except that individuals can hold accounts with the central bank. If private nodes maintain the codebase, then the monetary rules are not governed by the central bank and therefore the currency cannot be considered a central bank digital currency. For the purposes of analyzing digital assets as competing currencies, central bank digital currencies are not different from central bank currencies generally.

[8] https://www.riksbank.se/globalassets/media/statistik/betalningsstatistik/2018/payments-patterns-in-sweden-2018.pdf

[9] https://research.stlouisfed.org/publications/review/2018/07/16/payment-systems-and-privacy

2.3 Private Digital Currency Competition

There are a number of legal barriers to private digital currencies. These barriers demonstrate why they have the potential to impact the sovereign's monetary policy. Like all monopoly privileges, the rationale behind barriers to entry is to protect incumbents' rates of return. With respect to monetary policy, barriers to competitive currencies prop up the central bank's own currency.

Raskin and Yermack (2016) discuss legal tender laws as one of these barriers. Legal tender laws, however, only explain how a public currency initially can come to displace private currencies. Gresham's Law, which is popularly articulated as "bad money driving out the good," explains how debtors would prefer to pay and transact in depreciating currency and if they are able to do so, will. This has been described by Selgin (1996) as "placing buyers and sellers in a Prisoner's Dilemma in which the use of 'bad' money represents a unique noncooperative equilibrium." Once the state-backed currency takes hold, the network effects of money come into play and it will become a generally accepted medium of exchange, barring any major failure of the central bank. Were legal tender laws to be repealed, there is some skepticism that there would be a great deal of competition from other currencies.

Without taking a view on the relative potency of each of these barriers, this paper addresses two more barriers to competing private currencies: tax treatment and banking regulation.

With respect to tax treatment, we will look to the United States as an example of how the taxing power can disadvantage private currencies. When an individual's dollars appreciate, he does not have to pay either a capital gain or income tax. This is not the case with other competing forms of currency. When an individual's bitcoins, gold, or euros are sold at an appreciated value, this is a taxable event. The Internal Revenue Service has ruled that bitcoin is treated for federal tax purposes as property. Any disposition must be reported on Form 1040's Schedule D. The gains are taxed as either short- or long-term capital gains depending on whether the asset was held for over a year.

This discourages the use of private currencies as mediums of exchange in two primary ways.

First, it raises the actual cost of transactions and second, it increases reporting requirements such that there is greater friction in using alternatives to the U.S. dollar.

One additional legal barrier to the adoption of private digital currencies is the banking regulatory system. There are a number of laws and regulations that make it costly for a new entrant to establish a banking institution that can issue either its own private digital currency or service accounts in a decentralized private digital currency. One such barrier is the ability to obtain a banking charter from the Office of the Comptroller of the Currency. Another aspect of banking regulation is money transmission laws. In the United States, these state-level laws impose certain requirements upon entities that transmit money on behalf of others. These requirements include surety bonds, reporting requirements, and compliance regimes. Finally, at the federal level, the Bank Secrecy Act and other national security considerations require financial institutions to register as Money Service Businesses and establish and maintain anti-money laundering and know-your-customer programs that add additional cost. For established players, these regulatory hurdles are costs that have been integrated and in some cases, larger incumbents have welcomed such regulations and helped to draft them in order to protect themselves from competition.

It is beyond the scope of this paper to evaluate whether such barriers are normatively good or bad. The Modern Free Banking School has questioned many of these barriers. In the following section of the paper, we make a more narrow claim, which is that competing private digital currencies serve as a disciplining mechanism for government monetary policy.

3 Theoretical Analysis

This section models the interaction of a citizen and a government within a corrupt emerging market economy. Our analysis reveals that a private digital currency improves citizen welfare and encourages local investment. Moreover, the government finds permitting the private digital currency incentive compatible.

Our results arise because the private digital currency enables the citizen to achieve gains from diversification and because the existence of the private digital currency disciplines monetary policy. In turn, that diversification and disciplined monetary policy encourages the citizen to increase local investment. The increased local investment then benefits the government via taxation so that even a selfish government prefers permitting rather than prohibiting the private digital currency. The remainder of this section formalizes the aforementioned discussion.

3.1 Model

We focus on the first two dates, $t = 0, 1$, of an infinite horizon economy. The economy consists of a short-lived citizen and a short-lived government. At the initial date, $t = 0$, the government sets fiscal and regulatory policy while the citizen, cognizant of government policy decisions, makes an investment decision. Subsequently, uncertainty resolves, the government sets monetary policy and both the government and the citizen consume.

$$\begin{aligned}
&\max_{w_k, w_u, w_{dc} \geqslant 0} \mathbb{E}[r] - \frac{\gamma}{2}\mathbb{V}ar[r] \\
&s.t. \\
&\qquad r = \omega_0(w_k((1-\tau)r_k - \tau\pi) + w_{dc}r_{dc}) \\
&\qquad w_k + w_u + w_{dc} = 1 \\
&\qquad w_{dc}\mathcal{I}_{np} = 0
\end{aligned} \tag{1}$$

Problem 1 states the citizen's problem. The citizen possesses mean-variance preferences with risk-aversion $\gamma > 0$. She must distribute her wealth, $\omega_0 > 0$, across no more than three assets: productive capital, an unproductive asset, and a digital currency. We denote pre-tax productive capital real net returns by r_k so that $(1 - \tau)r_k - \tau\pi$ gives the post-tax productive capital real net returns with τ denoting the tax rate on nominal profits and π denoting the inflation rate. We denote pre-tax digital currency real net returns by r_{dc} and assume that digital currency holdings face no taxation so that r_{dc} also denotes the post-tax digital currency real net return. We assume no taxation of digital currencies to capture the relative difficulty of enforcing taxation of a private digital asset. We assume that the unproductive asset earns no real net return with probability one.

The citizen may always invest in productive capital and/ or the unproductive asset. However, the citizen may invest in the digital currency only if the government permits digital currency holdings. $\mathcal{I}_{np}$ denotes an indicator equaling one if the government does not permit the citizenry to hold the digital currency.

$$\begin{aligned}
&\max_{\tau,\pi,\mathcal{I}_{np}} \mathbb{E}[\tau\omega_0 w_k r_k + S(\tau,\pi,\mathcal{I}_{np})] \\
&s.t. \\
&\qquad 0 \leqslant \tau \leqslant 1 \\
&\qquad \pi \geqslant 0 \\
&\qquad \mathcal{I}_{np} \in \{0,1\}
\end{aligned} \tag{2}$$

Problem 2 states the government problem. The government selects a tax rate, τ, and whether to allow trading in the digital currency, $\mathcal{I}_{np}$, at the initial date, $t = 0$. Subsequent to resolution of uncertainty, at $t = 1$, the government selects an inflation rate, $\pi \geqslant 0$.

$$S(\tau,\pi,\mathcal{I}_{np}) = \pi\omega_0 w_k(1 + r_k)e^{-\lambda(\mathcal{I}_{np})\pi} \tag{3}$$

The government selfishly maximizes real revenues with no regard to citizen welfare. Government revenues arise from two sources: taxation and seigniorage. $\tau\omega_0 w_k r_k$ denotes real tax revenue whereas $S(\tau,\pi,\mathcal{I}_{np})$ denotes real seigniorage revenue. Akin to Cagan (1956), we invoke the exchange equation and assume exponential form for velocity of money so that Equation 3 holds. $\lambda(\mathcal{I}_{np})$ denotes a function that specifies the sensitivity of the velocity of money to inflation. We assume $\lambda(1) < \lambda(0)$ to reflect the relative ease of transacting with an additional currency available.

3.2 Model Solution

As previously noted, our model consists of two dates: $t = 0, 1$. At $t = 0$, the government selects a tax rate, τ, and a regulatory policy, $\mathcal{I}_{np}$. Then, taking τ and $\mathcal{I}_{np}$ as given and anticipating an inflation rate, π, the citizen selects a portfolio that solves Problem 1. Uncertainty resolves at the beginning of $t = 1$. Subsequently, the government selects an inflation rate, π, and pay-offs realize. We solve the model by backward induction.

At $t = 1$, the government sets an inflation rate to maximize seigniorage revenues. Increasing the inflation rate yields the government more units of currency but devalues each unit of the currency. Following Cagan (1956), we find an interior optimum for the government that depends upon the sensitivity of the velocity of money to inflation. When $\mathcal{I}_{np} = 0$, consumers may use the digital currency to facilitate an increased transaction frequency and thus the velocity of money becomes more sensitive to the inflation rate. The government internalizes that incremental sensitivity so that a permissive regulatory policy entails a credible commitment to restrained monetary policy.

At $t = 0$, the government sets fiscal and regulatory policy. Fiscal policy equates with selecting a tax rate for capital gains. Regulatory policy equates with selecting whether to permit private digital currency holdings.

With respect to fiscal policy, a lower tax rate translates to lower tax revenue holding capital investment constant. However, a lower tax rate also increases capital investment returns, thereby endogenously increasing capital investment, which in turn raises tax revenue. The government trades off these effects to select an optimal tax rate.

With respect to regulatory policy, permitting private digital currency holdings enables citizens to evade taxation by permitting investment in a non-taxed asset. This permissive regulatory policy also restrains the government's monetary policy for previously discussed reasons. Nonetheless, private digital currency investment provides diversification from capital investment (see, for example, Dyhrberg (2016)), so that a permissive regulatory policy may increase capital investment, which in turn increases government tax revenues.

3.3 Results

We begin by contrasting outcomes that arise under a permissive regulatory policy (i.e., $\mathcal{I}_{np} = 0$) with those that arise from a restrictive regulatory policy (i.e., $\mathcal{I}_{np} = 1$). This contrast enables us to deduce the effect of a private digital currency upon citizen welfare. Subsequently, we endogenously determine whether the government permits trading of the digital currency.

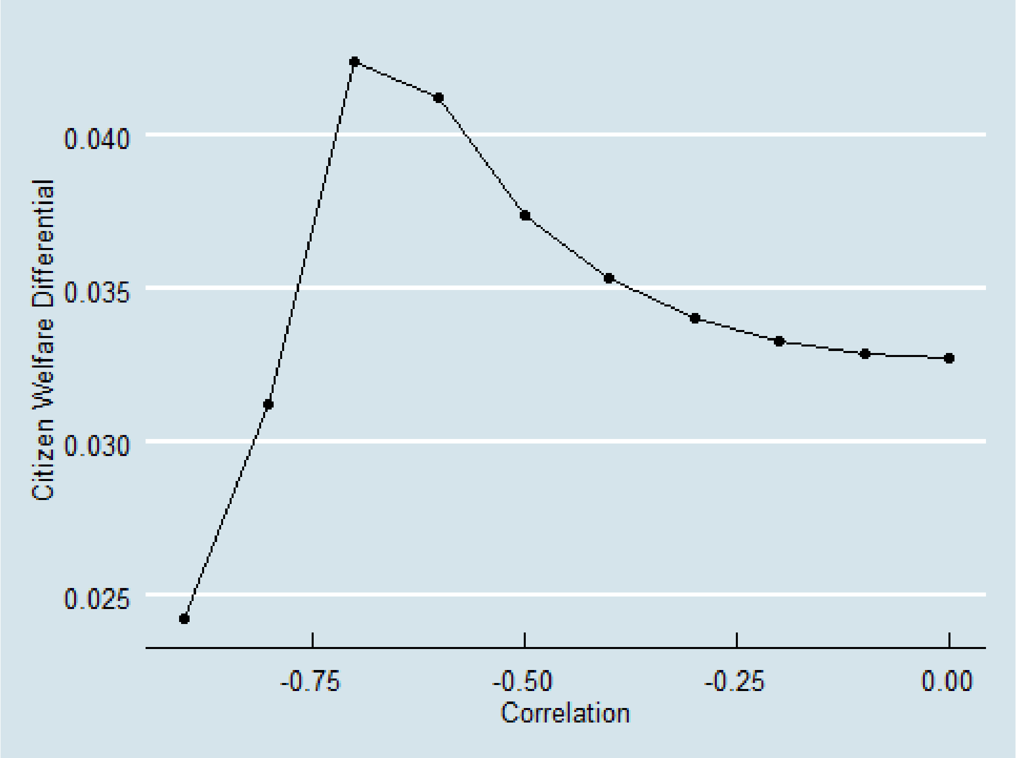

Figure 1: This figure depicts the difference between citizen utility under a permissive regulatory regime and citizen utility under a restrictive regulatory regime as $Corr(r_k, r_{dc})$ varies. Positive differences imply that citizens earn higher utility under a permissive regulatory regime.

Figure 1 establishes our first finding, that a private digital currency facilitates higher welfare for citizens. The welfare gains are especially pronounced for economies in which local investment correlates negatively with the private digital currency return. This finding arises because lower correlations facilitate more diversification which in turn induces higher citizen welfare. Nonetheless, irrespective of that correlation, the existence of the private digital

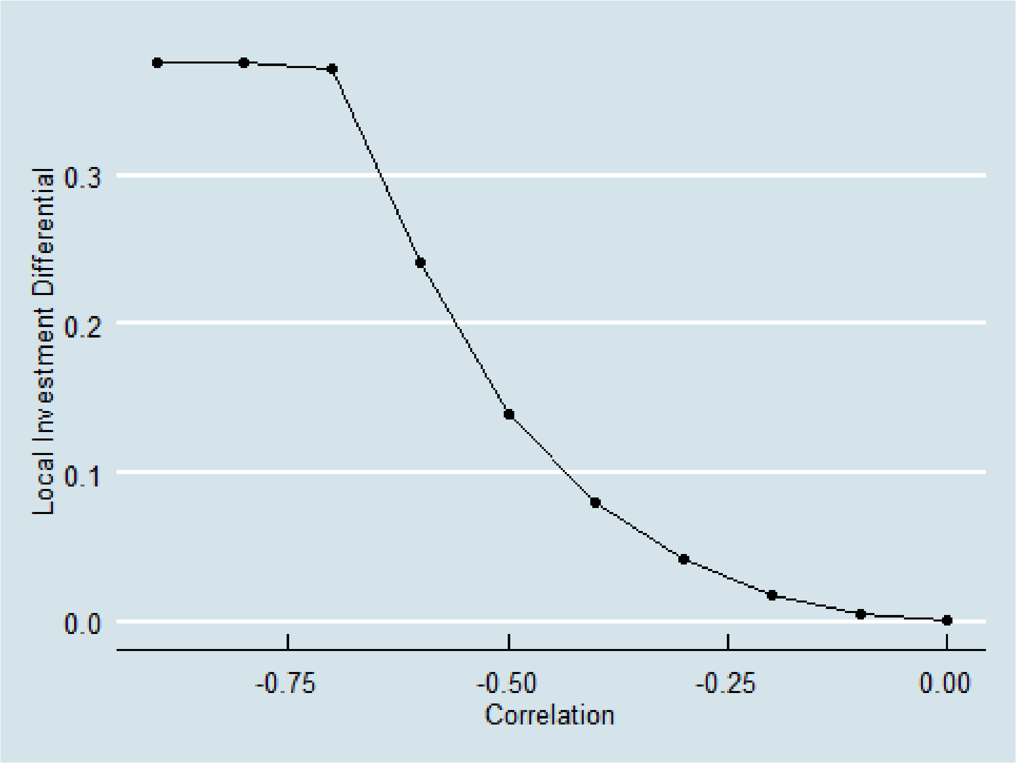

Figure 2: This figure depicts the difference between local investment under a permissive regulatory regime and that under a restrictive regulatory regime as $Corr(r_k, r_{dc})$ varies. Positive differences imply that citizens earn higher investment levels under a permissive regulatory regime.

currency imposes discipline upon monetary policy and thereby generates welfare gains for citizens.

Figure 2 establishes our second finding, that a private digital currency increases local investment within an emerging market economy. This finding arises because the private digital currency serves as a hedge asset (see, for example, Dyhrberg (2016) and Yu and Zhang (2018)) and therefore complements investment in the local economy. The increased investment effects are more pronounced when local investment returns correlate negatively with the private digital currency return.

Figure 3 highlights that governments generally benefit from a permissive regulatory policy. That benefit is especially large when correlation between local investment returns and the private digital currency return is negative in sign and large in absolute magnitude. The

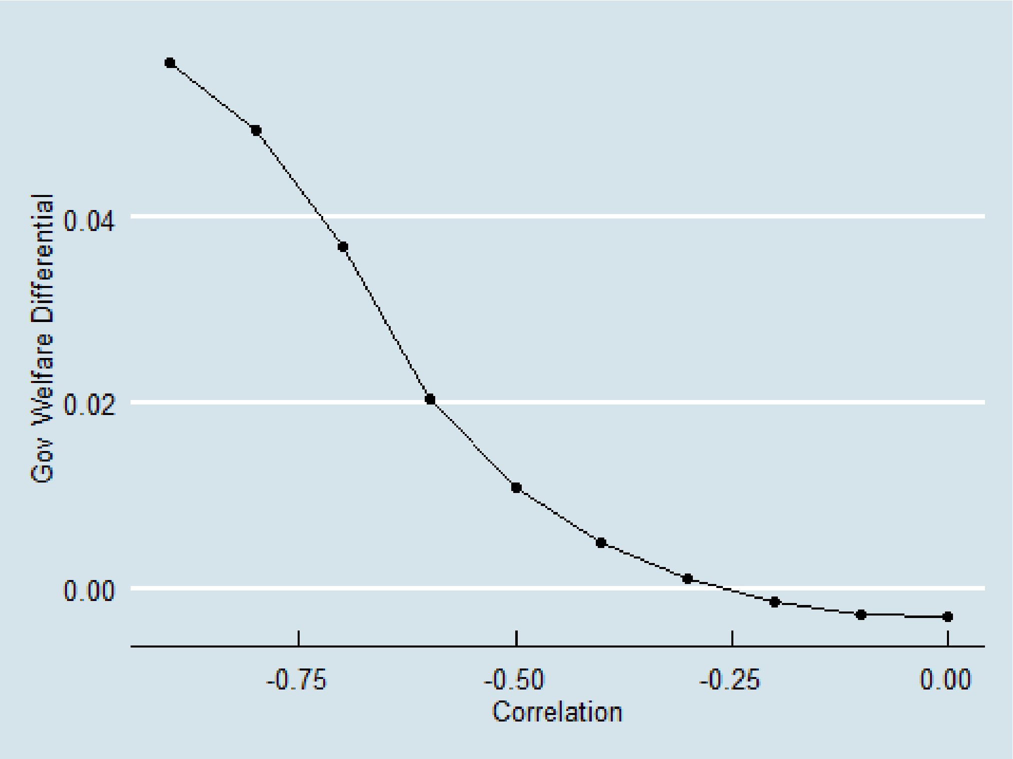

Figure 3: This figure depicts the difference between government revenues under a permissive regulatory regime and that under a restrictive regulatory regime as $Corr(r_k, r_{dc})$ varies. Positive differences imply that citizens earn higher government revenues under a permissive regulatory regime.

increased citizen welfare from permitting digital currencies enables the government to raise tax rates, which in turn increases government revenue. Thus, the government gains from permitting digital currencies by extracting some of the citizen welfare gains.

Our results highlight that a corrupt emerging market government generally finds permitting private digital currencies optimal. This result is particularly important because it implies that private digital currencies increase welfare in equilibrium within an emerging market setting despite selfish incentives of a corrupt government. In equilibrium, the government permits trading of private digital currencies. That permissive policy raises both citizen welfare and government welfare. As we have shown, the former arises through diversification gains and a credible commitment to restrained monetary policy, whereas the latter arises because the government exploits such gains to impose higher taxation.

4 Conclusion

This paper establishes a typology for digital currencies classified along the two axes of state-sponsorship and centralization. We conclude that private decentralized digital currencies are a novel invention with important welfare implications for emerging markets. We demonstrate that the existence of private digital currencies disciplines government policy, thereby generating welfare gains. Our work highlights that private digital currencies should not be analyzed as a replacement for traditional money but rather as an important alternative asset.

Whether private decentralized digital currencies will continue to proliferate is beyond the scope of this paper. The history of money, however, suggests that there will always be a demand for a non-state currency that serves as a check on the inflationary monetary tendencies of the sovereign. Should that demand persist, it is likely that some private decentralized digital currency will continue to exist. Our paper demonstrates that an alternative such as bitcoin is to be welcome both from the perspective of the individual and the government as it increases the total welfare of the nation.

References

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta (2019): "The Blockchain Folk Theorem," *Review of Financial Studies*, 32(5), 1662–1715.

Biais, B., C. Bisière, M. Bouvard, C. Casamatta, and A. J. Menkveld (2018): "Equilibrium Bitcoin Pricing," *Working Paper.*

Cagan, P. (1956): "The Monetary Dynamics of Hyperinflation," pp. 25–117. University of Chicago Press.

Chod, J., and E. Lyandres (2018): "A Theory of ICOs: Diversification, Agency, and Information Asymmetry," *Working Paper.*

Cong, L. W., and Z. He (2019): "Blockchain Disruption and Smart Contracts," *Review of Financial Studies*, 32(5), 1754–1797.

Cong, L. W., Y. Li, and N. Wang (2018): "Tokenomics: Dynamic Adoption and Valuation," *Working Paper.*

Dyhrberg, A. (2016): "Hedging Capabilities of Bitcoin. Is it the virtual gold?," *Finance Research Letters*, 16, 139 – 144.

Easley, D., M. O'Hara, and S. Basu (2019): "From Mining to Markets: The Evolution of Bitcoin Transaction Fees," *Journal of Financial Economics*, Forthcoming.

Foley, S., J. R. Karlsen, and T. J. Putnins (2019): "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?," *Review of Financial Studies*, 32(5), 1798–1853.

Griffin, J. M., and A. Shams (2018): "Is Bitcoin Really Un-Tethered?," *Working Paper.*

Harvey, C. (2016): "Cryptofinance," *Working Paper.*

Henderson, M. T., and M. Raskin (2019): "A Regulatory Classification of Digital Assets: Toward an Operational Howey Test for Cryptocurrencies, ICOs, and Other Digital Assets," *Columbia Law School Review*, 44.

Hinman, W. (2018): "Remarks at the Yahoo Finance All Markets Summit: Crypto," Remarks by SEC Director, Division of Corporation Finance. Available at https://perma.cc/W7N4-RN8N.

Hinzen, F. J., K. John, and F. Saleh (2019): "Bitcoin's Fatal Flaw: The Limited Adoption Problem," *NYU Stern Working Paper*.

Howell, S. T., M. Niessner, and D. Yermack (2019): "Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales," *NBER Working Paper*.

Huberman, G., J. D. Leshno, and C. Moallemi (2019): "An Economic Analysis of the Bitcoin Payment System," *Working Paper*.

Li, J., and W. Mann (2018): "Initial Coin Offerings and Platform Building," *Working Paper*.

Li, T., D. Shin, and B. Wang (2019): "Cryptocurrency Pump-and-Dump Schemes," *Working Paper*.

Makarov, I., and A. Schoar (2019): "Trading and Arbitrage in Cryptocurrency Markets," *Journal of Financial Economics*, Forthcoming.

Raskin, M., and D. Yermack (2016): "Digital Currencies, Decentralized Ledgers, and the Future of Central Banking," .

Saleh, F. (2019a): "Blockchain Without Waste: Proof-of-Stake," *Working Paper*.

——— (2019b): "Volatility and Welfare in a Crypto Economy," *Working Paper*.

Selgin, G. (1996): "Salvaging Gresham's Law: The Good, the Bad, and the Illegal," *Journal of Money, Credit and Banking*, 28(4), 637–649.

YERMACK, D. (2015): "Is Bitcoin a Real Currency? An economic appraisal," *Handbook of Digital Currency*, pp. 31–43.

——— (2017): "Corporate Governance and Blockchains," *Review of Finance*, 21, 7–31.

YU, G., AND J. ZHANG (2018): "Flight to Bitcoin," *Working Paper*.