International Immersion Program Papers

Student Papers

2017

In an Era of FinTech : Strategies of Government to Deal With Virtual Currencies

Kamolnich Swasdiphanich

Follow this and additional works at: http://chicagounbound.uchicago.edu/international_immersion_program_papers

In an Era of FinTech: Strategies of Governments to Deal with Virtual Currencies

Kamolnich Swasdiphanich*

I. Introduction

These days, the world is in the midst of technology's era, international organizations, governments, or even ordinary people are challenged by many un-known innovations. Some facilitate our lives, whereas some generate threat throughout the world. Most activities in human's daily life are transformed and data in every aspect is stored in the form of digital information which can be transferred and exchanged within a short period of time via online network. This, undoubtedly, includes information about finance-related transactions. In the past, human traded by bartering—exchanging one thing with another thing—on the basis of a mutual agreement. Then we used valuable objects, such as diamond, gold, and eventually currency, as a medium of exchange. As, however, in the past decade that a trend of *cashless society*[1] has been spreading out all around the world, financial transactions have been transforming, being conducted through credit cards, debit cards, online banking (internet banking, e-banking, or virtual banking)[2] or mobile banking.[3]

[1] *Cashless society* is an economic state whereby financial transactions are not conducted with physical money (i.e. banknotes and coins), but rather with the digital money.

[2] *Online banking* is an electronic payment system that customers can conduct financial transactions through financial institutions' website.

[3] *Mobile banking* is a service provided by financial institutions allowing customers to conduct financial transactions through mobile device.

However, no matter how far financial transactions have been transformed, financial institutions are, still, considered a core intermediary between two parties of the transactions. It can be said that financial institutions act as a third party who gain trust from both opposite parties involved in the transactions, or by way of technical explanation, a transaction conducted through a financial institution as a third party is a *trust-based model* transaction. Trust-based model transactions trigger a fundamental concern that despite strict laws and rules regulating financial institutions as a third party of financial transactions, to what extent parties involved in such transactions can rely on, or trust, those institutions; and how long that such financial institutions' reliability can last.

Trust in financial institutions become shaky after the collapse of economic system during the great panic evoked by the financial crisis 2008. Mistrust replaced trust and people began to seek an alternative. Based on this drawback of financial institutions and mistrust of people in financial regulations issued by the government, *Virtual Currency (VC)* has been invented, introducing an alternative venue in cyberspace that people can conduct financial transactions without any intermediary involved. Digital technologies, together with online network, were assigned a major role in financial market: creating VC as an alternative for those who have lost faith in institutions.

VC is one kind of *Financial Technology (FinTech)*.[4] It, among other kinds, is considered the most difficult type of FinTech to understand. The basis purpose of VC is to get rid of intermediaries, both financial institutions and governments, in financial activities by utilizing some sort of computer science. Most importantly, VC has no legal basis and are intangible; therefore, VC is almost impossible to oversee or control.

---

[4] *Financial Technology* or *FinTech* is a new technology and innovation utilized to compete against traditional financial institutions and intermediaries in the delivery of financial services. Sometimes it refers to an industry composed of companies that use such technology and innovation.

There are several characteristics of VC that are abusive toward the world's order in various aspects, such as economic stability and human rights. As for the former, since VC is not endorsed by any state, only accepted to be valuable by some groups of people, the value can fluctuate heavily within a short time, affecting people and business involved in the scheme. In addition, considering the human rights aspect, it has been a widespread concern that VC can be used to purchase illegal goods or escalate money laundering. These days, however, the situation of VC has become more intense due to the fact that it has been used to engage in international terrorism as a financing device. Governments, especially of threatened states, are provoked and have been trying, somewhat unsuccessfully, to control the usage of VC.

Despite such facts, some countries, such as China, still view VC positively. Even though the Chinese government has officially issued *the Notice on Precautions against the Risks of Bitcoins* and prohibits banks and payment institutions from dealing in Bitcoins, the People's Bank of China, in 2016, announced that they were considering issuing Chinese VC.[5] It is also worth to be noted that Bitcoins is only one type of VC. Hong Kong, as a main financial sector of China and Asia, in contrast, has not yet adopted any legislation specifically regulating VC[6] and has not yet taken any substantial step toward any end. Similar to China's approach, in 2013, a spokesmen of Singapore's central bank, the Monetary Authority of Singapore (MAS), warned consumers about trading in Bitcoins; however, they retained that they would not intervene in decisions of the private sector whether or not businesses would accept Bitcoins in exchange for their goods or services.[7] Although, in 2014, MAS announced that they were considering to regulate VC intermediaries in order to mitigate risks of those intermediaries

---

[5] *See* Sophia Yan, "China wants to launch its own digital currency," last modified January 22, 2016, http://money.cnn.com/2016/01/21/technology/china-digital-currency/.
[6] *Regulation of Bitcoin in Selected Jurisdictions* (Kentucky: The Law Library of Congress, 2016), 11.
[7] *See* Terence Lee, "Singapore Government Decides Not to Interfere with Bitcoin," last modified December 23, 2013, http://www.techinasia.com/singapore-government-decides-interfere-bitcoin/.

involving in money laundering and terrorism financing, there is, so far, no any further approach taken.

This paper will be divided mainly into three parts. Part II will elaborate basis knowledge about VC, focusing on technologies and computer science adopted in the scheme. Part III will be discussing selected legislations about VC in the United States, European Union, China, Hong Kong, and Singapore as the main global and Asian financial sectors. Also, it will discuss predicted subsequent steps of these countries assumed from the governments' attitudes toward VC. Finally, in part IV, the paper will propose frameworks for governments to deal with VC.

II. Overview of Virtual Currencies

VC is electronic data units generated from computerized mechanism. These data units are written by a person or a group of people to be utilized as an alternative to traditional currency—being a mediatory tool for exchanging goods or services. Since VC is data units stored in electronic form, VC is completely intangible. Although VC cannot be used legally to settle any debt or obligation, there are some groups of people accepting them as a medium of exchange, and, definitely, these people also accept VC in exchange for real currency. Technically and legally, VC has no value. The value, thus, comes purely from such groups of people's subjective endorsement which is unpredictably fluctuating, depending on periodic demand of VC. Due to this fact, the value of VC can fluctuate heavily within a short time, posing significant risk on consumers involved in the scheme and economic stability as a whole. To illustrate, in 2014, a company acting as a prominent VC intermediary in Japan was forced to close by cause of data cracking. The value of VC plummeted after then, rendering massive losses to other businesses and individuals.[8]

---

[8] *See* Bank of Thailand News issue 8/2014*, "Bitcoin and other similar electronic units," last modified March 18, 2014, https://www.bot.or.th/Thai/PressAndSpeeches/Press/News2557/n0857t.pdf.
   *(Only Thai version available)

A. Prominent Currencies of Virtual Currencies

There are several types, or currencies, of VC invented since the first launch of Bitcoins. These various types of VC, however, have somewhat similar purpose and operational functions. This section will elaborate various types of VC, covering all the most important features adopted in different types of VC, as follows:[9]

1) Bitcoins

Bitcoins is one of the most important VC in the world. Nowadays, Bitcoins earns and retains pervasive popularity among VC users; and is considered the VC that has the largest amount of users in the world. One can say that if mention VC, most people will automatically think of Bitcoins, always.

Bitcoins has been invented by a programmer using an alias: Satoshi Nakamoto, in 2008. Nakamoto disseminated his original idea through an e-mail list of cryptographers;[10] then, officially promulgated his invention in a written article under the title "Bitcoin: A Peer-to-Peer Electronic Cash System". After the first coin had been circulated, the Department of the Treasury of the United States categorized Bitcoins as VC since there was no central agency collecting and recording data of transactions conducted through Bitcoins system. However, the U.S. Financial Crimes Enforcement Network (FinCEN) claimed that there were actually two categories of VC, that is, centralized VC and decentralized VC,[11] triggering an ambiguity

---

[9] *See* Prableen Bajpai, "The 5 Most Important Virtual Currencies Other Than Bitcoin," last modified December 10, 2014, http://www.investopedia.com/articles/investing/121014/5-most-important-virtual-currencies-other-bitcoin.asp.

[10] *Cryptographer* is a person who constructs and analyzes protocols* that prevent third parties or the public from reading private messages.

*Protocol refers to a communication protocol which is a system of rules in telecommunications allowing at least two entities to transmit information via any kind of variation of a physical quantity. It can be implemented by hardware, software or a combination of both.

[11] *See* "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," November 19, 2013, https://www.fincen.gov/sites/default/files/2016-08/20131119.pdf.

whether financial data units recorded by a central institution are considered VC. It is worth to note again here that the main purpose of VC is to get rid of involvement of any central institution. Further, in early 2013, after a lawsuit filed against Liberty Reserve, a large agency producing centralized VC, FinCEN announced that Liberty Reserve was a financial institution[12] under the definition of Section 311 of the USA PATRIOT Act.[13] Under this analysis of FinCEN, any central agency engaging in VC scheme is considered a financial institution subject to the USA PATRIOT Act. As further elaborated in subsequent part, one of the characteristics of VC that generates problems in terms of overseeing and regulating is decentralization; hence, in this paper, VC refers to only decentralized VC. This paper will not discuss the ambiguity of the difference between centralized and decentralized VC.

2) Litecoins

Litecoins is the second largest VC, next below Bitcoins, in terms of user pool. The first coin of Litecoins has been circulated in 2011 by a programmer named Charlie Lee, which, unsurprisingly, was one of key executives of Bitcoins. The *Proof-of-work* system of Litecoins adopts a coding called *Scrypt*, developed from the Bitcoins' Proof-of-work system, so that *mining* process of Litecoins can be conducted through ordinary computers and achieve it with faster speed than Bitcoins. Additionally, *miners* of Litecoins will obtain more coins as a reward for mining, compared to those in Bitcoins system.[14]

Details about the Proof-of-work system, including mining and miner, will be provided later in the subsequent part.

---

[12] Ibid.

[13] *USA PATRIOT Act Section 311* (added 31 USC §5318A to the Bank Secrecy Act): Special measures for jurisdictions, financial institutions, international transactions, or types of accounts of primary money laundering concern

[14] Prableen Bajpai, "The 5 Most Important Virtual Currencies Other Than Bitcoin," last modified December 10, 2014, http://www.investopedia.com/articles/investing/121014/5-most-important-virtual-currencies-other-bitcoin.asp.

3) Darkcoins or Dash

Darkcoins was launched in 2014 by Evan Duffield. Later in March 25, 2015, the name was changed from Darkcoins to "Dash". One of major flaws of other VC's Proof-of-work system is transactional information being distributed to the public, or as we call the characteristic of decentralization. Duffield has solved this flaw, enhancing Darkcoins' autonomy, by adopting *Diffie-Hellman Key Exchange* along with the Proof-of-work system named X11; as a result, Darkcoins is considered the most autonomous VC. Moreover, Duffield has invented the *Proof-of-service* system and installed it in Darkcoins scheme in order to mitigate risks of cyber attack. The details will be further discussed in the subsequent part.

4) Peercoins

Peercoins, sometimes called PPCoin, Peer-to-Peer Coin or P2P Coin, was constructed by two program developers using pseudonyms Sunny King and Scott Nadal in 2012. Peercoins has been widely recognized as a VC, apart from the traditional Proof-of-work system, adopting the *Proof-of-stake* system. This approach generates significantly higher economic cost for those who intend to hack or crack the system.

5) Dogecoins

Dogecoins was firstly generated in 2013 by Billy Markus and Jackson Palmer. The operational function of Dogecoins is considerably similar to Bitcoins. However, in contrast to Bitcoins and other types of VC, Dogecoins does not have a ceiling limiting the amount of coins generated in the system; therefore, there are an extremely huge number of coins circulated in the scheme, compared to other types of VC, leading to a significant loss of value per coin. For this reason, Dogecoins is considered particularly useful for conducting transactions involved small amounts of money.

6) Primecoins

The first coin of Primecoins was distributed in 2013 by Sunny King, one of two

programmers who had created Peercoins a year before. The prominent feature of Primecoins is an application of prime number or prime chains composed of Cunningham chains and Bi-twin chains in the Proof-of-work system, facilitating miners in the mining process so that general people without superpower computers can be an effective miner of Peercoins as well.

B. Architecture behind Virtual Currencies: The Science of the Blockchain

The operating system of VC is composed of two main components, that is to say, the representation of value, and the payment and settlement mechanisms.[15] VC can also be categorized as centralized, decentralized and hybrid VC. Centralized VC refers to the VC with all functions (i.e. issuance of the currency, mechanisms to implement internal rules, and payment and settlement process) integrated under one central entity's control.[16] Yet, the central entity operating all functions of centralized VC is considered by some agencies, such as FinCEN, as a financial institution. As for decentralized VC, there is no central entity responsible for operating or controlling any function. Sometimes, some decentralized VC are grouped into hybrid type since the function of issuing coins is controlled by a central entity, limiting the number of coins circulated in the system. In this way, such VC will be able to keep their high value by pressing down the inflation rate. However, this is only an overview of all relevant functions. If we focus on functions related to conducting transactions, one word that occupies them all is "Blockchain".

The Blockchain technology or as called in short, Blockchain is *"a distributed database which maintains a list of records, each of which is known as blocks."*[17] Definitely, the Blockchain is not a technology especially created for VC and *"has profound implications for*

---

[15] Dong He et al., "Virtual Currencies and Beyond: Initial Considerations," *IMF Staff Discussion Note*, January 2016, 8.

[16] Ibid, 8.

[17] Tony Scott, *Blockchain Blueprint to dissecting the hidden economy! Smart contracts, Bitcoin and Financial technology* (CreateSpace Independent Publishing Platform, 2016), 12.

many institutions."[18] In online network, we can distribute data as many times as we desire; for instance, you can send a picture to one of your friends; then send it to another friend and so on. Digital money, however, is a different story. We cannot spend the same amount of money, or more specifically, the same coin, more than once. Without a mechanism to eradicate double-spending, VC would, undoubtedly, not be able to replace traditional FinTech adopted by financial institutions (e.g. online banking and mobile banking). Satoshi Nakamoto leveraged the Blockchain technology and cryptography to create a *consensus mechanism,*[19] solving, as he called it, *the double-spend problem.*[20]

As hinted previously, one of the most important characteristics of VC is decentralization. The meaning is very simple: the use of a common, fully public ledger.[21] To understand the term "public ledger", let's consider the current monetary systems. Apart from cash stored in wallets, most people keep their money with a trusted third party (e.g. financial institutions). These third parties place people's money in centralized ledger and provide financial services, such as credit card, to facilitate the owners of money to conduct financial transactions from anywhere. Centralized ledger, therefore, indicates a ledger with money of many people kept and managed by a central agency. On the other hand, public ledger implies to a ledger with money of many people kept and managed by the public. Prior to the invention of the internet, it is impossible to create such decentralized system within the scope of the global economy.[22] With a hand of the internet, global communication has been narrowed down significantly. Nakamoto took advantage from this point and envisioned a public ledger based on two fundamental assumptions: (1) a mechanism to publicly display each record-keeper's

---

[18] Don Tapscott and Alex Tapscott, *Blockchain Revolution How the technology behind Bitcoin is changing money, business and the world* (New York: Portfolio/Penguin, 2016), 8.
    [19] Ibid, 30.
    [20] *See* Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," last modified October 2008, https://bitcoin.org/bitcoin.pdf.
    [21] Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency How Bitcoin and the Blockchain are challenging the global economic order* (New York: Picador, 2016), 120.
    [22] Ibid, 122.

work and to maintain the integrity of the ledger that everyone agrees on its accuracy; and (2) incentives for individuals or firms to dedicate resources to the upkeep of such ledger.[23]

After an overview of the basis idea of the Blockchain, I will elaborate more about technical details which might be difficult to understand, but necessary to get the concept of economic and social challenges caused by VC.

1) Timestamping

In computing, timestamping is a technical term referring to the usage of a digital timestamp to provide a concurrent execution.[24] In VC context, timestamping means the system used to approve transactions conducted in the scheme, or, as we have roughly observed in the previous part, the Proof-of-work, the Proof-of-stake and the Proof-of-service system.

The Blockchain was built based on the unique qualification of *Hash function (Hash)*. Hash is a kind of computer operations investigating any set of data's accuracy. During the process of investigation, a computer will adjust a set of data into a number called *Hash value*; then, this Hash value will act as a *Checksum*, checking for such set of data's accuracy. The probability that two different sets of data will have the exactly same Checksum, or technically called the problem of *Collision*, depends on complexity of Hash function. For example, an identification number of Thai citizen is a sequence of 13 single numbers. In fact, only 12 first numbers can indicate a person's identity; whereas, the last number acts as the Checksum, assuring the accuracy of the first 12 numbers. As a result, if we know the Hash function of any person's identification number, we will be able to find the last number, or the Checksum, with only 12 first numbers in the sequence.

Nakamoto utilized this Hash function to endorse any transaction conducted in the Bitcoins system. First of all, after a transaction has been conducted, information related to such

---

[23] Ibid, 122.

[24] *See* N B Venkateswarlu, *Computer Science and Information Technology for GATE* (New Delhi: McGraw Hill Education, 2014), 5.37.

transaction will be distributed to the public that every user in the system can access. It can be said that every user is a custodian of the information. The Hash value will be designated to each transaction; and transactions which have already been endorsed will be grouped and chained together as a *block*. In each block, a number called *Nonce* is designated. This Nonce must be the number that can be inserted into the Hash function and make the Hash value of the first endorsed transaction in the block equal to 0 bits.[25]

To approve transactions, a miner has to group unendorsed transactions distributed in the system into a block; then calculate for the Nonce by randomly picking probable Hash functions. The correct Hash function must consist of the Nonce that makes the Hash value of the first transaction in the block equal to the value between 0 to 1 bit (0 bits).

For instance, let's assume that the 10,000[th] block has the Hash value equal to 0.000000abcd111. A miner must find the Nonce which, after inserting into the correct Hash function, makes the Hash value equal to this 0.000000abcd111. This process of calculation is called mining coin or mining. There must be, at least, six same results from six different miners in order to approve transactions within one block. After being endorsed, such block will be chained to previously endorsed blocks. To make any change in any particular already-endorsed block, one must, apart from re-calculating for the Nonce of the targeted block, re-calculate for the Nonce of every block tailed after the targeted block, causing a massive economic cost to do so. Hence, returns of committing fraud is considered unworthy, compared to the cost. This is the Proof-of-work system utilizing the science of the Blockchain, firstly adopted by Satoshi Nakamoto in the Bitcoins system.

---

[25] In computer systems, the smallest unit is "bit" which consists of only two value, that is, 0 and 1 (Yes or No). Computers receive an order in the form of a sequence of bits. However, when analyze to the level of quantum computer, there is a smaller unit than bit called "qubit". In Blockchain science, the term "0 bits" refers to a number in qubit unit which has value between 0 to 1 bit.
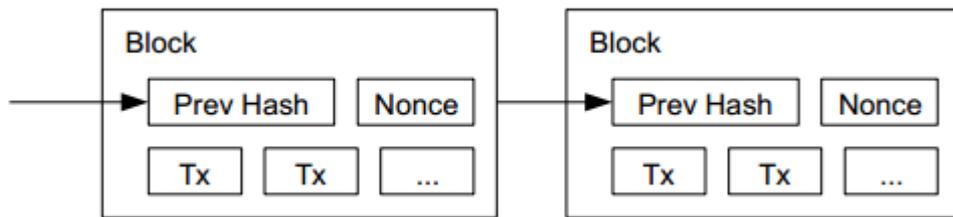
Figure 1: The Bitcoins' Proof-of-work system

Source: Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System,"
last modified October 2008, https://bitcoin.org/bitcoin.pdf.

The basis idea of the Proof-of-work system of other types of VC is somewhat similar to the Bitcoins'. One of major differences is an algorithm used to generate Hash functions, or so-called *Hash algorithm*, in each type of VC. To be more specific, Bitcoins and Peercoins use a Hash algorithm named SHA-256d. Litecoins and Dogecoins use Scrypt; whereas, Dash and Primecoins use X11 and 1CC/2CC/TWN respectively.

Each miner in the system will receive coins as a reward from mining, which highly consumes resources and energy of computers. As a consequence, one who possesses a superpower computer always achieves mining process faster than one with a lower-power computer. The efficiency of mining process is called *Hashrate*. Miners sometimes gather together to coordinate in mining process. If a miner pool occupies more than 50 percent of Hashrate in the system, such miner pool will achieve an ability to control the whole system. We call this phenomenon the *51 percent attack*. It is not a problem that can be easily solved as Nakamoto himself stated in his original paper that *"the bitcoin mining network could be guaranteed to treat everyone's transaction fairly and honestly so long as no single miner or mining group owned more than 50 percent of the hashing power."*[26] Malevolent users creating a block of fraudulent transactions will definitely fail to approve such block if they do not possess more than 50 percent of hashing power or Hashrate of the system. Owing to the

---

[26] Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency How Bitcoin and the Blockchain are challenging the global economic order* (New York: Picador, 2016), 151.

complexity of Hash functions, the probability that one would win enough of the mathematical puzzles in order to gain majority Hashrate is close to zero. Yet, for a powerful conglomerate, the story is different. In June 2014, the pool GHash.IO saw its share of total Hashrate becoming close to 50 percent, fluctuating between 40 percent and 50 percent throughout the month.[27]

The developer of Darkcoins had seen the problem of the 51 percent attack, including the waste of computer's resources and energy, in mining process. On average, mining one block of Bitcoins spends approximately ten minutes; however, each block must be approved six times by six different miners; thus, to approve only one block of Bitcoins, one hour of time is wasted. To solve both problems, the 51 percent attack and the waste of resources, Darkcoins therefore adopts the two-tier system. Before moving further into details about the Darkcoins' two-tier system, it is important to understand one technical term regularly found in computer science context, that is, a *node*. Node is defined as a single actor in the system. In the computer network, the computers are the nodes.[28]

In the Darkcoins two-tier system, there is an actor designated as a *masternode* operating the Proof-of-service system. Certain functions, such as creating new blocks, are managed by miners as the first-tier; whereas, in the second-tier, masternodes will handle other service-related functions, that is to say, PrivateSend, InstantSend and governance. PrivateSend is a coin-mixing service based on CoinJoin which has an underlying idea that, in order to retain autonomy of transactions' information in the system, the system has to pool all inputs from all nodes together, preventing a third party from figuring out which input comes from which node. To simplify, let's assume that there are four nodes: A, B, C and D in the system. A wants to pay 15 coins to B, and C wants to pay 10 coins to D. A then inputs 20 coins into the system and B has to input 5 coins as change. Likewise, C inputs 15 coins into the system and D inputs

---

[27] Ibid, 152.
[28] Roger Wattenhofer, *The Science of the Blockchain* (California: Inverted Forest, 2016), 5.

5 coins as change. To prevent other users from finding out that 20 coins input comes from A, 5 coins input comes from B and so on, all inputs have to be pooled together.
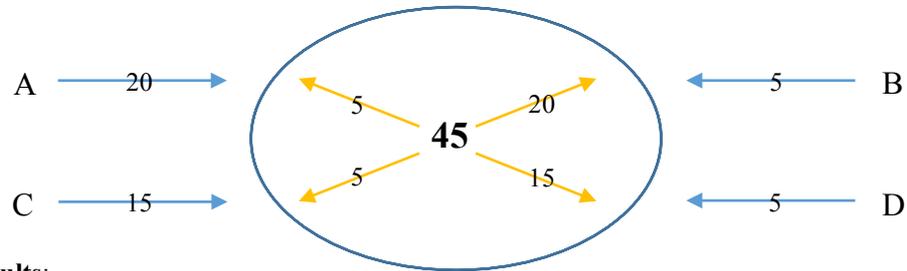
Final results:
A pays   -20+5 = **-15**
B receives 20-5 = **15**
C pays   -15+5 = **-10**
D receives 15-5 = **10**

Figure 2: The CoinJoin method

In this way, no one will be able to figure out which input comes from which user since all inputs are pooled together as a lump sum of 45 coins before further distributing to parties of the transactions. However, users can lock their inputs to be used for only their transactions by using InstantSend service. With this service, the transaction will be processed almost instantly, but users will not be able to enjoy the same level of autonomy as users of PrivateSpend service.

Masternodes in Darkcoins system can be anyone who possesses more than 1,000 coins.[29] Masternodes must retain this amount of coins in possession; otherwise, the status of masternodes will be automatically revoked. After any mining process being achieved, each masternode will receive 45 percent of reward,[30] as the same amount as a miner, even though masternodes do not have any role in mining at all. This significantly creates an incentive to become a masternode. At the same time, it also creates an incentive for masternodes themselves to oversee miners, mitigating a risk of the 51 percent attack. Further, the system of masternodes can also prevent the *Sybil attack*. The Sybil attack is an event when a user adopts some kinds of technique to create more than one identity for one node. Normally, one node can have only

---

[29] *See* "Masternodes," https://www.dash.org/masternodes2/.
[30] Ibid.

one identity. The requirement that a masternode must have more than 1,000 coins in possession, which means more than 1,000 coins per one identity, generates high cost for the Sybil attack since creating two identities of masternodes requires 2,000 coins, three identities requires 3,000 coins, and so on.

Additionally, the Darkcoins' Proof-of-work system deploys the Diffie-Hellman Key Exchange (D-H) method, enhancing the level of its autonomy. The parties using the D-H method will agree on some parts of transactions while keeping some parts secret. For example, A and B have agreed on a number P and a base G, so that both parties know P and G. Then, A chooses a secret number @, which B does not know, and sends B the input ($G^{@}$ mod P). Similarly, B chooses a secret number #, which A does not know, and sends A the input ($G^{#}$ mod P). Now, A has the input ($G^{#}$ mod P) and B has the input ($G^{@}$ mod P); whereas, A knows the secret number @ and B knows the secret number #. Next, A computes (($G^{#}$ mod P)$^{@}$ mod P)), and B computes (($G^{@}$ mod P)$^{#}$ mod P)), based on the assumption that (($G^{#}$ mod P)$^{@}$ mod P)) = (($G^{@}$ mod P)$^{#}$ mod P)). Finally, both A and B will reach the exactly same result without knowing the secret number of each other.[31] By deploying the D-H method, although the inputs are distributed to the public, no one can figure out the final result since only A knows the secret number @ and only B knows the secret number #.

The Proof-of-work system of Primecoins also features a unique technique. Miners in the Primecoins system have to figure out prime chains which are sequences of prime numbers. The Primecoins' Proof-of-work system accepts only three patterns of prime chains: Cunningham chain of the first kind, Cunningham chain of the second kind and Bi-twin chain. Consequently, mining coin in the Primecoins system does not consume too much computer's energy and resources as other types of VC because those three prime chains have fixed patterns

---

[31] *See* Bill Young, "Foundations of Computer Security Lecture 52: Diffie-Hellman Key Exchange," https://www.cs.utexas.edu/~byoung/cs361/lecture52.pdf.

which do not require highly complex calculation.

Next, we will move to the Proof-of-stake system initially adopted by Peercoins. In the Proof-of-stake system, a factor indicating an efficiency of mining process is not only the power of computers, but also the amount of coins possessed by each miner. The more coins a miner has, the more coins such miner can conduct mining. Thus, the probability of the 51 percent attack is relatively low because to commit the 51 percent attack, a malevolent miner must have, in possession, more than half of the amount of coins circulated in the system. However, the Proof-of-stake system triggers a new problem of monopoly since a miner who has a lot of coins in possession can mine for a lot of coins in return as well. In other words, this system encourages rich people (miners with a lot of coins) to seek more fortune (getting high reward from mining) for themselves and become even richer, whereas prevents the poor (miners with few coins) from getting better financially. Another advantage of the Proof-of-stake system is that users have an incentive to possess the large amount of coins, keeping the demand rate above the supply rate and suppressing the inflation.
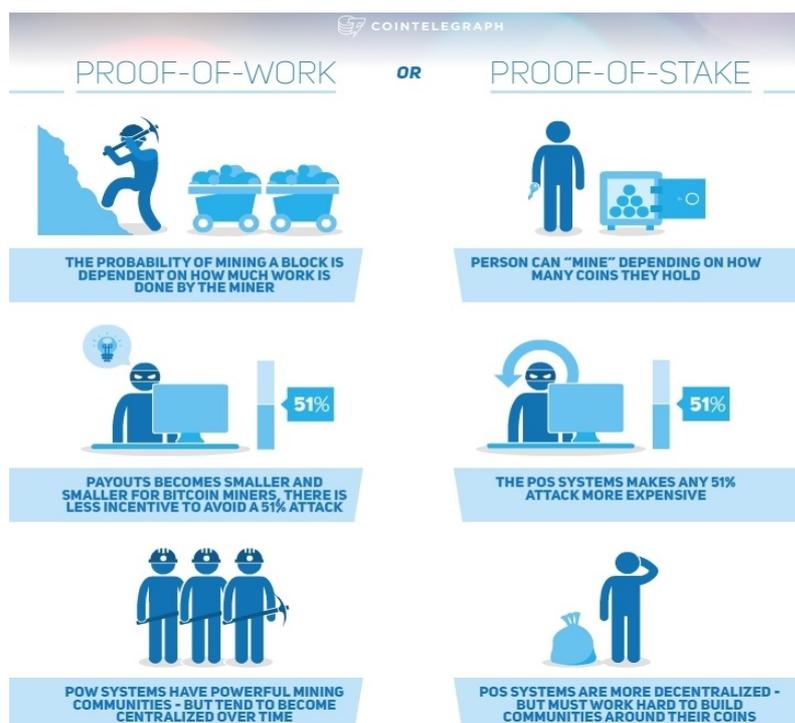

Figure 3: The difference between the Proof-of-work and the Proof-of-stake system

Source: "The Inevitable Failure of Proof-of-stake Blockchains and Why a New Algorithm is Needed (Op-Ed)," last modified May 24, 2015, https://cointelegraph.com/news/the-inevitable-failure-of-proof-of-stake-blockchains-and-why-a-new-algorithm-is-needed.

2) Conducting transactions

It has been a deceptive perception among users that VC is truly anonymous; however, in fact, it is not *entirely* anonymous. This part will elaborate the function of conducting transactions in the Bitcoins system since it is a principal idea for most types of VC.

There are three terms related to transactions conducted in the Bitcoins system, that is, *wallet address*, *public key* and *private key*. To start using Bitcoins, every user must generate a wallet address consisting of a complex string of numbers and letters (both lower- and uppercase). This wallet contains all relevant information and allows the owner of the wallet to spend or receive funds, similar to a bank account. The wallet address works as the owner's identification in the system. Each wallet address, also, contains pairs of a private key and a public key that are all related to each other mathematically.[32] The private key is used as a personal signature when the owner of each wallet wants to send funds to other people, or in other words, wants to spend money stored in the wallet. Whereas, the public key is used to confirm the owner's identity while receiving funds from other people.

Every user can generate their own public and private key pairs as many as they want. To receive payment, a user provides one of the public keys that they generated to a payer. Since each user is the only one knowing his/her own private key corresponding to such public key, he/she is the only one who can spend the money received by such public key.

Satoshi Nakamoto has brought us a prominent revolution of privacy model in financial world. The traditional privacy model deployed by banks and financial institutions limits access to the information to only parties involved in transactions and intermediaries or trusted third party. However, as Nakamoto noted, *"privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous."*[33] The only information that

---

[32] *See* Prypto, *Bitcoin for DUMMIES* (New Jersey: John Wiley & Sons, 2016), 79-90.
[33] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," last modified October 2008, https://bitcoin.org/bitcoin.pdf, 6.

the public can access is the fact that someone is sending an amount to someone else, but the public will not be able to link the transaction to anyone since true identities of users are concealed behind the wallet address and public keys. This is analogous to a privacy model used by stock exchanges, *"where the time and size of individual trades ... is made public, but without telling who the parties were."*[34]
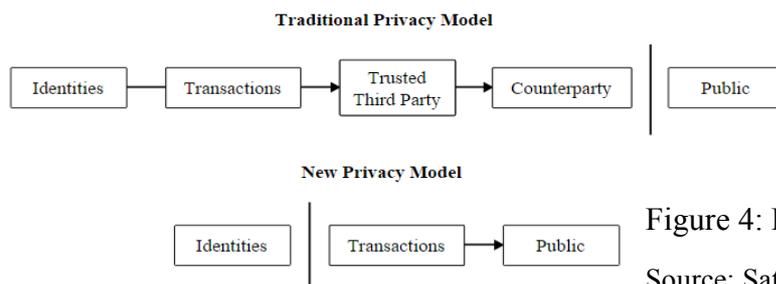

Figure 4: Privacy model

Source: Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," last modified October 2008, https://bitcoin.org/bitcoin.pdf, 6.

C. Pros and Cons of Virtual Currencies

VC is similar to a coin, having two sides. In many critiques related to pros and cons of VC, they can always be read otherwise; therefore, it is difficult to clearly categorize what is pros and what is cons of VC.

Let us first consider one of underlying characteristics of VC—decentralization. Contrast to other types of online payment systems, say, PayPal, which is part of eBay, users do not have to buy VC's software. That being said, there is technically no owner of the core software of VC.[35] In other words, anybody can download the code on the website for no cost, and start running it as a user or a miner. This characteristic provides people a more efficient and cheaper access to financial services, especially electronic payment services. However, the lack of ownership, in Intellectual Property Laws perspective, can be considered a flaw of the

---

[34] Ibid, 6.
[35] Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency How Bitcoin and the Blockchain are challenging the global economic order* (New York: Picador, 2016), 77.

system since any imitator can *"use the same or similar aspects of [the] ... system"*[36] by simply *"download the software, copy it, and build something new from it. Lawsuits for copyright or patent infringement are ... not concern."*[37] Yet, to examine whether this is actually a flaw, one major question needed to be answered prior to any further analysis is who is a stakeholder in Intellectual Property regime. As Satoshi Nakamoto who invented Bitcoins has never stepped out from shadow and claimed his stake—seemingly implying that he has no need of legal protection in this regard—there is no use to apply Intellectual Property Laws to VC and even more unreasonable to attach jargons of Intellectual Property infringement to any kind of VC that copied a basis system from Bitcoins.

Let us, next, consider a more serious concern about VC: being used as a tool to commit crimes. One of the most prominent explicit and widespread examples of threat that VC has exposed to the world outside the internet is a case of *the Silk Road*. Thomas R. Carper, the former Chairman of the Committee on Homeland Security and Governmental Affairs, United States Senate, gave a brief description about this case in his opening statement in the hearing before the Committee that, in 2013, *"[the United States] federal law enforcement took down and seized [the Silk Road,] an online marketplace ... on which many illegal products and services were bought and sold via bitcoin. The most popular products for sale were illegal drugs and forged documents. ... [A]pproximately $1.2 billion dollars in transactions were made through the Silk Road."*[38] As he subsequently commented that *"[t]he anonymity of the market place and near anonymity of the currency made it nearly impossible for law enforcement to track and, therefore made it an attractive place for criminal activity. ... Today, a number of similar enterprises that accept bitcoins are still in business, selling weapons, child*

---

[36] Ibid, 89.
[37] Ibid, 89.
[38] "Opening Statement of Chairman Thomas R. Carper Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies," November 18, 2013, https://www.hsgac.senate.gov/download/?id=a8de9c3e-c568-4d85-bd3c-1c2365695c47.

pornography, and even murder-for-hire services,"[39] it seems that VC is absolute villains that *"the federal government and society as a whole need to come together to figure out how to effectively deal with it."*[40] However, as Mythili Raman, then acting assistant attorney general, criminal division, the United States Department of Justice, claimed in the testimony presented in the same hearing, this point of view is a conclusion derived from looking *"at [V]irtual [C]urrencies through the lens of criminal law enforcement."*[41] Then, if we flip the coin and look at VC through the lens of businessperson, will the conclusion remain the same? It is true that products sold through the Silk Road site were illegal and morally offensive; still, the Silk Road was the first big Bitcoins business, proving that Bitcoins, or VC, *"could operate as a legitimate currency ... [and the Silk Road itself could be] a critical catalyst for this particularly rapid phase of community formation."*[42] The Silk Road, additionally, *"helped put bitcoin in the hands of thousands of newcomers, many of whom were now looking to use it for things other than drugs."*[43] In all, while the governmental entities view VC as a tool for criminals, the business sector see a promising potential from it.

Furthermore, although anonymity of VC can, definitely, mask wrongful behavior, VC allows and enhances law-abiding people to have privacy on the terms they want it. By this I mean, the use of VC provides people their own defined privacy and this privilege should not be diminished by governments.[44] In addition, the ease of using VC is beneficial not only to

---

[39] Ibid.
[40] Ibid.
[41] Committee on Homeland Security and Governmental Affairs United States Senate, *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies* (Washington: U.S. Government Printing Office, 2014), 7.
[42] Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency How Bitcoin and the Blockchain are challenging the global economic order* (New York: Picador, 2016), 87.
[43] Ibid, 87.
[44] *See* "Testimony of Patrick Murck General Counsel, the Bitcoin Foundation to the Senate Committee on Homeland Security and Governmental Affairs Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies," November 18, 2013, https://www.hsgac.senate.gov/download/?id=4cd1ff12-312d-429f-aa41-1d77034ec5a8.

criminals, but also to those who lack access to financial services.[45]

The anonymity and the ease of transferring VC, in contrast, incentivize criminals to threat victims to give ransom in a form of VC. As can be seen from an incident that has just happened at the time of this paper, the WannaCry ransomware program, firstly emerged on May 12, 2017, has been attacking users of Microsoft Windows all around the world in exchange for a large amount of Bitcoins.

As to economic aspects, VC supporters have depicted even more dreamy prospects. They claim that VC has built a road map to prosperity and global financial inclusion. More than two billion of the world's population that once lack of equal economic opportunity will be provided financial capabilities. VC, as a revolutionary FinTech, will create *"a whole new set of business models previously unimaginable that empower individuals as economic agents."*[46] Moreover, owing to Blockchain-based ledgers and the Proof-of-work system, transactional costs have been reduced significantly since any transaction conducted through the Blockchain system is *completely non-reversible*,[47] crushing down barriers to starting a company,[48] promoting startups and economic activities that these startups can accordingly generate.

On the other hand, anti-VC people have argued that VC is a threat toward an order of global economy due to the lack of oversight policies and concrete economic value. Fluctuation of VC's value is pursuant to a mutual agreement among users at a time, without any predictability, certainty or control. To give an illustration, in 2009, shortly after the first coin of Bitcoins had been circulated, 1 coin of Bitcoins (BTC) equaled to less than $1. However,

---

[45] Ibid.

[46] Don Tapscott and Alex Tapscott, *Blockchain Revolution How the technology behind Bitcoin is changing money, business and the world* (New York: Portfolio/Penguin, 2016), 179.

[47] Transactions conducted through financial institutions are not completely non-reversible because there are still disputes between parties of the transactions happening all the time. Normally, financial institutions integrate these dispute resolution costs into fees collected from parties of the transactions.

[48] Ibid, 179.

after the end of 2013, 1 BTC reached a peak at $1,240; then, in 2015, the value of 1 BTC plummeted to $450.[49] This characteristic of VC shows us that the value, including demand and supply rate, of VC is uncontrollable, rendering high risks to users, relevant businesses and ultimately economic stability in macro level.

III. Selected Laws and Regulations about Virtual Currencies

A. The United States

Although the usage of VC in the United States is not considered illegal, the U.S. government has not issued any regulation specifically controlling or overseeing the usage of VC. However, there are several existing legislations that can be interpret to cover VC; for instance, the Federal Criminal Mail and Wire Fraud Statutes, the Supreme court interpret this statute to cover the fraudulent actions in trading and exchanging VC.[50] Besides, the Constitution of the U.S. grants the Congress an authority to issue legislations regarding VC, considering from Article 1 of the Constitution: the Congress has power *"to coin Money ... [and] ... regulate the Value thereafter"*.[51] This Article, as analyzed by the Supreme court, has been, so far, interpret somewhat broadly.[52] Consequently, the definition of "money" in the Constitution Article 1 can be interpret to cover "digital money" as well.

In July 2016, the Miami-Dade Circuit Court held that VC was not "money" in the case *Florida v. Espinoza*. This case, the judge found for the defendant prosecuted for money-laundering involving VC, with the underlying opinion claiming that VC was certainly not

---

[49] Yessi Bello Perez, "Bitcoin Price Hits $450 For The First Time in 2015," last modified November 4, 2015, http://www.coindesk.com/bitcoin-hits-450-for-the-first-in-2015/.

[50] *See* U.S. Code Section 1341: Frauds and Swindles, and 18 U.S. Code Section 1343: Fraud by wire, radio, or television

[51] *See* the United States Constitution Article 1, Section 8, Clause 5

[52] Edward V. Murphy, M. Maureen Murphy and Michael V. Seitzinger, "Bitcoin: Questions, Answers, and Analysis of Legal Issues," last modified October 13, 2015, https://fas.org/sgp/crs/misc/R43339.pdf, 10.

considered money, the defendant, therefore, did not commit money laundering.[53] However, the federal and municipal governments think otherwise. They have recognized importance and influence, both positive and negative, that VC poses to the public. Thus, the government agencies have issued various guidance and standards regarding VC as described below. This paper will focus on only regulations and guidance issued by federal government agencies.

1) Internal Revenue Service (IRS)

Initially, although IRS saw VC as a kind of property that could be used only in online network—for example, exchanging for goods in online games—those who had VC income higher than outcome were subject to income taxation.[54]

Later, the Government Accountability Office (GAO), assigned by the Senate Finance Committee, issued a report noting that such IRS's guideline was not clear due to the lack of clarification which income category should be applied to VC, property, barter, foreign currency or financial instrument. Further, this guideline did not cover VC that could be used both in online and reality world, such as Bitcoins.[55] To comply with GAO's suggestion, IRS issued a new guideline designating that VC was property.[56]

2) The Consumer Financial Protection Bureau (CFPB)

In May 2014, CFPB received a report from GAO suggesting that CFPB should cooperate with other governmental entities to protect consumers from risks of using VC. In August, CFPB accordingly issued a guidance educating consumers about VC and its risks,

---

[53] *See* State of Florida v. Michel A. Espinoza, No. F14-2923, 2016, Circuit Court of the Eleventh Judicial Circuit in and for Miami-Dade County, Florida

[54] "Tax Consequences of Virtual World Transactions," last modified February 28, 2017, https://www.irs.gov/businesses/small-businesses-self-employed/tax-consequences-of-virtual-world-transactions.

[55] Edward V. Murphy, M. Maureen Murphy and Michael V. Seitzinger, "Bitcoin: Questions, Answers, and Analysis of Legal Issues," last modified October 13, 2015, https://fas.org/sgp/crs/misc/R43339.pdf, 10.

[56] "IRS Virtual Currency Guidance: Virtual Currency is Treated as Property for U.S. Federal Tax Purposes: General Rules for Property Transactions Apply," last modified September 14, 2016, https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance.

specifically emphasizing on Bitcoins.[57] In addition, CFPB also accepts complaints about VC filed by consumers.

3) Treasury's Financial Crimes Enforcement Network (FinCEN)

FinCEN issued a guidance relating to VC in 2013, indicating that users or VC-related businesses were not regarded as *Money Services Businesses (MSB)*; hence, any transaction conducted through VC system by these users or businesses was not part of *Money Transmission Services*, no need to register, record or report to FinCEN. However, as to businesses trading VC or exchanging VC for real currencies, they are *Money Transmitter* and subject to Bank Secrecy Act. Every regulation applied to traditional Money Transmitter is also applied to these businesses as well.[58]

4) Securities and Exchange Commission (SEC)

In the case *SEC v. Shavers* in 2013, the District Court held that Bitcoins could be used to buy goods or services and to exchange for real currencies. As a result, Bitcoins was considered "money". Investment Contract involving VC, thus, has become "Investment Contract" under Federal Securities Law and VC itself has become "Securities".[59]

5) Department of Homeland Security

Department of Homeland Security had a role in the case of Mt. Gox, which was a Japanese company trading Bitcoins both in the U.S. and Japan. The Department of Homeland Security saw that Mt. Gox engaged in financial services without permission, violating 18 U.S. Code Section 1960, so the Department of Homeland Security proceeded to seize the company's properties and accounts located in the U.S. Afterwards, Mt. Gox filed for bankruptcy in Japan.

---

[57] *See* "Risks to consumers posed by virtual currencies," last modified August 2014, http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.
[58] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," last modified March 18, 2013, http://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.
[59] *See* Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, No. 4:13-CV-416, 2013, United States District Court, Eastern District of Texas, Sherman Division

The company subsequently filed for protection under Chapter 15 of U.S. Bankruptcy Code and was granted as request.[60]

6) The Federal Reserve (FED)

In 2014, FED claimed that VC was not money and the operational system of VC was totally different from the system used in financial institutions, so that FED had no authority to control or oversee VC.[61] However, FED realized later that VC is a threat toward safety and soundness of financial institutions and economic stability; therefore, FED listed VC in "Watchful Waiting" for future consideration. Yet, FED, so far, has not issued any regulation or guideline regarding VC, except a research paper about Bitcoins.[62]

7) The Federal Bureau of Investigation (FBI)

FBI affirmed that, under current legal regime, prosecutors can forfeit VC through existing asset forfeiture laws as crime proceeds or as property involved in money laundering.[63] To be more specific, assets may be seized as proceeds of unlawful activity, defined in 18 U.S. Code Section 1956(c)(7) or as property involved in money laundering according to 18 U.S. Code Section 981(a)(1)(C) or 18 U.S. Code Section 982(a)(1).[64]

However, to conduct seizure of VC, FBI suggested that procedures provided by the current legal regime were not satisfying enough. Law enforcement officers must be authorized to take hold of or gain lawful access to the electronic media where the wallet resides. Then, FBI recommended an approach that VC should immediately be transferred to a government-

---

[60] "Bitcoin Firm Mt Gox wins brief US bankruptcy protection," last modified March 11, 2014, http://www.bbc.com/news/technology-26523826.

[61] Senate Committee on Banking, Housing, and Urban Affairs, "Semiannual Monetary Policy Report to the Congress," last modified February 27, 2014, http://www.banking.senate.gov/public/index.cfm?FuseAction=Newsroom.Video.

[62] Edward V. Murphy, M. Maureen Murphy and Michael V. Seitzinger, "Bitcoin: Questions, Answers, and Analysis of Legal Issues," last modified October 13, 2015, https://fas.org/sgp/crs/misc/R43339.pdf, 13.

[63] Brett Nigh and Alden Pelker, "Virtual Currency: Investigative Challenges and Opportunities," last modified September 8, 2015, https://leb.fbi.gov/2015/september/virtual-currency-investigative-challenges-and-opportunities.

[64] Ibid.

controlled wallet. This approach, according to FBI, was considered the most appropriate one since it would mitigate risks of criminals or suspects creating backup wallets.

This approach, nevertheless, should be noted that transferring VC from targeted wallets to the government-controlled wallet is an ordinary transaction conducted in the system that requires six endorsements from six different miners through mining process. There is no guarantee that the function of mining process will always work appropriately. As previously described, there is still the problem of 51 percent attack, which might trigger some errors in mining process and accordingly cause problems to the approach of VC seizure suggested by FBI.

B. The European Union

Prior to massive attacks by terrorists in several countries in the European Union (EU), EU passed no legislation regarding the status of VC. Only a report warning consumers about risks of trading Bitcoins was issued by the European Banking Authority (EBA). The report emphasized that VC was not regulated, generating a fatal legal loophole for criminals to utilize VC to commit crimes. The rationale for not regulating or overseeing VC, as raised by EU, was that VC was complicated and difficult to understand. Policymakers and regulators were still lack of proper knowledge to be responsible for VC and might render negative effects to the public rather than positive ones.[65] Although in Germany and France, VC services businesses must hold the same license as financial institutions, there were no substantial issues being raised by both countries and no big VC services companies located in both countries as well.

However, after an attack by terrorists in Paris in late 2015, EU was provoked significantly by the fact that VC was used as a tool for financing terrorism.[66] They,

---

[65] "Virtual Currencies Challenges following their introduction," last modified March 2016, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/579110/EPRS_BRI(2016)579110_EN.pdf.
[66] *See* "EU proposes stricter rules on Bitcoin, prepaid cards in terrorism fight," last modified July 5, 2016, http://www.reuters.com/article/us-eu-security-financing-idUSKCN0ZL1RH.

consequently, have started to amend *the Fourth Anti-Money Laundering Directive (the Fourth AMLD)*. The underlying proposed amendment is to broaden the definition of "money" to cover VC, and every transaction involving VC must be reported to the government agencies. Furthermore, they also plan to amend *the Payment Services Directive* that every payment service relating to VC must hold a license issued by the government.[67]

In the original Fourth AMLD, adopted in May 20, 2015, banks and payment institutions are under its scope, requiring them to comply with specific rules, ranging from specifying customer's identity, or so-called the "know your customers (KYC)" system, to monitoring financial transactions. VC operators, nonetheless, are left out.[68] After witnessing terrorism attacks in several countries throughout Europe, the European Commission proposed an amendment of the Fourth AMLD, bringing VC exchange platforms and custodian wallet providers[69] under the scope of the Directive.[70] In other words, according to this proposal, the KYC system will be applied to VC operators and platforms as the same as traditional financial institutions.

This proposal also addresses a question of why not just ban VC. No member state of EU or EBA, aside from issuing warnings about the risks that VC may entail, has actually banned them. The reason is simple as the Commission noted in the proposal that *"[VC is] often considered as a useful tool for international payment transfers, low cost money remittance and close to instantaneous payments."*[71] However, by applying the KYC system to VC, the

---

[67] "Virtual Currencies Challenges following their introduction," last modified March 2016, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/579110/EPRS_BRI(2016)579110_EN.pdf.

[68] *See* European Commission, "Questions and Answers: Anti-money Laundering Directive," last modified July 5, 2016, http://europa.eu/rapid/press-release_MEMO-16-2381_en.htm.

[69] *VC exchange platforms* are current exchange offices, trading VC for real currencies. *VC custodian wallet providers* are entities holding VC accounts on behalf of their customers, similarly to banks or payment institutions.

[70] European Commission, "Questions and Answers: Anti-money Laundering Directive," last modified July 5, 2016, http://europa.eu/rapid/press-release_MEMO-16-2381_en.htm.

[71] Ibid.

characteristic of decentralization of VC will be inevitably undermined, and, therefore, this proposed approach might be close to banning VC eventually.

C. The People's Republic of China and Hong Kong

"If you can't beat them, join them." This statement has been taken as a core concept of monetary policies in relation to VC by the Chinese government for some time.

The Chinese government views VC quite differently, seeing promising potential of VC as a device to promote economic activities and facilitate financial services. Although the Chinese government has officially issued *the Notice on Precautions against the Risks of Bitcoins*, prohibiting banks and payment institutions from dealing in Bitcoins, the People's Bank of China (PBoC), in 2016, announced that they were considering issuing Chinese VC. Prior to such announcement, in 2014, the PBoC had assembled a research team running its prototype cryptocurrency, or VC. It can be envisaged that by circulating PBoC-backed VC, the Chinese government will render a good opportunity to banks and other financial institutions to trump monopolies in payment services businesses (i.e. Alibaba's Alipay and Tencent's WeChat) since transaction costs will be lowered as the middleman is cut out of the process. To date, the research team has done trial runs of its prototype VC, stepping toward becoming one of the first major central banks issuing its own VC.[72] The research team also suggested an outline of how digital money could work as follows:[73]

- PBoC generates its own VC and transfers to commercial banks when more liquidity is needed.

- Customers can top up such VC from modified automated teller machines or from bank tellers. Then, customers store it in a wallet on their mobile phone or other device.

---

[72] "China Is Developing Its Own Digital Currency," last modified February 23, 2017, https://www.bloomberg.com/news/articles/2017-02-23/pboc-is-going-digital-as-mobile-payments-boom-transforms-economy.
[73] Ibid.

- Consumers can wire from their personal wallets to the merchant's account to purchase goods or services.

- The merchants deposit VC received from consumers into their commercial bank accounts.

Considering from the above outline, even though there is no clarification of how the Chinese government should designate the value of PBoC-backed VC, its value benchmark may be calculated quite differently from Chinese Yuan Renminbi (CYR) because the government intends to use this VC as an alternative to CYR to liquidate banks when necessary. There is no need to use VC in this task if the government has an authority to inject capital in the form of CYR into a failed bank. However, sometimes the government or private sectors do not have enough capital to liquidate big financial institutions, similar to what happened in the United States during the financial crisis 2008; and generating more money will severely damage economy.[74] As such, it is possible that the Chinese government intends to use VC as an alternative to CYR in this task in order to solve this problem. This triggers a question whether the Chinese government will authorize themselves to generate as many VC coins as they want without harming national economy. In saying that, I recall the value of CYR affected by the inflation rate as circulating more money in the system will definitely accelerate the inflation rate and decrease the value of the currency, affecting national economy as a whole. If the answer is yes—the Chinese government intends to authorize themselves to generate as many VC coins as needed without abusing economy, meaning that no matter how many they generate VC coins, the value of VC and CYR will not be affected—they must, as a first step, authorize themselves to freely designate value of such VC; otherwise, it will be driven by supply and

---

[74] If the government injects more money into the market, the inflation rate will immediately increase and the value of money will accordingly decrease. Normally, this approach, or so-called "Quantitative Easing (QE)", will be used only when the nation's economy is in the midst of a severe crisis and the market is in need of liquidation.

demand of the market; then, be out of control. To clarify, let's suppose that the Chinese government has an authority to generate coins of PBoC-backed VC as many as they want, but they do not have an authority to designate the value. When they want to inject capital into a failed bank using VC and they generate more coins into the system to do so, the value of such VC will, absolutely, decrease. This is a nature of currency, no matter in what form it is, digital or physical. Of course, VC that does not have stable value is not appropriate to be injected into financial institutions.

However, as suggested by the outline, the Chinese government wants to function its own VC through traditional commercial banks, which are subject to the requirement of a proper KYC system; as a consequence, there will be no anonymity characteristic in this VC and tradeoff is inevitable, just like the approach proposed by the European Commission as mentioned above.

Contrast to a positive perspective that the Chinese government has about VC, Bitcoins has spawned concerns on the surface. Confronting significantly high rate of inflation in Bitcoins[75] and a situation when a lot of people use Bitcoins to move money out of China,[76] PBoC summoned nine Bitcoins venues to a meeting in Beijing in early February, 2017, requesting them to halt Bitcoins withdrawals for a certain period of time. Two of the nine venues: Huobi and OKCoin, suspended withdrawals completely.[77]

As to Hong Kong, the authority shares the same perspective with the mainland Chinese government, seeing an abundant future of this Blockchain-based innovation. The flourish future of VC businesses in Hong Kong is reflected in a statement of Larry Cao, the director of content at the CFA institute in Hong Kong, saying that *"... [T]he impact of shifting to*

---

[75] Ibid.

[76] "China Bitcoin Exchanges Halt Withdrawals After PBOC Talks," last modified February 9, 2017, https://www.bloomberg.com/news/articles/2017-02-10/china-bitcoin-exchanges-halt-withdrawals-after-central-bank-talk.

[77] Ibid.

Blockchain-based digital money from the current payment structure goes beyond that. There's a potential you can pay anybody in the system, any bank, and any merchant directly. Blockchain will change the whole infrastructure. This is revolutionary."[78] Still, there was a prominent crime involving VC committed in Hong Kong. The website MyCoin in Hong Kong, which engaged in several Bitcoins-related businesses, induced investors to invest in a Bitcoins Ponzi scheme, deceiving them by promising to provide various special rewards to those whose investment reached the particular amount. The aggregated investors' loss was more than $8 millions.[79] However, both Hong Kong authority and the mainland Chinese government did not consider such problem seriously; thus, there has been no any regulation specifically addressing this problem issued so far.[80]

D. Singapore

The Singaporean government has quite balance perspectives about regulating VC. By this I mean, they realize risks that VC can be used by criminals to commit crimes (e.g. money laundering, purchasing illegal goods and financing terrorism), whereas, economic usefulness of VC cannot be ignored either, especially when Singapore is a country with economy mainly based on financial market. Agility and convenience to conduct transactions are, thus, absolutely crucial. With this rationale in mind, in 2014, the Monetary Authority of Singapore (MAS) issued a report guiding policymakers to properly settle a legal framework regarding VC. The focal part of this report emphasizes on regulating and overseeing one kind of VC services, that is, VC exchange and remittance in order to affirm that such business will not engage in money

---

[78] "China Is Developing Its Own Digital Currency," last modified February 23, 2017, https://www.bloomberg.com/news/articles/2017-02-23/pboc-is-going-digital-as-mobile-payments-boom-transforms-economy.

[79] Tanaya Macheel, "MyCoin Customers Report $8.1 Million in Losses to Hong Kong Police," last modified February 11, 2015, http://www.coindesk.com/mycoin-hong-kong-police-8-1-million/.

[80] *Regulation of Bitcoin in Selected Jurisdictions* (Kentucky: The Law Library of Congress, 2016), 11.

laundering or financing terrorism.[81] Notwithstanding such report, MAS has not yet proceeded anything substantial.[82]

Further, Singapore has laid down a taxation treatment of VC as follows:[83]

- Bookkeeping of income from selling goods or services

Any company or business with income from selling goods or services in the form of VC should record such income based on open market value and record it in Singapore Dollars. In the case that the open market value is unavailable, the company or business should use the rate of exchanging VC for Singapore Dollars at the time when the transactions are complete.

- Duty of paying tax

Profits, in the form of VC, gained from selling goods or services, or gained from mining coin process are considered as ordinary income. Those with such income have duty to pay tax at the same rate as personal income tax or corporate income tax as the case may be.

Investors who have capital gain from investing in VC do not have duty to pay capital gain tax since taxation law of Singapore does not recognize capital gain, both in real currencies or VC, as an income.

Apart from taxation law, Singapore has issued Sandbox regulatory, promoting FinTech; however, VC has not yet been included in the Sandbox scheme. Currently, MAS is working on the proposed regulations introduced for VC intermediaries operating in Singapore.[84] Nevertheless, VC, even though not yet regulated, is not illegal in Singapore, at least, not now.

---

[81] "MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks," last modified March 13, 2014, http://www.mas.gov.sg/news-and-publications/media-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.aspx.

[82] Alexander Loke, "Virtual Currency Regulation in Singapore," *Journal of Financial Regulation* (Oxford: Oxford University Press, 2015), 290-293.

[83] "Income Tax Treatment of Virtual Currencies," last modified May 15, 2015, https://www.iras.gov.sg/irashome/Businesses/Companies/Working-out-Corporate-Income-Taxes/Specific-topics/Income-Tax-Treatment-of-Virtual-Currencies/.

[84] "My FinTech Business involves cryptocurrencies. Do I need to apply for a licence?" last modified March 30, 2016, http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FAQs/Cryptocurrencies/2016/Cryptocurrencies-1.aspx.

In November 2016, MAS took an important move to explore the use of the Blockchain to facilitate interbank payment system.[85] Such move indicates that there is quite low probability that MAS will illegalize VC in the future.

IV. Strategies of Governments to Deal with Virtual Currencies

As previously discussed, although VC generates threats throughout the world's order in various aspects, it is also useful especially in terms of promoting economics and facilitating financial market functions. Therefore, governments, even of countries with high risks of terrorism and money laundering, are reluctant to completely ban VC. Figure 5 below shows us that there are only two countries in the world actually illegalizing Bitcoins. I use Bitcoins as a substitute for VC because Bitcoins is considered the most pervasively well-known VC these days.
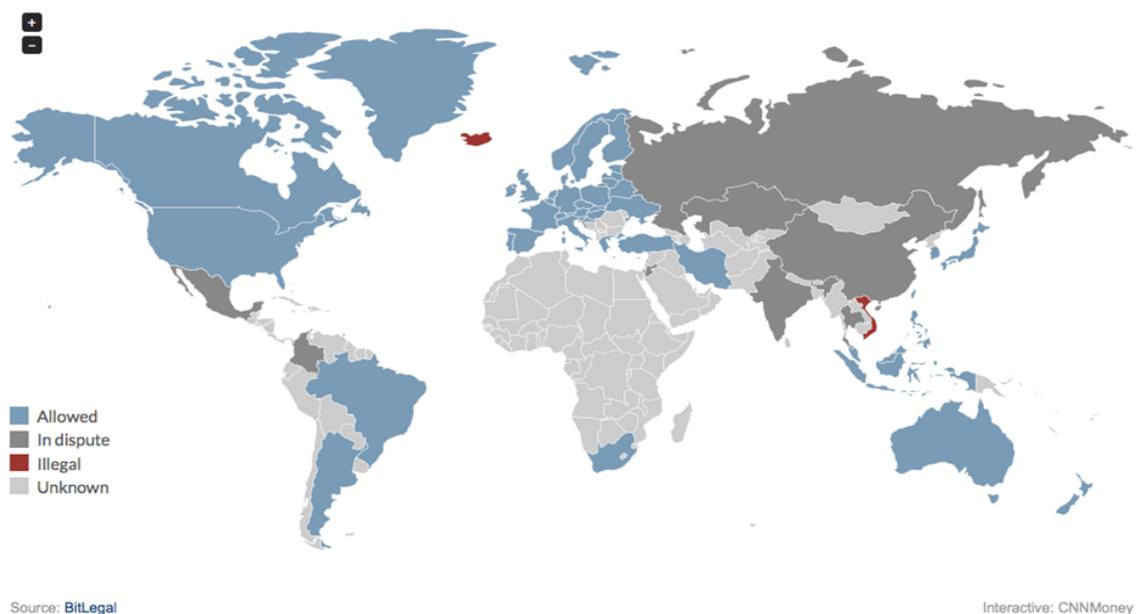

Figure 5: Bitcoins legal status around the world

Source: "Where is Bitcoin legal?"
http://money.cnn.com/interactive/technology/where-
is-bitcoin-legal/.

---

[85] "Singapore to launch blockchain project for interbank payments," last modified November 16, 2016, http://www.reuters.com/article/us-singapore-fintech-blockchain-idUSKBN13B07B?il=0.

From Figure 5, most authorities take hands-off approach, as the same as EU before Paris being attacked by terrorists, and China and Singapore before seeing potential of the Blockchain. I believe that this revolutionary innovation is a big thing in the FinTech era, both in positive and negative way; however, without an appropriate legal framework, VC will become closer to a villain either in criminal law perspective or in economics perspective. After considering different approaches taken by selected countries described in part III, I propose some frameworks that can be categorized into four main aspects as follows:

1) The framework for VC-related businesses supervision

Issues regarding VC-related businesses are one of the focal concerns of the United States and EU. They, definitely, should be addressed as the most important issue in VC regime as these businesses engage in a lot of high-value transactions, possessing and transmitting momentous amount of VC circulated in the system. It might be too far away from the concerns to see these businesses through the same lens as financial institutions; however, they cannot be considered as a kind of general companies, not involving in financial sector, as well. As such, it is important for these VC-related companies to retain their safety and soundness, as the same as traditional financial institutions.

In general, there is a capital requirement for banks and financial institutions. The most prevalent standard adopted globally is the *Basel III*, developed by *the Basel Committee on Banking Supervision* after the Basel II had failed to prevent financial institutions from collapsing during the financial crisis 2008. A methodology to calculate how much capital and liquidity that each bank must reserve, according to the Basel III, is based on customers' deposits that each bank keeps at a time.[86] We have to, firstly, understand the core business of traditional banks covered under the Basel III. These banks pay interest to customers who deposit money

---

[86] *See* "Basel III An easy to understand Summary,"
http://www.icreate.in/pdf/Basel%20III%20-%20An%20easy%20to%20understand%20summary.pdf.

with the banks, and lend such deposits to other customers, then collect interest from them. That being said, the amount of money deposited with the banks fluctuates all the time since the banks partly lend that money to other customers. The Basel III sets standard for the minimum capital that each bank must retain, depending on how much deposits they keep. This requirement cannot be applied to VC-related businesses seeing the difference between the core functions of banks and VC-related businesses.

Nevertheless, capital retained in any company can also indicate the size of the company and the quality of a management team. Provided that a company can achieve both aspects: having an appropriate size and having a fair management team, safety and soundness of such company are somewhat guaranteed. As a result, I propose that governments should require a VC-related business to hold a license; and at the time of applying for the license, such company must have a certain amount of capital, affirming its size, stability and management quality. This is entirely different from the capital requirement applied to banks set by the Basel III. The Basel III requires that capital of banks must always be remained, at least, no less than the designated benchmark while running the business, apart from registered capital requirement at the time that those banks applied for the licenses. To simplify, there are two types of capital requirement: (1) Capital requirement and (2) Registered capital requirement. The first type is calculated based on the amount of deposits held by banks at a time, so it is not suitable to be applied to VC-related businesses. However, VC-related businesses should be subject to the second type of the capital requirement to guarantee that they are capable to deal with this complicated and risky financial services.

Further, these days, development of VC scheme has been moving forward second by second. There is high potential that in the very near future, there will be VC-related businesses that engage in the taking-deposits-and-making-loans business like banks. The time when both types of capital requirement must be taken into consideration is approaching.

2) The framework for consumer protection

Generally, consumer protection measures have two major categories, that is, the measure requiring states to take action and the other one is that private actors must be active. As for the first category, it is a typical type when a consumer is exploited by a manufacturer. Such consumer can file a complaint to the Bureau of Consumer Protection; then, it is a responsibility of the bureau to react. For the second one, we normally find it in sophisticated issues such as investment in crowdfunding portals. In such issues, it is a burden for legislators to make sure that consumers are qualified enough to fend for themselves.

VC are unquestionably complicated for those who do not have proper basic knowledge. As a result, before allowing people to register, the system should provide reasonable training session. Afterward, a questionnaire testing such knowledge should be fulfilled with 100 percent correct answers. The training and questionnaire should cover an individual interest, operations of the system and risks against the public if deployed unsuitably.

3) The framework for illegal usage prevention

Due to anonymity characteristic of VC, it is nearly impossible for law enforcement officers to track criminals committing crimes through VC scheme. The only way that considered feasible is adopting the KYC system.

In VC system, as described in details in part II, users generate their own wallet addresses, private keys and public keys, and can generate as many as they want. Although authorities want to adopt the KYC system, authenticating users' identities, by requiring users to indicate their identities in wallet addresses, private keys or public keys, users can simply lie and fill in those fields with whatever they want. Still, the KYC system is viable in the VC scheme provided that a central agency is granted an authority to vouch for authenticity of public keys, similar to certificate authorities in the HTTPS ecosystem (e.g. world wide webs or

www).[87] In other words, the KYC system needs a hand of the central agency to appropriately function, undermining what is perhaps the main goal of VC—decentralization. However, after considering intense situations of money laundering and terrorism all around the world, the KYC system is inevitable, so as the central agency. I believe that undermining decentralization characteristic of VC will not result in undermining the whole system of VC, especially when governments truly promote this Blockchain-based innovation.

4) The framework for economic stability

As VC value can fluctuate significantly within a short time, the Central Banks or agencies responsible for issuing monetary policies must take a close look and should be authorized to prohibit exchange VC for real currencies for a period of time when considered necessary. Although it might not be helpful for VC-related businesses, general people who are involved in the scheme are protected and each national economy has a decent safeguard.

Another issue that is related to economic stability and considerably related to national security is cyber attack prevention. Even though it might be unlikely for high-tiered attackers to dedicate resources to VC as a prioritized target, it is still worth taking into consideration. When attack in cyberspace occurs, non-state actors or users in the system are indeed the first group of people recognizing. However, the sophistication and power of computers of non-state actors tend to be not high enough to prevent or retaliate the opponent. At this point, it is essential to arrange co-operation between state-level agencies and individuals. The government agencies undertaking IT issues must have experts in VC and be always ready to conform with complaints filed by private actors. Furthermore, this agency must be provided authority to shut down the system at anytime when needed. The amount of coins stored in each wallet address

---

[87] *See* Zakir Durumeric, James Kasten, Michael Bailey and J. Alex Halderman, "Analysis of the HTTPS Certificate Ecosystem," http://conferences.sigcomm.org/imc/2013/papers/imc257-durumericAemb.pdf.

after cyberspace attacks should be equal to the record at the moment that the system is cut off. This fact must be understood by users during the training session.

V. Conclusion

Nowadays, VC has become more important in financial sector. Thanks to the Blockchain technology, users of VC can retain their own terms of privacy and conduct financial transactions within a short time with relatively low cost. However, criminals also utilize VC to commit crimes, especially money laundering and financing terrorism. Countries confronting threats in this regard, such as the United States and EU, are seriously considering whether to supervise VC, whereas some countries, such as China, see a promising future of VC and want to use it to promote their economy.

I propose four frameworks to deal with VC. First is the framework for VC-related businesses supervision. Governments should have a registered capital requirement applied to these businesses in order to affirm that they are in appropriate size and are capable enough to deal with this complicated and risky scheme. Second is the framework for consumer protection. Adapting from a consumer protection measure in crowdfunding portals, there should be a requirement that consumers, before being allowed to register in the system, must pass training sessions, educating them about the complexity and risks of VC scheme, so that they are equipped with proper knowledge to fend for themselves. Third is the framework for illegal usage prevention. I see that it is inevitable to undermine some aspects of VC's decentralization. It is necessary to have a central agency to oversee and supervise the KYC system adopted in VC system; otherwise, it is almost impossible to track criminals using VC to commit crimes. Finally, the last proposal is the framework for economic stability. To prevent harm that VC might cause to the world outside the online network, central banks or agencies responsible for issuing monetary policies should be authorized to prohibit exchange VC for real currencies

when necessary. Moreover, there should be an agency co-operating with private sector to prevent cyberspace attacks.

Bibliography

Prableen Bajpai, "The 5 Most Important Virtual Currencies Other Than Bitcoin," last
modified December 10, 2014,
http://www.investopedia.com/articles/investing/121014/5-most-important-virtual-
currencies-other-bitcoin.asp.

Jeb Boone, "DEA undertakes first ever seizure of bitcoins by US law enforcement officials,"
last modified July 8, 2013, https://www.pri.org/stories/2013-07-08/dea-undertakes-
first-ever-seizure-bitcoins-us-law-enforcement-officials.

Zakir Durumeric, James Kasten, Michael Bailey and J. Alex Halderman, "Analysis of the
HTTPS Certificate Ecosystem,"
http://conferences.sigcomm.org/imc/2013/papers/imc257-durumericAemb.pdf.

Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima,
Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and
Concepcion Verdugo-Yepes, "Virtual Currencies and Beyond: Initial Considerations,"
IMF Staff Discussion Note, January 2016,
https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

Lars Hilse, *TREAT-ASSESSMENT: BITCOIN Danger to the United States' National Security
and her Economic & Commercial Interests* (Bunsoh: Lars Hilse, 2013).

Terence Lee, "Singapore Government Decides Not to Interfere with Bitcoin," last modified
December 23, 2013, http://www.techinasia.com/singapore-government-decides-
interfere-bitcoin/.

Alexander Loke, "Virtual Currency Regulation in Singapore," *Journal of Financial
Regulation* (Oxford: Oxford University Press, 2015).

Tanaya Macheel, "MyCoin Customers Report $8.1 Million in Losses to Hong Kong Police,"
last modified February 11, 2015, http://www.coindesk.com/mycoin-hong-kong-
police-8-1-million/.

J. Anthony Malone, *BITCOIN AND OTHER VIRTUAL CURRENCIES FOR THE 21ST
CENTURY* (California: NoHoMedia, 2016).

Edward V. Murphy, M. Maureen Murphy and Michael V. Seitzinger, "Bitcoin: Questions,
Answers, and Analysis of Legal Issues,"
https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," last modified October
2008, https://bitcoin.org/bitcoin.pdf.

Brett Nigh and Alden Pelker, "Virtual Currency: Investigative Challenges and Opportunities," last modified September 8, 2015, https://leb.fbi.gov/2015/september/virtual-currency-investigative-challenges-and-opportunities.

Yessi Bello Perez, "Bitcoin Price Hits $450 For The First Time in 2015," last modified 4, 2015, http://www.coindesk.com/bitcoin-hits-450-for-the-first-in-2015/.

Prypto, *Bitcoin for DUMMIES* (New Jersey: John Wiley & Sons, 2016).

Tony Scott, *Blockchain Blueprint to dissecting the hidden economy! Smart contracts, Bitcoin and Financial technology* (CreateSpace Independent Publishing Platform, 2016).

Don Tapscott and Alex Tapscott, *Blockchain Revolution How the technology behind Bitcoin is changing money, business and the world* (New York: Portfolio/Penguin, 2016).

N B Venkateswarlu, *Computer Science and Information Technology for GATE* (New Delhi: McGraw Hill Education, 2014).

Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency How Bitcoin and the Blockchain are challenging the global economic order* (New York: Picador, 2016).

Roger Wattenhofer, *The Science of the Blockchain* (California: Inverted Forest, 2016).

Sophia Yan, "China wants to launch its own digital currency," last modified January 22, 2016, http://money.cnn.com/2016/01/21/technology/china-digital-currency/.

Bill Young, "Foundations of Computer Security Lecture 52: Diffie-Hellman Key Exchange," https://www.cs.utexas.edu/~byoung/cs361/lecture52.pdf.

Bank of Thailand News issue 8/2014*, "Bitcoin and other similar electronic units," last modified March 18, 2014, https://www.bot.or.th/Thai/PressAndSpeeches/Press/News2557/n0857t.pdf.

European Commission, "Questions and Answers: Anti-money Laundering Directive," last modified July 5, 2016, http://europa.eu/rapid/press-release_MEMO-16-2381_en.htm.

FATF Standards, Recommendation 4 "Provisional measures and confiscation" February, 2012, http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

Global Legal Research Directorate Staff, the Law Library of Congress, *Regulation of Bitcoin in Selected Jurisdictions* (Kentucky: The Law Library of Congress, 2016).

Senate Committee on Banking, Housing, and Urban Affairs, "Semiannual Monetary Policy Report to the Congress," last modified February 27, 2014, http://www.banking.senate.gov/public/index.cfm?FuseAction=Newsroom.Video.

United States Government Accountability Office, *VIRTUAL CURRENCIES Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*, "Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate" (Kentucky: GAO, 2016).

Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies, "Hearing before the Committee on Homeland Security and Governmental Affairs United States Senate" (Washington: U.S. Government Printing Office, 2014).

The Present and Future Impact of Virtual Currency, "Joint hearing before the Subcommittee on National Security and International Trade and Finance and the Subcommittee on Economic Policy of the Committee on Banking, Housing, and Urban Affairs United States Senate" (Washington: U.S. Government Printing Office, 2014).

"Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," last modified March 18, 2013, http://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

"Basel III An easy to understand Summary," http://www.icreate.in/pdf/Basel%20III%20-%20An%20easy%20to%20understand%20summary.pdf.

"Bitcoin Firm Mt Gox wins brief US bankruptcy protection," last modified March 11, 2014, http://www.bbc.com/news/technology-26523826.

"China Bitcoin Exchanges Halt Withdrawals After PBOC Talks," last modified February 9, 2017, https://www.bloomberg.com/news/articles/2017-02-10/china-bitcoin-exchanges-halt-withdrawals-after-central-bank-talk.

"China Is Developing Its Own Digital Currency," last modified February 23, 2017, https://www.bloomberg.com/news/articles/2017-02-23/pboc-is-going-digital-as-mobile-payments-boom-transforms-economy.

"EU proposes stricter rules on Bitcoin, prepaid cards in terrorism fight," last modified July 5, 2016, http://www.reuters.com/article/us-eu-security-financing-idUSKCN0ZL1RH.

"Income Tax Treatment of Virtual Currencies," last modified May 15, 2015, https://www.iras.gov.sg/irashome/Businesses/Companies/Working-out-Corporate-Income-Taxes/Specific-topics/Income-Tax-Treatment-of-Virtual-Currencies/.

"IRS Virtual Currency Guidance: Virtual Currency is Treated as Property for U.S. Federal Tax Purposes: General Rules for Property Transactions Apply," last modified September 14, 2016, https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance.

"MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks," last modified March 13, 2014, http://www.mas.gov.sg/news-and-publications/media-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.aspx.

"Masternodes," https://www.dash.org/masternodes2/.

"My FinTech Business involves cryptocurrencies. Do I need to apply for a licence?" last modified March 30, 2016, http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FAQs/Cryptocurrencies/2016/Cryptocurrencies-1.aspx.

"Opening Statement of Chairman Thomas R. Carper Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies," November 18, 2013, https://www.hsgac.senate.gov/download/?id=a8de9c3e-c568-4d85-bd3c-1c2365695c47.

"Risks to consumers posed by virtual currencies," last modified August 2014, http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.

"Singapore to launch blockchain project for interbank payments," last modified November 16, 2016, http://www.reuters.com/article/us-singapore-fintech-blockchain-idUSKBN13B07B?il=0.

"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," November 19, 2013, https://www.fincen.gov/sites/ default/files/2016-08/20131119.pdf.

"Tax Consequences of Virtual World Transactions," last modified February 28, 2017, https://www.irs.gov/businesses/small-businesses-self-employed/tax-consequences-of-virtual-world-transactions.

"Testimony of Patrick Murck General Counsel, the Bitcoin Foundation to the Senate Committee on Homeland Security and Governmental Affairs Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies," November 18, 2013, https://www.hsgac.senate.gov/download/?id=4cd1ff12-312d-429f-aa41-1d77034ec5a8.

United Nations Office on Drugs and Crime, Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, Module 4 Seizure of Virtual Currencies, June, 2014, https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf.

"Virtual Currencies Challenges following their introduction," last modified March 2016, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/579110/EPRS_BRI(2016)579110_EN.pdf.