

UNIVERSITY OF CENTRAL OKLAHOMA

Edmond, Oklahoma

Jackson College of Graduate Studies

A Bit Like Cash:

Understanding Cash-for-Bitcoin Transactions Through Individual Vendors

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

In partial fulfillment of the requirements

For the degree of

MASTER OF SCIENCE IN FORENSIC SCIENCE

By

Stephanie Joy Robberson

Edmond, Oklahoma

2017

A Bit Like Cash:

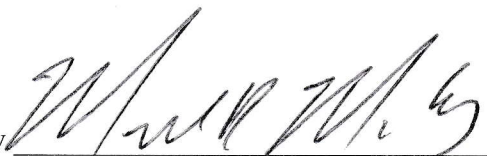
Understanding Cash-for-Bitcoin Transactions Through Individual Vendors

By: Stephanie Joy Robberson

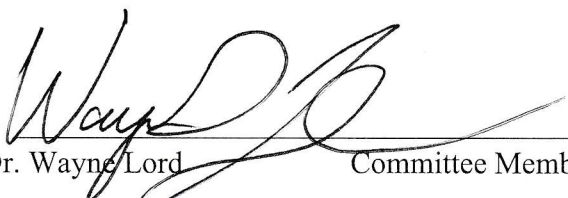
A THESIS

APPROVED FOR THE W. ROGER WEBB FORENSIC SCIENCE INSTITUTE

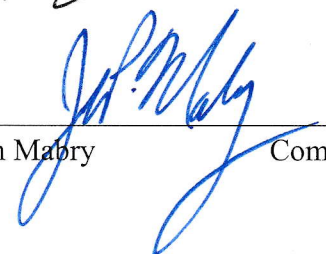
APRIL 2017

By 

Dr. Mark McCoy Committee Chair



Dr. Wayne Lord Committee Member



Dr. John Mabry Committee Member

TABLE OF CONTENTS

Abstract.....	5
Acknowledgements.....	6
INTRODUCTION.....	7
Statement of the Problem.....	8
Purpose of the Study.....	8
Research Questions.....	9
Significance to the Field.....	9
Limitations.....	10
Ethical Considerations.....	10
LITERATURE REVIEW.....	12
Bitcoin.....	12
<i>What is Bitcoin?</i>	12
<i>How Does Bitcoin Have Value?</i>	15
<i>Double-Spending and the 51% Problem</i>	16
<i>Who Uses Bitcoin, and How Do They Purchase It?</i>	17
Cryptocurrency and Crime.....	18
Silk Road Takedown.....	18
FinCEN Regulations for Money Transmitters.....	20
Wallet and Trading Privacy Policies.....	22
Bitcoin and Cash Trades.....	22
METHODS.....	25
Population.....	25
Data Collection.....	28
Measurement Instrument.....	30
Validity and Reliability.....	31
RESULTS.....	33
Demographic Data Results.....	33
FinCEN Knowledge and Compliance Results.....	37
Opinion Results.....	41
Open Ended Question Results.....	43
<i>Libertarian, and Proud of It</i>	43
<i>Government Control of Currency</i>	44
<i>Willing but Wary to Help Law Enforcement</i>	44
<i>Selling a Commodity, Not a Responsibility</i>	46
<i>Summary</i>	47
DISCUSSION.....	49
Limitations.....	57
Recommendations for Future Research.....	57

Conclusions.....	58
References.....	60

TABLE OF FIGURES

Figure 1. Bitcoin’s Blockchain Ledger.....	14
Figure 2. Bitcoin’s Pseudo-Anonymous Transaction Structure.....	14
Figure 3. Projection of Estimated Bitcoin to be Mined.....	16
Figure 4. Silk Road “Drugs” Page.....	19
Figure 5. Bitcoin’s Preferred Currency Exchange Options.....	23
Figure 6. Gender of Participants.....	33
Figure 7. Age Ranges.....	34
Figure 8. Ethnicity.....	34
Figure 9. Highest Level of Education.....	35
Figure 10. Total Household Income in 2016.....	36
Figure 11. Marital Status.....	36
Figure 12. Area of Employment Outside of Bitcoin Sales.....	37
Figure 13. Sales of Personally Mined Bitcoin.....	38
Figure 14. Websites Used to Advertise Bitcoin Sales.....	38
Figure 15. States in Which Vendors Sell Bitcoin.....	39
Figure 16. Registered as a Money Transmitter.....	39
Figure 17. Customer Information Recorded by Vendors.....	40
Figure 18. Opinions Survey Results.....	42

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.

Acknowledgements

This project would not have been possible without the guidance of Dr. Mark McCoy. Thank you for being open for questions at all times and direct with your advice. Your momentum for carrying out this research kept me focused on the end goal, and your confidence in the usefulness of this data and my abilities to collect and process it made this project not only feasible but fun. Thank you for your guidance and friendship.

Dr. Wayne Lord and Dr. John Mabry, members of this project committee, must be thanked for their work on this research as well. Dr. Lord, thank you for being my teaching mentor and challenging me to lead others when I did not have much faith in my ability to do so. Dr. Mabry, thank you for welcoming me into the FSI family from our first meeting to our frequent chats around the building. You two have made the FSI feel like home, and I am grateful for your wisdom, confidence, and warmth.

I would like to thank the Forensic Science Institute's faculty and staff for the many learning and leadership opportunities I have encountered. Thank you all for your willingness to lend advice, criticism, and kindness.

I would like to thank the strong women in my life who have challenged me to always do my best work by doing their best work. To friends from Beaumont, Baylor, and the FSI, thank you for your tenacity.

Finally, my family deserves all of the thanks I can give. To Dad, thanks for encouraging me to pursue a higher degree and for still loving me even though I live in Oklahoma. To Mom and MJ, thanks for your emotional support when I saw too many gory medicolegal photos. Thanks to my in-laws for making Oklahoma feel like home. And thank you to my husband Garrett for listening to me talk about Bitcoin for two years. Thank you all for your love and support.

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. Many 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.

Statement of the Problem

While there have been case law and computer science related studies about Bitcoin, no one has recorded data about the people who sell bitcoin for cash. When law enforcement officials work on bitcoin-related investigations, they have nothing to prepare a strategy for approaching cash-for-bitcoin vendors. It is also not known how cash-for-bitcoin vendors feel about law enforcement or if they have any willingness to assist with investigations about their customers. FinCEN rulings about Bitcoin require cash-for-bitcoin vendors to register as money transmitter services and keep records on customer transactions, but since these are cash sales, there is not an easy paper trail to hold vendors accountable for their FinCEN-mandated responsibilities. We do not know if vendors are aware of FinCEN rules, have registered through FinCEN, or record any identification information about customers.

Purpose of the Study

This study was designed to fill the gap in knowledge about cash-for-bitcoin vendors' personal demographic information, knowledge of and compliance with FinCEN regulations, and personal opinions about government control of currencies and working with law enforcement officials.

Research Questions

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?

Significance to the Field

Successful profiling can be attempted with a large pool of historical case data. There is currently no pooled data about the demographics of cash-for-bitcoin vendors. By contacting this group, the research community can learn what basic demographics these vendors share, if any. While the response pool for this project is entirely too small to make a reasonable profile of a cash-for-bitcoin vendor, this project is the first drop of demographic data for this group, and future studies with this survey in different parts of the country can help profilers see stronger demographic trends for this group.

Walking into any situation blindly is ill-advised for investigators. For law enforcement officials investigating customers of cash-for-bitcoin vendors, it is helpful to know how vendors feel about officers of the law. With a bit of background knowledge about the political ideals of this group, investigators can more easily plan an approach for getting their questions answered.

While FinCEN's ruling about digital currencies might be well-known to white collar crime investigators, it is unknown if cash-for-bitcoin vendors are familiar with or follow these laws. Information from this survey could help FinCEN understand how well vendors are receiving and understanding digital currency laws.

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.

Limitations

This study had a small sample size gathered as a convenience sample through available cash-for-bitcoin advertisements on LocalBitcoins.com, Craigslist, and Backpage. In any instance of survey research, there is no way to verify that answers given to the researcher are accurate, especially questions about the respondent's opinion.

Ethical Considerations

Before any cash-for-bitcoin vendors were contacted, this project was submitted to and approved by the University of Central Oklahoma's Institutional Review Board (IRB). Survey settings were manipulated to block the IP addresses of respondents to ensure anonymity. All data collected in this project was stored in password-protected accounts accessible to only the

researcher. Data files will be securely deleted upon completion of this project.

Literature Review

Introduction

Although it has been used for legitimate investments and trade, Bitcoin, a pseudo-anonymous digital currency, has been embraced by criminals. The structure of the currency is a bit abstract and takes explanation for law enforcement officials to know what they are up against. The Financial Crimes Enforcement Network (FinCEN) has issued federal regulations for Bitcoin money transmitter services, but there is no way of knowing if cash-for-bitcoin vendors are aware of these regulations or are following these rules. This project surveyed cash-for-bitcoin vendors to determine their personal demographic information, knowledge of and compliance with FinCEN rules, and personal opinions regarding government control of currency and assisting law enforcement.

The literature review will explain what Bitcoin is and how it functions technologically and economically. The Silk Road case will be explored to explain how Bitcoin has been used for criminal transactions. FinCEN regulations will be explained along with weaknesses within these regulations for law enforcement investigating Bitcoin-funded criminal activity.

Bitcoin

What is Bitcoin?

Of all cryptocurrencies on the market, none have achieved the popularity or publicity of Bitcoin. Created in 2009 by an anonymous coder and mathematician under the pen name Satoshi Nakamoto, Bitcoin is an international digital currency (Dostov & Shust, 2014). Nakamoto created Bitcoin out of systemic frustration. The world economy was sinking, and Nakamoto along with other currency theorists felt that traditional banking systems could not be trusted.

From a design standpoint, Nakamoto's Bitcoin is described as "breathtaking in both its technological complexity as well as its fundamental simplicity" (Wenker, 2014, p. 146). The complexity is easily perceived by Bitcoin novices reading up on the topic: almost all publications about the cryptocurrency devote pages worth of explanations of the intricacies of Bitcoin system architecture. At its essence, Bitcoin operates as a peer-to-peer network of programmers who solve complicated numerical puzzles to make and record transactions.

In Nakamoto's description of Bitcoin, he states that it is a "system based on cryptographic proof instead of trust" (Wenker, 2014, p. 147). To establish that cryptographic proof, every transaction of bitcoin must be verified by the network. When coinholders make a transaction, the entire network receives word that one user has spent x amount of bitcoins, and another user is to receive x amount of bitcoins in the form of a numerical puzzle. From there, "miners" race to solve this puzzle through a trial-and-error, entirely digital process. When a lucky miner solves the puzzle, proof of work is submitted to the network as a new block and verified. The miner receives a certain number of bitcoins as payment for their work, thus incentivizing everyone in the network to put forth the computing power to solve the algorithms for all transactions (Maurer, Nelms, & Swartz, 2013). The number of bitcoins in the miner's reward fluctuates with the Bitcoin market, but as of January 2017, the reward number is 12.5 bitcoins.

The transaction is added to the "blockchain" which acts as a ledger for all bitcoin transactions since Nakamoto's "Genesis block"- the first fifty bitcoins introduced (Maurer et al., 2013, p. 265). The blockchain contains limited information about transactions (Figure 1).

Figure 1

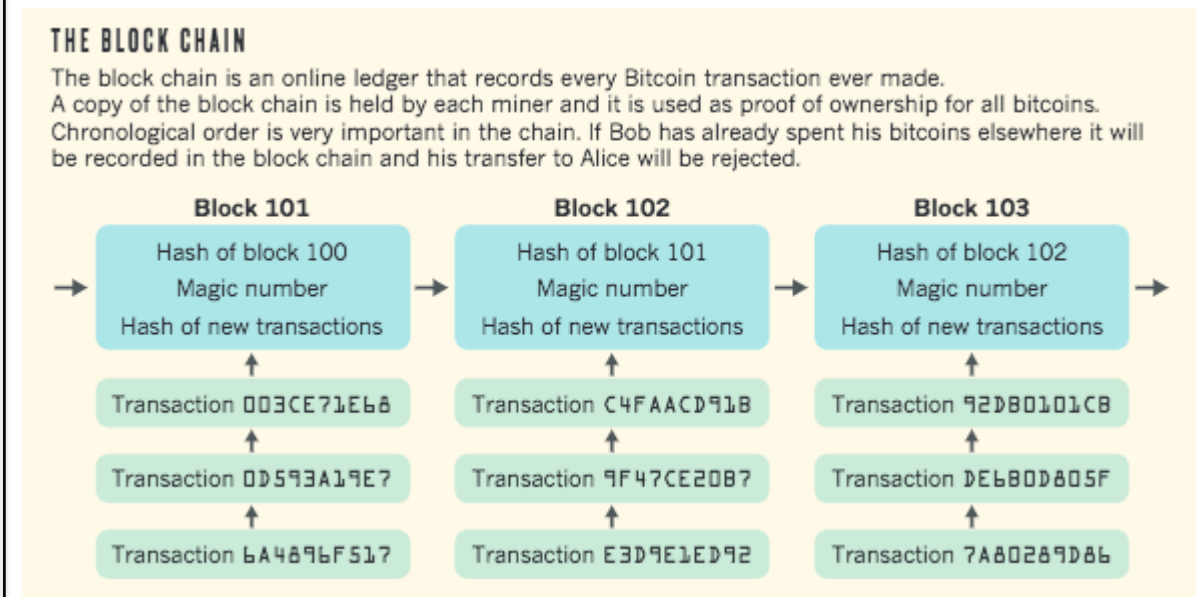


Figure 1. Explanation of Bitcoin’s blockchain ledger. From “Bitcoin and Beyond,” by A.

Extance, 2015, *Nature*, 526 (7571), p. 22. Copyright 2015 by MacMillan Publishers Limited.

Bitcoin is often referred to as a “pseudo-anonymous” cryptocurrency (Figure 2) because the blockchain lists every single bitcoin transaction but does not record a name of the giver or receiver of bitcoins (Wenker, 2014, p. 154).

Figure 2



Figure 2. Explanation of Bitcoin’s pseudo-anonymous transaction structure. The example in red shows a traditional non-private transaction, while the example in green illustrates what information appears in Bitcoin’s blockchain. From “Excellent Privacy,” retrieved from <https://bitcoin.org/en/bitcoin-core/features/privacy>. Copyright 2015 by Bitcoin.org.

How Does Bitcoin Have Value?

While physical mining can unearth precious metals, Bitcoin miners do not have heaps of gold to show for their labors. Bitcoin miners use computer power to solve algorithms generated by Bitcoin transactions.

Typically, currency is backed by gold or the federal promise that the currency will be accepted. While digital currencies lack this physical valuer, two things give value to Bitcoin. First, Nakamoto set a creation cap on this cryptocurrency (Figure 3). A little less than 21 million bitcoins will ever be created (Maurer et al., 2013). This upper bound acts like a perfect gold-standard economy and staves off inflation. In fact, as miners get closer and closer to the 21 million bitcoin cap, smaller Bitcoin rewards will be given for solving block algorithms and each bitcoin will be worth more within the limiting supply (Maurer et al., 2013).

Secondly, energy required to run miners' computer programs is seen as the labor resource behind the currency. As the 21 million bitcoin cap approaches, transaction algorithms will become more complex, requiring more energy and stronger computing power to mine (Maurer et al., 2013). This will only add value to the currency, but it will favor large Bitcoin mining operations over the individual enthusiast.

Figure 3

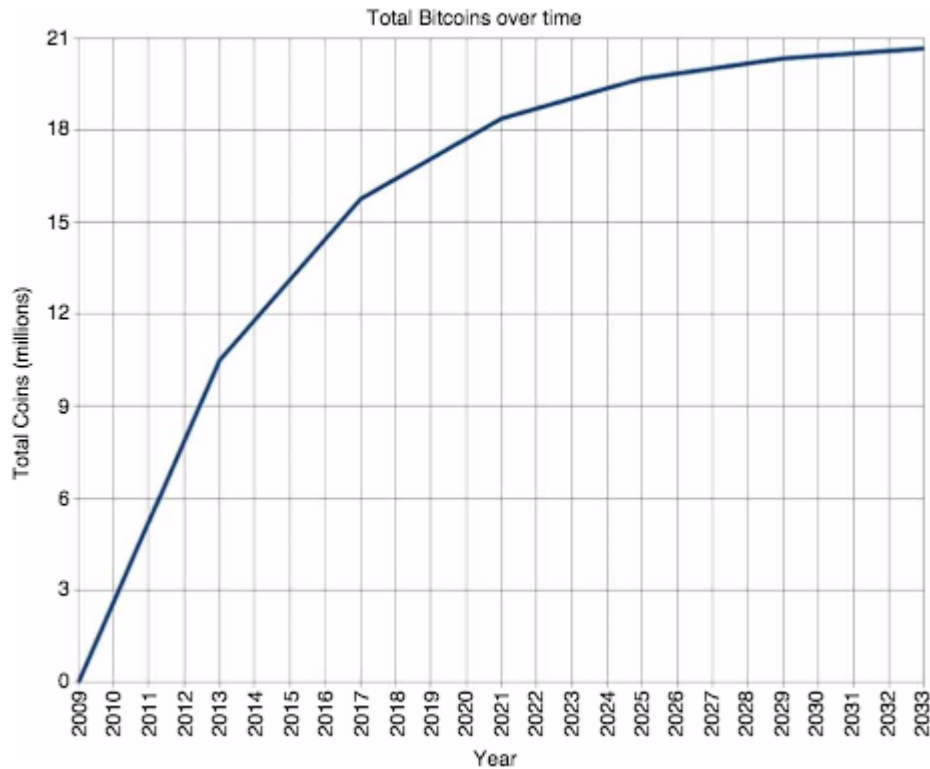


Figure 3. Projection of estimated Bitcoin to be mined over time. From ““When Perhaps the Real Problem is Money Itself!?: The Practical Materiality of Bitcoin,” by B. Maurer, T. Nelms, and L. Swartz, 2013, *Social Semiotics*, 23 (2), p. 271. Copyright 2013 by Taylor & Francis.

Double-Spending and the 51% Problem

A common theoretical issue with digital currency is how to prevent users from using the same denomination twice. In a cash transaction, the buyer hands physical dollars to the seller. From that point, the buyer no longer possesses those dollars. They cannot be spent by the buyer again.

In a digital transaction, developers must ensure that their currency cannot be traded more than once. Bitcoin solves the double-spending problem by operating as a “decentralized verification system” where all computers within the network authenticate a transaction and add it to the blockchain (Maurer et al., 2013, p. 264). It is universally recognized through the blockchain ledger that a buyer spent those bitcoins and the bitcoins were transferred to a seller, much like taking a \$5 bill out of a wallet, giving it to a seller, and putting the \$5 bill into his or her wallet.

However, Bitcoin’s cash-like system is not perfect, and double spending could happen. It takes 51% of Bitcoin’s total user computing power to consistently verify transactions. If 51% of the computer power supporting Bitcoin was owned by one group, the system could be compromised (Singh, 2015).

The 51% Problem has not yet happened, but it would not be surprising for a group to reach that threshold. When Bitcoin debuted in 2009, miners were commonly “tech geeks and dedicated libertarians” operating on personal computers for reasons of personal amusement or disdain for government regulated currency (Wenker, 2014, p. 159). As more bitcoins are generated, more computing power is needed to solve more complex algorithms. Now, large professional organizations have the largest share of the Bitcoin mining market since they can afford advanced hardware needed to mine efficiently (Wenker, 2014).

Who Uses Bitcoin, and How Do They Purchase It?

Miners are not the sole users of Bitcoin. In fact, most users of Bitcoin are not miners: web geeks, entrepreneurs, and investors play a big role in the Bitcoin market. In 2014, the Massachusetts Institute of Technology (MIT) Bitcoin Club gave all 4,500 undergraduates \$100

of Bitcoin each (Cusumano, 2014). Entrepreneurs such as Richard Branson of Virgin Atlantic and Jerry Yang of Yahoo have funded Bitcoin wallet startups (Cusumano, 2014).

Non-miners can get Bitcoin through an exchange provider. International exchange providers are listed on Bitcoin's website. Through these outlets, buyers can connect bank accounts and/or credit cards to trade fiat money for Bitcoin.

Another route for obtaining Bitcoin is to trade cash to a miner or Bitcoin trader. Websites such as LocalBitcoins.com allow users to search for Bitcoin merchants in their vicinity. Craigslist and Backpage also have advertisements for cash-for-Bitcoin transactions.

Cryptocurrency and Crime

Silk Road Takedown

With any cash-like or pseudo-anonymous payment system, there is bound to be a seedy underworld of users seeking to covertly cover criminal tracks. Bitcoin gained notoriety in 2013 with the takedown of the Darknet site Silk Road (Figure 4). Silk Road was an online marketplace for illegal substances including cocaine, cannabis, ecstasy, heroin, and amphetamines (Maras, 2014).

To access Silk Road or any shifty site in Darknet, users downloaded Tor, a "privacy-enhancing application originally created by the USA Naval Research Laboratory" (Maras, 2014, p. 22). A 2013 NSA report described Tor as "the King of high secure, low latency Internet Anonymity" with "no contenders for the throne in waiting" ("Tor: The King," 2013). Tor was created with the intention of aiding Internet users in countries with strong Internet censorship policies, but the program has gained many fans in the criminal sector.

Silk Road as an online marketplace operated much as Etsy does: individual vendors listed their wares, product information, shipping details, and price and received feedback for

transactions. All Silk Road transactions were paid in Bitcoin through an escrow system. When a buyer made a purchase, the buyer's bitcoins entered a Silk Road escrow account, and when the seller shipped the purchased item, the bitcoins were transferred from the escrow account to the seller (Maras, 2014). To ensure anonymity within the escrow system, Silk Road created a code tumbler that further muddled the already complex Bitcoin wallet address codes that made it “nearly impossible to link...[a] payment with any coins leaving the site” (Maras, 2014, p. 23).

Figure 4

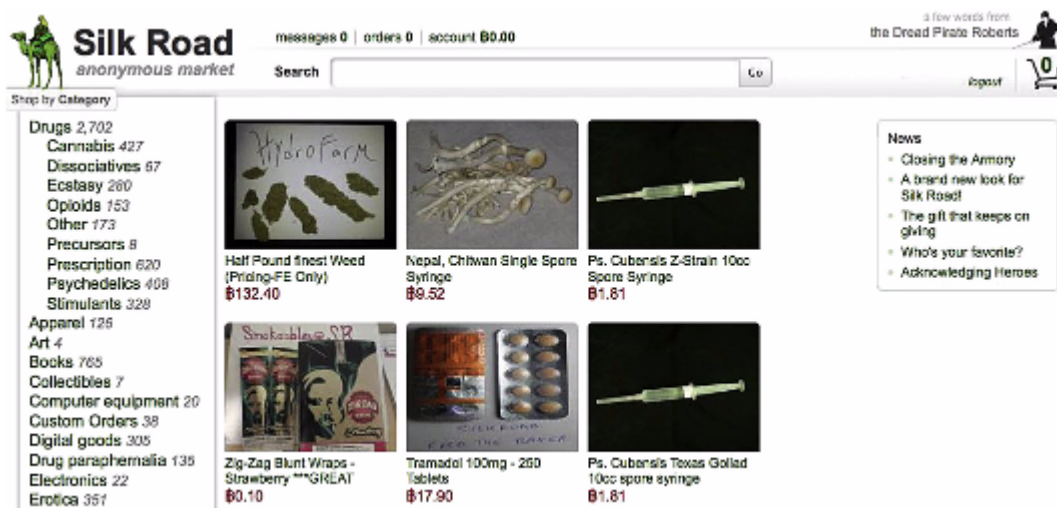


Figure 4. Screenshot of the “Drugs” page on Silk Road. From “I Shop Online - Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia,” by A. Phelps and A. Watt, 2014, *Digital Investigation*, 11, p. 267. Copyright 2014 by Crown Copyright.

Silk Road enjoyed relative secrecy until 2011 when *Gawker* released an article called “The Underground Website Where You Can Buy Any Drug Imaginable” (Wenker, 2014). With such an attention-grabbing title, news of the marketplace spread quickly, and two weeks after publication, Senators Chuck Schumer and Joe Manchin sent an open letter to the US Attorney

General demanding the takedown of Silk Road and “the untraceable peer-to-peer currency known as Bitcoins” involved in all transactions (Wenker, 2014, p. 165).

This launched a full-scale federal investigation of Silk Road that resulted in the arrest of the “Dread Pirate Roberts” Ross Ulbricht, the site’s administrator. He was charged in Baltimore with “knowingly and unlawfully combined, conspired, confederated and agreed with others...to distribute and possess with intent to distribute controlled substances and attempted murder of a former employee” (Maras, 2014, p. 23). In New York, he was charged with violating narcotics laws, money laundering, computer hacking, “conspiracy to murder a witness; and continuing criminal enterprise” (Maras, 2014, p. 23). Following investigation of Silk Road, the site was shut down, and law enforcement seized Ulbricht’s personal bitcoins and those owned by the website for a total of 174,000 bitcoins (Wenker, 2014). Today, that amount equals roughly \$201,817,380 USD.

FinCEN Regulations for Money Transmitters

Unsurprisingly, the publicity surrounding Silk Road’s takedown gave Bitcoin a bad reputation as a currency only for criminals. A 2012 FBI bulletin warned that if Bitcoin’s popularity grew, it could become an “increasingly useful tool for various illegal activities beyond the cyber realm,” and since Bitcoin operates without a central authority, “law enforcement faces difficulties detecting suspicious activity, identifying users, and obtaining transaction records” (Wenker, 2014, p. 167).

However, the FBI notes that “law enforcement may be able to take advantage of the nexus at which criminals convert their Bitcoins into fiat currency” (Wenker, 2014, p. 167). To take advantage of this data, the Financial Crimes Enforcement Network (FinCEN) of the US

Treasury Department has issued and drawn attention to two important measures regulating reporting requirements for digital currencies.

Firstly, FinCEN has required Bitcoin transmitter services to register as money transmitters. The legal requirements for Bitcoin exchanges decree that “exchangers of virtual currencies must register with FinCEN, and institute certain recordkeeping, reporting and [Anti-Money Laundering (AML)] program control measures” (Kirby, 2014, p. 1). This law puts the onus on currency exchangers to practice good record keeping policies on all users changing Bitcoin for fiat money or vice versa. Because of this, some Bitcoin transmission services now require a government issued ID to open an account or require bank account and routing numbers to facilitate currency trades. This applies to large-scale operations as well as individual miners who trade Bitcoin. Under this rule, miners who use personally mined bitcoins to purchase goods or services are not required to report to FinCEN, but large-scale operations and individual miners who trade Bitcoin for fiat money must register as money transmitters (Kirby, 2014).

Secondly, FinCEN brought attention to how the Bank Secrecy Act (BSA) applies to Bitcoin. The BSA was enacted in 1970 to end money laundering through banks and other financial institutions (Singh, 2015). It requires financial institutions to “disclose the identities of parties to transactions in excess of \$10,000 in Currency Transaction Reports (CTRs)” (Singh, 2015, p. 5). Additionally, the BSA mandates that financial institutions file Suspicious Activity Reports (SARs) “for suspected-illegal transactions and implement anti-money-laundering programs” (Singh, 2015, p. 5). Building on the BSA, the USA Patriot Act of 2001 makes “operating an unlicensed money-transmission business a felony” (Singh, 2015, p. 5).

Wallet and Trading Privacy Policies

The two measures above have made it nearly impossible to trade fiat money for Bitcoin online without leaving some kind of identification trail. While this steers away from Bitcoin's initial goal of having a digital cryptocurrency unregulated by the government, it certainly helps law enforcement officials and the IRS track suspicious transactions and potential money laundering schemes. Bitcoin users who trade fiat money for the cryptocurrency can potentially leave an identification trail in two places: the money transmission service and the Bitcoin wallet.

An examination of privacy policies for Bitcoin exchanges listed on Bitcoin's website shows that the exchanges will disclose personal information about users if subpoenaed or otherwise required by law to do so. Some Bitcoin wallets such as Coinbase are connected to fiat currency exchanges. Under the privacy policy in place for the exchange, law enforcement can subpoena these companies for wallet transaction information as well as currency exchange information.

However, Bitcoin users who are serious about privacy and are computer literate opt for desktop, hardware, or even paper wallet services that do not require sharing personal identification information with any party. They must only supply a wallet address for transactions, and they can change that wallet address with each transaction to stay under the radar.

Bitcoin and Cash Trades

It is pretty easy for federal agencies to get large-scale Bitcoin currency transaction services to follow reporting regulations. If these companies are large enough or strong enough to make it onto Bitcoin's website as exchange companies, they are exposed in a convenient list for FinCEN to verify compliance with regulations (Figure 5).

Figure 5

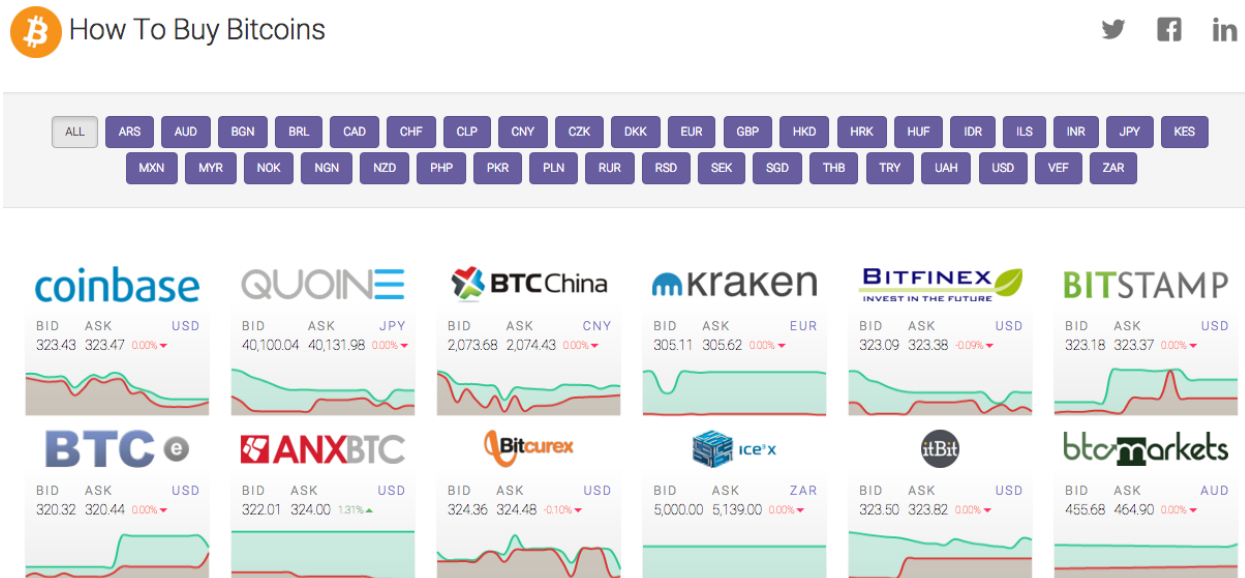


Figure 5. Screenshot of popular currency exchange operations. One hundred and five are listed.

From “How to Buy Bitcoins.” Accessed 22 Nov. 2015 from <http://howtobuybitcoins.info/>

Federal law mandates that even small-time miners who trade Bitcoin for fiat currency must register as a money transmission service through FinCEN (Singh, 2015), but FinCEN is not easily able to check that these traders are up to code.

FinCEN may have some luck obtaining identification information through cash-for-Bitcoin marketplaces such as LocalBitcoins.com. Through this website, users can search for miners or Bitcoin transmitters in a geographic area. While the privacy policy for this website states LocalBitcoins.com will share registered user information with law enforcement if subpoenaed, not all trades on this website require user registration.

Summary

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.

Methods

Introduction

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.

The following research questions were addressed in this study:

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?

Population

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. The convenience sampling method works well with small populations in descriptive studies. Too little was known about cash-for-bitcoin vendors to build a large and diverse enough group for random sampling. Therefore, a convenience sampling method was chosen to carry out this study.

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 I had to select the Map option 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 were recorded in a master Excel spreadsheet for each user. 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, 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, 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 the following blurb to the LocalBitcoins.com seller message boards:

Stephanie Robberson, a grad student at the University of Central Oklahoma, is conducting a descriptive study to gain understanding of cash-for-Bitcoin vendors in Oklahoma and surrounding states. This will provide insight for future human and drug trafficking cases involving Bitcoin. Responses will not collect identifying information unless you wish to share it. Link is

https://uco.co1.qualtrics.com/SE/?SID=SV_e5NYCDo6rJhnrvf or people can call or text her at _____. Email is _____.

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

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 them that said:

Hi, this is Steph Robberson. I'm a grad student at the University of Central Oklahoma researching Bitcoin. Do you have a few minutes to talk about your experience?"

If a positive response was received, the following text message was sent:

Thank you for getting back to me. I developed a survey to learn more about selling Bitcoin. You can take it online or we can talk through it by call or text. Link here:
https://uco.co1.qualtrics.com/SE/?SID=SV_e5NYCDo6rJhnrvf.

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. The University of Central Oklahoma provides free access to Qualtrics services for UCO students and faculty, and all surveys through the university have a header with the UCO logo. This helps legitimize the project and foster confidence in respondents that their data will be protected, not turned over to law enforcement officials.

When respondents clicked the survey link, the first page of the survey contained the following message:

Thank you for taking the time to participate in this study. This is a descriptive study designed to gain understanding of the demographics, practices, attitudes, and beliefs of cash-for-Bitcoin vendors in Oklahoma and the surrounding states. There are no legal risks in taking this survey as responses will not include identification information.

Findings will add to the limited knowledge base concerning people who sell Bitcoin for cash and provide insight for future investigations involving human and drug trafficking.

This project has been approved by the University of Central Oklahoma Institutional Review Board, #16197.

Participation in this study is purely voluntary. If you feel uncomfortable, you can end the survey at any time. The survey will take 5 to 10 minutes to complete. If you wish to continue, please click the yellow button below.

Please direct questions to:

Graduate Student: Stephanie Robberson sparks10@uco.edu

Faculty Advisor: Mark McCoy mmccoy@uco.edu

UCO IRB: irb@uco.edu

Project Validation: <https://www.uco.edu/forensics/Research/index.asp>

By clicking the yellow button to proceed with the survey, participants consented to share their data for this project. Responses were recorded within Qualtrics response database in the researcher's password protected user account.

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. In all cases of phone interviewing through text messaging or phone calls, participants were told that participation in the study was purely voluntary and they could quit at any time. Protection of data and the purpose of the project were discussed before proceeding with interviews. Notes from these interviews were created in a password protected account for Google Docs and stored within Google Drive.

Measurement Instrument

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 following statements were listed:

1. Paper currency should be federally regulated.
2. Digital currency should be federally regulated.
3. I trust the federal government to handle Bitcoin exchange information appropriately.
4. I trust law enforcement will handle Bitcoin exchange information appropriately.
5. I would contact law enforcement if my Bitcoin buyer told me they planned to use the currency on an illegal purchase.
6. If law enforcement approached me about a case involving my customer, I would provide general descriptive information.
7. If law enforcement approached me about a case involving my customer, I would provide specific identifying information.

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.

Validity and Reliability

The measurement instrument for this project is a survey created by the researcher, and this project is the first time cash-for-bitcoin vendors have taken this survey. There was no pilot study for this survey; if anything, this is the pilot study. The researcher’s Co-PI and thesis project committee, all doctoral-level researchers, reviewed and approved the survey. Additionally, the University of Central Oklahoma’s Institutional Review Board (IRB) reviewed and approved the survey used for this project.

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.

Results

Findings from this study include data from 27 online survey responses, two oral semi-structured interviews through phone calls, and one semi-structured interview through text message from cash-for-bitcoin vendors in Oklahoma, Texas, Missouri, Arkansas, Kansas, Colorado, and New Mexico (N=30).

Demographic Data Results

Demographic questions revealed that 86.67% of respondents were male, and 13.33% of respondents were female (Figure 6). No respondents were under the age of 18. 26.67% of respondents were between the ages of 18 and 24, 30% between 25 and 34 years old, 26.67% between 35 to 44 years old, 10% between 45 to 54 years old, 3.33% between 55 and 64 years old, and 3.33% were age 65 or older (Figure 7).

Figure 6- Gender of Participants

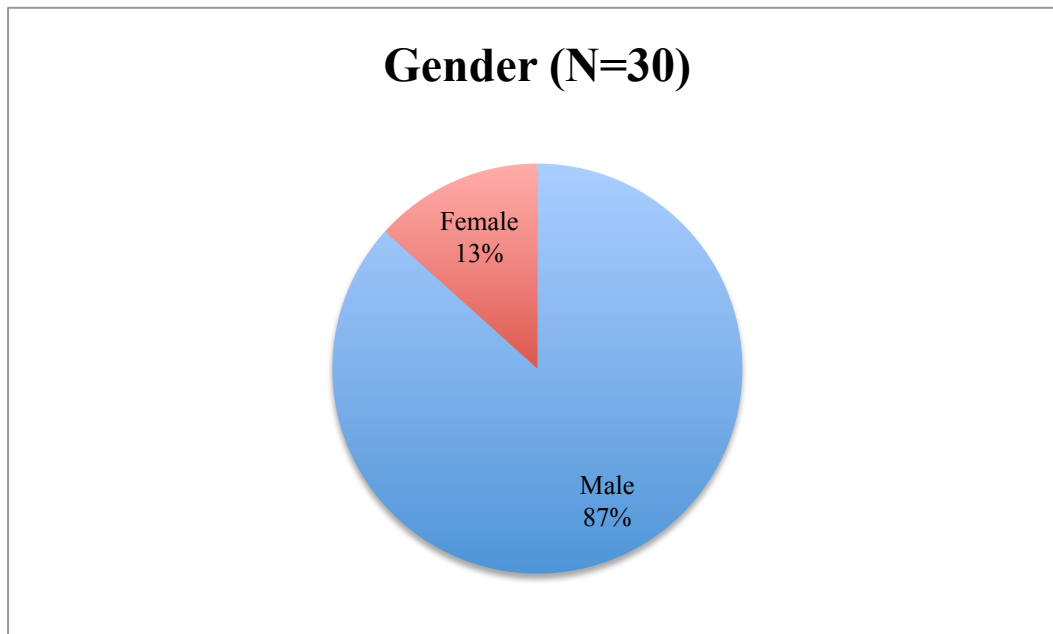
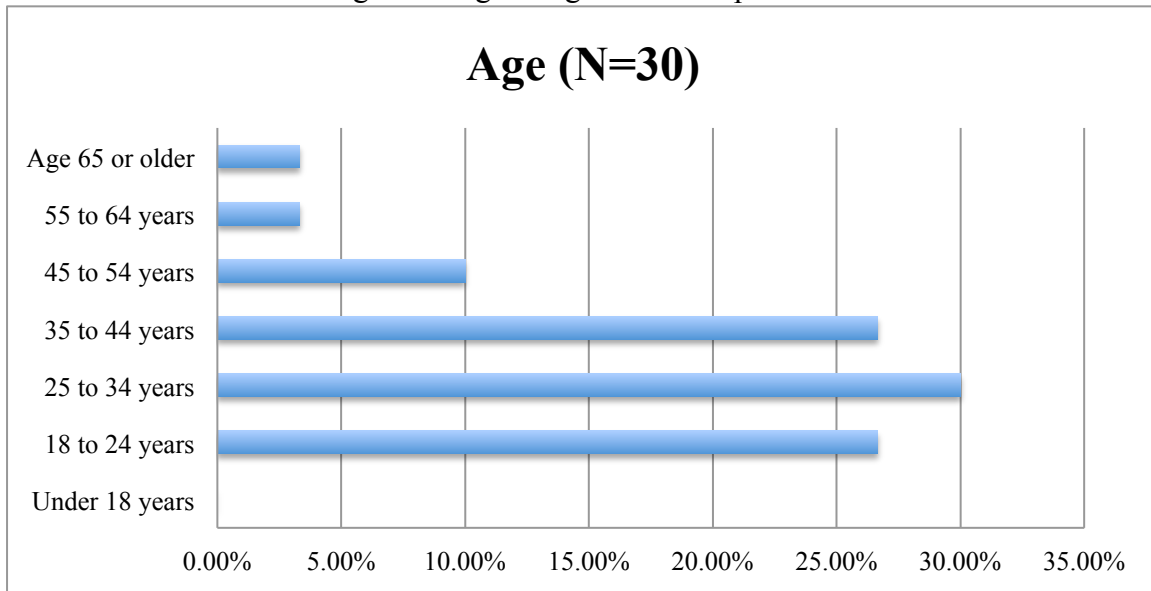
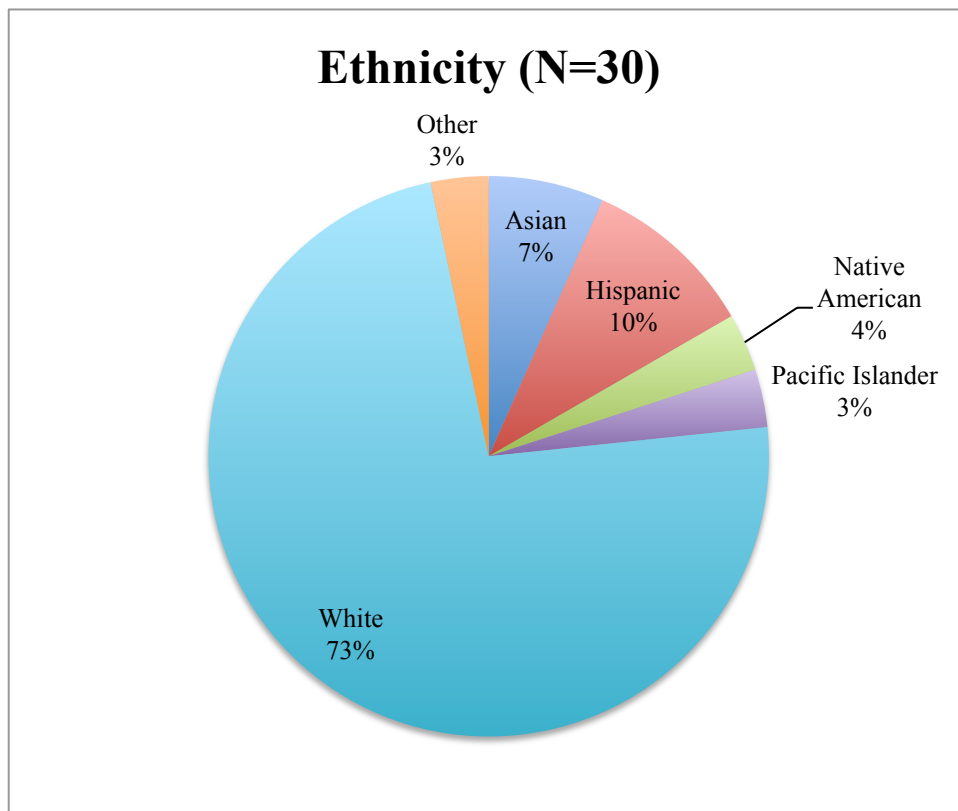


Figure 7- Age Ranges of Participants



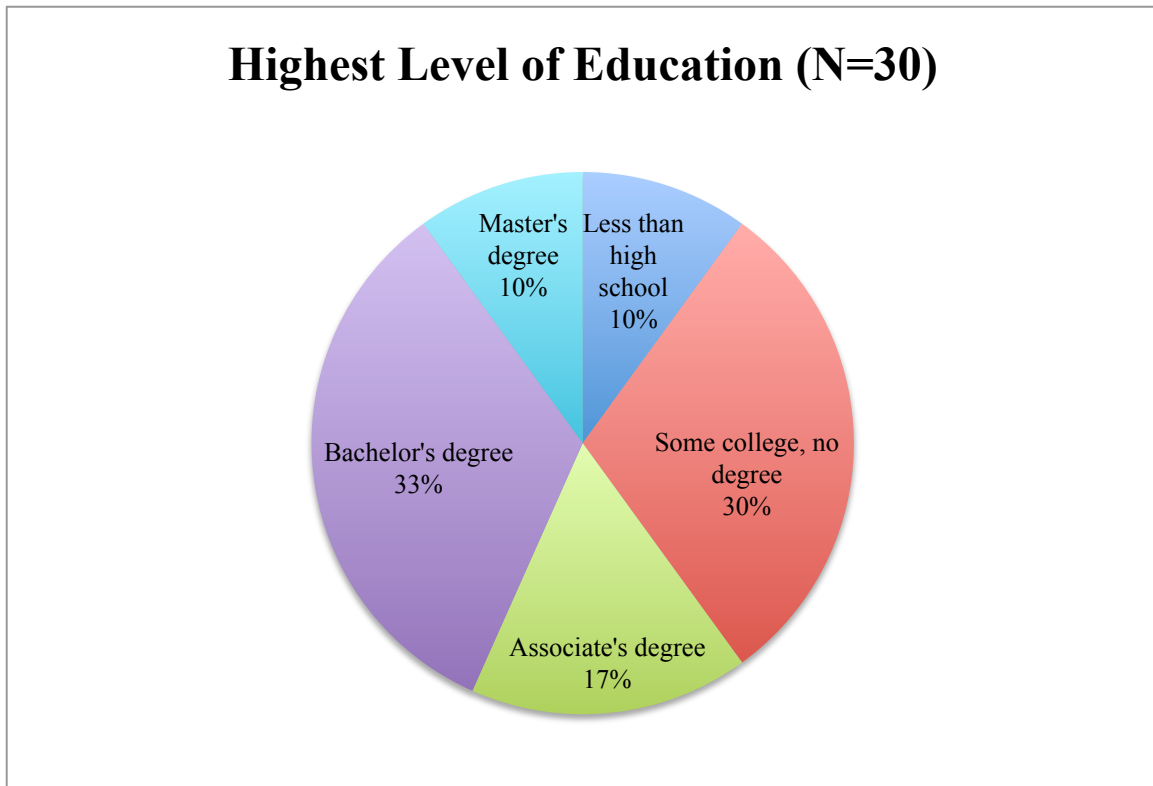
No respondents were African American. 73.33% were White, 10% were Hispanic, 6.62% were Asian, 3.33% were Native American, 3.33% were Pacific Islanders, and 3.33% were labeled as “Other” and wrote in “Brown/Arabic” as their ethnicity (Figure 8).

Figure 8- Ethnicity of Participants



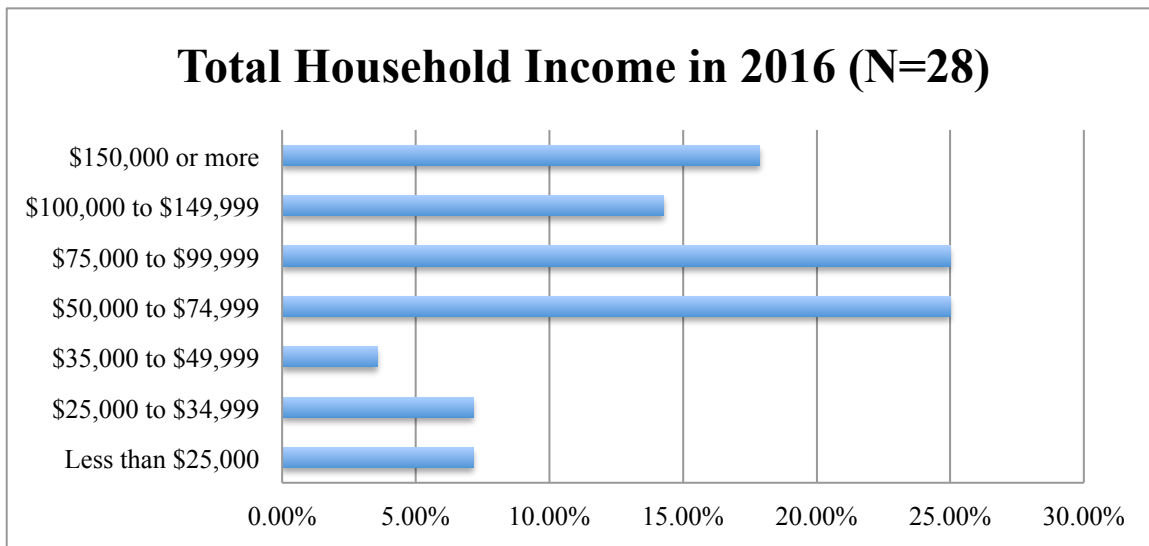
10% of respondents did not complete high school. 30% took some college classes but did not earn a degree. 16.67% of respondents earned an Associate's Degree, 33.33% earned a bachelor's degree, and 10% earned a master's degree (Figure 9). Zero respondents completed a doctoral-level degree.

Figure 9- Highest Level of Education



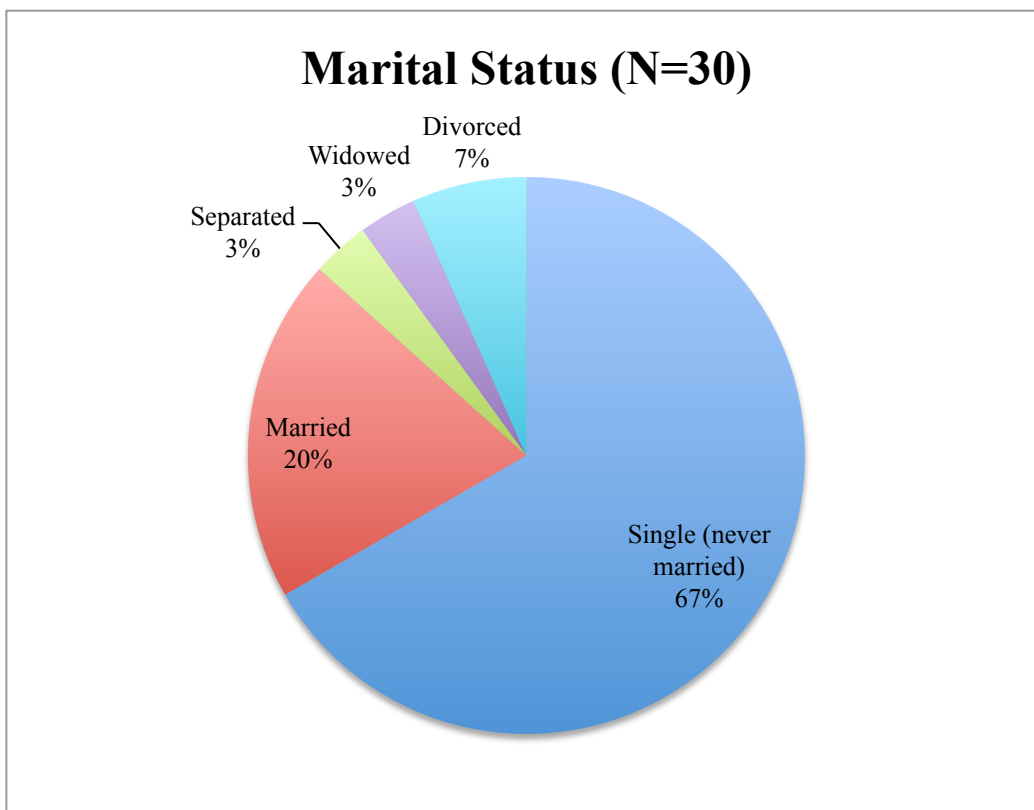
7.14% of respondents reported earning a household income of less than \$25,000 in 2016. 7.14 % earned between \$25,000 and \$34,999, 3.57% earned between \$35,000 and \$49,999, 25% earned between \$50,000 and \$74,999, 25% earned between \$75,000 and \$99,999, 14.29% earned between \$100,000 and \$149,999, and 17.86% earned \$150,000 or more (Figure 10).

Figure 10- Total Household Income in 2016



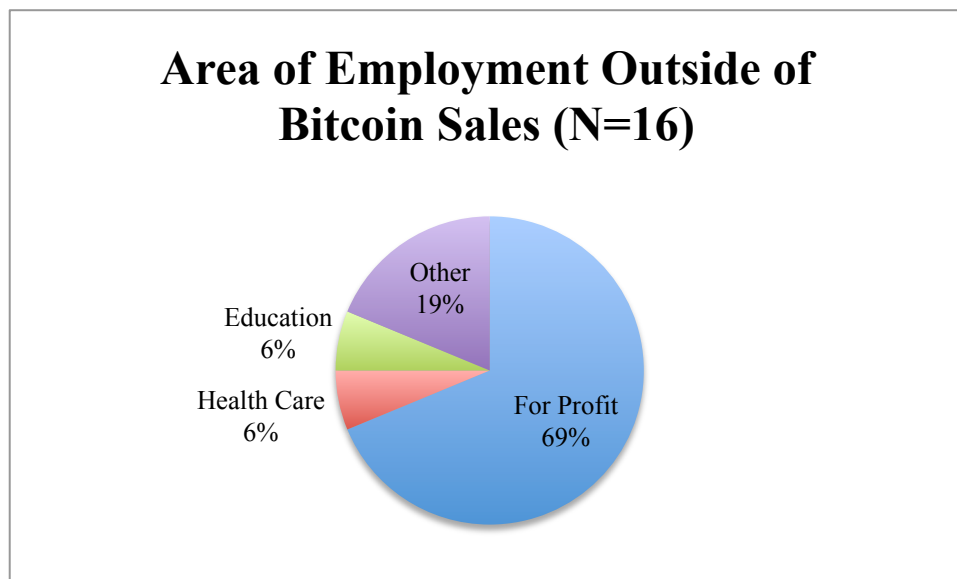
67.67% of survey participants were single (never married). 20% were married, 3.33% were separated, 3.33% were widowed, and 6.67% were divorced (Figure 11).

Figure 11- Marital Status



54.84% of respondents have a job outside of their cash-for-bitcoin business, and 45.16% do not. Of those who do have another job, 68.75% work for a for-profit company, 6.25% work in the health care industry, 6.25% work in education, and 18.75% work in a different field. Respondents who selected the “other field” option typed in they are a “business owner,” “self employed,” or provide “computer consulting.” Zero participants listed careers with nonprofits or the government (Figure 12).

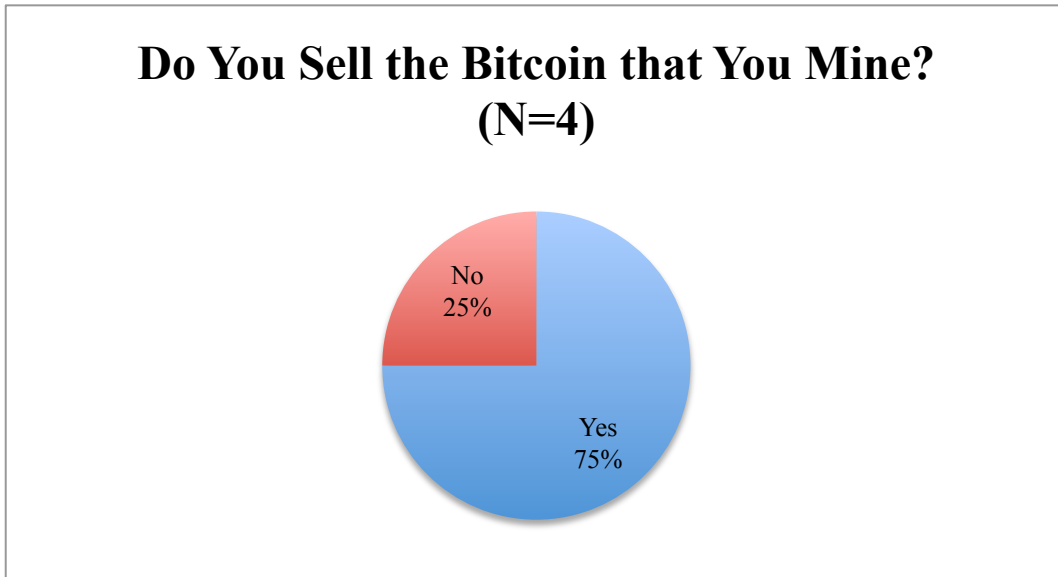
Figure 12- Area of Employment Outside of Bitcoin Sales



FinCEN Knowledge and Compliance Results

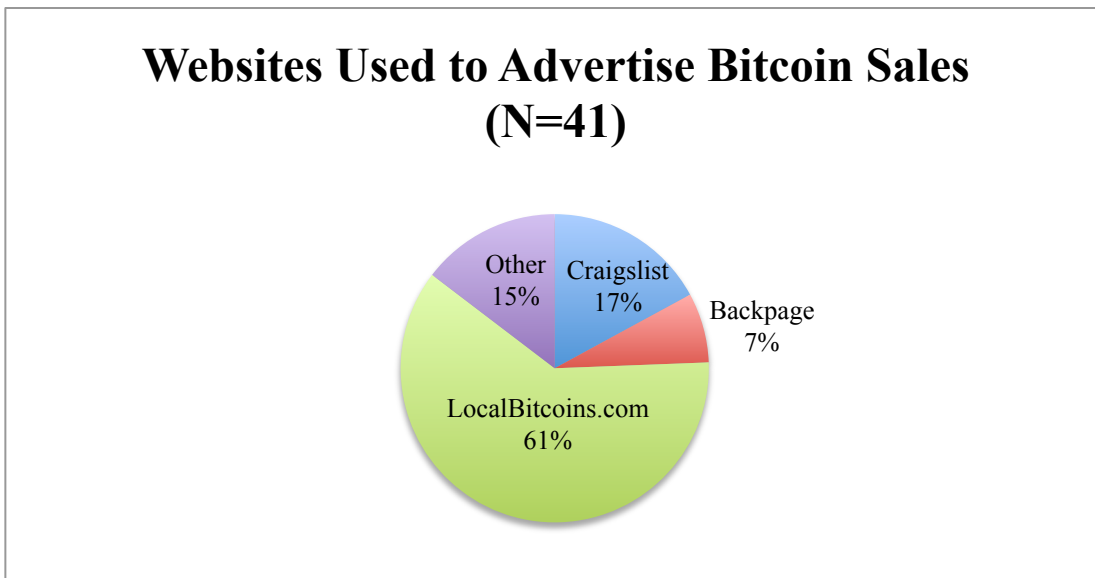
A majority of cash-for-bitcoin vendor participants, 84.62%, do not mine their own bitcoin. Only 15.38% mine their own bitcoin. Of the vendors who do mine their own bitcoin, 75% sell the bitcoin that they mine, and 25% do not sell the bitcoin that they mine (Figure 13).

Figure 13- Sales of Personally Mined Bitcoin



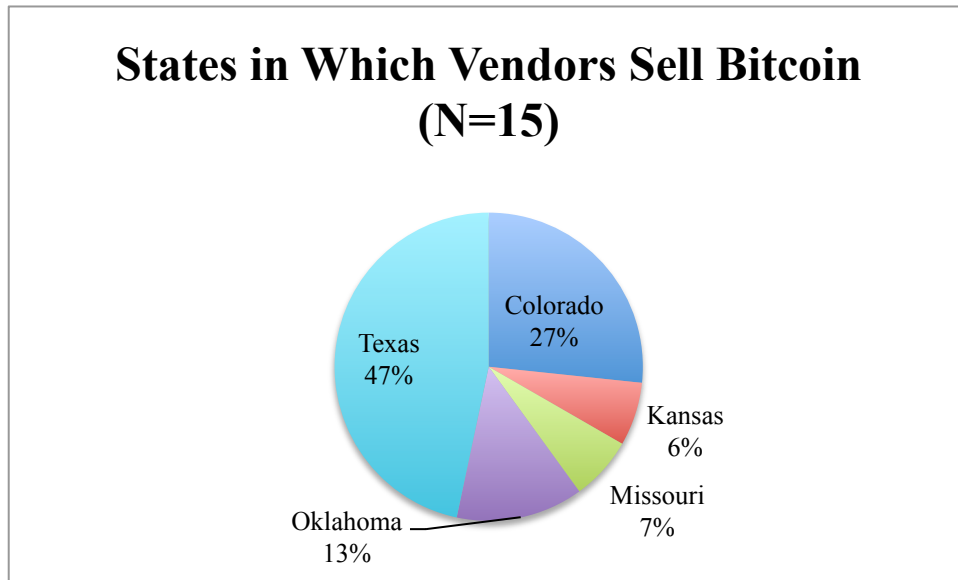
26.92% of respondents use Craigslist to advertise bitcoin sales. 11.54% use Backpage, 96.15% use LocalBitcoins.com, and 23.08% selected “Other” to say they use a different website. Other reported websites used to advertise bitcoin include Kijiji, calssifieds, Paxful, Bitquick, Bitsquare, Mycelium, and utxo.ux (Figure 14).

Figure 14- Websites Used to Advertise Bitcoin Sales



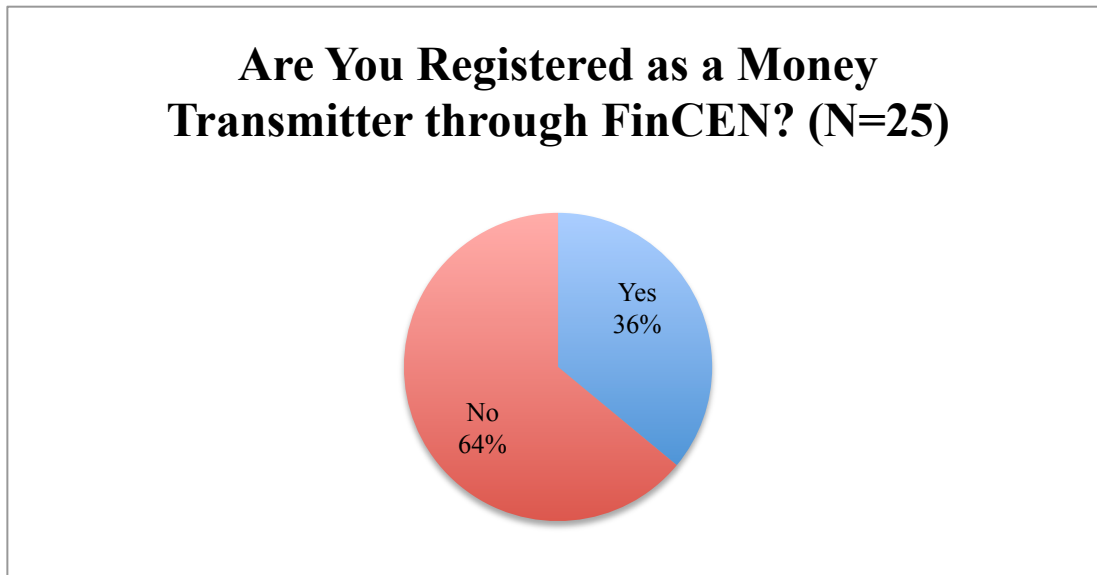
46.67% of respondents sell bitcoin in Texas. 26.67% sell in Colorado, 13.33% sell in Oklahoma, 6.67% sell in Kansas, 6.67% sell in Missouri. Zero respondents replied from Arkansas and New Mexico (Figure 15).

Figure 15- States in Which Vendors Sell Bitcoin



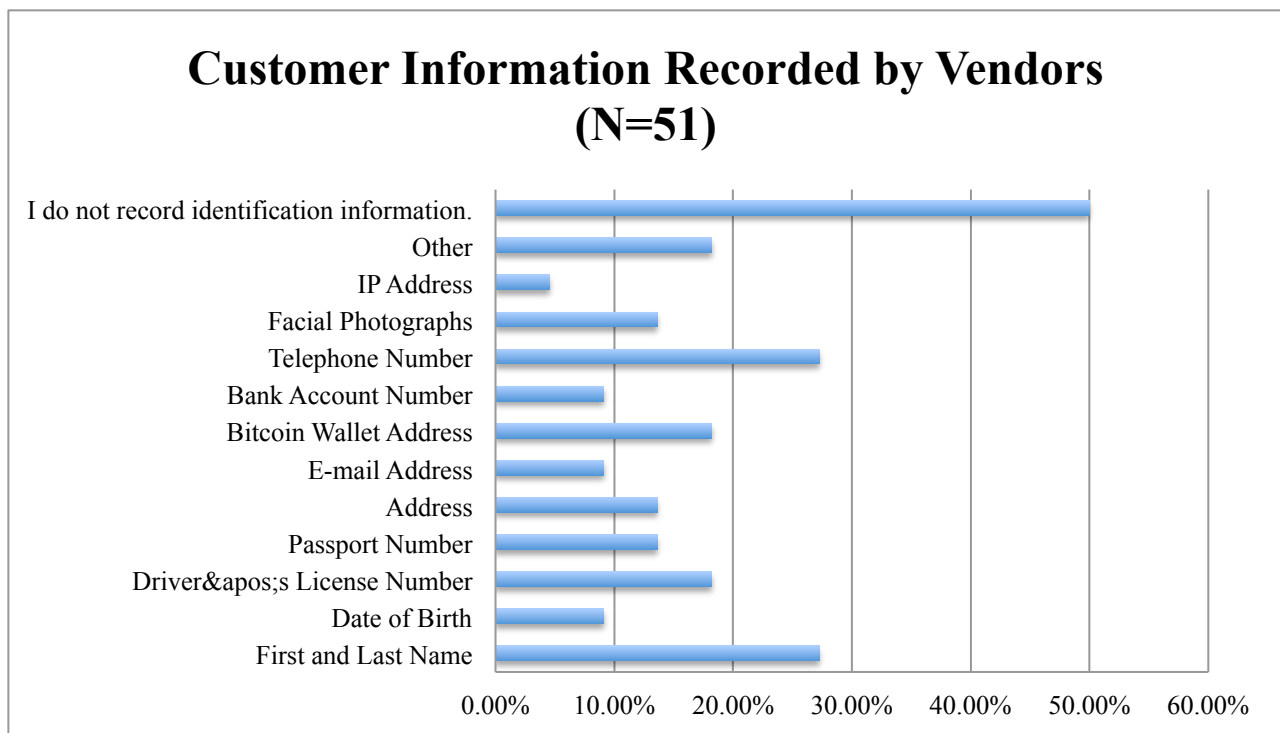
In regard to federal regulations concerning bitcoin, 80% of respondents are aware of federal regulations concerning the transmission of bitcoin. 20% are unaware of these laws. 36% of respondents are registered as money transmitters through the Financial Crimes Enforcement Network (FinCEN). 64% are not registered with FinCEN (Figure 16).

Figure 16- Registered as a Money Transmitter



Participants in this survey were asked what forms of identification information they record about customers, if any. 50% of respondents reported that they do not record identification information about their customers. 27.27% record the customer’s first and last name, 2.27% record a phone number, 18.18% record a driver’s license number, 18.18% record a bitcoin wallet address, 13.64% record a passport number, 13.64% record an address, 13.64% record facial photographs, 9.09% record a date of birth, 9.09% record an e-mail address, 9.09% record a bank account number, and 4.55% record an IP address for their customers. Zero respondents reported recording a customer’s social security number or license plate number. 18.18% selected “Other” (Figure 17). For the respondents who selected “Other,” one wrote that he or she recorded ID information for transactions with more than \$3,000. Another respondent stated that the amount of information recorded depended on the transaction amount and how and where the transaction took place. One respondent recorded that he or she recorded a “mental profile” of the client.

Figure 17- Customer Information Recorded by Vendors



Opinion Results

In the final survey section, a series of seven statements were listed, and respondents used a Likert scale to express if they completely disagree, slightly disagree, slightly agree, or completely agree with the statement.

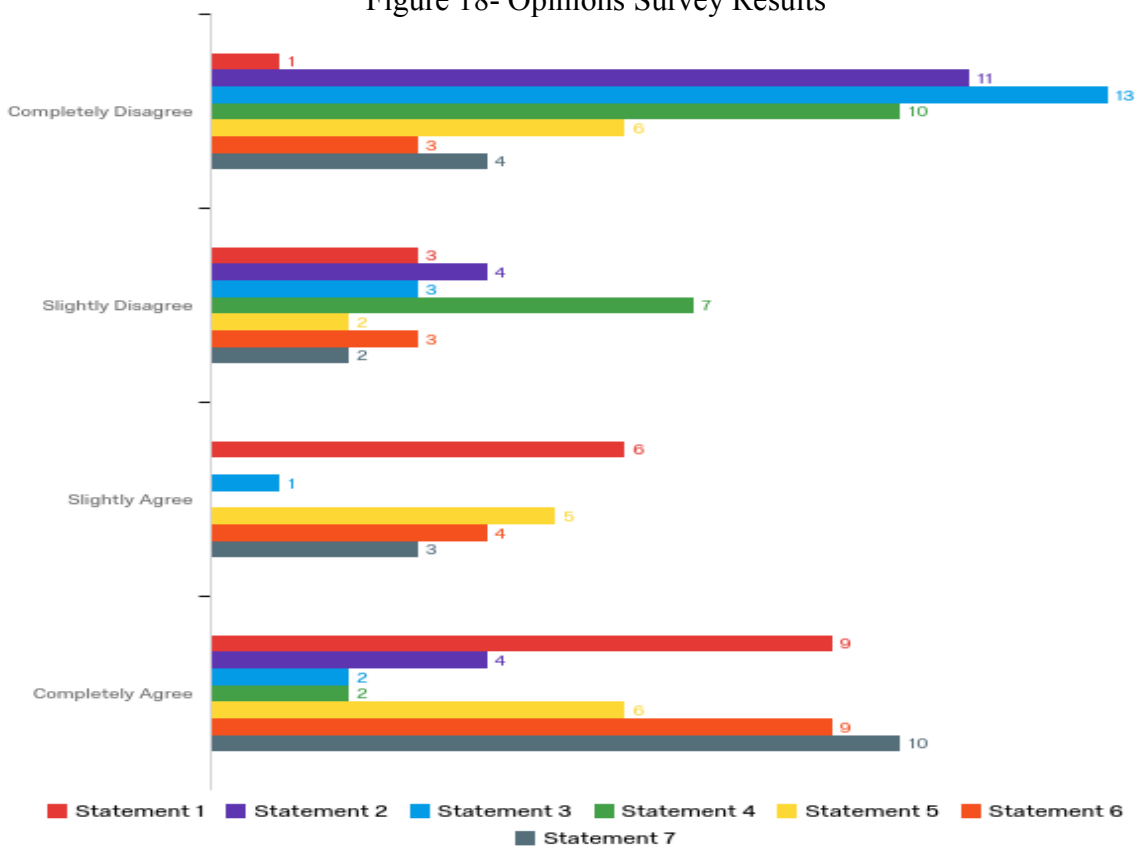
Statement 1 says, “Paper currency should be federally regulated.” 5.26% of respondents completely disagree, 15.79% slightly disagree, 31.58% slightly agree, and 47.37% completely agree. Statement 2 says, “Digital currency should be federally regulated.” 57% of respondents completely disagree, 21.05% slightly disagree, 0% slightly agree, and 21.05% completely agree (Figure 18).

Statement 3 says, “I trust the federal government to handle Bitcoin exchange information appropriately.” 68.42% of participants completely disagree, 15.79% slightly disagree, 5.26% slightly agree, and 10.53% completely agree. Statement 4 says, “I trust law enforcement will handle Bitcoin exchange information appropriately.” 52.63% completely disagree, 36.84% slightly disagree, 0% slightly agree, and 10.53% completely agree (Figure 18).

Statement 5 says, “I would contact law enforcement if my Bitcoin buyer told me they planned to use the currency on an illegal purchase.” 31.58% completely disagree, 10.53% slightly disagree, 26.32% slightly agree, and 31.58% completely agree.

Statement 6 says, “If law enforcement approached me about a case involving my customer, I would provide general descriptive information.” 15.79% completely disagree, 15.79% slightly disagree, 21.05% slightly agree, and 47.37% completely agree. Statement 7 says, “If law enforcement approached me about a case involving my customer, I would provide specific identifying information.” 21.05% completely disagree, 10.53% slightly disagree, 15.79% slightly agree, and 52.63% completely agree (Figure 18).

Figure 18- Opinions Survey Results



Statement #	Question	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

Open Ended Question Results

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 Libertarians, 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.

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.

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.

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.

Summary

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.

Discussion

Introduction

Criminals have adopted Bitcoin, a digital currency, as an easy-to-use form of money that cannot be as easily traced back to them as a credit card or bank account. After the Silk Road, a Darknet marketplace for drugs, was taken down, the Financial Crimes Enforcement Network (FinCEN) applied specific regulations for money transmissions involving Bitcoin.

The purpose of this study was to learn more about demographic information, knowledge of and compliance with FinCEN regulations, and opinions regarding government and law enforcement among cash-for-bitcoin vendors in Oklahoma, Texas, Arkansas, Colorado, Missouri, New Mexico, and Kansas.

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%).

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 Crimes Enforcement Network (FinCEN).

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:

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?

Thank you for your time. I can be reached by email or by phone at _____.

Thank you,

- Stephanie Robberson

Forensic Science Institute

University of Central Oklahoma

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.

<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 (Financial Crimes Enforcement Network [FinCEN], 2013, 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. First, 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 Craigslist and Backpage 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 licence 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.

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, 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.

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. 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 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.” 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. 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.

Limitations

This study had a small sample size gathered as a convenience sample through available cash-for-bitcoin advertisements on LocalBitcoins.com, Craigslist, and Backpage. In any instance of survey research, there is no way to verify that answers given to the researcher are accurate, especially questions about the respondent’s opinion.

Recommendations for Future Research

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 willing to 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.

Conclusions

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/hottopics/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>

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/hottopics/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/hottopics/lnacademic