

# The Expansion of Bitcoin

Courtney Hayslett  
Department of Computer Science  
Hampton University  
hayslett.courtney@gmail.com

Jean Muhammad  
Department of Computer Science  
Hampton University  
jeana.muhammad@hamptonu.edu

## ABSTRACT

This study aims to analyze Bitcoin as well as the security encompassing cryptocurrencies. It includes information acquired from a plethora of resources on the inside and outside looking into the world of Bitcoin and online peer-to-peer methods of payment. It also includes interviews from experts in the field of Bitcoin, currency, and a survey completed by everyday users of online currency. Detailed analysis that includes research on currently used online payments and Bitcoin are accurately displayed in this paper.

## CCS CONCEPTS

• **Security and privacy** → Cryptography; • **Information systems** → Data encryption

## KEYWORDS

Bitcoin, Digital Currency, Security, Cryptocurrencies

## ACM Reference format:

C. Hayslett, J. Muhammad. 2017. The Expansion of Bitcoin. In *Proceedings of 2017 ADMI Symposium*, Virginia Beach, Virginia USA, March 23-26, 2017.

## 1 INTRODUCTION

Bitcoin is a rising star in the crypto-currency field. It is the topic at every cybersecurity conference from BlackHat USA to DEFCON. With success stories resulting in the management of Bitcoins, more and more users are added everyday to the largest crypto-currency ever made. David Marcus the CEO of Paypal once was quoted saying:

“I really like Bitcoin. I own Bitcoins. It's a store of value, a distributed ledger. It's a great place to put assets, especially in places like Argentina with 40 percent inflation, where \$1 today is worth 60 cents in a year, and a government's currency does not hold value. It's also a good investment vehicle if you have an appetite for risk. But it won't be a currency until volatility slows down.”

As Bitcoin is expanding and more and more users are being added to the constantly growing Bitcoins it is important to analyze the past and look towards the future of currency exchanges. So why can't Bitcoin become the norm?

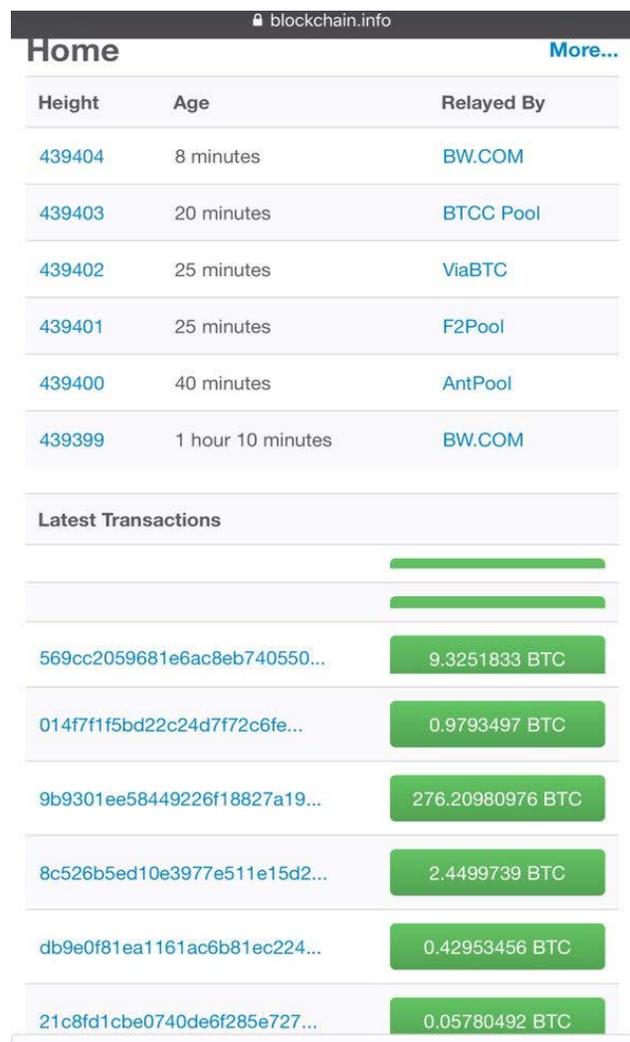


Figure 1: Life Feed of Bitcoin Trading.

## 2 MOTIVATION

The first time Hayslett heard about Bitcoin was from a friend in her Engineering Foundations II class back in the fall of 2010. Bitcoin was founded on October 31, 2008, by Satoshi Nakamoto. Hayslett was amazed by the concept, and researched into the methodology of Bitcoin as a tool for its users. Interest turned into keen motivation to seek more and more knowledge as Hayslett delved deeper into emerging technologies and currencies along with cybersecurity. Miss Hayslett then saw the concept of Bitcoin appear in the blockbuster movie 'Dope' which came out in January 2015. It was mentioned by name at least half a dozen times and the movie literally starts out with the main character saying something along the lines of "money is over as we know it and everyone will soon be using Bitcoin". The movie 'Dope' was the first movie to accept Bitcoin for ticket purchases. So for Open Road, seeking out an innovative, high-tech payment system for tickets seemed like a natural move. "Bitcoin is an integral part of 'Dope' and we could not be more excited to bring this unique new opportunity to moviegoers," Open Road Chief Marketing Officer Jason Cassidy said in a statement. (Thewrap.com)

Getting the word out about Bitcoin to a broad audience was a great move to help millennials get involved in the wave of digital currency. Hayslett is fascinated in new concepts that help normal or everyday people have opportunities to create and help sustain wealth. Bitcoin bends formal legality norms, however great leaders question the rules and break them in order to achieve greatness. Perhaps Bitcoin once it evolves more will be the exception to normal banking systems.

Although the first word in digital currency today is Bitcoin, the history of Bitcoin does not begin with simple facts and figures. It piggybacks off of a concept begun by E- Gold in 1996. The representation of money was always cash, paper bills and metal coins. The digital revolution has made money ever increasingly become virtual, and less physical. Today only 8% of the world's currency exists in the physical cash form. E- Gold was the attempt to return to gold- backed currency.

In 1971 credit cards became the most used system of money. The first form of truly digital money is Bitcoin. Bitcoin was designed for the era of information and solves many disadvantages of physical and electronic money. It is the first scarce digital resource to ever exist. One bitcoin is made of one million bits, you can send Bitcoin in real time by text, paper for free. Bitcoin cannot be faked and is global through open sourced technology. Most users of Bitcoin use it because of the discreet purchases they can make whether it be legal or illegal substances or services.

## 3 BITCOIN

### 3.1 Review: Bitcoin

Bitcoin is a type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. Bitcoin is transforming the way we look at financial

services. Within bitcoin there is a blockchain which is a ledger or information.

Bitcoin is the world's first completely decentralized digital currency. For decades, digital currencies such as Facebook credits and Microsoft points are digital currencies have existed. PayPal, Visa, and MasterCard differs from Bitcoin because Bitcoin is decentralized. Facebook and Microsoft makes up tokens for their points and credits and hands them out. With Bitcoin, there is no Bitcoin company, there is no building or Bitcoin server which makes it unique because it is completely distributed. For the first time, it is a way to share value online without a third-party intermediary. In the past to share peer-to-peer a middleman would be needed, Bitcoin is cutting out the middleman. Bitcoin's ledger is distributed peer-to-peer with all the users. Currently one single Bitcoin is worth \$766.98 in US dollar currency.

### 3.2 Bitcoin Blockchain

Bitcoin is an online currency with a security system run by a massive network of total strangers. Trusting strangers with your data, information, and digital information may sound unconventional, but it is a revolution in distributed computing. It is all based on the Blockchain an open ledger that stores a history of financial transactions, however Blockchains can be adapted to store any kind of digital information imaginable. The development of systems like Blockchain can be the future of all secure digital transactions. Old security models focus on locking people out, Bitcoins model focuses on letting everyone in.

Blockchain uses self-interest and greed to secure your bitcoins. You don't need trust to share and update your digital records. Understand the Bitcoin Blockchain is crucial to acquiring bitcoins. A Bitcoin is a private key, half of a digital signature that proves you own a bitcoin. [5] The other half is a public key; a record of the public key is stored in the blockchain.

Individual blocks contain multiple transactions, each of which refers to an earlier record of the chain. If you want to purchase something with Bitcoins, you broadcast a request, the request is reviewed by all the computers on the bitcoin peer-to-peer network. These computers and their owners are called miners. Miners scoop up the most recent request into a block, they run the new block and the previous blocks through a set of calculations called hash functions. It is a competition, with all the miners racing to solve a complex cryptographic puzzle. [8] The more computing power you have the more likely you are to solve it first. After solving a block the miner tacks it onto the end of the blockchain. Then they broadcast it to their peers, who check the work and start using the new version of the blockchain.

The first miner to solve the block is rewarded with newly minted bitcoins. Minting coins isn't the only point of mining. The puzzles are so complex that every new block make the previous blocks makes the blockchain extremely secure. Hacking the blockchain would require tremendous speed. To alter just one transaction, the attacker would need to change the information in that block and in every block, that comes after it, all before the blockchain is updated. With countless miners working on the blockchain simultaneously this would require massive amounts of

computing power. More than half of the power being committed to the bitcoin network at any given time. The self-interest of individual miners adds up, creating a selfish and self-protecting secure system. Personal allegiance is replaced with mathematical confidence. The Bitcoin Blockchain is a public database that everyone can see, anyone can add to, and no one can destroy.

There are many pros and cons to Bitcoin and security is a major deal breaker for most. Bitcoin uses transparency in anonymity, many users refuse to disclose their identity and have multiple accounts depending on their transactions and needs. [15] The Bitcoin Blockchain makes the transactions transparent because it is a large ledger that encrypts each transaction when it gets processed. A major consequence of using Bitcoin is the lack of regulation, there are NO REFUNDS on Bitcoin. If your account is compromised, your money is gone Bitcoin does not have any method of insurance. Once you pay or trade Bitcoins and you don't receive products or goods, those Bitcoins you traded are gone forever. Bitcoin is controlled by a network of machines and has no complete or central regulation authority overseeing the system that is Bitcoin. The speed of Bitcoin is a major advantage because the money transfer is extremely quick. Within minutes' amounts of money is transferred into your bank account, there is not a wait or hold for five to seven business days like Bank of America, Cash App, or Wells Fargo Bank. Rather than trying to stifle or control virtual currencies, US governmental entities recognize the long-term value of virtual currencies and are trying to create a regulatory regime to foster growth and development, and an atmosphere where institutional and retail investors are protected. [5]

#### 4 METHODOLOGY

The methodology the researcher chose to answer the problem statement consisted of a couple different strategies. The first being the conducting of an interviews from technical experts in the field whom have worked at the Internal Research Service and has conducted research on Bitcoin. The second being a is a Senior security researcher at Trust Wave's Spider Labs. The third being the interview of a startup investor who has many ties to the application security field that has been researching and kept abreast on the issues surrounding Bitcoin for the past few years. The fourth interview was with Dr. Edward Pyatt, the Chairman of the Department of Banking and Finance at Hampton University. Dr. Pyatt was an economic and financial analyst at Fortune 500 companies prior to his tenure at Hampton University. Finally, the researcher has conducted a survey gauging the interest and level of competency on the concept of digital currency, as well as different areas of Bitcoin, and interest in education above and beyond.

##### 4.1 Interviews

The researcher's first interview was with Dr. Danny Barnes, DDS, a former Information Technology specialist for the United States' Internal Revenue Service working from November 2011 through January 2015. Dr. Barnes first heard about Bitcoin in late 2006, early 2007 when he was pursuing is Doctoral degree. The

researcher asked Dr. Barnes a plethora of interview questions from how Bitcoin works? How did you hear about it and when? Did it shake up the IRS at all in their concern with Bitcoin? Would you recommend Bitcoin to anyone? In reply to these questions Dr. Barnes replied by saying,

“Bitcoin is not regulated because you cannot tax “internet money” that is ether and compiled of 0's and 1's. The value of Bitcoin fluctuates so much so that it loses value as quickly as it gains value, which is linked to a huge trust issue for users, and the public at large.”

Dr. Barnes began the interview with the importance of the legitimacy of currency. “Most currency is backed by tangible objects such as rare gems, gold, paper, and not imagined value.” Dr. Barnes called intangible currency online “scary” because it has no stable proof of market value. Dr. Barnes believes nothing electronic and online is 100% secure. He would heavily caution against the use of Bitcoin since it isn't backed by anything and has no set value for bitcoin and what it is worth. Dr. Barnes stated that Bitcoin caught his eye when usage began to rise in the spring of 2014, and in late 2016 he sees it gaining steam again. Dr. Barnes said that Bitcoin is, “One of the riskiest investments one individual can ever make.” Dr. Barnes knows a few folks who regularly use their Bitcoins and they think it is “the best thing since sliced bread.”

When asked, what could be the biggest downfall of Bitcoin Dr. Barnes believes it would be the lack of stability in the backing of Bitcoin. Dr. Barnes will be impressed when Steve Wozniak or Bill Gates begins to deal in Bitcoin and puts their stamp of approval on it. Elon Musk made PayPal, yet he does not use Bitcoin. “I believe it is a scam to rip people off and operate in the shadows.” The researcher asked Dr. Barnes what it would take for Bitcoin to participate in the new internet of money Bitcoin. Dr. Barnes detailed step by step his answer below:

1. It needs to be backed by a solid foundation
2. It should be based on a comparison of value
3. Bitcoin should establish a holding area or server like the Internal Revenue Service and Federal Reserve
4. There is a need for consistent standards. For example, how many can be printed or made and distributed. How many 1's and 0's fly on the Ethernet every day? There must be regulation in this system.

Researcher Hayslett researched a Bitcoin developer, Daniel Chechik who has had experience in Senior Security Researcher at Trustwave SpiderLabs demonstrated a Malleability Theory in Practice at BlackHat USA in 2014. Mr. Chechik's presentation at BlackHat expanded on how Bitcoin transactions were broken down. Bitcoin Transactions are broken two into two categories and built from two main components. The first being Inputs which are the source of coins, and Outputs which is the amount and the redeemer's bitcoin address. Transactions of Bitcoin add a level of

security because one must confirm you have an amount of coins by having a reference, with a public key of the person the coins are going to, as well as a signature for the transaction.

Dr. Pyatt's interview had a strictly business angle, since Dr. Pyatt's expertise is in the financial sector. Dr. Pyatt has been watching Bitcoin's fluctuations with a concerning eye. Dr. Pyatt believes Bitcoin is too volatile to flourish for everyday users. Dr. Pyatt challenged the validity of Bitcoin calling it extremely responsive and unstable. Dr. Pyatt called the system of Bitcoin a get rich quick scheme, that seems like a scam without true regulation. "It is too risky for me to personally partake in, and I urge others to not do so now" Dr. Pyatt says.

The final interviewee has a plethora of knowledge in application development and is continually abreast of Bitcoin and digital currencies like it. Mr. Bruce Chittenden is a startup entrepreneur and assistant professor at Hampton University. Mr. Chittenden not only holds stock from various oil and technology companies, but actively participates in conversations about digital currency. The following is the conversation he had with Miss Hayslett.

Hayslett: Do you think Bitcoin will fail?

Chittenden: It will only fail if users stop using it and the value decreases on its own. Bitcoin can surely be destroyed when People see no value it in it anymore.

Hayslett: What are your thoughts regarding Bitcoin regulation?

Chittenden: If they had a central banker for regulation purposes taking bitcoins out and adding bitcoins on will incorporate stability. Bitcoin seems to be a combination of a computer science and financial project, but lacks a central banker. I think it needs Janet Yellen, the Chair of the Board of Governors of the Federal Reserve System or maybe Mario Draghi, the President of the European Union Banking System.

Hayslett: What are your thoughts on the security aspect of Bitcoin?

Chittenden: Bitcoin isn't tracked, criminals use to launder money which can move money from country to country without detection. I would never utilize Bitcoin; however, it sounds like an interested research project.

For above and beyond continuation of this whitepaper would be the ability for researcher Hayslett to acquire and buy goods using Bitcoin. The first step would be to open a separate bank account not linked to any savings or checking accounts that hold large sums of money. The researcher would deposit two hundred dollars into the "honeypot" account. Create a Bitcoin wallet that holds and stores my Bitcoins and transactions. Locate Hayslett

Bitcoin address, and finally buy Bitcoins! The researcher would then locate which businesses accept Bitcoin as a form of payment. The closest company to the researcher that does is as follows:

- Foodler.com
- Food Delivery Services
- 48 US States, District of Columbia 20018
- United States of America

To gain a deeper understanding on the background information, the researcher had to conduct literary critiques on professional white papers, and published articles related to the validity of Bitcoin, and the overall foundation of its impact on society. [3] By performing a literary critique the researcher could hone in on a unique perspective of making Bitcoin mainstream. Which after conducting various interviews with field experts is what Bitcoin lacks as far as the concept of needing to cross over to open and existing markets.

#### 4.2 Survey and Results

To conduct this research sufficiently and successfully, the researcher first had to create a survey to examine individual's personal background, their knowledge and thoughts towards Bitcoin. The survey had exactly 8 multiple choice questions. It was comprised of a wide range of questions pertaining to where someone's interest lies regarding online currency. The survey was used to gauge the interest of people in Bitcoin and their current state of knowledge on digital currency usage.

Creating the survey the researcher wanted to gather responses from people in different times in their life, to gauge their opinion on risky business propositions such as the use of Bitcoin.

There were a total of *100 active participants* who completed the survey. The questions provided were examined and related to the introduction and education of Bitcoin in general. From business analysts working at Accenture Consulting firm, to second year, five- year MBA majors at Hampton University took my survey. An observation the researcher expected to see was the little knowledge known about how to acquire a Bitcoin, since it is not widely publicized.

*Survey Results: 100 responses*

#### Personal Background

1. How old are you?

Under 18 years old	<b>1</b>	1%
18 - 24 years old	<b>86</b>	86%
25 - 40 years old	<b>7</b>	7%
41 - 50 years old	<b>1</b>	1%
51+ years old	<b>5</b>	5%

2. Are you a female or male?

Female	<b>66</b>	66%
Male	<b>34</b>	34%

3. How familiar are you with using digital currency?

1 (No familiarity)	27	27%
2	20	20%
3	29	29%
4	16	16%
5 (Extremely familiar)	8	8%

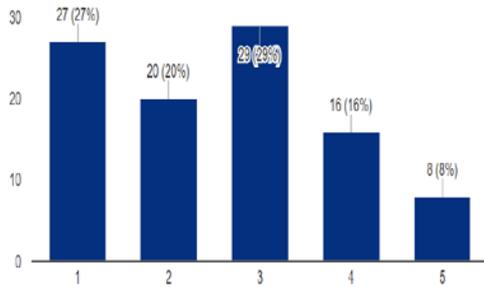


Figure 2: Data depicting results from survey on digital currency familiarity

4. Are you knowledgeable of Bitcoin?

1 (No familiarity)	52	52%
2	22	22%
3	14	14%
4	10	10%
5 (Extremely familiar)	2	2%

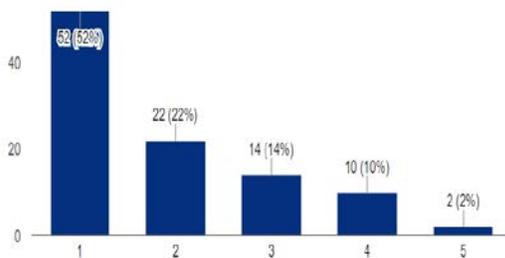


Figure 3: Data depicting knowledge of Bitcoin

5. Do you own Bitcoins?

Yes	4	4%
No	96	96%

6. Do you know how to acquire Bitcoins?

Yes	16	16%
No	84	84%

7. Do you think Bitcoin is too risky for you to participate in?

Yes	39	39%
No	61	61%

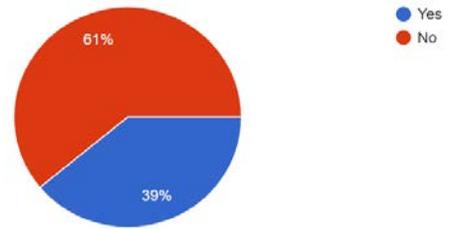


Figure 4: Data depicting Bitcoin Risk

8. Would you like to learn more about digital currency?

Yes, I'm interested	57	57%
No, I'm not interested	17	17%
Maybe	26	26%

#### 4.2 Analysis of Results

Statistics show that males have a greater inclination to attempt risky situations than females. [2] For example the car insurance rates for males are higher than females. The gender divide explains the underlying reasons humans take risk. Men take more risks than women, and especially financial and recreational risk. It goes back to the cultural of honor where men feel like they need to defend themselves and assert their masculinity to protect their honor. Taking risks is one way to do that. Men tend to be less risk seeking when they grow older.

Per the New Coin Desk Report from CoinDesk.com the greatest percentage of Bitcoin users at 39.4% are between the ages of 25-34 years old. The second largest percentage of users are in the 34- 44 age group at 21.99%. 90% of Bitcoin users are males, and 65.8% of the 3,515 surveyed users identified as White. [2]

Referring to the survey conducted it can be concluded that more than half of the surveyed participants are relatively interested in digital currency. About 26% of the people surveyed might be interested in learning more about digital currency in general. More than half, at 61% of surveyed believe Bitcoin is too risky to participate in.

#### 4 CONCLUSIONS

In conclusion, Bitcoin is continually expanding regardless of the great mask of anonymity millions of users hide under. Regardless of the great amount of lack of legality and governance, it is a way to buy and sell products discreetly. Once users get comfortable with operating in the gray and under the radar attention to Bitcoin and usage will skyrocket once more. By educating everyday users on a new digital currency, a spike in usage would follow. Per the data collected 57% of surveyed people would like to learn more about Bitcoin and will perhaps google it on their own time. However, Bitcoin is not easily marketed to people unless it is on Reddit.com, chat rooms, or on the Dark Web it is hard for everyday users to fully understand and participate in this new idea of currency.

Sir Richard Branson said in an interview with Bloomberg, "I think it is working. There will be currencies like it that might work even better, but in the meantime, there's a big industry around Bitcoin." Throughout the research conducted, extensive interview sessions with experts in the field, and hearing from consumers many conclusions have been drawn. First and foremost, Bitcoin is extremely risky and most are not interested in jumping off the ledge into the unknown. [6] Secondly, Bitcoin is challenging in that you are putting your trust and hard earned money into a mathematical algorithm passed along the internet without a margin for error.

Although experts are constantly debating on the validity of Bitcoin and using it in everyday life, Miss Hayslett believes the concept can grow to have a high impact on the world as we know it. Miss Hayslett is excited and looks forward to researching more and keeping up with Bitcoin as she will invest and jump with two feet into the unknown when the time and resources are right. Researcher Hayslett believes risk is what makes the business world turn and having confidence in a system will either work in your favor, or not and whatever is meant to be is meant to be. It appears people today are too timid to take a leap of faith and throw their money away or towards an idea. On the other hand, Bill Gates was mocked as well as Einstein before making great discoveries that have changed our world and society today. Money, dollar bills, and Bitcoins are all relative, the idea of peer to peer currency is the most prominent idea now, not the actual Bitcoins but the system overall. The researcher wants to see users give Bitcoin a chance by using professional and reputable resources to enter the Bitcoin market. Legality must come into play when using untraceable purchases and selling markets. Once the law or a regulation agency is implemented is when Hayslett will truly gauge the value of Bitcoin.

Because Bitcoin has roughly 300,000 transactions a day, soon would be a great time to enter the world of Bitcoin to expand and grow your money. I highly recommend more research needs to be performed to provide a complete recommendation on a case by case basis on whether someone should participate in Bitcoin.

#### Acknowledgement

Researcher Courtney Hayslett would like to thank Dr. Muhammad for giving her an outlet to research a topic she is most interested in. I would also like to thank the Department of Computer Science

at Hampton University which has supplied me with well-versed and experienced professors as well as assistant professors that provided an inside consider an emerging concept in digital currency field. This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant no. DGE-1303409 (PI/co-PI: Dr. Chutima Boonthum-Denecke, Dr. Jean Muhammad).

#### REFERENCES

- [1] Ciaian, P., Rajcaniova, M. & Kancs, . *Inf Syst E-Bus Manage* (2016) 14: 883. doi:10.1007/s10257-016-0304-0
- [2] Sundheim, D. (2014). Do Women Take as Many Risks as Men? Retrieved December 13, 2016, from <https://hbr.org/2013/02/do-women-take-as-many-risks-as>
- [3] Antonopoulos, A. 2014. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA: O'Reilly Media.]
- [4] Evan L. Greebel, Kathleen Moriarty, Claudia Callaway, Gregory Xethalis, (2015) "Recent key Bitcoin and virtual currency regulatory and law enforcement developments", *Journal of Investment Compliance*, Vol. 16 Iss: 1, pp.13 - 18
- [5] Mark Edwin Burge. "Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law" *67 Hastings Law Journal* 1493 (2016).
- [6] Alex Biryukov and Dmitry Khovratovich and Ivan Pustogarov. *Deanonymisation of clients in Bitcoin P2P network*. CoRR, abs/1405.7418, 2014
- [7] <http://www.thewrap.com/hollywood-studios-win-injunction-against-streaming-service-vidangel/>
- [8] CHAP Carmona, AnaisBlowers, Misty 2015 *The Bitcoin: The Currency of the Future, Fuel of Terror Evolution of Cyber Technologies and Operations to 2035* 127- 135 Springer International Publishing Cham 978-3-319-23585-1 [http://dx.doi.org/10.1007/978-3-319-23585-1\\_9](http://dx.doi.org/10.1007/978-3-319-23585-1_9) 10.1007/978-3-319-23585-1\_9 Carmona2015
- [9] Jeffrey Simser, (2015) "Bitcoin and modern alchemy: in code we trust", *Journal of Financial Crime*, Vol. 22 Iss: 2, pp.156 - 169
- [10] Characteristics of Bitcoin users: an analysis of Google search dataAaron Yelowitz and Matthew Wilson Applied Economics Letters Vol. 22 , Iss. 13,2015
- [11] Koblitz, N. & Menezes, A.J. *Des. Codes Cryptogr.* (2016) 78: 87. doi:10.1007/s10623-015-0148-5
- [12] Cocco, L., Concas, G. & Marchesi, M. *J Econ Interact Coord* (2015). doi:10.1007/s11403-015-0168-2
- [13] Kraft, D. *Peer-to-Peer Netw. Appl.* (2016) 9: 397. doi:10.1007/s12083-015-0347-x
- [14] Bal, A. 2015. "How to Tax Bitcoin?" In *Handbook of Digital Currency*, edited by David Lee Kuo Chuen, 267-282. San Diego, CA: Academic Press
- [15] Bohr, J and M. Bashir. 2014. "Who Uses Bitcoin? An Exploration of the Bitcoin Community." *IEEE*., 2014 Twelfth Annual International Conference on Privacy, Security and Trust (PST), 23–24 July 2014 , Toronto. Accessed 13 August 2015. <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6890928>