Virtual Currency is Becoming Reality:Is it Opportunity or Disaster?

Hak J. Kim
VIRTUAL CURRENCY IS BECOMING REALITY: IS IT OPPORTUNITY OR DISASTER?

By Hak J. Kim*

I. INTRODUCTION

Virtual Currency (VC) has recently become a key issue in finance field as a new type of payment system. With the advance of Internet technologies (i.e., computing and encryption), VC is rapidly evolving. According to Market & Research survey (2014), global virtual currency market has increased and will grow at the 8.52% in the compound annual growth rate (CAGR) during the period 2013-2018.

VC is a new financial product and has an extraordinarily dynamic nature of appealing to both financial markets and financial technologies. The pace of change is going to accelerate in next several years. However, VC is difficult for an average person to understand it because it is different from traditional currency (i.e., bills and coins). For example, the real currency in coins or bills and its transactions occurs through banks or other financial institutions, while VC is not involved this trusted party (or institutions). Instead, it uses a private peer-to-peer network. In that point, people concerns about the safety of money transactions and wonder how it maintains the value without physical objects. We will discuss these issues next section.

VC provides much potentials in financial payment system including faster (actually real-time) transfer and a reduction of transaction fee. However, it also has several concerns such as cyber security, illegal money laundering (i.e., crimes and terrors), and its unstable value.

VC has been little regulation and the development of its regulation is not easy because of its basic characteristics (i.e., transaction through a private peer-to-peer network and just an intangible object - bit). Recently several states begin to work for the development of regulatory rules for VC.

The New York Department of Financial Services (DFS) announced the final BitLicense Regulatory Framework for virtual currency businesses in New York on June 3, 2015. According to this regulation, virtual currency companies require a license to operate virtual currency business in New York State; for example, a holding customer can fund and exchange virtual currencies to dollars or other currencies.

In this paper, we present the conceptual-level understanding of virtual currency instead of its implementation details of how it is used in practice, and investigate current

* Associate Professor, Zarb School of Business, Hofstra University.

status of virtual currency focused on government regulation. Section II introduces the basics of virtual currency (VC) including concepts, history, system structure, and technology. Blockchain will be introduced as a core technology of VC. Section III identifies how virtual currency operates in market and how virtual currency is regulated by government. We conclude that virtual currency is becoming reality and its potential as the future of new payment system, but also has some concerns like cyber security and money laundering, in Section IV.

II. VIRTUAL CURRENCY

Fiat Currency vs. Virtual Currency

The main paradigm of Fiat Currency (FC) is the existence of the trusted 3rd party (i.e., banks and other financial institutes) to operate the financial system. FC traditionally uses physical objects (i.e., coins and bills), but recently introduces electronical payment through online system. Virtual Currency (VC) is created by an individual without involving any 3rd parties (i.e., government like federal/state reserve agencies). It is completely open to the public; that means anyone can create VC and use it for transaction. There is no need to go through banks for transactions. VC is an intangible object. It is just a bit.

Digital Currency vs. Virtual Currency

Digital currency is used to facilitate payment for physical goods and services. We pay money to obtain such currency, thus it has real value and can be exchanged at various locations depending on the terms and conditions. For example, Amazon coins is used to purchase books from amazon. It a direct relation with real world currency. At every given point we can calculate how much is the value of one amazon coin.

Virtual Currency (VC) is a type of cyber currency. Cyber currency is not based on physical reality like the coins collected in a mobile game. It has no value in real world and cannot be used in real world transactions. For example, we cannot use that currency for buying a book. There is no direct relation between these currencies and the real world currencies. VC is also called crypto currency. Example of a crypto currency is Bitcoin. Since its inception in 2009 by anonymous developer Satoshi Nakamoto. Bitcoin, a well-known Internet virtual currency, was introduced in 2009 and since then has received world-wide attention. However, many people think that Bitcoin is still difficult to understand because it uses a plethora of new concepts and complex technologies.

Financial System: Traditional vs. VC

The operation of money transfer between traditional financial systems and VC system is different. Figure 1 shows the conceptual system diagram and operation process of

---

6 Bitcoin.com
money transfer in two financial systems. For simple comparison, we make a scenario a simplified financial market with four people.

First of all, let's see the traditional financial system. Alice wants to transfer money ($50) to Bob or Charlie or David. Up until now, she has typically done it through a trusted 3rd party (i.e., banks or other financial institutions). This financial institute moves money for Alice after identifying Alice and the other party (i.e., Bob/Charlie/David)'s financial accounts, taking a small fee in the process. This process will take about three or more days to complete this transaction.

Unlike the traditional financial system, virtual currency system does not need a 3rd trusted entity as a medium. That means people talk directly to each other. It is faster (No wait time) than the traditional financial system in regards to a money transfer. It is also cheaper since there is no fee since there is no 3rd party. Instead of an intermediary, virtual currency system uses blockchain, which is a core technology of virtual currency system. The concept of blockchain will be explained in next section.

Now let's start with the scenario. Alice has $100 from the beginning which creates the first transaction. Now she wants to transfer $50 to Bob. This second transaction creates a link with the already existing transaction (link 1) and is recorded in both party's computers. After that, Bob attempts to move $30 to Charlie as a third transaction. As a result of this transaction, another link (link 2) is created between the third transaction and the second transaction. The next transaction between Charlie and David for a $10 transaction occurs. Link 3 is created as the same with the previous process. A chain of transaction is built. This is one of the reasons that this transaction in virtual currency is open and public to everyone.

In this virtual currency system, anyone in this network can see where the money is and how much money each one has in its pocket. Further, everyone can decide whether this transaction is valid or not. For example, if Alice attempts to move $150 to David, everyone in the network can see immediately that this is not a valid transaction because she started with $100 and does not have $150. This transaction will not be part of the chain.

Virtual currency system is not centralized, but distributed. Each individual user of the virtual currency system is able to obtain a copy of the ledger of each of his or her transactions. For example, David has a copy of the ledger about his transaction and holds it in his note. Alice can do the same and have a copy of the ledger. Anyone else who participates

![Figure 1. Comparison of Money Transfer Process](image-url)
in this network holds a chain of transactions. So, the ledger is distributed. We do not need the centralized place that holds those ledgers.

However, we create another problem. When people have various copies of the ledger within the network, the copies of the ledgers should be synchronized with each other to avoid any inconsistencies between the transactions. They should have the same copy (or version) of the ledger. For example, Bob wants to move $50 to David. Then, Bob will publish and broadcast this transaction to the network. Everyone in the network can see immediately that Bob wants to move $50 to David. This is an invalidated transaction because it has not been selected yet.

In order to go in depth about the network, we need to understand the concept of miner. A miner is a special node that holds the ledger. It is essentially a record-keeper, verifying and validating all of the transactions. Let's take for example in this case, Alice is a miner. Alice will compete with other miners to verify the information and sort these transactions into blocks. If Alice is the first to take this transaction, she gets a financial reward.

We need to understand what it means to win the competition. In order to be the first miner that is able to take this transaction and add to the ledger, a miner needs to do two things. First, (s)he needs to validate new transaction. It will be easily completed because the ledger is open and (s)he can immediately calculate whether someone has that amount to make the transfer. Second, a miner needs to find a special key that will enable this miner to take the previous transaction, erase it, and lock the new transaction. In order to find this scheme, this miner needs to invest computational power and time because the search for the key is random.

### III. CURRENT STATUS OF VIRTUAL CURRENCY

**Technology: Blockchain**

Blockchain has been emerged as a core technology of VC. Since there is no precedent technology in VC, companies are waiting for the validation of this technology including uses and benefits.

Blockchain is defined as a ledger that records everything happened in a chronological timeline. It tracks the history of all events and maintains their value. The information stored in the ledger is distributed through a peer-to-peer network. This network is dynamic and keeps growing with the increasing number of transactions. Since each participant in the network has a copy of the ledger’s data and distributed through network, all

---

VIRTUAL CURRENCY IS BECOMING REALITY

of the participants in a transaction has the same real-time ledger. Blockchain effectively removes the step of establishing trust between each of the parties, and instead allows for transparency between all participants in the transaction.

Figure 2 shows an example of blockchain process. Each block maintains its a hash, which is copied from the previous block (marked 'red-color'). It is a kind of chain from previous to the current. Modification in the blockchain is cumbersome and impractical because one change in a block would require a change to each subsequent block that comes after it.

Blockchain has four key elements; transaction, miners, blocks, and proof of work. The first element is transaction. Whenever VC is exchanged, it becomes a transaction. Each transaction is combined together and then forms a block later. Since each transaction is copied, one individual cannot prove legitimacy of VC. So, there has to a process to establish legitimacy of VC.

The second component is miners. Miners are people who monitor transactions as well as determine whether each transaction is legitimate or not. Each transaction carries encrypted keys of the payer and payee, and then form a block. At that time, miners decrypt this block, determine if the transaction was valid, and then publish their proof of work. Other miners can then verify this proof of work. The miners create a system of integrity by verifying each transaction by different people. This establishes the legitimacy of the transaction in that particular block. Why do miners go through such hassle? Every time a miner decrypts a block

---

14 Id.
he/she gets a compensation of 25 bitcoins. The monetary reward stimulates a miner to review other transactions while adding more legitimacy to the system of integrity.

The third component is blocks. As addressed above, when miners group several transactions together, it forms a block. These blocks contain the encrypted public keys of the payer and payee. All these blocks put together forms a chain. The blockchain is the core of bitcoin. It works as a ledger for all transactions. Every transaction goes through the block chain. Although this is open source, every user has a unique private and public key that identifies each user. This ensures anonymity and makes transaction untraceable.

The fourth component is proof of work. This is the sole way of verifying the legitimacy of a VC. As soon as the transactions are broadcasted, miners around the world start decrypting the blocks. The first one to publish verified proof of work, gets rewarded some VCs. This is the only way of generating new VCs.

Figure 3 shows the procedure of blockchain. Each transaction broadcasts to users every 10 minutes and then get together to form a block. The block is decrypted for the validation of transaction by the group of users. After its validation, the next transaction will be preceded.

Figure 3. The Procedure of Blockchain

**Market: Bitcoin**

At present, the most popular virtual currency (VC) in the market is Bitcoin. It is the currency of the Internet and the 90 percent of VC market value. Its daily transaction volume recorded US$70 million in 2015.

**What is Bitcoin?**

Bitcoin is a distributed, peer-to-peer, and encrypted currency. Unlike the traditional financial system, it is completely private without relying on a third-party intermediary. That means it is issued by an individual instead of by a government. However,

---

17 Id.
19 https://blockchain.info
bitcoin is a different kind of a digital currency\textsuperscript{21}. It breaks down conventional thinking in many aspects; for example, there is no central regulatory body, it introduces the mining concept, the open-ledger (blockchain), the way miners are rewarded, how the transporting value is determined by its packet size and not value, the hash rate, and the concept of limited supply. Bitcoin is a decentralized ledger, which means that there is no consolidated point for all of the ledgers to congregate at. Instead, the operation is distributed across many people in such a way that people who use the ledger can trust that what it says is actually true.

Bitcoin is a crypto currency\textsuperscript{22}. There is no trail of where it came from or where it is going, and apart from the sender and receiver, no one can know what the transaction was. Bitcoin can be considered as currency because it can be exchanged for goods and services. Furthermore, it is completely digital. Since every transaction takes place digitally, you cannot hand over a physical coin or a bill to someone to complete a bitcoin transaction.

Unlike traditional currencies, bitcoins are managed without any central authority (i.e., government, company, or bank). While this may be a disadvantage, bitcoin can be stronger to inflation. With bitcoin, we can be our own bank and perform all of our transactions.

Bitcoin is a ledger to record any events related to accounts and money transactions. Those transactions are stored on computers which are used for bitcoin transaction. Any numbers in this ledger is no meaning in the physical world. The number does not intrinsically have any value; rather, the only value is the willingness of the people to trade real goods and services for the high number reflected on their account.

Bitcoin can be exchanged in transactions, but its uniqueness lies in creating it. Banks does not print it and government does not regulate it. Rather, it does not belong to any nation. Only way to create a new bitcoin is to mine it. In reality, it is simply a verification of a bitcoin transaction. Anybody who verifies the transaction gets a reward in the form of newly created bitcoins. Rewards keeps miners interested in verification and thus keeps the system safer from frauds. This method creates a mix between security and transparency of a bitcoin.

\textbf{Dynamics of Bitcoin's Price}\textsuperscript{23}

The first transaction of bitcoin was a pizza order on May 22, 2010 in Florida by the user (Laszlo). The amount was 10,000 BTC for two pizzas\textsuperscript{24}. At that time price was around at $0.008.

On 11 April 2013, the bitcoin price grew to $0.08, which raises 1000% from July 2010. After that, the price of bitcoin was raised daily by 10% and finally recorded $266 which is the top of a price. However, the value of bitcoin was much fluctuated from $150–$200 in November 2013, rising to $600, and finally broke $1,000 on November 27, 2013.

The rising bitcoin was fallen because of bitcoin ban in China by a false report\textsuperscript{25}. Chinese government would seek to prohibit banks from working with digital currency

\textsuperscript{23} Summarized contents in Wikipedia.org.
\textsuperscript{24} Laszlo's pizza for $76,880 Archived April 12, 2014, at the Wayback Machine.
exchanges. After that, its price fell to $300 in 2015. In June 2016, bitcoin price again reached by $750.

Figure 1 shows the graph of Bitcoin price index from 2012 – 2016. Bitcoin’s price has been unstable (see Figure 1) with high price volatility.

![Figure 1. Price Volatility of Bitcoin (source: bitcoincharts.com, 2016)](image)

IV. REGULATION OF VIRTUAL CURRENCY

**Technology and Regulation**

Generally, a collision occurs between regulation and technology. Technology is growing fast and is advancing an innovative way of business, while regulation is conservative and slower than expected because it broadly may affect to other non-technology fields. For example, let’s see the financial industry. Information technology is rapidly introduced in financial systems and products and changed the way of financing (i.e., smart loans and customized insurances based on big data analysis), which is called ‘Fin Tech’. These innovative ways of finance territory have no regulations. Traditionally, a financial sector is required to have very tight regulation, but in the world today there are exceptions to these rules. In agile regulatory perspective, regulation in the finance industry should be updated quickly.

VCs are growing very fast in technologies as well as markets. Their companies develop new types of VCs and do businesses differently to sell and buy VCs. As a result, suddenly both technology and regulation are trying to coexist with each other. Both sides have a responsibility to find common ground to have loosely regulated virtual currency coexist with regular, highly regulated currency.

Congress

Congress shows continuing interest in VC, but is still at the exploratory stage. There are several hearing activities to be held by several Committees. On November 18, 2013\textsuperscript{29}, the first hearing for virtual currency (VC) was held in Congress. In this hearing, Congressmen pointed out issues of bitcoin’s skyrocketing price and its illicit use for crimes.

The Government Accountability Office (GAO) issued a report \textsuperscript{30}, “Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges,” in May 2014, which is in response to the request from the Senate Homeland Security and Government Affairs Committee. In this report, the GAO described the efforts of federal agencies and law enforcement agencies to virtual currency, but pointed out the lack of efforts to protect consumers. So the report recommended that the Consumer Financial Protection Bureau (CFPB) \textsuperscript{31} should more attention to consumer protection by its participating in interagency task forces. As of the date of the GAO inquiry, the CFPB responded that it would do all efforts to deal with virtual currency by communicating with federal, state, and international regulators. It also would identify interagency working groups addressing VCs and enhance its own work for consumer protection.

On March 16, 2016, the US House Subcommittee on Commerce, Manufacturing, and Trade held a meeting on digital currency and blockchain technology\textsuperscript{32}. In this hearing, there echoed many concerns of VCs including a consumer’s lack of understanding about VC, consumer protection, VC’s high price volatility, money laundering, and terrorism financing. This hearing mostly consisted of educating the congressmen on the basics of bitcoin, blockchain and digital currencies.

Federal/State Government

Unlike Congress, federal government agencies are actively scrutinizing VCs for not preventing crimes and hackers.

The Securities and Exchange Commission (SEC) Office of Investor Education and Advocacy issued an investor alert on bitcoin and other VC-related investments on May 8, 2014\textsuperscript{33}. It described a heightened fraud risk of bitcoin investment. It also provided the links to past SEC and FINRA investor alerts on digital currency, ITS VC guidance, and VC’s recent lawsuits and cases.

\textsuperscript{29} The first hearing on “Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies” in US Congress on November 18, 2013.


\textsuperscript{31} See http://www.consumerfinance.gov/


The Internal Revenue Service (IRS) issued a notice to provide answers about frequently asked questions on VC (i.e., bitcoin) in March, 2914. According to this notice, VC can be used for pay tax as a property for federal tax purposes.

Some states (i.e., California, Connecticut, and New York) are studying and have been moving to develop rules for virtual currencies for protecting users and supporting the expansion of market. For assisting those states to develop regulations of VCs, the Conference of State Bank Supervisors (CSBS) released a CSBS Model Regulatory Framework on September 15, 2015. In this model, the CSBS addressed several key issues including definition of VC, covered activities, licensing requirements, on ramp, use of licensing system, financial strength and stability, consumer protection, cyber security, and supervision.

The BitLicense Regulatory Framework: A Case

The New York Department of Financial Services (DFS) announced the final BitLicense regulatory framework for virtual currency businesses in New York on June 3, 2015. It is the first state regulation to address virtual currency firms. This regulatory framework is a crucial step forward for the maturation of the Bitcoin blockchain protocol and other virtual currency businesses. This framework is created after the two-year regulatory inquiry that the NY State DFS began in 2013.

The key characteristics of the BitLicense regulation framework are summarized as follows;

First, the regulation framework focuses on only material changes to companies' products or business models (i.e., a wallet service for offering exchange services). Minor things (i.e., software upgrades) are not controlled.
Second, the regulation framework applies to virtual currency businesses (firms), not software developers. A regulator is interested in the need for heightened regulatory scrutiny to help ensure that consumer’s money does not just disappear into a black hole.

Third, the regulation framework prefers a one stop application submission for licenses (i.e., BitLicense and the money transmitter license) that covers all the bases companies need.

Fourth, companies that already file suspicious activity reports SARS with federal regulators such as Vincent do not have to file a duplicate set up those stores. The goal of regulation is to avoid duplication where possible.

Fifth, companies also would not need prior approval from DFS for every new round of venture capital funding. Generally, a company only needs prior approval, if the investor wants to direct the management and policies up the firm, which is known regulatory jargon is being a control person.

New York State DFS granted a trust company charter under the New York Banking Law to itBit Trust Company on May 6, 2015. As a result, itBit became the first chartered and prudentially regulated virtual currency exchange in the United States. It started business in New York and gradually spread in the nation.

V. CONCLUDING REMARKS

Summary

In the above, we attempted to understand virtual currencies (VCs) and investigated its current status, focusing on technology, market, and the regulation of VC.

The existing payments system (i.e., banks and other financial institutes) with physical objects (coins and bills) is safe, secure, and appropriately regulated. It is also centralized, publicized, and visible. While the VC system (i.e., no trusted 3rd party) with an intangible object (i.e., electronic bits) is unreliable, unsecure, and unregulated. It is also decentralized, privatized, and invisible. However, with the recent development of core technology (i.e., blockchain), VC get completely different impression to users as well as regulatory agencies. It means that VC is secure, faster, and cheaper. Because of that, the market of VC is rapidly growing.

Regulatory organizations (i.e., Federal/State government agencies) began to develop the regulatory framework of VC for consumer protection and anti-money laundering. We believe that its regulation will promote and support companies that use new emerging technologies to develop better financial products. For example, the final BitLicense Regulation Framework from New York State Department of Financial Services (DFS) will give consumers greater trust about VC and promote investment to VC market.

Future of VC

VC is now becoming a reality and can rapidly change the existing financial systems. People no longer talk about how it can be used in real life. Instead, they think of how it can be

45 itBit.com https://www.itbit.com/
used better for their businesses. VCs have a lot of potential benefits including faster (i.e., real-time) and cheaper (i.e., lower fees) transactions.

The critical success of VC is the participation of government to encourage businesses to put it to use. Because of the development of regulation by government, people will be able to better understand it. VC has the potential to transform the interplay between government, companies and individuals. It can enable more efficient interactions between government and businesses regarding taxes and other payments. For example, VC can be used for dealing with social security tax combined with social security systems which include federal government, employers, their payroll service providers, beneficiaries, and working individuals. That future is coming, but it's slower.

**Challenges**

As addressed in the above, Bitcoin, a typical VC, has high volatility for its price which means that its value significantly fluctuates on a daily basis. Its price volatility makes it hard to predict the financial market and difficult for companies to be able to trust Bitcoin.

Currently VC market is growing rapidly, however its users and size of transactions are still small. As of 2016, the total value of VC market is about US $7 billion, while U.S. currency is US$1.4 trillion. Because of that, the acceptance in the real-world business is limited and VC’s use as a medium of exchange is significantly restricted.

Since the nature of VC is borderless, it can be used for tax evasion, money laundering, and terrorist financing. In the national level, regulatory agencies are currently developing the regulation framework to protect consumers. However, there is no guideline for the international level regulatory framework including technology standards and practices. Current VC’s lack of legal status in the international level will limit foreign virtual exchange and increase illegal money laundering activities.