



THE JOURNAL OF
**DIGITAL FORENSICS,
SECURITY AND LAW**

**Journal of Digital Forensics,
Security and Law**

Volume 13 | Number 2

Article 5

October 2018

A Bit Like Cash: Understanding Cash-For-Bitcoin Transactions Through Individual Vendors


Stephanie J. Robberson

University of Central Oklahoma, stephrobberson@gmail.com

Mark R. McCoy

University of Central Oklahoma, mmccoy@uco.edu

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Banking and Finance Law Commons](#), [Computer Law Commons](#), [Criminology Commons](#), [Criminology and Criminal Justice Commons](#), [Information Security Commons](#), [Law and Economics Commons](#), [Other Economics Commons](#), and the [Social and Cultural Anthropology Commons](#)

Recommended Citation

Robberson, Stephanie J. and McCoy, Mark R. (2018) "A Bit Like Cash: Understanding Cash-For-Bitcoin Transactions Through Individual Vendors," *Journal of Digital Forensics, Security and Law*. Vol. 13 : No. 2 , Article 5.

DOI: <https://doi.org/10.15394/jdfsl.2018.1449>

Available at: <https://commons.erau.edu/jdfsl/vol13/iss2/5>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL



A BIT LIKE CASH: UNDERSTANDING CASH-FOR-BITCOIN TRANSACTIONS THROUGH INDIVIDUAL VENDORS

Stephanie J. Robberson, M.S.

Mark R. McCoy, Ed.D.

University of Central Oklahoma

Edmond, OK 73034

405-974-6914

stephrobberson@gmail.com | mmccoy@uco.edu

ABSTRACT

As technology improves and economies become more globalized, the concept of currency has evolved. Bitcoin, a cryptographic digital currency, has been embraced as a secure and convenient type of money. Due to its security and privacy for the user, Bitcoin is a good tool for conducting criminal trades. The Financial Crimes Enforcement Network (FinCEN) has regulations in place to make identification information of Bitcoin purchasers accessible to law enforcement, but enforcing these rules with cash-for-Bitcoin traders is difficult. This study surveyed cash-for-Bitcoin vendors in Oklahoma, Texas, Arkansas, Missouri, Kansas, Colorado, and New Mexico to determine personal demographic information, knowledge of and compliance with FinCEN regulations, and opinions regarding government control of currency and willingness to work with law enforcement among vendors.

Keywords: Bitcoin, FinCEN, digital currency, investigation, law enforcement

1. INTRODUCTION

The theatrics of illegal purchasing are ingrained in our culture: little illustrates shady dealings as well as people swapping a briefcase full of cash. While this form of payment was popular for pseudo-anonymous dealings for years, purchasers have the whole world as a marketplace to explore now via the Internet.

Swapping country-specific currencies for transactions between nations can be time consuming and costly through conversion. To avoid the hassle, the tech-literate have adopted global digital currencies. Cryptocurrencies have been created to

meet the need for easy exchanges through the Internet. Cryptocurrencies use “effective mathematical tricks” to protect information in monetary transactions (Dostov & Shust, 2014, p. 249).

Normal banking and credit systems already use some cryptographic protections but lack the convenience and privacy afforded through digital currencies. Some have seen more success than others, but the most stable, private, and convenient digital cryptocurrency on the market is Bitcoin.

Bitcoin operates without a central server and spreads transaction

information to every node in the network across the blockchain, which acts as a ledger. The amount of Bitcoin sent and received is recorded in the ledger, but identification information is not. This pseudo-anonymous feature of the cryptocurrency is lauded by investors seeking general privacy, although it has been problematic for law enforcement.

After the highly publicized takedown of the Darknet drug market website Silk Road, federal regulations through the Financial Crimes Enforcement Network (FinCEN) have made it easier for law enforcement officials to gain access to identification information for suspicious individuals and transactions.

However, individual Bitcoin vendors trade coins for cash locally, and information regarding their FinCEN compliance as money transmitters has not yet been questioned. This study surveyed individual cash-for-Bitcoin vendors in Oklahoma, Texas, Arkansas, Kansas, New Mexico, Missouri, and Colorado to gain insight to these vendors' understanding of FinCEN obligations, record keeping practices, and attitudes toward cooperating with law enforcement. The following research questions guided this project:

1. What are the general personal demographics of cash-for-bitcoin vendors?
2. Do these vendors have knowledge of and are they compliant with regulations from FinCEN?

3. What identification information do cash-for-bitcoin vendors collect about their customers?

4. What do these vendors think about government regulation of currency?

5. How do cash-for-bitcoin vendors feel about law enforcement?

6. Would these vendors be willing to assist law enforcement in investigations concerning their customers?

Clearly, Bitcoin creates new challenges for law enforcement officials. Illegal transactions for drugs, forged documents, and weapons through Darknet sites favor the use of Bitcoin as payment, and services such as contract killing and human trafficking can be compensated through the cryptocurrency. Money launderers are finding Bitcoin to be helpful in hiding assets. Not all Bitcoin users have criminal intentions, but it cannot be denied that the high-tech portion of the criminal sector is aware of Bitcoin and knows how to manipulate currency transactions for maximum privacy. Understanding the people who trade bitcoin for cash is key for investigations of customers using the cryptocurrency for shady dealings.

Bitcoin's pseudo-anonymous structure and ease of global use make it an appealing option for currency. It has been used for criminal acts on a great scale such as the Silk Road online marketplace. To apprehend criminals using Bitcoin, the FBI suggested that investigators look at how the purchaser

chooses to get bitcoin. For individual criminals, mining for bitcoin is a waste of time. Large-scale mining operations with unbeatable hardware exist, and it is not efficient for one miner to challenge this system. Criminals could use websites to turn money from bank accounts into bitcoin, but these websites require specific identification information from users in order to comply with FinCEN regulations. The solo criminal's only logical option is to trade cash for bitcoin with a vendor who does not follow FinCEN regulations.

Little is known about cash-for-bitcoin vendors. This project surveyed these vendors to find out general demographic information, familiarity and compliance with FinCEN regulations, and opinions concerning government control of currency and willingness to assist law enforcement in investigations about vendors' customers.

2. METHODOLOGY

A descriptive research method using survey and semi-structured interview data was chosen to address the research questions for this study. Descriptive research allows for an in-depth, humanistic understanding of a topic where data does not already exist in abundance.

Sample data was collected on January 2, 2017 from three different sources: LocalBitcoins.com, Craigslist, and Backpage. A convenience sampling method was chosen in which

all potential cash-for-bitcoin vendors in Oklahoma, Texas, New Mexico, Missouri, Arkansas, Kansas, and Colorado were contacted.

Each source provided different information about the vendors. Sample members from LocalBitcoins.com were collected by using the Quick Search tool. "In Person- Cash" was selected as the payment method. The state name was typed into the location box. A short list of sellers appeared, but the Map option needed to be selected to see all available cash-for-bitcoin vendors in the state. From there, a vendor profile for each vendor in the state could be selected. The vendor's username, customer rating, price per bitcoin, trade limit range, city, preferred meeting place, and direct link to the posting for each user were recorded in a master Excel spreadsheet. If the vendor provided a phone number or an email address, this was also recorded in the spreadsheet.

Craigslist cash-for-bitcoin vendors were found by visiting all city or regional Craigslist websites for the states of Oklahoma, Texas, New Mexico, Arkansas, Missouri, Kansas, and Colorado. Since Craigslist does not provide a system for public usernames for sellers, only the posting date, city, post identification number, Craigslist anonymized email address, and direct link to the post were recorded. Direct phone numbers were also recorded if provided in the advertisement by the vendor.

Backpage's user system works similarly to Craigslist. The Backpage portion of the sample was collected by searching all city or regional Backpage websites for Oklahoma, Texas, New Mexico, Arkansas, Missouri, Kansas, and Colorado. The posting date, city, post identification number, and direct link to the post were recorded in the master Excel file. No direct phone numbers were available. One personal email was provided and recorded.

After collecting potential sample data, several groups of users were excluded from contact. All posts about Bitcoin ATMs were removed from this study. All duplicate posts for the same vendors were removed. Users without a means of direct contact such as a phone number or email address from LocalBitcoins.com were removed as the website frowns upon users messaging vendors without intent to purchase Bitcoin. Eight Craigslist postings were excluded because they were deleted and inaccessible at the time of outreach.

With these groups removed, the total original population size included 43 individual cash-for-bitcoin vendors. 14 of these came from LocalBitcoins.com, 10 came from Craigslist, and 19 came from Backpage.

The actual population size cannot be known definitively. After conducting a phone interview with a LocalBitcoins.com vendor, he posted a link to the survey along with summary of the project to the LocalBitcoins.com seller message boards. This led to a

snowball sample in which vendors outside of the original population may have taken the survey. Since this project is the first to collect this type of data from cash-for-bitcoin vendors, the researcher and Co-PI determined that any response would be a good one and welcomed sharing of the survey link. In total, 30 participants filled out the online survey or answered the survey questions through text messaging or oral interview.

Data collection occurred during January and February of 2017. If a direct phone number was provided on a vendor's online post, a text message was sent to the vendor to request participation in the project.

The researcher used a password protected Google Voice account to create a new phone number for this research. Text messages and phone calls were sent and received through the Google Voice number to protect the researcher's personal phone number during this project.

The survey link took participants to a Qualtrics survey page. Qualtrics is an online survey and data management tool. An online survey format was selected to conduct this study because of the ease of distribution and familiarity with technology that this population has. A setting was selected to block IP addresses and anonymize responses in order to protect the identity of participants. This helped to legitimize the project and foster confidence in respondents that their

data would be protected, not turned over to law enforcement officials.

In addition to directly accessing the online survey, several participants chose to answer the survey questions over the phone. One respondent answered the survey questions one by one through text messaging. Two respondents answered the survey questions through oral interviews over the phone. One respondent submitted the online survey and called to discuss his thoughts further. Oral phone interviews were semi-structured and allowed interviewees to give deep explanations for their answers to survey questions.

This survey was developed to explore three areas of information about cash-for-bitcoin vendors: personal demographics, knowledge of and compliance with FinCEN regulations, and attitudes toward government and law enforcement.

The demographic section of the survey asked and provided answer choices for participants to report gender, age range, ethnicity, education, income, marital status, and jobs outside of selling Bitcoin.

Section Two asked specific questions about vendors' Bitcoin business practices and familiarity with FinCEN. Participants were asked if they personally mine bitcoin and what websites they advertise their bitcoin businesses with. Respondents were asked if they were aware of federal regulations regarding bitcoin transmission and if they were registered

as a money transmitter through FinCEN. FinCEN's anti-money laundering measures require money transmitters to record identification information for customers, so participants were asked to select all identification information they record about their customers.

The final phase of the survey asked respondents to share their opinions about government and law enforcement in relation to Bitcoin. Seven statements were listed, and participants used a Likert scale to report their levels of agreement or disagreement with the statement. Options included "Completely Disagree," "Slightly Disagree," "Slightly Agree," and "Completely Agree." Four answer options for this scale were selected purposefully to eliminate a middle-of-the-road "Neither Agree Nor Disagree" answer.

The survey closed with an open-ended response box for participants to elaborate on any of their answers if they wished to do so. A text entry box was provided for respondents to give a pen name to be referred to if quoted in this report.

Questions on the survey that are statements of fact such as gender or whether or not a respondent mines their own Bitcoin should be reliable and repeatable answers if individuals retake the survey. The opinion portion with Likert-scale ratings might change hourly based upon current events or personal experiences and emotions of vendors. These responses might not be

as repeatable as statement-of-fact questions. More trials of administering this survey would be needed to assess reliability.

In any interview or survey research project, there is a threat of receiving misinformation due to an interviewee's social desirability bias. There is no way to fact check the responses to this survey or peer into respondents' minds to discern their opinions in the final survey phase of this project. Even though responses are anonymous and this was communicated to respondents, this survey asks sensitive questions. With this, there is a risk of lies entering survey response pool due to fear of arrest.

3. RESULTS AND DISCUSSION

The first research question examined in this study was, "What are the general personal demographics of cash-for-bitcoin vendors?" Survey participants were predominately male (86.67%) and White (73.33%) (Table 1).

83.34% of respondents fell between the ages of 18 and 44. Only 16.66% of respondents were older than 45 years old. Bitcoin is a shiny, attractive reimagination of currency based on technology. Younger generations might easily adopt Bitcoin due to familiarity with (and reliance upon) online banking systems and a stronger trust in technology than in government. For an age group that sees money as pure numbers increasing and decreasing on a credit card statement and not a stack of cash or gold, understanding the purely

digital structure of Bitcoin is not a big stretch.

90% of respondents ranged from having completed some college classes to having completed a master's degree. This is an educated, intelligent group of people. Managing a business takes smarts, and managing a slightly sketchy business takes even more planning and care.

Even though this is a smart group, 67.85% of respondents made less than \$100,000 in total household income in 2016. In part, this could be due to marital status and having only one income for the household. 80% of respondents are single, separated, widowed, or divorced, implying that household income might come from only one breadwinner.

53.33% of respondents have a job outside of selling Bitcoin. Of these, 68.75% work at for-profit organizations. 18.75% selected "Other" as their job type and entered home business type jobs such as "computer consulting", "self employed", and "business owner". This could point to cash-for-bitcoin sales as a hobby or a side business to bring in extra money.

The second research question examined was, "Do these vendors have knowledge of and are they compliant with regulations from FinCEN?" 80% of respondents said they are aware of federal financial regulations concerning the transmission of Bitcoin, but only 36% are registered as a money transmitter through the Financial

Table 1 Survey Results for Demographic Data

Characteristic		n	%	Characteristic		n	%
Sex		30		Total Household Income 2016		28	
	Male	26	86.67		Less than \$25,000	2	7.14
	Female	4	13.33		\$25,000 to \$34,999	2	7.14
Age		30			\$35,000 to \$49,000	1	3.57
	Under 18 Years	0	0.00		\$50,000 to \$74,999	7	25.00
	18-24 Years	8	26.67		\$75,000 to \$99,999	7	25.00
	25-34 Years	9	30.00		\$100,000 to \$149,999	4	14.29
	35-44 Years	8	26.67		\$150,000 or more	5	17.86
	45-54 Years	3	10.00	Marital Status		30	
	55-65 Years	1	3.33		Single (Never Married)	20	66.67
	65+ Years	1	3.33		Married	6	20.00
Ethnicity		30			Separated	1	3.33
	African American	0	0.00		Widowed	1	3.33
	Asian	2	6.67		Divorced	2	6.67
	Hispanic	3	10.00	Job Outside of Bitcoin Sales		30	
	Native American	1	3.33		Yes	16	53.33
	Pacific Islander	1	3.33		No	14	46.67
	White	22	73.33	Area of Work Outside Bitcoin Sales		16	
	Other	1	3.33		For Profit	11	68.75
Education		30			Non Profit	0	0.00
	Less than High School	3	10.00		Government	0	0.00
	Some College, No Degree	9	30.00		Health Care	1	6.25
	Associates Degree	5	16.67		Education	1	6.25
	Bachelors Degree	10	33.33		Other	3	18.75
	Masters Degree	3	10.00				
	Ph.D, law or medical degree	0	0.00				

Crimes Enforcement Network (FinCEN) (Table 2).

A phone interview provided more understanding to these percentages. Tom said, “As far as I know, person to person transactions aren’t regulated yet.” He went on to say regulations for digital currencies differ from state to state “since the government hasn’t really figured out what Bitcoin is.” Hoping to clarify this matter further, FinCEN was contacted via email. The following email was sent with the researcher’s contact information:

Hello,

My name is Stephanie Robberson, and I am currently writing a thesis about people who sell bitcoin for cash. This is a survey research

project in which I am gathering information about these vendors' demographics, compliance with FinCEN regulations, and attitudes toward government and law enforcement. Do you have any resources that specify the reporting/registration duties of these cash-for-bitcoin money transmitters? What are the penalties for vendors who choose to not register as money transmitters?

One day later, the following message was received:

Please refer to Jen Shasky's 2013 Congressional testimony, which sums up our stance on virtual currency and references our guidance, two admin rulings, and Liberty Reserve 311 action.

Table 2 Survey Results for FinCEN Compliance

Characteristic		n	%
Do You Mine Bitcoin?		26	
	Yes	4	15.38
	No	22	84.62
Do You Sell the Bitcoin You Mine?		4	
	Yes	3	75.00
	No	1	25.00
Which Websites Do You Use to Advertise Bitcoin Sales?		41	
	Craigslist	7	17.07
	Backpage	3	7.32
	LocalBitcoins.com	25	60.98
	Other	6	14.63
In Which State Do You Sell Bitcoin?		15	
	Arkansas	0	0.00
	Colorado	4	26.67
	Kansas	1	6.67
	Missouri	1	6.67
	New Mexico	0	0.00
	Oklahoma	2	13.33
	Texas	7	46.67

<https://www.fincen.gov/sites/default/files/2016-08/20131119.pdf>

A little more research into all of the pieces of information mentioned in the Testimony should give you what you need.

FinCEN's Resource Center

This statement from Jen Shasky was made in November 2013. The document contains a basic explanation of what a digital currency is and how Bitcoin works. It goes on to explain that Bitcoin is the perfect tool for money laundering, and steps must be taken to

control the currency. In describing the responsibilities of bitcoin vendors, FinCEN said the following:

In the simplest of terms, FinCEN's guidance explains that administrators or exchangers of virtual currencies must register with FinCEN, and institute certain recordkeeping, reporting and AML program control measures, unless an exception to these requirements applies....The guidance clarifies definitions and expectations to ensure that businesses engaged in such activities are aware of their

regulatory responsibilities, including registering appropriately. Furthermore, FinCEN closely coordinates with its state regulatory counterparts to encourage appropriate application of FinCEN guidance as part of the states' separate AML compliance oversight of financial institutions. (p. 9-10).

Clearly, these are not the "simplest of terms." First, the statement requires exchangers of bitcoin to register with FinCEN. FinCEN provided no information on how to do this. A Google search of "FinCEN register" came up with a result of a "Money Services Business (MSB) Registration" page on fincen.gov. A bulletin on this page from 2012 is posted rerouting visitors to another website to register. This takes visitors to the BSA E-Filing System website. On this site, there is no mention of digital currencies or money transmitter services. The page bombards the visitor with acronyms including FBAR, BSA, RMSB, CTR, SAR, DOEP, and NAICS.

While they are able to access this website, this is inaccessible to cash-for-bitcoin vendors. This group is immediately suspicious of click-through links. While conducting this research, the survey link was sent through text message to respondents. One respondent chose to participate only if the survey questions were texted to him one by one. BTCMiner said, "Don't send links if you want to be taken seriously. Just friendly advice.

People who operate in the bitcoin world are targets for phishing scams all the time." FinCEN's outdated bulletin riddled with click-through links might deter cash-for-bitcoin vendors from exploring the current registration website.

If the cash-for-bitcoin vendors make it to the current BSA filing website, they will see acronyms everywhere without explanation of what they stand for. As a Libertarian group already suspicious of government agencies, this language is alienating and alarming to cash-for-bitcoin vendors.

FinCEN's statement claims that they have "clarifi[ed]...expectations" to make sure businesses know "their regulatory responsibilities," but these responsibilities are still ambiguous to some cash-for-bitcoin vendors. Adding to the confusion are differing state-level court decisions ruling Bitcoin as real currency or false currency.

To combat this confusion, we recommend that FinCEN create a guide or bulletin for sellers of digital currencies. This document should be clear and concise, not only listing the reporting and registration responsibilities for these vendors but also how to register and file reports. To create a unified message, this bulletin should be shared with state, county, and city-level law enforcement officials. To spread the word, this bulletin should be shared on user message boards on LocalBitcoins.com, and posts should be created on Craigslis.com and Backpage.com and renewed biweekly or monthly. Cash-

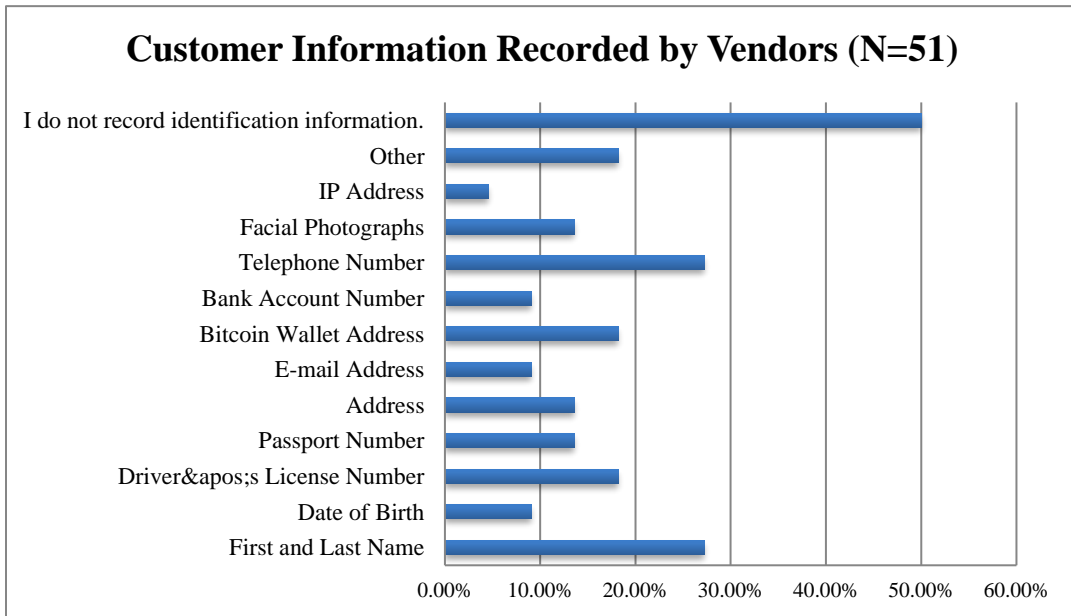
for-bitcoin vendors are a network and know one another, so if the bulletin can be shared with select vendors, they can share the document with their contacts, and the contacts will read it if it comes from a trusted cash-for-bitcoin vendor.

The third research question for this project was, “What identification information do cash-for-bitcoin vendors collect about their customers?” 27.27% of vendors record the first and last names of their customers, and 27.27% collect phone numbers. 18.18% record the customer’s driver’s license number, 18.18% record a Bitcoin wallet address, and 18.18% selected the “Other” option. For these “Other” responses, two participants said the amount of identification information recorded depends on the transaction amount. One respondent records a

“mental profile,” and the last open ended response said this question was “too invasive, sorry.” 13.64% record a passport number, 13.64% record a physical address, and 13.64% record a facial photograph of the customer. 9.09% record the customer’s date of birth, 9.09% record a bank account number, and 9.09% record an e-mail address. 4.55% record an IP address (Table 3).

This question is important for two reasons. Firstly, identification information collection is required of money transmitter services by FinCEN’s Anti-Money Laundering (AML) measures. To be fully compliant with FinCEN regulations, customer identification information needs to be recorded. FinCEN is not specific about the identification information needed,

Table 3 Customer Identification Information Recorded by Cash for Bitcoin Vendors



and this should be added to the aforementioned bulletin. Secondly, if law enforcement officers need information regarding a customer of a cash-for-bitcoin vendor, the data provided from this survey question can help them know what specific questions to ask vendors or give specific language for a subpoena for information.

3.1 Libertarian, and Proud of It

A theme that emerged early on in this project is that most respondents are staunch Libertarians. The Libertarian Party “strongly oppose[s] any government interference into...personal, family, and business decisions” urging Americans to “pursue their interests as they see fit as long as they do no harm to another” (“About the Libertarian Party,” n.d.). Libertarians abhor intrusive government practices in commerce which explains why cash-for-bitcoin vendors have flocked to this political party.

In open-ended response areas for this project, participants used the actual word “Libertarian” to describe their ideology four times. In a phone interview, Topher stated that his clients prefer to meet face to face “because they are Libertarians” and believe the government does not have a place in person-to-person transactions. Tom, in a different phone interview, stated, “I’m a pretty strong Libertarian.” He went on to say that his clients are “pretty Libertarian, pretty smart, and mostly pretty harmless.” An anonymous online survey responder

stated, “I am a strong Libertarian.” Clearly, this group identifies as Libertarian, and this view seems to be a strong source of unity among bitcoin vendors and customers.

A tenet of Libertarianism is to “reduce the size and intrusiveness of government,” and survey and interview responses reflect this goal (“About the Libertarian Party,” n.d.).

The whole point of bitcoin is to get rid of a third party. - Rob, phone interview

Ideally, [bitcoin trading] would just be a peer-to-peer involuntary thing. - Tom, phone interview

The less personal identifiers that the government has, the safer its citizens are. - Topher, phone interview

Libertarian viewpoints wind throughout all open-ended survey responses, but these specific instances of using the actual word “Libertarian” and cutting out a third party from transactions give a strong unity to these participants.

3.2 Government Control of Currency

While respondents tended to dislike government control, they seemed to agree that paper currency should be federally regulated. BtcMiner said, “The government should regulate paper currency because they create and distribute their own.” Topher strongly agreed that paper currency should be federally regulated “because if it’s not,

there's too strong a possibility of counterfeiting." Tom believes, "The very nature of fiat currency is that it's regulated." When Rob was asked if he agreed with this statement, he said, "Yes! Duh!" There seems to be emphatic agreement that fiat currency needs government regulation among survey responders.

The opposite viewpoint is held for federal regulation of digital currency. Topher believes that Bitcoin is "not as easy to counterfeit" so it does not need federal protection. He says Bitcoin is the "21st century version of cash. Everyone who uses it serves a purpose, and part of that purpose is to not be tied to any federal institution." BtcMiner explained, "A peer-to-peer currency is a death sentence for centralized and controlled capital, so naturally, large governments don't like it." Bitcoin, a threat to controlled capital, has inspired federal regulations for digital currencies, but respondents believe the government should not set the rules in this new system.

3.3 Willing but Wary to Help Law Enforcement

For the most part, respondents seem willing to help law enforcement with cases involving customers, to an extent. Open-ended responses generally stated vendors would provide customer information to law enforcement if they were (1) legally required to do so, or (2) the customer was using bitcoin for highly nefarious operations.

They would need to show me a warrant before I give out any info. - UserNotFound, online survey

If law enforcement approached me with a case I would provide all customer information I had IF I was presented with a subpoena for that info specifically. -Anonymous, online survey

I would have to know what that illegal activity is and that was truly what [the customer] intended to use [the bitcoin] for. If they were using my service to launder money for terrorist organizations, I would report it. - Topher, phone interview

I would try to work with law enforcement to a certain degree, but I know what most of my buyers use [bitcoin] for and would not be willing to share the information regarding each person directly. - Greg, online survey

I'd have to take that on a case by case basis. I probably would give them a phone number and show them my text messages. - Tom, phone interview

While respondents seem to be willing to work with law enforcement if legally obligated to do so, day-to-day interactions with and stories about officers have created a strong distrust of law enforcement. Respondents fear being taken advantage of and robbed by people in power positions.

I don't have a strong trust with law enforcement. I would need to see evidence and make sure they

weren't just on a fishing trip. - Topher, phone interview

You hear stories about cops stealing Bitcoin from people. It's easy to target a Bitcoin trader, steal his phone, and send his Bitcoin to your wallet. - Rob, phone interview

The single biggest fear of a bitcoin trader isn't being robbed or scammed by your customers, it's being robbed and scammed by law enforcement. Civil forfeiture is VERY real and you are guilty until proven innocent at your own expense. I can defend myself if a person breaks into my house or tries to rob me on the street, but if they have a uniform on, they can do whatever they want and I have to roll over and take it. - Anonymous, online survey

Clearly, fear of civil forfeiture runs deep within this group. Because of this, cash-for-bitcoin vendors need hard evidence of customer wrongdoing or a subpoena to feel more comfortable interacting with law enforcement or investigators in positions of power.

3.4 Selling a Commodity, Not a Responsibility

Another theme observed in open-response areas of this survey was a need to justify that the act of selling bitcoin for cash was not in itself criminal, and it does not matter what the customer uses bitcoin for. Tom, in a phone interview, explained that selling bitcoin was the same as selling a cell phone. Most of the time, a customer buying a

cell phone will use it for calling and text messaging people, checking e-mail, keeping up with a calendar, taking pictures, and checking social media. These customers could potentially use the cell phone to create an IED, but one way or another, they will purchase a cell phone from somewhere. The person who sold the cell phone is not responsible if the customer turns it into a bomb.

Similarly, most of his clients use Bitcoin for pure purposes, but there is always a risk that his clients could trade bitcoin for something terrible. He summed up this theme by saying, "I have my moral stance and I have my legal stance. It's just a commodity as far as I'm concerned." Vendors seem unconcerned with what the bitcoin they sell will be used for.

I think it's mostly used for drugs, just like cash. - Rob, phone interview

I sell Bitcoin. I pay my taxes. It's none of my business what they do with it. - Tom, phone interview

99% of digital currency uses are for child porn, drugs, guns, anonymous services, money laundering, tax evasion, stolen credit cards etc... - Anonymous, online survey

While vendors might not care what a client could potentially do with Bitcoin, they will blacklist customers who tell them directly that they will use the bitcoin purchased to do something illegal.

Odds are the person that says they will use bitcoin for an illegal purchase IS law enforcement. I would simply deny the transaction and blacklist the individual. If they had given me any info prior to their confession, I would use it to file an SAR. - Anonymous, online survey

If it was something really nefarious, I'd help out [with the investigation]. I wouldn't put myself in legal jeopardy for a client. - Tom, phone interview

Most people involved in shady things aren't very smart...it's not a smart person, and it's not someone I can deal with. - Tom, phone interview

If customers are dim enough to disclose their evil plans for using Bitcoin, cash-for-bitcoin vendors will assume they are law enforcement officials trying to catch them for not filing the correct paperwork, or they will assume that the customer is not trustworthy and will blacklist them from current and future trades.

From all of these themes, it can be observed that the cash-for-bitcoin vendor community is staunchly Libertarian and employs high standards of trust for dealing with law enforcement and conducting day-to-day business with customers. While these vendors believe the government should not regulate digital currencies, they are willing to work with law enforcement in investigations involving their customers if they are presented with hard evidence of criminal activity

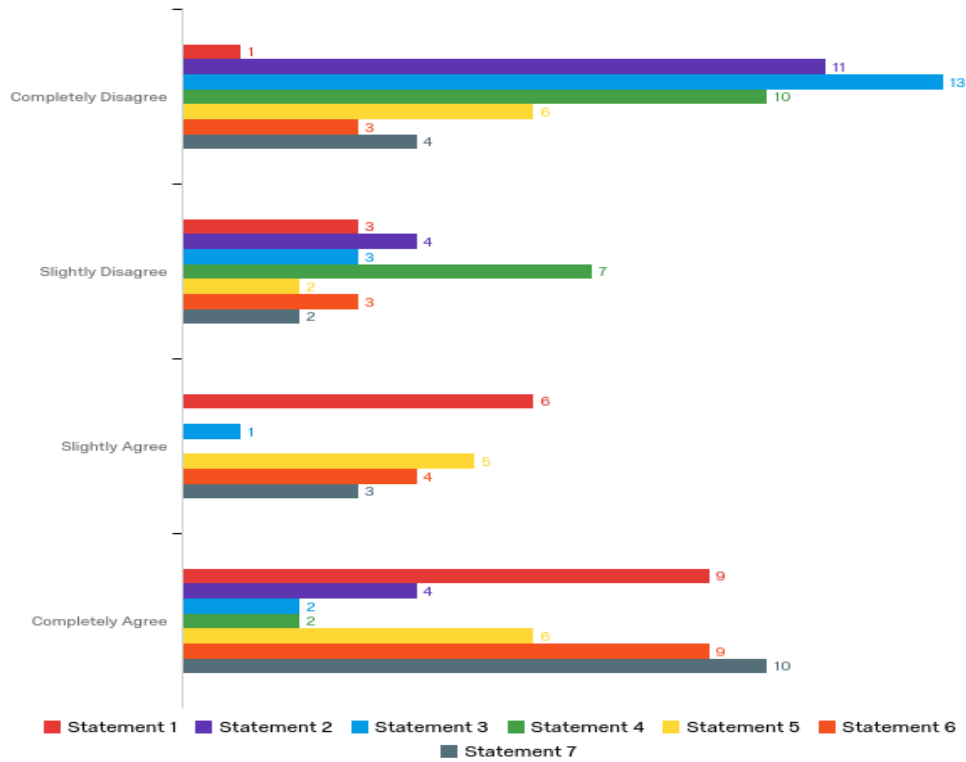
and are subpoenaed for specific information. Although these vendors generally do not ask what customers will use purchased bitcoin for, they can recognize a bad business decision when they see it, and they will not work with careless or clearly devious customers.

3.5 Vendor Opinions

The fourth research question for this project was, "What do these vendors think about government regulation of currency?" 78.95% of respondents either slightly or completely agree that paper currency should be federally regulated, but 78.94% either slightly or completely disagree that digital currency should be federally regulated (Table 4). 84.21% of respondents either slightly or completely disagree with the statement "I trust the federal government to handle Bitcoin exchange information appropriately."

Although vendors believe there should be a federal hand guiding fiat currencies, they see Bitcoin as a totally different system that should not be regulated by the government. Topher, in a phone interview, explained that fiat currency needs federal protection because it can be easily counterfeited. Counterfeiting is not seen as a large threat in the bitcoin market, so it does not need federal protection. He said, "Part of [each bitcoin user's] purpose is to not be tied to any federal institution." When Tom was asked if digital currencies should be federally regulated, he replied, "Nah, that's a terrible idea." Cash-for-bitcoin vendors have strong feelings about keeping the

Table 4 Survey Results of Vendors' Opinions



Statement #	Statement	Completely Disagree	Slightly Disagree	Slightly Agree	Completely Agree	Total
1	Paper currency should be federally regulated.	5.26%	15.79%	31.58%	47.37%	19
2	Digital currency should be federally regulated.	57.89%	21.05%	0.00%	21.05%	19
3	I trust the federal government to handle Bitcoin exchange information appropriately.	68.42%	15.79%	5.26%	10.53%	19
4	I trust law enforcement will handle Bitcoin exchange information appropriately.	52.63%	36.84%	0.00%	10.53%	19
5	I would contact law enforcement if my Bitcoin buyer told me they planned to use the currency on an illegal purchase.	31.58%	10.53%	26.32%	31.58%	19
6	If law enforcement approached me about a case involving my customer, I would provide general descriptive information.	15.79%	15.79%	21.05%	47.37%	19
7	If law enforcement approached me about a case involving my customer, I would provide specific identifying information.	21.05%	10.53%	15.79%	52.63%	19

government out of Bitcoin. This ties in with Libertarian ideals in keeping the government out of person-to-person trade.

The fifth research question for this project asked, “How do cash-for-bitcoin vendors feel about law enforcement?” The short answer is that vendors are uncomfortable and untrusting of law enforcement. 89.47% of participants either slightly or completely disagree with the statement, “I trust law enforcement will handle Bitcoin exchange information appropriately” (Table 4). In open-ended responses, participants reported a strong fear of civil forfeiture when dealing with law enforcement. Rob, in a phone interview, spoke about a business interaction with a person posing as a police officer. The customer showed up at a McDonald’s restaurant where they had agreed to make a trade. The supposed officer was driving a beige Lexus. Rob demanded to see his driver’s license before making the trade, but the officer refused. Rob felt unsafe dealing with this man, so he called off the trade. He said, “It’s easy to target a bitcoin trader, steal his phone, and send his bitcoin to your wallet...You hear stories about cops stealing bitcoin from people.” He also believes federal agents stole bitcoin in the Silk Road case. Whether this distrust of law enforcement arises from personal business interactions or stories told throughout the bitcoin vendor community, this group does not believe that law enforcement officials have vendors’ best interests at heart.

There is no way to know who could be a crooked officer, but we must work to improve relationships between law enforcement and cash-for-bitcoin vendors. One way to do this is to introduce officers to heads of bitcoin related clubs at universities and in communities. After forming a relationship with leadership within these groups, officers should attend meetings and interact with members to show that not all law enforcement officials are thieves or horrible people. Agents investigating digital crimes or digital forensic analysts might be a good fit for this community partnership role as they can speak intelligently about digital issues. If any agents are Bitcoin hobbyists, they would be perfect candidates for community outreach with bitcoin vendors.

The sixth and final research question asked was, “Would these vendors be willing to assist law enforcement in investigations concerning their customers?” Survey data said 57.9% of respondents slightly or completely agree with the statement, “I would contact law enforcement if my Bitcoin buyer told me they planned to use the currency on an illegal purchase,” but 31.58% completely disagreed (Table 4). In a phone interview, Topher said, “If [customers were] using my service to launder money for terrorist organizations, I would report it.” Tom said, “If it was something really nefarious, I’d help out.” Vendors are unconcerned with customers using bitcoin to buy drugs, but they are more

likely to report inhumane crimes like terrorism or crimes against children.

68.42% of respondents either slightly or completely agreed that if law enforcement approached them about a case involving their customer, they would provide general descriptive information, and the same amount either slightly or completely agreed that they would provide specific identification information about these customers. This goes along with the theme that these vendors believe they are selling a commodity, not a responsibility. In a phone interview, Tom said, "I wouldn't put myself in legal jeopardy for a client." Generally speaking, if the risk is greater than the reward, vendors will hand over information about customers.

Due to distrust of law enforcement, it would be wise to approach cash-for-bitcoin vendors with a warrant for specific identification information about their customers. Greg, in an online survey, said, "I would try to work with law enforcement to a certain degree, but I know what most of my buyers use [bitcoin] for and would not be willing to share the information regarding each person directly." Other responses generalize the need for a warrant for specific identification information to ensure the officers were not on a "fishing trip," as Topher called it in a phone interview. These vendors are smart people who fear being taken advantage of by law enforcement, so approaching them with specific questions about a customer and

bringing a warrant along is the best approach for recruiting investigatory assistance.

4. RECOMMENDATIONS AND CONCLUSION

A wider sample size could bolster trends seen in this project. To widen the sample, a nationwide study could be done in the future. Additionally, the search method for vendors through LocalBitcoins.com was limited to in-person cash trades. Future studies could also collect sample data for bitcoin trades for cashier's checks, cash by mail, cash deposit, or Western Union transfers on this website.

Another source for information is college Bitcoin clubs. Rob, in a phone interview, knew that a Bitcoin enthusiast club existed at his alma mater and suggested that the researcher attend meetings to get a better feel for what was going on in the world of digital currencies. Future researchers would do well to explore this option and cultivate relationships with members of these organizations.

Cash-for-bitcoin vendors are wary of people approaching them for information about their business. For this project, the researcher chose to text message vendors and tell them right off the bat that their knowledge was needed for a research project, not a bitcoin transaction. To ensure that they were not speaking with a law enforcement official, several respondents asked to see the researcher's student identification card, receive an e-mail

from the researcher's official University of Central Oklahoma e-mail address, or examine the researcher on LinkedIn. Openness from the researcher during this process was critical for these vendors to feel safe and share information.

Only two people contacted were upset that they were being messaged about something besides business. Most vendors were friendly and generous with the information they provided. Many wished the researcher good luck with her master's thesis project, and several requested to read the finished project. This is a group of educated people, and they appreciate the effort that research projects take. They are proud to share business success stories and seem to be flattered by someone saying that the knowledge they have of their business and customers is critically important for preventing heinous crimes.

Cash-for-bitcoin vendors in Oklahoma and the surrounding states tend to be single white males under the age of 45. Most have at least some level of college education ranging from taking a few classes to completing a master's degree. A slight majority of respondents have a job outside of selling bitcoin, mostly in the for-profit sector. Most cash-for-bitcoin vendors do not mine their own bitcoin.

80% of respondents are aware of federal regulations concerning the

transmission of bitcoin, but only 36% are registered as money transmitters through FinCEN. Half of respondents claimed that they do not record any identification information about their customers. This could be due to FinCEN's vague regulations and less-than-friendly website or differing state laws concerning bitcoin transmission. In either case, FinCEN needs to get federal, state, county, and city law enforcement on the same page about specific record keeping duties for cash-for-bitcoin vendors.

Survey questions about respondents' personal opinions showed discomfort with the federal government regulating digital currencies. While most respondents agreed to help law enforcement in investigations concerning their customers, open-ended questions revealed that vendors need to be presented with evidence of criminal activity and a warrant for specific information about a customer to provide assistance in these investigations.

Cash-for-bitcoin vendors do not trust law enforcement and fear interacting with investigators will lead to civil forfeiture of their own bitcoin. Efforts should be taken by law enforcement agencies to reach out to Bitcoin club leadership and members to strengthen relationships. This could aid efforts to investigate bitcoin related crimes in the future.

REFERENCES

- About the Libertarian party*. Retrieved from <https://www.lp.org/about/>
- Cusumano, M. A. (2014). The Bitcoin ecosystem: speculating on how the Bitcoin economy might evolve. *Communications of the ACM*, 57 (10), 22-24. doi : 10.1145/2661047
- Dostov, V. & Shust, P. (2014). Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?. *Journal of Financial Crime*, 21 (3), 249-263. doi : 10.1108/JFC-06-2013-0043
- Excellent privacy*. Retrieved from <https://bitcoin.org/en/bitcoin-core/features/privacy>
- Extance, A. (2015). Bitcoin and beyond. *Nature*, 526 (7571), 21-23. doi : 10.1038/526021a
- Financial Crimes Enforcement Network. (Nov. 19, 2013). *Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury: Before the United States Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance, Subcommittee on Economic Policy*. Retrieved from <https://www.fincen.gov/sites/default/files/2016-08/20131119.pdf>
- Kirby, P. (2014). Virtually possible: how to strengthen Bitcoin regulation within the current regulatory framework. *North Carolina Law Review*, 93 (198), 1-32. retrieved from www.lexisnexis.com/hottopic/lnacademic
- Maras, M. H. (2014). Inside Darknet: the takedown of Silk Road. *Centre for Crime and Justice Studies*, 98, 22-23. doi : 10.1080/09627251.2014.984541
- Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. *Social Semiotics*, 23 (2), 261-277. <http://dx.doi.org/10.1080/10350330.2013.777594>
- Phelps, A. & Watt, A. (2014). I shop online - recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation*, 11, 261-272. <http://dx.doi.org/10.1016/j.diin.2014.08.001>
- Robberson, S. J. (2017). *A bit like cash: understanding cash for bitcoin transactions through individual vendors* (Masters thesis). Retrieved from ProQuest Dissertations and Theses. (10607702)
- Singh, K. (2015). The new wild west: preventing money laundering in the Bitcoin network. *Northwestern Journal of Technology and Intellectual Property*, 37, 1-39. Retrieved from www.lexisnexis.com/hottopic/lnacademic
- Tor: 'the king of high-secure, low-latency anonymity'* (2013, Oct. 4). Retrieved from <http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity>
- Wenker, N. (2014). Online currencies, real-world chaos: the struggle to regulate the rise of Bitcoin. *Texas Review of Law and Politics*, 19 (1), 145-197. Retrieved from www.lexisnexis.com/hottopic/lnacademic