Economic Inquiry

THE POLITICAL ECONOMY OF BITCOIN

JOSHUA R. HENDRICKSON, THOMAS L. HOGAN and WILLIAM J. LUTHER*

The recent proliferation of bitcoin has been a boon for users but might pose problems for governments. Indeed, some governments have already taken steps to ban or discourage the use of bitcoin. In a model with endogenous matching and random consumption preferences, we find multiple monetary equilibria including one in which bitcoin coexists with official currency. We then identify the conditions under which government transactions policy might deter the use of bitcoin. We show that such a policy becomes more difficult if some users strictly prefer bitcoin because they can avoid other users holding the official currency in the matching process. (*JEL* C78, E41, E42, E50)

I. INTRODUCTION

On October 14, 2013, Baidu, a web services company that runs the largest search engine in China, began accepting bitcoin. This single action opened the bitcoin network to roughly 570 million internet users in China and prompted other internet companies to consider the cryptocurrency more seriously. The closing price of bitcoin, which averaged just $124 over the 2-week period prior to the announcement, increased to $170 over the 2-week period following the announcement.[1] As the demand for bitcoin increased, the authorities took notice. The People's Bank of China issued a statement on December 5, 2013 prohibiting financial institutions and payment companies from buying, selling, quoting prices in, or insuring products linked to bitcoin. Baidu stopped accepting bitcoin the very next day.

China is not the only user; although the network of bitcoin users is relatively small at present and economists are, for the most part, skeptical that bitcoin will ever gain widespread acceptance, the rapid growth of the bitcoin network has prompted some governments to ban or discourage the use of bitcoin.[2] Government officials seem to worry that bitcoin, which offers a secure and quasi-anonymous way to make digital payments, will be used for illicit transactions and will impede the administration of monetary policy or raising revenues. In some important respects, the legal issues surrounding bitcoin echo older debates. "The idea that governments issue 'money' and declare what qualifies as 'legal tender' is an ancient notion," Middlebrook and Hughes (2014, 848) explain. "The history of regulating money and legal tender suggests that it is not likely that governments will surrender their privileges to regulate cryptocurrency issuers, exchanges, administrators, or users."

Can a government successfully prevent bitcoin transactions? In what follows, we consider

*The authors would like to thank our anonymous reviewers and the session participants at the Association of Private Enterprise Education annual conference for helpful comments and suggestions. Thomas Hogan is currently a committee staff member in the U.S. Senate. The views presented here are those of the authors alone and do not reflect the views of any individual Senator or committee.

Hendrickson: Department of Economics, University of Mississippi, University, MS 38677. Phone 662-915-7579, Fax 662-915-6943, E-mail jrhendr1@olemiss.edu

Hogan: Johnson Center for Political Economy, Troy University, Troy, AL 36082. Phone 334-808-6582, Fax 334-670-3708, E-mail tlhogan@troy.edu

Luther: Department of Economics, Kenyon College, Gambier, OH 43022. Phone 703-662-1349, E-mail lutherw@kenyon.edu

1. Closing prices used in these calculations come from the Bitstamp exchange, as reported at http://www.bitcoincharts.com/.

2. Luther (Forthcoming, b) explains why bitcoin is unlikely to be adopted in the absence of significant monetary instability or government support. See also Luther and White (2014) and Luther (Forthcoming, a).

ABBREVIATIONS

CFTC: Commodities Futures Trading Commission
FinCEN: Financial Crimes Enforcement Network
IRS: Internal Revenue Service
OIEA: Office of Investor Education and Advocacy
SEC: Securities and Exchange Commission
USMS: U.S. Marshall Service
VAT: Value Added Taxes

Economic Inquiry
(ISSN 0095-2583)
Vol. 54, No. 2, April 2016, 925–939

doi:10.1111/ecin.12291
Online Early publication November 2, 2015

whether government transactions policy would eliminate the use of bitcoin or simply relegate its use to areas effectively beyond the reach of government (e.g., black markets, small-value exchange, etc.). Using a monetary model with endogenous search and random consumption preferences developed by Hogan and Luther (2014), we articulate the conditions under which a government-issued currency and bitcoin might coexist, as well as the conditions under which one or neither of the different forms of money circulate. Then, we impose a government transactions policy whereby those agents controlled by the government refuse to accept bitcoin as payment and examine the effects of this policy on the circulation of bitcoin.

The model employed herein combines insights from Kiyotaki and Wright (1993), in which agents are matched randomly for trade, and Corbae et al. (2003), in which agents deliberately choose with whom to trade. Agents in the model deliberately choose with whom to trade, but are then subject to random consumption preferences. One way to think of this assumption is that agents who wish to consume arrive at a place where they would like to make a purchase, but might decide not to buy anything. Although the decision to buy is random, the choice of where to shop is not.[3] Allowing agents to choose their trading partners means that some transactions might exist beyond the reach of government.

The use of a government transactions policy follows from Aiyagari and Wallace (1997) and Li and Wright (1998). Others have used government transactions policies to consider the implications of competing money assets. However, our analysis differs from previous works in important ways. For example, Lotz and Rocheteau (2002) consider whether a government transactions policy can support the launch of a new currency. They use a random matching model and only consider a transactions policy that compels agents to hold government-issued money. Similarly, Waller and Curtis (2003) consider the use of government transactions policy in the context of competing international currencies. They also limit considerations to the random matching model.

We maintain that the matching mechanism is important when considering monetary competition and control. In an endogenous matching environment, where an agent's type and money holdings are observable, a producing agent might seek to avoid someone holding a particular type of money that the agent does not wish to accept. In a random matching environment, by contrast, agents will occasionally be matched with such partners. As a result, they might accept a particular type of money that they would prefer not to if the surplus from trade is non-negative.[4] Such features seem especially relevant in the context of bitcoin, which some users employ to make illicit transactions. If an agent who prefers to transact with bitcoin can avoid those holding the official currency favored by government, some transactions are effectively (though only probabilistically) beyond the reach of the state.[5] Such scenarios cannot be studied in traditional random matching models or in simple endogenous matching models, but only in models that employ endogenous matching where consumers can have preferences for particular goods.

In general, we find that the government's refusal to accept bitcoin is not, in and of itself, sufficient to prevent bitcoin transactions in equilibrium. To eliminate all bitcoin transactions, the government must control a sufficient size of the economy. This size is a function of preferences, the cost of production, and exogenous variables in the model. The size threshold is also dependent on the fraction of agents who are willing to accept the official currency. If every agent is willing to accept the official currency, then the size threshold for the government is lower and it is easier to prevent the circulation of bitcoin. On the other hand, if there are agents who strictly prefer bitcoin, a refusal to accept the official currency on the part of these agents would make it more difficult, in some cases impossible, for the government to prevent the circulation of bitcoin. We conclude by exploring the country characteristics that might make bitcoin more likely to succeed or more resistant to government

3. This framework is similar to the partially directed search model of Goldberg (2007), who assumes that agents know what good they want, but that the particular trading partner is random.

4. This point is similar to that made by Corbae et al. (2002) regarding the importance of inside versus outside money. In short, Calvacanti and Wallace (1999) argue that inside money yields superior allocations to outside money. However, this advantage is due to the existence of random matching. If someone capable of issuing inside money is randomly matched with a producer, trade is possible even though neither of them is holding outside money. With endogenous matching, however, these two individuals would never meet.

5. Of course, this presupposes some bitcoin is held by private agents. If the government were to acquire all the available bitcoin, one could no longer choose to match with someone holding bitcoin and execute a transaction that the government does not approve.

intervention and by discussing potential areas for future research.

II. BITCOIN AND THE GOVERNMENT

Bitcoin is a digital currency that provides a secure, low-cost platform for electronic payments. Developed by Nakamoto (2008), the bitcoin network was launched in 2009 and has grown considerably in recent years.[6] The rapid growth of the bitcoin network, combined with some of the unique features of the currency, has prompted governments to take notice. Some governments have even taken steps to prohibit its citizens from transacting with bitcoin. In this section, we provide a brief primer on bitcoin and consider government responses to its use.

The bitcoin protocol processes transactions over a distributed network using public–private key technology. When a sender transfers funds to a recipient using the bitcoin client, a transaction request is generated. The sender confirms access to the funds being sent with his private key and identifies the recipient by her public key. Once a transaction request is signed with a sender's private key, anyone on the network can use the sender's public key to verify that the legitimate account holder approved the request.

The transaction request is bundled into a block with other transactions being made. All users running the bitcoin client effectively compete to process the transactions block. This involves solving a complicated cryptography problem, which basically amounts to a brute force search for an essentially random string of characters. The solution to the cryptography problem certifies that the transaction block being processed is consistent with the existing blockchain, a public record of all past transactions.[7] Once a user on the network successfully hashes the block and six other users verify the solution, the blockchain is modified to reflect the transactions referenced in the processed block. The recipient can now use her private key to generate a new transactions request, transferring the recently received funds to someone else. Processing transactions in this manner ensures that a user does not spend the same balance twice without relying on a central clearinghouse authority.

Users running the bitcoin client are rewarded whenever they are the first to successfully process a block of transactions. The reward comes in the form of newly created bitcoin, known as the coinbase. The bitcoin protocol varies the difficulty of processing the block of transactions to ensure that, on average, one block is processed every 10 minutes. The number of coins in the coinbase is cut in half every 210,000 blocks (or, roughly, 4 years). As such, the total supply of bitcoin in circulation grows at a predictable rate, asymptotically approaching 21 million.[8] The last bitcoin is scheduled to enter circulation in September 2140.[9]

Bitcoin has several features that, while offering advantages to users over traditional currencies, also provide grounds for government action to discourage or prevent bitcoin use.[10] In general, justifications for government action come in two forms: bitcoin (1) enables private agents to complete illegal transactions, which a government has already committed to prohibit or (2) precludes a government from accomplishing tasks assigned to it, such as conducting monetary policy or raising revenues. We identify several of these features below.

The bitcoin system operates largely outside traditional financial institutions and without regard to national borders. As such, many users have been able to circumvent the existing regulatory framework. When transacting with bitcoin, there are no disclosures, no reporting, and no inquiries on large transactions. Regardless of origin, there is no distinction between sending funds to Arkansas or Afghanistan.

Furthermore, users on the system are identifiable only by their virtual addresses. Some intermediaries, like Coinbase, require users link their bitcoin address to a traditional bank account. However, it is possible to use bitcoin without creating an account with such intermediaries. As such, users can acquire bitcoin and transact without even identifying themselves in the physical world. For this reason, we say that bitcoin

6. White (2015) compares the market capitalization of bitcoin to supplies of state fiat currencies. With a market capitalization of $5.4 billion, bitcoin is on par with national currencies like the Bahamas dollar ($6.2b), Botswana pula ($5.7b), Ugandan shilling, ($5.3b), and Moldovan leu ($4.5b).

7. Luther and Olson (2015) maintain that bitcoin can be classified as "memory" since "bitcoin functions as a public record-keeping device" (p. 1).

8. Network computers may also charge fees for transaction processing. This practice is currently used as an optional premium to expedite transactions. As growth in the quantity of bitcoins declines, however, it is likely that fee-based transactions will become an important source of revenue for transaction processing on the bitcoin network.

9. Hendrickson and Luther (2014) consider the value of bitcoin in the period after the supply is fixed.

10. Luther (2015) considers popular justifications for regulating bitcoin.

enables pseudonymous exchange. Bitcoins are processed over a distributed network, so there is no central entity in the system. A user's relative importance is determined by the amount of computing power she is providing to the system and no single user is essential to the process.

The lack of regulation can be viewed in two very different lights. On the one hand, it means the bitcoin network has not been held back by regulations enacted prior to the spread of e-commerce. Even if such regulations were well intended when enacted, it is reasonable to expect at least some are inappropriate given the current state of technology. From this perspective, bitcoin provides a useful workaround in an antiquated legal environment. At the same time, one must recognize that at least some of the laws in place reflect the desire to monitor or prevent a given set of transactions. Traditional financial accounts can be frozen if parties to a transaction are engaged in illegal activities. Payments on traditional networks can be reversed. Traditional account holders are easy to identify in the physical world. With bitcoin, in contrast, accounts cannot be frozen, transactions cannot be reversed, and account holders might not be easy to identify.

The features outlined above make bitcoin especially useful for conducting illegal transactions. For example, there are roughly 50 known gambling sites in operation that accept payments and make payouts in bitcoin. These sites host a diverse set of games. The most popular, SatoshiDice, allows users to send a bet to a unique address that corresponds to a number from 1 to 64,000. The system then generates a lucky number by hashing a combination of the transaction ID and a secret string that is changed daily.[11] If the number of the address where the bet was sent is lower than the lucky number, the user wins the respective payout. In total, players bet ฿1,787,470 in 2012 (Matonis 2013).[12] Another site, bitZino, offers blackjack, video poker, roulette, and craps. It serviced ฿664,192 in bets in 2012. Still others, like BetMoose, offer peer-to-peer social betting where users can create bets on anything. Users can also run their own books on the site, taking a cut from the total bet pot they generate. Since these sites accept payments and make payouts in bitcoin, it is difficult to prevent those users in jurisdictions where gambling is illegal from participating. Also, once they participate, it is difficult to identify them and mete out the requisite punishment.

TABLE 1

Top 20 Categories of Goods for Sale, the Number of Items Offered, and the Percentage of Total Goods Offered on the Silk Road from February 3, 2012 through July 24, 2012

Category	Number of Items Listed	Percentage of Total Items Listed
Weed	3,338	13.70
Drugs	2,194	9.00
Prescription	1,784	7.30
Benzos	1,193	4.90
Books	955	3.90
Cannabis	877	3.60
Hash	820	3.40
Cocaine	630	2.60
Pills	473	1.90
Blotter (LSD)	440	1.80
Money	405	1.70
MDMA (ecstasy)	393	1.60
Erotica	385	1.60
Steroids, PEDs	376	1.50
Seeds	374	1.50
Heroin	370	1.50
DMT	343	1.40
Opioids	342	1.40
Stimulants	291	1.20
Digital goods	260	1.10

Source: Christin (2013). Reprinted with permission.

The illegal transactions facilitated by bitcoin are not limited to gambling. In February 2011, the pseudonymous Dread Pirate Roberts launched the Silk Road, an online marketplace where users could buy (and sell) illicit goods and services with (for) bitcoin.[13] Illicit transactions on the Silk Road mostly involved illegal drugs.[14] Table 1, reproduced from Christin (2013), shows the top 20 categories of goods for sale, the number of items offered, and the percent of total goods offered from February 3, 2012 through July 24, 2012. Tables 2 and 3, also reproduced from Christin (2013), present the most frequent countries from which items were advertised to be shipped over the period and the destinations

11. The secret string is made public once replaced so that users can verify that hashes are legitimate.

12. We use the symbol ฿ to denote quantities of money denominated in bitcoin.

13. Since the Silk Road was operated as a Tor hidden service, users could browse it anonymously without fear that their traffic might be monitored by the authorities.

14. As Christin (2013, 214) reports, the Silk Road sellers' guide advised against selling "anything who's (sic) purpose is to harm or defraud, such as stolen items or info, stolen credit cards, counterfeit currency, personal info, assassinations, and weapons of any kind." Users were also instructed "not to list anything related to pedophilia." Weapons and ammunition sales were permitted from the site's founding until March 4, 2012, when they were transferred to The Armory, a sister site. Due to a lack of business, the latter closed in August 2012.

TABLE 2
Advertised Shipping Origin of Goods Listed on the Silk Road from February 3, 2012 through July 24, 2012

Advertised Shipping Origin	Percentage of Listings
United States	43.83
Undeclared	16.29
United Kingdom	10.15
Netherlands	6.52
Canada	5.89
Germany	4.51
Australia	3.19
India	1.23
Italy	1.03
China	0.98
Spain	0.94
France	0.82

Source: Christin (2013). Reprinted with permission.

TABLE 3
Acceptable Shipping Destinations for Goods Listed on the Silk Road from February 3, 2012 through July 24, 2012

Acceptable Shipping Destination	Percentage of Listings
Worldwide	49.67
United States	35.15
European Union	6.19
Canada	6.05
United Kingdom	3.66
Australia	2.87
Worldwide, except United States	1.39
Germany	1.03
Norway	0.70
Switzerland	0.62
New Zealand	0.56
Undeclared	0.26

Source: Christin (2013). Reprinted with permission.

sellers were willing to ship to.[15] Christin (2013) estimates sales on the Silk Road totaled over $1.22 million per month.

In October 2013, the FBI capture of Ross William Ulbricht, alleged to be the Dread Pirate Roberts, at the Glen Park Branch Library in San Francisco resulted in the shutdown of the Silk Road. Roughly ฿144,000, worth around $15.1 million at the time, were seized in the process.[16] However, this accomplished little in terms of thwarting the illegal transactions. By November 2013, the Silk Road 2.0 had sprung up.[17] It, too, would be shut down in November 2014, when Blake Benthall, alleged to be the site's pseudonymous leader Defcon, was arrested. Within hours of its shutdown, Silk Road 3.0 had launched.[18] At present, illicit transactions are also being made with bitcoin via Agora Marketplace.

In addition to drugs and gambling, some have speculated that bitcoin might provide an effective vehicle for funding terrorists. Several startups, like Coincove, have attempted to break into the remittances market by providing on-the-ground exchanges in developing countries, where users can withdraw the local-currency equivalent of bitcoin sent from abroad. To the extent that such services do not comply with know-your-customer laws, they enable users to transfer funds across borders without the scrutiny imposed by traditional remittance companies.[19] As such, funds might be sent with the intent to fund organizations whose interests are to undermine the safety and security of others.

As discussed above, bitcoin enables private agents to complete illegal transactions. It might also preclude a government from accomplishing its monetary policy goals or raising revenues. Recall that an algorithm regulates the supply of bitcoin in circulation. As such, the supply grows steadily, with the rate declining over time. Moreover, this algorithm is built into the bitcoin protocol. It cannot be modified by a central monetary authority—government backed or otherwise—without the consent of a majority of users on the system.[20]

15. Percentages do not sum to 100 in the latter because some sellers were willing to ship to multiple destinations.

16. Ulbricht pleaded not guilty to seven charges of narcotics trafficking, criminal enterprise, computer hacking, and money laundering. In July 2014, the U.S. Marshall Service (USMS) auctioned ฿30,000 seized from the Silk Road. Although the actual bid value was not released, market exchange rates on the day of the sale put the value at around $17.4 million. The USMS is scheduled to auction another ฿50,000 in November 2014. In February 2015, Ulbricht was convicted of all seven charges. He was sentenced to life in prison in May 2015.

17. Since encrypted copies of the site's source code have been distributed, a new site can be recreated rather quickly following a shutdown.

18. Silk Road 3.0 resulted from the strategic name change of Diabolus Market, a cannabis-only marketplace that had launched less than a month earlier. It no longer bills itself as cannabis-only.

19. In fact, Coincove initially attempted to enter the remittances market through existing legal channels. The expenses involved in satisfying the licensing and regulatory requirements proved too much, however. They have since scaled back their business plan to focus exclusively on facilitating bitcoin transactions in Mexico.

20. Such a change would require modifying the bitcoin protocol. Users would confirm the modification by downloading and using the new protocol.

To the extent that individuals replace their holdings of official currency with bitcoin, the relevant monetary authority loses control of the total money supply (i.e., official currency plus bitcoin and any other alternatives employed). This is a relatively minor concern at present because the network of bitcoin users is small and dispersed across the world. Consider the extent to which the Federal Reserve has lost control of the money supply from the introduction of bitcoin. The market capitalization of bitcoin is around $5.4 billion (White 2015), which is roughly 0.14% of the dollar plus bitcoin monetary base. Hence, even if all users were replacing dollar holdings with bitcoin (and they are not), it would have little effect on the Fed's ability to engage in monetary policy at present. Nonetheless, it is a potential concern in the event that bitcoin use continues to increase.

Much the same can be said about the effect of bitcoin on federal budgets. Governments earn seigniorage by holding interest-bearing assets purchased with non-interest-bearing notes. These revenues are relatively small, especially in high-income countries. For example, remittances from the Fed to the Treasury totaled just $79.6 billion in 2013, or 0.53% of current expenditures by the federal government. Moreover, as discussed above, the extent to which dollar holdings have been replaced by bitcoin is negligible at present. Nonetheless, an increase in the demand for bitcoin would reduce the government's ability to raise revenues from seigniorage. As such, bitcoin's effect on federal budgets could serve as a justification to discourage or prevent biticoin use.

We have shown that some of bitcoin's features make it especially useful for illegal transactions and, at least in the future, might preclude a government from conducting monetary policy or raising revenues. As such, there are grounds for government action. Actual government responses vary from outright acceptance to outright banning of bitcoin. Some governments have opted for a middle ground, attempting to regulate the bitcoin market; many, however, have left bitcoin in a legal grey area. We discuss examples of each below.

BitLegal tracks the legal status of virtual currencies like bitcoin around the world. It denotes the legal environment in each nation as "Permissive," "Contentious," or "Hostile." The legality of bitcoin, as assessed by BitLegal (2014), is presented for 63 nations in Table 4. Since the legal status is subject to change in many countries, we include the date that the status was last updated for each country. Fifty-four nations are deemed permissive. The legal status is contentious in

TABLE 4
The Legal Status of Bitcoin, by Nation

Nation	Status	Updated
Argentina	Permissive	January 30, 2014
Australia	Permissive	March 24, 2014
Austria	Permissive	March 6, 2014
Belarus	Permissive	January 30, 2014
Belgium	Permissive	January 21, 2014
Brazil	Permissive	April 8, 2014
Bulgaria	Permissive	April 8, 2014
Canada	Permissive	February 1, 2014
China	Contentious	March 23, 2014
Colombia	Permissive	March 26, 2014
Croatia	Permissive	February 3, 2014
Cyprus	Permissive	February 3, 2014
Czech Republic	Permissive	January 26, 2014
Denmark	Permissive	March 23, 2014
Estonia	Permissive	February 3, 2014
Finland	Permissive	January 20, 2014
France	Permissive	January 29, 2014
Germany	Permissive	February 23, 2014
Greece	Permissive	February 13, 2014
Greenland	Permissive	January 12, 2014
Hong Kong	Permissive	January 24, 2014
Hungary	Permissive	February 19, 2014
Iceland	Hostile	January 26, 2014
India	Contentious	January 23, 2014
Indonesia	Permissive	February 6, 2014
Iran	Permissive	March 11, 2014
Ireland	Permissive	January 6, 2014
Israel	Permissive	February 19, 2014
Italy	Permissive	February 4, 2014
Japan	Permissive	March 23, 2014
Jersey	Permissive	April 24, 2014
Jordan	Contentious	February 23, 2014
Kazakhstan	Contentious	February 4, 2014
Latvia	Permissive	February 7, 2014
Lebanon	Permissive	January 26, 2014
Lithuania	Permissive	February 10, 2014
Luxembourg	Permissive	March 24, 2014
Malaysia	Permissive	February 1, 2014
Malta	Permissive	February 4, 2014
Mexico	Contentious	March 11, 2014
Netherlands	Permissive	January 1, 1970
New Zealand	Permissive	February 19, 2014
Norway	Permissive	January 20, 2014
Philippines	Permissive	March 11, 2014
Poland	Permissive	May 28, 2014
Portugal	Permissive	February 4, 2014
Russia	Contentious	February 6, 2014
Singapore	Permissive	March 24, 2014
Slovakia	Permissive	February 4, 2014
Slovenia	Permissive	February 20, 2014
South Africa	Permissive	February 20, 2014
South Korea	Permissive	February 1, 2014
Spain	Permissive	February 4, 2014
Sweden	Permissive	July 26, 2014
Switzerland	Permissive	February 1, 2014
Taiwan	Permissive	February 3, 2014
Thailand	Contentious	July 30, 2014
Trinidad and Tobago	Permissive	March 24, 2014
Turkey	Permissive	February 4, 2014
Ukraine	Permissive	November 12, 2014
United Kingdom	Permissive	March 24, 2014
United States	Permissive	March 23, 2014
Vietnam	Hostile	February 28, 2014

Source: BitLegal (2014). Reprinted with permission.

seven nations. Two nations are hostile toward bitcoin. The legal status of bitcoin in those nations not presented is unknown.

Of those nations considered permissive, some have explicitly accepted bitcoin use. In August 2013, the German Finance Ministry recognized bitcoin as "private money" similar to other financial instruments. In a statement released to the press, Finance Committee member Frank Schaeffler, who pushed for the legal classification of bitcoin in Germany, declared, "We should have competition in the production of money. I have long been a proponent of Friedrich August von Hayek's scheme to denationalize money. Bitcoins are a first step in this direction" (Clinch 2013). BitLegal (2014) reports that it is legal to buy, sell, transact with, and mine bitcoin in Germany. Germans are expected to pay value added taxes (VAT) on purchases made with bitcoin. They are not required to pay capital gains taxes on bitcoin mined or acquired via exchange, unless they hold the assets for less than a year.

The two nations with hostile legal environments toward bitcoin are Iceland and Vietnam. According to BitLegal (2014), Icelanders can legally own bitcoin. However, capital controls introduced in 2008 to prevent citizens from offloading the króna made buying of bitcoin illegal in Iceland. These rules do not prevent one from selling bitcoin for króna.

The legal situation in Iceland has been made murky with the introduction of Auroracoin, an altcoin modeled after bitcoin.[21] Auroracoin's founder, Baldur Friggjar Odinsson, hoped to generate acceptance for the novel cryptocurrency by distributing 31.8 Auroracoin to every resident in Iceland. Residency would be verified with Iceland's Islykill (Icekey) national registry. The government approved Odinsson's application to integrate Islykill in early 2014. As of November 2014, 3,615,963.4 of the 10,500,000 pre-mined Auroracoins have been claimed. Some hope the introduction of Auroracoin will prompt a re-evaluation of the legal status of cryptocurrencies in Iceland.

In Vietnam, financial institutions are prohibited from transacting with bitcoin. However, BitLegal (2014) maintains that it is legal to own bitcoin in Vietnam. It is unclear whether one can legally buy, sell, transact with, or mine bitcoin. As such, it is also unclear whether the Vietnamese are expected to pay taxes on bitcoin transactions, income from exchanges and mining, or capital gains from holding bitcoin.

Uncertainty over the legal status of bitcoin in Vietnam is not unique. China, India, Jordan, Kazakhstan, Mexico, Russia, and Thailand are listed as contentious. As noted in the Introduction, China restricts businesses from using bitcoin. However, it permits individuals to own and use Bitcoin at their own risk. Where to draw the line between businesses and individuals is not so clear. As in China, Jordan prohibits financial institutions from using bitcoin.

It is legal to own, buy, sell, transact with, and mine bitcoin in India. However, in December 2013, the Reserve Bank of India issued a statement warning the public about the potential financial, operational, legal, customer protection, and security risks of bitcoin. It also made clear that it was examining the legal status of bitcoin under existing law, including Foreign Exchange and Payment Systems laws and regulations. Two days later, Indian Rupee to Bitcoin, the primary bitcoin trading platform in India, suspended operations. The Reserve Bank of India has not clarified the legal status of bitcoin in the time since. The Bank of Thailand offered a similar warning in March 2014. As in India, it did not go so far as to state it is illegal to own, buy, sell, transact with, or mine bitcoin in Thailand.

The governments of Kazakhstan, Mexico, and Russia have yet to issue official statements on the legal status of bitcoin. In a February 2014 press conference, Central Bank Governor Kairat Kelimbetov suggested that the National Bank of Kazakhstan could move to classify bitcoin as a ponzi scheme. However, no action has been taken to date. In Mexico, it is currently legal to own, buy, sell, transact with, and mine bitcoin. However, BitLegal (2014) reports that institutions might be required to register with the Central Bank. The legal prospects of bitcoin look bleakest in Russia, where it is apparently illegal to own, buy, sell, and transact with bitcoin.[22] A draft bill released by the Ministry of Finance of the Russian Federation would impose fines on users, miners, and service providers. Regardless of the outcome, ambiguity over the legal status of bitcoin in these countries is not good for the cryptocurrency. As Grinberg (2011, 182) notes, "That it may exist in a legal grey area may significantly hamper demand for bitcoins."

Even where it is legal, excessive regulation might dissuade users from adopting bitcoin.

21. Techincally, Auroracoin is based on the litecoin protocol. However, litecoin was modeled after bitcoin.

22. BitLegal (2014) states that it is unclear whether mining is prohibited.

Consider the regulatory environment of the United States. The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) ruled in 2013 that, although a user of virtual currency cannot be regulated, an administrator or exchanger of such currency may be regulated as money services businesses subject to the money laundering provisions of the Banking Secrecy Act.[23] The Commodities Futures Trading Commission (CFTC) has also declared itself a legal regulator of bitcoin. Commissioner Bart Chilton stated that the CFTC "could regulate it if we wanted. That is very clear," because some users purchase bitcoin for investment purposes (Miedema 2013). Although the U.S. Securities and Exchange Commission (SEC) has declared no official rules for bitcoin, the Office of Investor Education and Advocacy (OIEA) has warned investors about scams and ponzi schemes regarding virtual currencies (OIEA 2013). Finally, the Internal Revenue Service (IRS) has declared that bitcoin will be taxed as property rather than currency.[24] Some ambiguity remains regarding whether changes in the value of bitcoin should be classified as an ordinary or capital gain.[25] With so many potential layers of regulation, some users might prefer to continue using traditional payment vehicles.

State governments have also taken actions to regulate the usage of bitcoin. The New York Department of Financial Services has issued a 40-page rule proposal (Tile 23, Ch.I, Part 200) to license and regulate the use of virtual currencies such as bitcoin, a move which many fear will set the tone for regulation in other states. "Companies who are looking to become compliant in all 50 of the US States will eventually have to deal with separate regulations in each state" (Madore). There is still much uncertainty regarding the evolution of regulations at the state and national levels.

Concerns over bitcoin's ability to facilitate unlawful transactions and preclude governments from conducting monetary policy or raising revenues provide grounds for intervention. As discussed above, some governments have already taken steps to discourage or prohibit the use of bitcoin. Their actions presuppose that such efforts can have the desired effect. In what follows, we develop a model to consider whether government transactions policy can discourage private actors from using bitcoin. Our model differs from others found in the literature in that agents first choose a trading partner. Other models used to consider government transactions policy rely on random matching. The endogenous matching decision in our model is based, in part, on the type of goods other agents produce and the type of money, official currency or bitcoin, other agents holds. The endogenous matching protocol is especially relevant in the context of bitcoin, since an agent might prefer to transact with bitcoin in order to make purchases prohibited by the government.

III. THE MODEL

In the model considered herein, time is discrete and continues forever. There is a set of agents $A = [0, 1]$ that is divided into G types. The number of goods is equal to the number of types such that each type-i agent produces good i. Each type-i agent consumes a subset of goods. The number of goods consumed is the same for each type, but the subset of goods consumed varies by type. Specifically, we denote the number of goods each type consumes as $n < G$. Each individual consumes a subset of the good-types available. Goods are neither storable nor divisible. Consumption of any good in agent i's subset generates utility, U_t. The production cost for each agent is denoted as C_t. There are two intrinsically worthless objects, currency and bitcoin.[26] Unlike goods, currency and bitcoin are both storable. They are also indivisible.

There are two types of money in this framework, currency and bitcoin. Each individual is indexed by type, by currency balances $m \in \{0, 1\}$, and bitcoin balances $b \in \{0, 1\}$. At the beginning of time a fraction of agents, M, are endowed with currency and a fraction of agents, B, are endowed with bitcoin. The remaining agents, $1 - M - B$ have no initial endowment.[27] The total supply

23. Specifically, "a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter. In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency" (FinCEN 2013).

24. Despite some previous reports to the contrary, a recent notice from the IRS (2014, 2) confirms "For federal tax purposes, virtual currency is treated as property."

25. According to the IRS (2014, 3): "The character of the gain or loss generally depends on whether the virtual currency is a capital asset in the hands of the taxpayer."

26. In the context of the model, currency refers to some official fiat currency.

27. We assume here that $M + B < .5$, such that there is some fraction of agents who initially do not receive an endowment.

of currency is $M \in (0, 1)$ and the total supply of bitcoins is $B \in (0, 1)$. Again, both assets are indivisible. An agent's type and money balances are publicly observable. An agent's trading history is not observable and therefore all trades are anonymous.

Let s_t denotes the aggregate state of the economy at time t. At each point in time, for a given state of the economy, an economic agent decides who to match with and, once matched, whether or not to trade. It is assumed that an individual endowed with money must consume before producing. Given that neither goods nor either type of money is divisible, this implies that when two agents meet they can either barter in the case of a double coincidence of wants or they must exchange goods for money or money for goods.

The two stages of the trade process can be understood as follows. The first stage is the process by which two agents are matched pairwise. The matching process follows Corbae et al. (2003). At each date t the set of agents A can be partioned into two subsets of size 1 or 2 referred to as coalitions. The matching rule can then be defined as a function of the economy, $\theta(s_t)$.[28] A trading rule, $\tau(\theta_t, s_t)$, summarizes the trading decision given a partition, θ, and the state of the economy, s_t. An equilibrium can then be thought of as a trading rule and a matching function for a given state of the economy such that no economic agent has an incentive to deviate.

The second stage of the trade process involves the decision of whether or not to trade. It is in this regard that the present model differs from the directed matching framework of Corbae et al. (2003). Specifically, it is assumed that, once matched, each agent receives a preference shock such that they are willing to choose one of the n goods from which they derive utility. In other words, there are n types of shops that a given agent would choose to show up to trade. The probability that a given agent wants to consume at the shop is $\frac{1}{n} \equiv \rho$. If the agent wants to consume in the match, the agent with money can then offer whichever type of money they are holding, currency or bitcoin, in exchange for the good. Again, since both money and goods are indivisible, this implies an exchange of one unit of currency or bitcoin in exchange for one good. The agent that is not holding money then has a choice of whether to accept the particular type of money offered.

28. The matching function here differs from Corbae et al. in that they assume that the matching function is determined by the state of the economy and extrinsic uncertainty. The inclusion of the latter is to include the possibility of sunspot equilibria. We abstract from this in the present model.

A. *Monetary and Nonmonetary Equilibria*

We will confine our analysis to steady state equilibria. Given that there are two types of money, there are four possible equilibria to consider. The first equilibrium is a nonmonetary equilibrium. This occurs when agents who are not holding money are unwilling to accept both currency and bitcoin. The second equilibrium is one in which agents are willing to accept currency, but not bitcoin. The third equilibrium is one in which agents are willing to accept bitcoin, but not currency. Finally, the fourth equilibrium is one in which agents are willing to accept both currency and bitcoin. The conditions under which these equilibria hold are outlined more formally below.

It is important to determine in any pairwise meeting the probability that a monetary exchange takes place. Recall that agents with money must consume prior to producing. This implies that a monetary exchange will take place if one agent has currency or bitcoin and another agent does not have any type of money. One can think of the probability that monetary exchange takes place as the ratio of the probability of success to the probability of failure. For example, the fraction of agents holding currency is M. The fraction of agents who do not hold either of the money assets is $1 - M - B$. We denote the probability of an agent that is not holding money is matched with an agent that is holding currency as $a_{0,m}$. It follows that $a_{0,m} = \frac{M}{1-M-B}$. Correspondingly, the probability that an agent that is not holding money is able to conduct monetary trade with an agent holding bitcoin is $a_{0,b} = \frac{B}{1-M-B}$. The probability that an agent without money cannot engage in a monetary exchange is given as $1 - a_{0,m} - a_{0,b}$.

We can outline similar probabilities for those agents entering the match with either bitcoin or currency. We denote the probability of monetary exchange for an agent entering with currency or bitcoin as a_m and a_b, respectively. It follows that $a_m = min\left\{1, \frac{1-M-B}{M}\right\}$ and $a_b = min\left\{1, \frac{1-M-B}{B}\right\}$.

Consider a match in which monetary exchange is possible. It does not necessarily follow that a monetary exchange will take place. First, it must be true that the agent that is holding money wants to consume the good that their trading partner produces. Second, the agent that is not holding money must accept the type of money that their

trading partner offers in exchange for the good. Let π be the probability that a random agent in the economy accepts currency and θ be the probability that a random agent in the economy accepts bitcoin. In addition, let $\Pi(\pi)$ and $\Theta(\theta)$ be the best response of an agent without money as to whether they should accept currency and bitcoin, respectively.

Let V_0 denote the value function of an agent that is not holding money, V_m denote the value function of an agent holding currency, and V_b denote the value function of an agent holding bitcoin. These value functions can be written as

$$(1)\quad rV_0 = \left(1 - a_{0,m} - a_{0,b}\right)\rho^2 (U - C) + \max_{\Pi\in[0,1]} a_{0,m}\Pi(\pi)\,\rho\left(V_m - V_0 - C\right) + \max_{\Theta\in[0,1]} a_{0,b}\Theta(\theta)\,\rho\left(V_b - V_0 - C\right)$$

$$(2)\quad rV_m = a_m\pi\rho\left(U + V_0 - V_m\right) - \delta_m$$

$$(3)\quad rV_b = a_b\theta\rho\left(U + V_0 - V_b\right) - \delta_b$$

where r is the discount rate, δ_m is the storage cost of currency, and δ_b is the storage cost of bitcoin. Given the value functions, we can now provide the conditions for each of the four possible equilibria.

A Currency Equilibrium.

DEFINITION 1. *A currency equilibrium is an equilibrium in which currency, but not bitcoin, is accepted in exchange. A currency equilibrium exists if:*

1. $\pi = 1$ *or* $\pi = \hat{\pi}$ *where*

$$\hat{\pi} = \frac{\left(1 - a_{0,m} - a_{0,b}\right)\rho}{a_m} + \frac{rC + \delta_m}{a_m\rho(U - C)}$$

2. $\theta < \hat{\theta}$ *where*

$$\hat{\theta} = \begin{cases} \frac{(1-a_{0,m}-a_{0,b})\rho}{a_b} + \frac{rC+\delta_b}{a_b\rho(U-C)} + \frac{a_{0,m}(V_m-V_0-C)}{a_b(U-C)} & \text{if} \quad V_m - V_o - C > 0 \\ \frac{(1-a_{0,m}-a_{0,b})\rho}{a_b} + \frac{rC+\delta_b}{a_b\rho(U-C)} & \text{if} \quad V_m - V_o - C = 0 \end{cases}$$

Whether or not each asset is accepted in the course of exchange is determined by the best response of an agent without money when offered either bitcoin or currency. The best response Π is a function of the probability that a random agent accepts currency. The best response Θ is a function of the probability that a random agent accepts bitcoin. The present model is symmetric, which implies that $\Pi(\pi) = \pi$ and $\Theta(\theta) = \theta$. With regards to each asset, there are three possible outcomes to consider. Consider the case of currency. From the value functions above, the expected value of accepting currency for an agent that does not have money is $a_{0,m}\rho(V_m - V_0 - C)$. This expected value is positive if $(V_m - V_0 - C) > 0$, zero if $V_m - V_0 - C = 0$, and negative if $V_m - V_0 - C < 0$. If expected value of accepting currency is negative, no agent will ever accept currency. If the expected value of accepting currency is positive, then every agent will accept currency. If the expected value of accepting currency is zero, then agents are indifferent about accepting currency. Formally, the best response can be written as

$$\Pi = \begin{cases} 0 & \text{if} \quad V_m - V_0 - C < 0 \\ (0,1) & \text{if} \quad V_m - V_0 - C = 0 \\ 1 & \text{if} \quad V_m - V_0 - C > 0 \end{cases}$$

It is important to note, however, that there is a specific threshold probability, $\hat{\pi}$, at which currency will be held in equilibrium. One can solve for this threshold probability by setting $V_m - V_0 - C$ equals to zero and combining Equations (1) and (2).[29] This provides a unique solution, $\hat{\pi}$, such that there are three possible probabilities for accepting currency in equilibrium: $\pi = 0$, $\pi = \hat{\pi}$, and $\pi = 1$. If the fraction of random agents accepting currency is above this threshold, then everyone will accept currency in equilibrium. If the fraction of random agents accepting currency is below the threshold, then no one will accept currency in equilibrium. It follows that currency will be accepted in equilibrium whenever $\pi \geq \hat{\pi}$. This is shown as the first characteristic of a currency-only equilibrium above.

A similar threshold probability exists for the acceptance of bitcoin. This threshold probability can be solved for in the same way as that for currency, by setting $V_b - V_0 - C = 0$ and using Equations (1) and (3) to solve for $\hat{\theta}$. In a currency-only equilibrium, it must be true that the fraction of agents accepting bitcoins is below this threshold value. Note that the equilibrium

29. This solution is shown in detail in the Appendix.

fraction of agents accepting currency is important for determining the threshold probability of accepting bitcoin. In other words, holding everything else constant, the threshold probability for determining whether bitcoin is accepted in equilibrium is higher if all agents accept currency in equilibrium as opposed to the fraction, $\hat{\pi}$.

A Bitcoin Equilibrium.

DEFINITION 2. *A bitcoin equilibrium is an equilibrium in which bitcoin, but not currency, is accepted in exchange. A bitcoin equilibrium exists if:*

1. $\theta = 1$ *or* $\theta = \hat{\theta}$ *where*

$$\hat{\theta} = \frac{\left(1 - a_{0,m} - a_{0,b}\right)\rho}{a_b} + \frac{rC + \delta_b}{a_b \rho\,(U - C)}$$

2. $\pi < \hat{\pi}$ *where*

$$\hat{\pi} = \begin{cases} \frac{(1-a_{0,m}-a_{0,b})\rho}{a_m} + \frac{rC+\delta_m}{a_m\rho(U-C)} + \frac{a_{0,b}(V_b-V_0-C)}{a_m(U-C)} & \text{if} \quad V_b - V_o - C > 0 \\ \frac{(1-a_{0,m}-a_{0,b})\rho}{a_m} + \frac{rC+\delta_m}{a_m\rho(U-C)} & \text{if} \quad V_b - V_o - C = 0 \end{cases}$$

A bitcoin-only equilibrium is one in which the fraction of random agents willing to accept bitcoin is above the threshold probability, but the fraction of random agents willing to accept currency is below the corresponding threshold probability. Again, note that the threshold probability for currency is higher if every agent accepts bitcoin.

The Coexistence of Currency and Bitcoin.

DEFINITION 3. *A coexistence equilibrium is an equilibrium in which both currency and bitcoin are accepted in exchange. A coexistence equilibrium exists if:*

1. $\pi = 1$ *or* $\pi = \hat{\pi}$ *where*

$$\hat{\pi} = \begin{cases} \frac{(1-a_{0,m}-a_{0,b})\rho}{a_m} + \frac{rC+\delta_m}{a_m\rho(U-C)} + \frac{a_{0,b}(V_b-V_0-C)}{a_m(U-C)} & \text{if} \quad V_b - V_o - C > 0 \\ \frac{(1-a_{0,m}-a_{0,b})\rho}{a_m} + \frac{rC+\delta_m}{a_m\rho(U-C)} & \text{if} \quad V_b - V_o - C = 0 \end{cases}$$

2. $\theta = 1$ *or* $\theta = \hat{\theta}$ *where*

$$\hat{\theta} = \begin{cases} \frac{(1-a_{0,m}-a_{0,b})\rho}{a_b} + \frac{rC+\delta_b}{a_b\rho(U-C)} + \frac{a_{0,m}(V_m-V_0-C)}{a_b(U-C)} & \text{if} \quad V_m - V_o - C > 0 \\ \frac{(1-a_{0,m}-a_{0,b})\rho}{a_b} + \frac{rC+\delta_b}{a_b\rho(U-C)} & \text{if} \quad V_m - V_o - C = 0 \end{cases}$$

In the coexistence equilibrium, there is a sufficient fraction of agents willing to accept both bitcoin and currency.

A Nonmonetary Equilibrium.

DEFINITION 4. *A nonmonetary equilibrium is an equilibrium in which neither bitcoin nor currency is accepted in equilibrium. A nonmonetary equilibrium exists if:*

1. $\pi < \hat{\pi}$ *where*

$$\hat{\pi} = \frac{\left(1 - a_{0,m} - a_{0,b}\right)\rho}{a_m} + \frac{rC + \delta_m}{a_m \rho\,(U - C)}$$

2. $\theta < \hat{\theta}$ *where*

$$\hat{\theta} = \frac{\left(1 - a_{0,m} - a_{0,b}\right)\rho}{a_b} + \frac{rC + \delta_b}{a_b \rho\,(U - C)}$$

A nonmonetary equilibrium exists when both the fraction of random agents willing to accept currency and the fraction of random agents willing to accept bitcoin are each below their threshold probabilities.

IV. GOVERNMENT TRANSACTIONS POLICY

The preceding analysis outlined the conditions under which bitcoin and currency would be held in equilibrium. From the perspective of political economy, the equilibria in which bitcoin circulates and the potential for governments to prevent such equilibria are of particular interest.

In a typical competitive market, new goods displace old goods. This is the well-known

process of creative destruction. In the case of bitcoin, however, the new alternative medium of exchange does not exist in a competitive market, but rather is competing with a spectrum of government-controlled fiat monies. A government might have an incentive to prevent the acceptance of bitcoin, perhaps because the coexistence of currency and bitcoin places restrictions on monetary policy and potentially limits seigniorage or enables transactions that the government might wish to preclude.[30]

Can government effectively ban bitcoin as a medium of exchange if everyone were willing to accept it? To analyze this question, we proceed using the methodology of Aiyagari and Wallace (1997).[31] Specifically, we assume there is some fraction of agents that are government agents. Furthermore, it is assumed that these agents can be directed to enact particular policies on behalf of the government. Recall that each agent is indexed by type and holdings of currency and bitcoin. As a result, a private agent does not know that he is interacting with a government agent and therefore cannot avoid the government agents, as such, in the matching process. However, as an agent's type and money holdings are observable, a producing agent might avoid someone holding currency (or bitcoin) if they wish to transact exclusively in bitcoin (or currency).

To determine whether the government can successfully ensure an equilibrium without bitcoin, we consider the policy where government agents all agree to accept currency as payment, but refuse to accept bitcoin. We then ask whether the government can guarantee an equilibrium in which bitcoin does not circulate by using such a policy.

Let $\phi \in (0,1)$ be the fraction of government agents and $1-\phi$ the fraction of private agents. We denote θ_g as the probability that a random government agent will accept bitcoin and θ_p as the probability that a random private agent will accept bitcoin. It follows that the probability that a random agent of any type will accept bitcoin is a weighted average of these two probabilities, $\theta = \phi\theta_g + (1-\phi)\theta_p$. Suppose that private agents are all willing to accept bitcoin, but that government agents refuse to accept bitcoin. It is now possible to consider whether the government could prevent an equilibrium in which bitcoin is accepted through a transactions policy in which they refuse to accept bitcoin.

PROPOSITION 1. *If all private agents are willing to accept bitcoin ($\theta_p = 1$), but government agents never accept bitcoin ($\theta_g = 0$), then the government can successfully eliminate an equilibrium in which bitcoin circulates in equilibrium iff $\phi > \widehat{\phi}$, where*

$$\widehat{\phi} = \begin{cases} \frac{1-(1-a_{0,m}-a_{0,b})\rho}{a_b} - \frac{rC+\delta_b}{a_b\rho(U-C)} - \frac{a_{0,m}\rho(V_m-V_0-C)}{a_b\rho(U-C)} & \text{if } V_m - V_0 - C > 0 \\ \frac{1-(1-a_{0,m}-a_{0,b})\rho}{a_b} - \frac{rC+\delta_b}{a_b\rho(U-C)} & \text{if } V_m - V_0 - C \leq 0 \end{cases}$$

Proof. If $V_b - V_0 - C = 0$, combining Equations (1) and (3) yields a unique value of θ, denoted $\widehat{\theta}$. It follows that for any $\theta > \widehat{\theta}$, it must be true that $V_b - V_0 - C > 0$ and therefore in equilibrium $\theta = 1$. For any $\theta < \widehat{\theta}$, it must be true that in equilibrium $\theta = 0$. Thus, the condition for an equilibrium in which bitcoin is not accepted is $\theta < \widehat{\theta}$. To solve for $\widehat{\theta}$, note that $rV_b - rV_0 - rC = 0$. Substituting Equations (1) and (3) yields

$$\left[a_b\widehat{\theta}\rho - \left(1 - a_{0,m} - a_{0,b}\right)\rho^2\right](U-C) - a_{0,m}\Pi(\pi)\rho\left(V_m - V_0 - C\right) - \delta_b - rC = 0$$

where $\widehat{\theta}$ is the unique value that solves this expression. Solving for $\widehat{\theta}$ yields

$$\widehat{\theta} = \begin{cases} \frac{1-a_{0,m}-a_{0,b}}{a_b} + \frac{rC+\delta_b}{a_b\rho(U-C)} + \frac{a_{0,m}(V_m-V_0-C)}{a_b(U-C)} & \text{if } V_m - V_0 - C > 0 \\ \frac{1-a_{0,m}-a_{0,b}}{a_b} + \frac{rC+\delta_b}{a_b\rho(U-C)} & \text{if } V_m - V_0 - C \leq 0 \end{cases} \tag{4}$$

■

As shown above, in the presence of government agents, the probability a random agent accepts bitcoin is a weighted average of the

30. In the extreme case, the displacement of currency by bitcoin would eliminate any role for monetary policy and any source of seigniorage.

31. Salter and Luther (2014) offer a broader view of the roles government might play in determining the medium of exchange. See also, Selgin (1994, 817–21).

probabilities corresponding to government and private agents, $\theta = \phi\theta_g + (1-\phi)\theta_p$. If the government refuses to accept bitcoin, but private agents always accept bitcoin, this implies that $\theta = (1-\phi)$. Hence, there is an unique size of government, $\hat{\phi}$ that satisfies $\hat{\theta} = 1 - \hat{\phi}$. In addition, the condition under which bitcoin is not accepted, $\theta < \hat{\theta}$, can be re-written as $1 - \phi < 1 - \hat{\phi}$, or $\phi > \hat{\phi}$. Using Equation (4) above, $\hat{\phi}$ is given as

$$\hat{\phi} = \begin{cases} 1 - \frac{1-a_{0,m}-a_{0,b}}{a_b} - \frac{rC+\delta_b}{a_b\rho(U-C)} - \frac{a_{0,m}(V_m-V_0-C)}{a_b(U-C)} & \text{if } V_m - V_0 - C > 0 \\ 1 - \frac{1-a_{0,m}-a_{0,b}}{a_b} - \frac{rC+\delta_b}{a_b\rho(U-C)} & \text{if } V_m - V_0 - C \leq 0 \end{cases}$$

The government's refusal to accept bitcoins has important implications for the threshold probability that a random agent will accept bitcoins, $\hat{\theta}$. Since $\theta = 1 - \phi$, the proportion of government agents is important. In particular, a larger proportion of government agents implies a lower θ, thereby increasing the likelihood that θ is below the threshold. The proposition shows that the government can only prevent an equilibrium in which bitcoin is accepted if the government is of a particular size. Specifically, the proposition implies that the government cannot preclude the use of bitcoins as a medium of exchange simply by refusing to accept bitcoins. The government can only do so if this ban is backed by a sufficient power to do so.

It is important to note that the degree of market power necessary to preclude the use of bitcoins is low if all agents are willing to accept currency. That is, the size threshold of the government necessary to prevent bitcoin circulation is dependent, in part, on the probability that a random agent is willing to accept *currency*. If every agent is wiling to accept currency, then the threshold for the size of government is low, which makes it easier for the government to prevent the acceptance of bitcoin in equilibrium. In addition, it follows that if a subset of agents had a preference for bitcoin rather than currency, they could limit the government's ability to prevent bitcoin circulation by refusing to accept currency.

V. CONCLUSION

Bitcoin is certainly one of the most interesting recent developments in modern monetary economies. It enables users to make secure and pseudonymous payments. Although many users value the private nature of bitcoin, some government officials seem to be concerned. Specifically, they note that bitcoin might facilitate illicit transactions and disrupt government activities like conducting monetary policy and raising revenues. For these reasons, some governments have attempted to ban or discourage the use of bitcoin.

We have considered the extent to which these government efforts might be successful. In the existing literature, similar considerations have been made by employing random matching models. However, the random matching protocol is not well suited for questions of monetary competition and control. Our model, in contrast, endogenizes the matching process: an agent preferring to transact with bitcoin might avoid those holding the official currency favored by the government. This means that, except in the case where all bitcoin is held by the government, some transactions are effectively (though only probabilistically) beyond the reach of the state.

Employing a monetary model with endogenous search and random consumption preferences, we find that the government's refusal to accept bitcoin is not typically sufficient to prevent their acceptance in equilibrium. The government must be of a particular size to prevent the circulation of bitcoin and the size threshold depends crucially on the fraction of agents willing to accept the official currency. Interestingly, our work suggests that bitcoin might continue on as a niche money, even if the government proactively discourages its use, so long as some individuals are sufficiently committed to accepting bitcoin.

We hope the model employed herein is a useful first step toward understanding why bitcoin thrives in some communities, but not others, and why some governments seem more interested than others in dissuading its use. We note that the commitments of individuals to accept bitcoin and of governments to discourage its use are exogenous in our model. Future efforts should attempt to explain the precise frictions that give rise to such preferences. Why do certain groups prefer bitcoin to their official currency? Do these preferences depend on the goods traded and/or the location of trading partners? Why do

some governments aggressively resist the use of bitcoin? Are such preferences related to the general level of control exercised in an economy and/or particular objectives of a government? These questions, which concern the deep-level forces at play, are admittedly beyond the scope of the current analysis but might provide fodder for future research.

While our analysis deals exclusively with the surface-level forces, we nonetheless find it worthwhile to offer some casual predictions concerning the deep-level forces that future work might consider. We expect the preference for bitcoin is higher in countries with complementary goods, such as greater levels of technology and access to the internet, but also where the official domestic currency is a poor substitute due to inflationary practices by the central bank. Such governments, insofar as they depend to a greater extent on seigniorage, may also prefer to maintain the dominance of their official local currencies by preventing the proliferation of bitcoin. Moreover, if there are gains from specialization in deterrence, those with greater levels of market intervention may be more effective at stemming the use of bitcoin as well. Countries with larger informal markets, on the other hand, may experience large gains from adopting bitcoin and, as with specialization in deterrence, the informal networks already in existence might allow bitcoin to thrive beyond the reach of the state. If substantiated by theory, these casual predictions might explain China's early efforts to prohibit bitcoin, but also the survival of underground and online bitcoin markets. With a fuller understanding of such deep-level forces, one might be better suited to consider the political economy of bitcoin in other countries such as Iceland, India, and the United States.

APPENDIX

Section III of the paper presents four possible equilibria. This appendix outlines how to derive the equilibrium conditions.

Consider an agent who is not holding currency or bitcoin. Let $\Pi(\pi)$ be the best response of the agent as to whether they should accept currency given that a fraction π of agents are willing to accept currency. Also, let $\Theta(\theta)$ be the best response as to whether the agent should accept bitcoin given that a fraction of agents, θ, are willing to accept bitcoin. As the model is symmetric, $\Pi(\pi)=\pi$ and $\Theta(\theta)=\theta$.

Let $V_m - V_0 - C$ be the value of accepting currency. Let $V_b - V_0 - C$ be the value of accepting bitcoin. If $V_m - V_0 - C > 0$, then the expected value of accepting currency is positive and thus all agents will accept currency (i.e., $\pi = 1$). Similarly, if $V_b - V_0 - C > 0$, then the expected value of accepting bitcoin is positive and all agents will accept bitcoin (i.e., $\theta = 1$). If the expected value of accepting either currency or bitcoin is negative, then no agents will accept the respective form of money (i.e., $\pi = 0$ and $\theta = 0$, respectively).

If the expected value of holding currency is equal to zero, then agents are indifferent about holding currency and $\pi \in (0, 1)$. Similarly, if the expected value of holding bitcoin is equal to zero, then agents are indifferent about holding bitcoin and $\theta \in (0, 1)$. For each currency and bitcoin, respectively, there are unique values for π and θ at which the assets will be accepted. The threshold value for holding currency is denoted as $\hat{\pi}$ and the threshold value for holding bitcoin as $\hat{\theta}$. One can solve for these unique values as follows.

An agent is indifferent between holding currency if

$$V_m - V_0 - C = 0.$$

Equivalently, this can be written as

$$rV_m - rV_0 - rC = 0.$$

From Equations (1)–(3) above it follows that

$$a_m \pi \rho \left(U + V_0 - V_m\right) - \delta_m - \left(1 - a_{0,m} - a_{0,b}\right)$$
$$\rho^2 (U - C) - \Theta(\theta)\, \rho \left(V_b - V_0 - C\right) - rC = 0.$$

Note that there is a unique value of $\pi = \hat{\pi}$ that solves this expression. This solution is given as

$$\hat{\pi} = \frac{\left(1 - a_{0,m} - a_{0,b}\right)\rho}{a_m} + \frac{rC + \delta_m}{a_m \rho (U - C)} + \Theta(\theta)\, \frac{a_{0,b}\left(V_b - V_0 - C\right)}{a_m (U - C)}.$$

Note that, in this case, the threshold value, $\hat{\pi}$, is dependent upon whether bitcoin is accepted. If bitcoin is accepted by all agents, then $V_b - V_0 - C > 0$ and $\theta = 1$. This condition can be re-written as

$$\hat{\pi} = \frac{\left(1 - a_{0,m} - a_{0,b}\right)\rho}{a_m} + \frac{rC + \delta_m}{a_m \rho (U - C)} + \frac{a_{0,b}\left(V_b - V_0 - C\right)}{a_m (U - C)}.$$

However, if $\theta < 1$, then the condition for accepting currency is independent of the expected value of accepting bitcoin as either $V_b - V_0 - C = 0$ or $\theta = 0$:

$$\hat{\pi} = \frac{\left(1 - a_{0,m} - a_{0,b}\right)\rho}{a_m} + \frac{rC + \delta_m}{a_m \rho (U - C)}.$$

A corresponding result can be found for bitcoin.

It follows that currency will be held in equilibrium if $\pi = 1$ or if $\pi = \hat{\pi}$. Similarly, bitcoin will be held in equilibrium if $\theta = 1$ or if $\theta = \hat{\theta}$.

REFERENCES

Aiyagari, S. R., and N. Wallace. "Government Transaction Policy, the Medium of Exchange, and Welfare." *Journal of Economic Theory*, 74(1), 1997, 1–18.

BitLegal. "List." 2014. Accessed November 26, 2014. http://bitlegal.io/list

Calvacanti, R., and N. Wallace. "A Model of Private Bank-Note Issue." *Review of Economic Dynamics*, 2(1), 1999, 104–36.

Christin, N. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." WWW '13: Proceedings of the 22nd International Conference on World Wide Web, 2013, 213–23.

Clinch, M. "Bitcoin Recognized by Germany as 'Private Money'." CNBC, August 13, 2013. Accessed November 26, 2014. http://www.cnbc.com/id/100971898#.

Corbae, D., T. Temzelides, and R. Wright. "Matching and Money." *American Economic Review*, 92(2), 2002, 67–71.

Corbae, D., T. Temzelides, and R. Wright. "Directed Matching and Monetary Exchange." *Econometrica*, 71(3), 2003, 731–56.

Financial Crimes Enforcement Network. "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Guidance FIN-2013-G001. 2013. Accessed March 18, 2013. http://fincen.gov/statutes/_regs/guidance/html/FIN-2013-G001.html.

Goldberg, D. "Money with Partially Directed Search." *Journal of Monetary Economics*, 54(4), 2007, 979–93.

Grinberg, R. "Bitcoin: An Innovative Alternative Digital Currency." *Hastings Science & Technology Law Journal*, 4(1), 2011, 159–208.

Hendrickson, J. R., and W. J. Luther. "The Value of Bitcoin in the Year 2141 (And Beyond!)." Working Paper, 2014.

Hogan, T. L., and W. J. Luther. "Endogenous Matching and Money with Random Consumption Preferences." Working Paper, 2014. Accessed July 1, 2015. http://papers.ssrn.com/sol3/papers.cfm?abstract&uscore;id=2423949.

Internal Revenue Service. "Notice 2014-21." 2014. Accessed March 25, 2014. http://www.irs.gov/irb/2014-16_IRB/ar12.html.

Kiyotaki, N., and R. Wright. "A Search-Theoretic Approach to Monetary Economics." *American Economic Review*, 83(1), 1993, 63–77.

Li, Y., and R. Wright. "Government Transaction Policy, Media of Exchange, and Prices." *Journal of Economic Theory*, 81(2), 1998, 290–313.

Lotz, S., and G. Rocheteau. "On the Launching of a New Currency." *Journal of Money, Credit, and Banking*, 34(3), 2002, 563–88.

Luther, W. J. "Regulating Bitcoin: On What Grounds?" Working Paper, 2015. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2631307.

———. Forthcoming-a. "Bitcoin and the Future of Digital Payments." *Independent Review*.

———. Forthcoming-b. "Cryptocurrencies, Network Effects, and Switching Costs." *Contemporary Economic Policy*.

Luther, W. J., and J. Olson. "Bitcoin Is Memory." *Journal of Prices & Markets*, 3(3), 2015, 22–33.

Luther, W. J., and L. H. White. "Can Bitcoin Become a Major Currency?" *Cayman Financial Review*, 36, 2014, 78–79.

Madore, P. H. "Final New York Bitcoin Regulation Released: BitLicense." *Crypto Coin News*, April 6, 2015. Accessed May 2, 2015. https://www.cryptocoinsnews.com/final-new-york-bitcoin-regulation-released-bitlicense/.

Matonis, J. "Bitcoin Casinos Release 2012 Earnings." Forbes, 2013. Accessed November 26, 2014. http://www.forbes.com/sites/jonmatonis/2013/01/22/bitcoin-casinos-release-2012-earnings/.

Middlebrook, S. T., and S. J. Hughes. "Regulating Cryptocurrencies in the United States: Current Issues and Future Directions." *William Mitchell Law Review*, 40(2), 2014, 813–48.

Miedema, B. "Regulator Mulls Setting Rules for Digital Currency Bitcoin," Reuters, 2013. Accessed May 6, 2013. http://www.reuters.com/article/2013/05/06/net-us-bitcoin-regulation-idUSBRE9450Y520130506.

Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." Working Paper, 2008. Accessed November 26, 2014. https://bitcoin.org/bitcoin.pdf.

Office of Investor Education and Advocacy. "Investor Alert: Ponzi Schemes Using Virtual Currencies," Investor.gov, 2013. Accessed March 23, 2013. http://investor.gov/news-alerts/investor-alerts/investor-alert-ponzi-schemes-using-virtual-currencies.

Salter, A. W., and W. J. Luther. "Synthesizing the State and Spontaneous Order Theories of Money." *Advances in Austrian Economics*, 18, 2014, 161–78.

Selgin, G. "On Ensuring the Acceptability of a New Fiat Money." *Journal of Money, Credit, and Banking*, 26(4), 1994, 808–26.

Waller, C. J., and E. S. Curtis. "Currency Restrictions, Government Transaction Policies and Currency Exchange." *Economic Theory*, 21(1), 2003, 19–42.

White, L. H. "The Market for Cryptocurrencies." *Cato Journal*, 35(2), 2015, 383–402.