CENTRAL
EUROPEAN
UNIVERSITY

CAN BITCOIN BE SELF-REGULATORY LEGAL TENDER? : A COMPARATIVE ANALYSIS OF UNITED STATES, EUROPEAN UNION AND ISLAMIC LEGAL SYSTEMS

By Mohammad Mahmoud Ibrahim Tayel

LL.M. SHORT THESIS
COURSE: European Company Law
PROFESSOR: Caterina Sganga.
Central European University
1051 Budapest, Nador utca 9.
Hungary

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

The thesis provides a comparative overview of US, EU and Islamic legal classifications of Bitcoin as legal tender. Focusing on the volatility and irreversibility issues, the thesis shows that the volatility is caused by external factors and not internal factors of the money. Historically, the thesis shows that these factors are used to be efficiently regulated by self-regulatory standard, namely the gold standard. The dominant underlying reason of the gold standard is the scarcity of the gold, which is considered to be the basis of Bitcoin. However, the thesis explores that usefulness and qualitative effort of the commodity are the real policy rationale behind the gold, which is manifested in the dual purpose mining process of Bitcoin. This model serves as the key to recognize Bitcoin as legal tender in the US and the Islamic business laws, with an exception to EU due to the single sovereignty currency and market. The irreversibility, in turn, is discovered to not be an issue *per se*. In addition, it shows that the traditional regulations in the selected jurisdictions of the consumer protection rules are applicable to Bitcoin transactions.

INTRODUCTION

Virtual currencies in cyberspace spread around the world in two stages: in a closed-flaw centralized format exchangeable for traditional US dollars backed by governmental debt, such as the Linden Dollar; then in an opened-flaw, debased and decentralized network which had its own value-measurement, such as Bitcoin. Bitcoin's network can be understood as analogous to the ant colony. Each ant is a unit in a decentralized caste-based community, and their functioning and exchanging of services are operating in light of trusted network norms.[1]

The marketplace of Bitcoin has experienced an exponential growth, with around 14 million Bitcoin (BTC)[2] in cyberspace circulation with an estimated transaction volume of 46 billion USD.[3] On one hand, there is still no solid rationale for why Bitcoin has taken off to such a spectacular extent; some researches referred to the novelty of Bitcoin's design and features as well as its immediate global availability over the cyberspace,[4] while others referred to its resistance-power to inflation[5] or the gold repatriation movement.[6] On the other hand, there are still disputes on the accurate classification of Bitcoin, whether it is valuable money, private currency or a priced commodity, which thereby has an impact on its implications and regulatory framework. Hence, it became a realm of critical swamp with confusing yardsticks and serious heated rhetoric.

Globally, money is considered the backbone of the national and international trade. That is the reason why its measurement has to be based on a clear standard in order to create certainty

[1] Andreas Antonopoulos, 'Preface', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014)

[2] Blockchain, ' Total Bitcoins in Circulation' < http://blockchain.info/charts/total-bitcoins> accessed 10 February 2015

[3] Blockchain, ' Currency Stats' < https://blockchain.info/stats > accessed 10 February 2015

[4] Florian Glaser 'and others, 'Bitcoin-Asset or Currency? Revealing Users Hidden Intentions' (2014) < http://ecis2014.eu/E-poster/files/0917-file1.pdf > accessed 22 March 2015

[5] Andreas Antonopoulos, 'ch1', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014)

[6] Koos Jansen and Tuur Demeester, 'The Gold Repatriation Movement' < http://www.bullionstar.com/blogs/koos-jansen/tag/bitcoin/ > accessed 5 March 2015

and mirror the dual-duties of the transactional relationships without spillover effect. The thesis attempts to provide a clear classification of Bitcoin by unwrapping its layers and features and compare it with traditional money and commodities. The legal analysis of the subject beforehand will be conducted in light of US, EU and Islamic business law (IBL) for practical and theoretical considerations.

Practically speaking, the selected jurisdictions are due to the wide growth of Bitcoin users and Bitcoin-ATM across the US, EU and the Arabian Gulf.[7] It has been reported that there are over 1.6 million users of a US-based Bitcoin exchange called "Coin-base" which is licensed to operate in half of US states,[8] and it is now embarking on European expansion.[9] Another practical consideration for the selected jurisdiction is the tendency towards digitalization whether in Europe (the Digital Agenda for Europe[10]) or in the Gulf (Dubai Smart Government Program[11] and Capital of Islamic Economy[12]).

Theoretically speaking, Bitcoin is not radically different from conventional methods of exchange, but there is widespread ambivalence about it among the general public. A recent survey in the UAE Bitcoin market revealed that 73% of the participants were uncertain of the level of compliance of Bitcoin with IBL.[13] Similarly, US lawmakers are in dispute on its classification. Regardless of the fact that the Internal Revenue Service (IRS) has assigned Bitcoin as barter on the grounds of the market-orientated approach,[14] the growth of Bitcoin is still a serious challenge for the US Federal Reserve as a barrier to meet its ability and

---

[7] Coindesk <http://www.coindesk.com/bitcoin-atm-map/ > accessed 7 February 2015

[8] Chris Isidore, 'First U.S.-Based Bitcoin Exchange Opens' *CNN* (26 January 2015), <http://money.cnn.com/2015/01/26/investing/bitcoin-exchange-coinbase/> accessed 7 February 2015

[9] Tanaya Macheel , 'Coinbase Expands European Service to 5 More Markets' Coindesk (October 2, 2014) < http://www.coindesk.com/coinbase-expands-european-service/ > accessed 5 March 2015

[10] <http://ec.europa.eu/digital-agenda/digital-agenda-europe > accessed 7 February 2015 , "The aim of DAE strategy expressly mentioned as "to reboot Europe's economy and help Europe's citizens and businesses to get the most out of digital technologies"

[11] <http://www.tradearabia.com/news/MISC_274175.html> accessed7 February 2015, "E-Pay system for online payment of Dubai government fees witnessed a 25 percent increase from the previous year on the ground of recent statistics from Dubai Smart Government Department (DSG)" <http://www.tradearabia.com/news/MISC_274175.html> accessed7 February 2015

[12] Thomson Reuters, 'Global Islamic Economy Report (2013)' < http://www.dinarstandard.com/state-global-islamic-economy-report-2013/> accessed 7 February 2015

[13] Anu Singhal and Aqila Rafiuddin, 'Role of Bitcoin on Economy' (2014) 2(1) WCECS 4<http://www.iaeng.org/publication/WCECS2014/WCECS2014_pp1028-1033.pdf>accessed 22 March 2015

[14] CNBC <http://www.cnbc.com/id/101515483> accessed 7 February 2015

objectives.[15] Likewise, some of the European member states such as Finland[16] and Germany have taken action regarding Bitcoin. While Finland considers Bitcoin as priced commodity, Germany has recognized it as private currency[17] yet other countries at European level by and large are in the wait-and-see stage.

The thesis is divided into four chapters; chapter one will provide an explanation of the building blocks of Bitcoin, by exploring the fundamental mechanism, governing codes, history and development of Bitcoin protocol and currency. Given its technical functioning, the legal classification will be followed by in Chapter two which will compare the mechanism and policy rationale of money and priced commodities vis-à-vis Bitcoin from a historical perspective and examining whether the current building blocks of Bitcoin resemble the features of precious-commodity money, which used to be self-regulated or paper money, which has to be regulated, concluding that it can be self-regulated in some jurisdiction unless it is not volatile. In chapter three, the thesis shows the main reasons behind the volatility of Bitcoin and argues that the policy rationale behind the precious metal as a monetary value was not as claimed solely due to its deflationary nature and scarcity, but rather due to the effort exerted and cash-cost (cost of production to get the precious metal). Hence, the thesis will conclude that the digital money, in order to resemble the stability features of precious metals in its purchasing power, has to be standardized according to its usefulness and economic energy of its production (i.e. BTC backed by valuable economic energy) alongside the legal analysis of dual-purpose analysis of mining Bitcoin. Last but not least, it will shed light on consumer protection-related issues (e.g. irreversibility and privacy issues with reference to the compared jurisdictions).

---

[15] Craig Elwell and M. Maureen Murphy and Michael Seitzinger , 'Bitcoin; Questions, Answers and Analysis of Legal Issues' (2015) Congressional Research Service 2 < http://www.fas.org/sgp/crs/misc/R43339.pdf> accessed 22 March 2015

[16] Europarl < http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-003807&language=EN > accessed: 7 February 2015

[17] Matt Clinch,' Bitcoin Recognized by Germany as 'Private money' (2013) < http://www.cnbc.com/id/100971898> accessed 7 February 2015

CHAPTER 1: THE BUILDING BLOCKS OF BITCOIN

To evaluate regulatory efficiency in a meaningful and credible way, it is important to break down each of the related features of Bitcoin, both as money and as a digital payment scheme, and compare it with the traditional monetary scheme. Only then can the legal and economic implications could be adequately measured.

1.1 What is Bitcoin protocol?

In the cyberspace, Bitcoin is widely known as a means of exchanging value between contracting parties in an open-flow system. It gives the contracting parties the ability to purchase, transfer and exchange values directly, and without intermediaries such as financial institutions or governmental intervention. Unlike traditional monetary schemes, Bitcoin is governed by built-in algorithm/computer codes, which constitutes the building blocks of its digital crypto-currency. The way this works can be better understood with an example.

The case is about a group of transacting parties who live in a decentralized trust network not yet governed by computer codes. Each of them has a special value (skills/profession), *inter alia*: Alice (freelance translator), John (car-mechanic), Mary (dentist) and Adam (restaurant owner).

Adam offered a gift-card with a value of 100 meals and drinks for dental service from Mary. The gift-card was payable to any holder on demand and was authenticated by specific signature and notarized by time-stamp. Mary had no willingness to eat out, but she accepted the offer since she would use the gift-card as a medium of exchange with a third party. She then signed, notarized and exchanged the card for a translating work provided by a freelance translator, Alice.

4

Meanwhile Alice's place of residence was far away from the restaurant, so she accepted the offer after the car mechanic who was fixing her car (John) expressed his willingness to exchange his labor and car parts for the card. Hence, Alice followed the process of exchanging the card after signing and notarizing it. John therefore consumed the value of the card.

The decentralized scheme mentioned above as an example is highly impractical for everyday transactions in a fast-paced global economy. Furthermore, these issues include disputes over the value of a chosen medium of exchange, the trust of the decentralized network, signature forgery, counterfeiting by the issuer and the imbalance in the market. Any of these issues are capable to lessen the incentive of the referred entities and produce a negative economic impact on the community's welfare.

In lived experience of conventional financial markets, the regulatory framework throughout history was be managed and ruled by three main models. The first model is the centralized power model, which attempts to regulate and ensure the financial equilibrium of the market. The second model is the natural standard model, such as the precious metals, which regulates the market with no human authority or intervention. The last model is the decentralized algorithm-based model, which is represented in Bitcoin. [18]

Bitcoin has similarities and differences to the imaginary decentralized community. By examining each feature separately, we could argue that the decentralized feature of Bitcoin is similar to the imaginary case in sense that users/entities work together to validate transactions. Each user validates the transaction by functioning as an input for the value already transferred, and as an output for the value to be transferred and so on and so forth (as shown

---

[18] This categorization strands on the observation of the historical events and legal rationales as will be explored in the following chapters

in Figure 1). After all, the transactions overall form what is called the chain/hash, whereby everyone in the Bitcoin network accepts the authoritative record of ownership.[19] This is the essence of the Bitcoin design according to the theoretical author of the currency, Wei Dai (1998). According to him, the efficient cooperation among the decentralized users in the crypto-community requires a medium of exchange whereby users participate in its issuance process and thus confirm its legitimacy.[20]

With regard to the signature forgery issue, this is highly unlikely in Bitcoin. The e-signature of Bitcoin is an advanced electronic signature which consists of a mathematically related private and public key. The public key is similar to a bank account number, while the private is akin to a secret PIN,[21] albeit with a much more advanced technique. It should be noted that these features of Bitcoin have already played an essential role in preserving the digital money from counterfeiting/double spending. By introducing the network timestamps/digital signatures, users can prove their ownership of the value and provide legitimate grounds for any claims.[22]

---

[19] Andreas Antonopoulos, 'ch8', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014)

[20] Wei Dai, 'B-Money' < http://www.weidai.com/bmoney.txt, 1998> accessed 10 February 2015

[21] Andreas Antonopoulos, 'ch4', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014) *(("Alice's key provides the signature that unlocks those previous transaction outputs, thereby proving to the bitcoin network that she owns the funds. She attaches the payment for coffee to Bob's address, thereby "encumbering" that output with the requirement that Bob produces a signature in order to spend that amount. This represents a transfer of value between Alice and Bob"))*

[22] Nakamoto Satoshi, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008), < https://bitcoin.org/bitcoin.pdf > accessed 22 March 2015 *(("by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work"))*
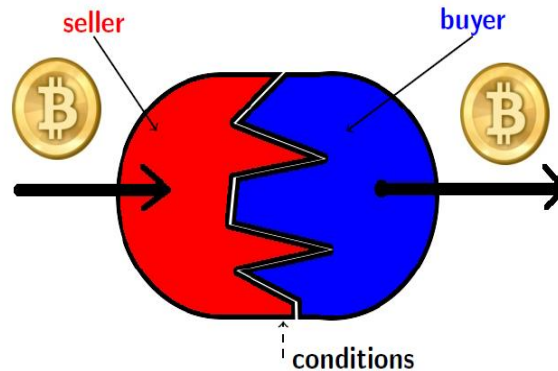
Figure 1: Digital hash chain[23]

Unlike the imaginary decentralized group, the second distinguished feature of Bitcoin is its transparency. All users of Bitcoin are able to trace and follow the chain of transaction, since the platform is transparent. It is accessible throughout a public ledger known as Block-chain. Hence, Bitcoin is not fully anonymous, but it is pseudonymous in the sense that users' public addresses can be monitored but not identified in order not to prevent abuse by hackers.

The last comparable feature is the value determination/purchasing power of Bitcoin. Unlike the gift-card of the imaginary decentralized group, which can be issued and printed easily by the restaurant owner, Bitcoin is designed to be finite and diminishing (approximately every four years) in order to resist inflation, preserve its purchasing power and avoid volatility. However, despite these measures it remains highly volatile (Figure 2).[24]

[23] Laszlo Csirmaz, 'Secret of Bitcoin', CEU Net workshop 4 (2014)

[24] Bitcoin magazine <https://bitcoinmagazine.com/wp-content/uploads/2013/08/bitcoin-volatility-compared.png> accessed 4 March 2015

7
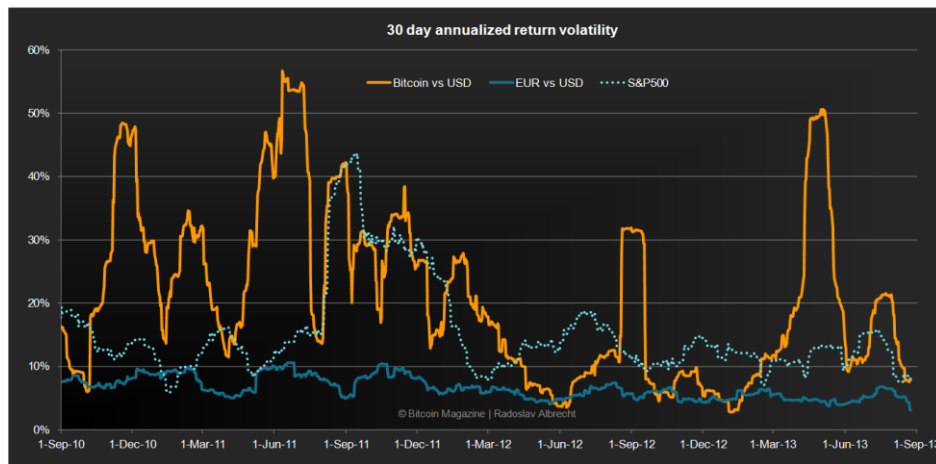
Figure 2: Thirty day annualized return volatility

As explored above, Bitcoin is a digital medium of exchange used by digital transacting parties. These transacting parties exchange value directly peer-to-peer without any financial or governmental interference. In order to ensure the legitimacy of Bitcoin's ownership, users participate together in a voting-like algorithm-based system known as proof-of-work, which provides the emergent consensus of all transactions between the output and input chain. These transactions are finally recorded on the authoritative record of ownership known as the block-chain. It is publically distributed and can be accessed by any users.

1.2 What is Bitcoin's currency? Who issues it?

Antonopoulos answered these questions, he stated that "The exception to the output and input chain is a special type of transaction called the coinbase transaction, which is the first transaction in each block".[25] Satoshi referred to this transaction as "the first transaction in a block… starts a new coin owned by the creator of the block… provides a way to initially distribute coins into circulation, since there is no central authority to issue them".[26] As currencies are printed and gold is minted, Bitcoin is digitally created through a process called

---

[25] Andreas Antonopoulos, 'ch5', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014)

[26] Nakamoto Satoshi, 'Bitcoin: A Peer-to-Peer Electronic Cash System' 4 (2008)

8

mining. The miners of Bitcoin are decentralized programmers who have two functions. The first function is to create brand-new chains for hashing new transactions. Hence, they simultaneously issue new Bitcoin payable to themselves as a reward for mining. The second function is to verify the existing transactions of the users against payable-fees for the verification-services.

The mining process is regulated between the miners by built-in algorithms protocol. This algorithms-based system adjusts the average of success between the miners every 10 minutes. It is inherently finite and deflationary. That means that Bitcoin is halved every four years and a fixed total amount of coins are in circulation (currently set at 21 million).[27]

As a result, the more Bitcoin is diminished, the more difficult it becomes to find the target solution for the mathematical problem, and thus it becomes harder to win a new Bitcoin. To simplify, we can imagine the following game as stated by the cryptocurrency researcher Andreas M. Anthonpoulous:

> Imagine a game where players throw a pair of dice repeatedly, trying to throw less than a specified target. In the first round, the target is 12. Unless you throw double-six, you win. In the next round the target is 11. Players must throw 10 or less to win, again an easy task. Let's say a few rounds later the target is down to 5. Now, more than half the dice throws will add up to more than 5 and therefore be invalid. It takes exponentially more dice throws to win, the lower the target

---

[27] Andreas Antonopoulos, 'ch8', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014) *((The amount of newly created bitcoin a miner can add to a block decreases approximately every four years (or precisely every 210,000 blocks). It started at 50 bitcoin per block in January of 2009 and halved to 25 bitcoin per block in November of 2012. It will halve again to 12.5 bitcoin per block sometime in 2016. Based on this formula, bitcoin mining rewards decrease exponentially until approximately the year 2140, when all bitcoin (20.99999998 million) will have been issued. After 2140, no new bitcoins will be issued))*

gets. Eventually, when the target is 2 (the minimum possible), only one throw out of every 36, or 2% of them, will produce a winning result.[28]

The rule of the hashing/mining is a purely random, chance-based process. There is no guideline or procedure in advance on how to win a newly issued Bitcoin. In other words, the issuance of Bitcoin currently is a purely speculative zero-sum game in which the loss for Alice is a gain for Bob.

1.3 The history and development of Bitcoin's codes

Bitcoin is radically different from the imaginary decentralized community. While the transactions of the latter are mainly based on trust, Bitcoin users are governed by computer codes/features. These codes/features stand on 20 years of research in several fields, including cryptography, peer-to-peer network, decentralized consensus, economics, corporate governance, e-signature and currencies.[29]

The earliest research was about the anonymity feature. In 1982, David Chaum introduced the concept of the cryptographic signature public/private key which has to be certified, used and widely distributed by a central authority.[30] In 1999, Tomas Sander, and Amnon Ta-Shma attempted to replace the centralized anonymity with a decentralized hint-based system, which can prove the authentication of the ownership claim without a need for revealing the identity of the transacting parties, this system also known as zero-knowledge technique. However the result was not effectively workable.[31]

---

[28]ibid

[29] Andreas Antonopoulos, 'ch9', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014)

[30]Ian Miers 'and others', 'Anonymous Distributed E-cash from Bitcoin' 12 (2013)

<http://isi.jhu.edu/~mgreen/ZerocoinOakland.pdf> accessed 22 March 2015

[31] Ibid

Unlike the anonymity concern, Wei Dai proposed in 1993 another E-cash system which was grounded on the decentralized scheme. He argued that the centralized power is unnecessary whenever fraud is self-preventable which usually the case among the participants whose identity and physical location are unknown. In addition, they could efficiently operate under a self-regulatory platform when the creation of money is resulted from collective efforts of the network members. The self-preventable security is governed by the broadcasting their work anonymously and the value-measurement standard is governed by computing effort.[32] In 2008, a pseudonym programmer known as "Satoshi Nakamoto" introduced further update version for the decentralized pseudonymity E-cash system widely known as "Bitcoin". The key to his innovation was that he had successfully sorted out the double spending (counterfeiting) problem. ". He introduced the digital signatures as a time stamping and witness of the ownership, in order to secure the network from counterfeiting. In addition to that, Satoshi introduced the rarity of the gold as a value-measurement standard of the Bitcoin currency.

Many security researchers have confirmed the efficiency of the system, such as Dan Kaminsky, the Chief Scientist of White Ops and specialist in detecting malware activity. He admitted in a CNN interview that the Bitcoin protocol is a new generation of metacode that remains solid and safe because of decentralized nature (the no-single-point of attack network), although other metacodes surrounding the network could be hacked (indeed, this has already been experienced).[33] Unlike Satoshi's assumption,[34] the nodes and users of the network are

---

[32] Wei Dai, 'B-Money' < http://www.weidai.com/bmoney.txt, 1998> accessed 10 February 2015

[33] CNN, *'Inside Man; Making Cents Out of Bitcoin'* (February 19, 2015)

<http://transcripts.cnn.com/TRANSCRIPTS/1502/19/inm.01.html > accessed 1 March 2015

[34] Nakamoto Satoshi, 'Bitcoin: A Peer-to-Peer Electronic Cash System' 12 (2008)

11

neither all honest nor highly trusted, especially in case of storing the funds in a web-wallet (a third party host provider), as the following table shows.[35]

Table 1: Bitcoin thefts

Date	Pace	Type	missing BTC	USD value
Jun 2011	Mt.Gox	exch	2,000	$47,000
Jun 2011	MyBitcoin	wallet	79,000	$1,100,000
May 2012	Bitconica	exh	38,000	$91,000
Jun 2012	Bitconica	exch	40,000	$305,000
Sep 2012	Bitfloor	exch	24,000	$250,000
Oct 2013	Inputs.io	wallet	4,100	$1,200,000
Nov 2013	GBL (Kína)	exch	4,100	$4,100,000
Feb 2014	Mt.Gox	exch	850,000	$500,000,000
Mar 2014	Flexcoin	wallet	900	$600,000

An alleged Bitcoin theft in 2011 was monitored by some researchers who were able to track the subsequent spending and transactions and identify the user by employing several data analysis tools[36]. This highlighted the privacy concerns in the Bitcoin E-cash scheme, which was the idea behind the development of other anonymity-focused digital currencies such as Zero-coin, Zero-cash, Monero and Darkcoin.

Zero-coin, as an example, is a theoretical approach introduced in 2013 that allows users to prove their legitimacy of ownership without the need to the chain of signatures as proof of

---

[35] Laszlo Csirmaz, 'Secret of Bitcoin', CEU Net workshop 31 (2014)

[36] See 'An Analysis of Anonymity in the Bitcoin System' 21-23 (2011) <http://arxiv.org/pdf/1107.4524.pdf?origin=publication_detail> accessed 22 March 2015, according to F. Reid and M. Harrigan, they were able to trace 60 transactions involving 441.83 BTC over a 70-day period.

work, (as will be explored in more details in chapter 3) [37]. The main objective is to make it fully private from the eyes of any potential hackers. Since Zero-coin reveals the payment destinations and amounts, the same cryptography researchers developed it further into "Zero-cash" on the ground of the hint-based technique (zero-knowledge).in order to make it absolutely anonymous[38].

Concerning other governing codes of Bitcoin, such as the limitations, the decreasing rate and mining, these properties were enhanced and developed as well. For example, with regard to the "limitation and decreasing code" of Bitcoin, some cryptocurrency researchers have examined the ability of issuance digital cryptocurrencies without restrictive limitations. They have progressed about five different types of digital crypto-currencies in this regard. As an example is Peercoin, which is inherently able to issue new currency without being constrained by a fixed total amount.[39]

The mining code however is designed to secure the network by the solving a chance-based mathematical problem. This code has upgraded further by the cryptocurrency researchers. In 2013, it was the year of launching three developed built-in code with dual purpose. The dual purpose proof-of-work in this case is not only to secure the network, but also to be useful and valuable result. The applications of this could be significant in scientific disciplines such as protein-folding research or indeed in a broad range of academic research.[40]

---

[37] Ian Miers 'and others', 'Anonymous Distributed E-cash from Bitcoin' 1 (2013) <http://isi.jhu.edu/~mgreen/ZerocoinOakland.pdf> accessed 22 March 2015

[38] Ian Miers 'and others', 'Decentralized Anonymous Payments from Bitcoin', (Extended version) (2014). <http://zerocash-project.org/media/pdf/zerocash-oakland2014.pdf>accessed 22 March 2015

[39] Andreas Antonopoulos, 'ch9', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014)

[40] Ibid

1.4 The technical classification of Bitcoin's protocol and currency

As intended by the framers, Bitcoin is not an end (priced commodity) but a mere means (medium of exchange). It does not have intrinsic value, neither is it considered a valuable commodity, a physical coin nor even a digital coin *per se*. Instead, the monetary value of Bitcoin is implied in the purchasing power of the digital signatures that reflects the value transferred from sender/seller to recipient/buyer,[41] as Satoshi functionally defined it: "digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin".[42] The protocol of Bitcoin is not solely designed for the users whose disposable value mutually suits each other's need. In fact, it is widely used as a means/cash between the users, which is inherently possible to be stored at digital wallet.[43]

---

[41] Ibid ch1

[42] Wei Dai, 'B-Money' < http://www.weidai.com/bmoney.txt, 1998> accessed 10 February 2015

[43] Open source software, can be accessed either from smartphone, laptop, IPad or any computing device

CHAPTER 2: THE LEGAL CLASSIFICATION OF BITCOIN PROTOCOL AND CURRENCY

Traditionally, the effectiveness and the flexibility of payment in cash money has simplified the exchanging value process between the parties, besides mitigating the cost burden inherent in earlier forms of trade, such as bartering, whereby consumers used to exchange goods or services of intrinsic value simultaneously.[44]

At first glance, it could be assumed *de facto* that Bitcoin could be categorized as gold-like, since the users of Bitcoin do not exchange simultaneously any intrinsic value as they do in a barter exchange. Besides, it is a decreasing and a finite governing-code. However, in reality the issues surrounding Bitcoin make classification extremely complex, such as being subject to the legal approaches of different jurisdictions, in addition to the academic paradigms and policy rationales that struggle to grasp what Bitcoin actually is.

To determine the precise classification of digital cryptocurrency in cyberspace, a functioning examination of Bitcoin protocol is needed. In principle, currencies performing similar functions should have similar regulation, thus the following sections compare Bitcoin's protocol with other functioning kinds of payment in kind, such as bartering and payment in cash.

2.1 Bitcoin protocol vis-à-vis barter

Historically, priced commodities have been used worldwide as a medium of exchange between parties. Inherently valuable commodities in different physical forms were directly

---

[44] Investopedia, <http://www.investopedia.com/terms/t/trade.asp> accessed 7 February 2015

bartered for other physical goods (e.g. cattle, stones, milk etc.).[45] In a functional perspective, the protocol of payment between the two transacting parties is mainly payment in kind. Their consideration is mutually on the intrinsic value of the exchanged goods/services.

Over time, with the growing sophistication and volume of trade, barter became too inefficient thus not only due to the problems of "divisibility" but also due to "the double coincidence of wants". The fundamental difficulty of "double coincidence of wants" is the rarity of situations where the seller (Alice) wants the service of the buyer (Bob), and the latter needs the goods of the former simultaneously, at the same time and the same place.[46] They both engaged in a trade and they both want what the other is offering.

Conversely, if the parties entered into the transaction without consideration of utilizing the physical goods in order to resell to a third party, the parties are going to bear high transaction fees. As indicated by recent research: "If we return to the use of a cow for payment, we see that it imposes serious costs on the new owner of the cow, the cow has to eat and perhaps even be milked regularly, even if the new owner does not want or need the milk".[47] To assume that Bitcoin protocol is barter exchange means that Bitcoin as a currency has an inherent/intrinsic value that suits the buyer's need *per se*. However, as noted above, Bitcoin as a currency are stored in digital walled and primarily used to purchase goods/services in an open-flow network, which implies that Bitcoin has no intrinsic value *per se*, but it either backed by an intrinsic value or not backed at all.

45James J. Angel and Douglas McCabe, 'The Ethics of Payments' (2014) MSB 20057, 4 < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379233> accessed 22 March 2015

46 Alvin Roth 'and others', 'Efficient Kidney Exchange: Coincidence of Wants in a Markets with Compatibility-Based Preferences' (2007) American Economic Review 97(3) 829<http://dash.harvard.edu/bitstream/handle/1/2562809/Roth_Kidney3way.pdf> accessed 22 March 2015

47 James J. Angel and Douglas McCabe, 'The Ethics of Payments' (2014) MSB 20057, 7 < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379233> accessed 22 March 2015

16

One may counter-argue that the US Internal Revenue Service (IRS) issued a notice considering therein how the protocol of Bitcoin should be classified; they classified Bitcoin's protocol as barter[48], which implies their view on the currency of Bitcoin as a priced commodity. We assumed that IRS has regarded Bitcoin's protocol as such on the grounds of two practical considerations: Bitcoin currencies are traded for traditional money and exchanged by auction platform; and the number of Bitcoin users is the highest in US (Figure 3).[49]

The IRS intended to impose taxes on Bitcoin to undermine its growing appeal (which de facto undermines the US dollar and thus the revenues of the IRS, albeit to a negligible extent), by obliging the transacting parties of Bitcoin to report any profit or loss resulting from any sale as well as subjecting any capital gain to taxation.[50] However, this was the outcome of one US government department's encounter with Bitcoin; a deeper level of analysis is necessary to fully comprehend the way the US and other jurisdictions have dealt with the currency.

---

[48] Richard Rubin and Carter Dougherty, 'Bitcoin Is Property Not Currency in Tax System, IRS Says' < http://www.bloomberg.com/news/articles/2014-03-25/bitcoin-is-property-not-currency-in-tax-system-irs-says> accessed 26 March 2015 "The U.S. government will treat Bitcoin as property for tax purposes, applying rules it uses to govern stocks and barter transactions, the Internal Revenue Service said in its first substantive ruling on the issue"

[49] <http://getaddr.bitnodes.io/> accessed 11 March 2015

[50] Primavera De Filippi, 'Bitcoin: a regulatory nightmare to a libertarian dream', Internet Policy Review 3 (2) (2014) 7 <http://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream> accessed 22 March 2015.

6520 nodes

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2463 (37.78%)
2	Germany	632 (9.69%)
3	France	440 (6.75%)
4	United Kingdom	438 (6.72%)
5	Canada	332 (5.09%)
6	Netherlands	300 (4.60%)
7	Russian Federation	210 (3.22%)
8	Sweden	120 (1.84%)
9	China	119 (1.83%)
10	Australia	108 (1.66%)

More (89) »
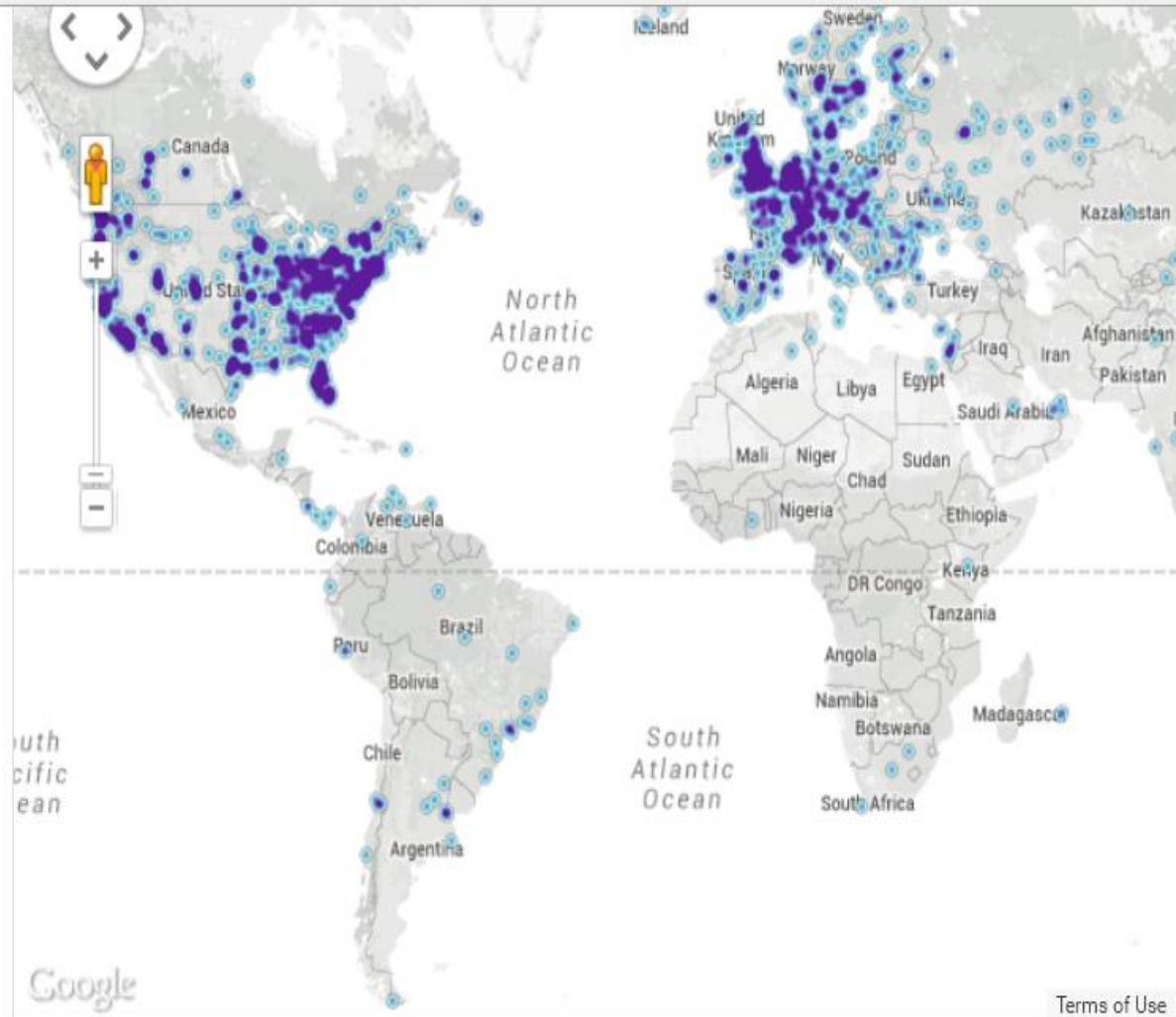
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

Figure 3: Main concentration of reachable Bitcoin nodes (in North America and Europe)

2.1.1 Bitcoin protocol vis-à-vis barter in the US

The common-law have revealed that terms "barter" and "sale" are not used as synonym in the legal sense. This was a plain statement of Justice Ervin in the Supreme Court case *State v. Albarty*[51]. He said: - "The words 'barter' and 'sell' are not used in this statute as synonyms. 'Barter' is a contract by which parties exchange one commodity for another. It differs from a sale, in that the latter is a transfer of goods for a specified price, payable in money".

Justice Ervin therefore, cited several cases in support of his argument in the *Speigle v. Meredith* case.[52] In this case, the issue arose before the district court of Indiana-whether the conveyance of land in consideration of coupon bonds is a sale of the land or barter exchange. The court adopted a narrow definition of sale by examining the other terms;- "barter" and "exchange" and it held that the bill was "a sale of lands" on the basis of the following arguments:-

> A sale of lands does not necessarily suppose a sale for cash. The term barter is not applied to contracts' concerning land, but to such only as relate to goods and chattels. (. . .) This transaction therefore was not barter. (. . .) the term "exchange" is a mutual grant of equal interests" as a fee simple for a fee simple, a lease of twenty years for a lease of twenty years, and the like (. . .) this, therefore was not an exchange, for it was a transfer of lands for coupon bond.[53]

Likewise, the IRS defined the barter transaction in a narrow sense. As an illustration example of bartering exchange, the IRS refers to "a plumber exchanging plumbing services for the

---

[51] *State v. Albarty*, 76 S.E.2d 381 (1953)

[52] *Speigle v. Meredith*, 22 F. Cas. 910 (1868)

[53] Ibid

19

dental services of a dentist".[54] It could be argued that the mentioned narrow sense of the term contradicts the IRS's own classification on Bitcoin's transaction as barter. However, it seems as noted that the policy rationale of IRS is as suggested by recent research to undermine Bitcoin's mass appeal.[55]

2.1.2 Bitcoin protocol vis-à-vis barter in the EU

Notwithstanding that the European Commission has not issued a specific Directive on either payment in kind (barter) or payment in a decentralized scheme (Bitcoin), the plain language of the EU regulatory bodies intended to classify Bitcoin as private money rather than priced commodities. For example, in 2012 the European Central Bank defined it as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community".[56]

The European Banking Authority (EBA) defined it similarly in 2013.[57] More recently, in 2014 the EBA acknowledged the differences between the bartering and Bitcoin protocol by indicating to the essence of the use: "VCs [virtual currencies] (Bitcoin)[58] can be used as a 'medium of exchange' to obtain goods and services from one holder, such as a private person or company, to another. This avoids the inconveniences of a barter system, i.e. the need for a coincidence of wants between the two parties involved in the transaction".[59]

---

[54] See Topic 420 – Bartering Income, I.R.S. (2015) < http://www.irs.gov/taxtopics/tc420.html > accessed 11 February 2015

[55] Cara R. Baros, 'Barter, Bearer, and Bitcoin: The Likely Future of Stateless Virtual Money' (2014) UMiami Bus L Rev 23 (201) 4 <http://repository.law.miami.edu/cgi/viewcontent.cgi?article=1018&context=umblr>23 March 2015

[56] European Central Bank, 'Virtual currency schemes' (2012) 5 <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 11 March 2015

[57] European banking authority, 'EBA Opinion on virtual currencies', (2013) EBA/WRG (1) 1<http://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf> accessed 11 March 2015.

[58] (Bitcoin) added

[59] European banking authority, 'EBA Opinion on virtual currencies', (2014) EBA/Op (8) 12 < http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 11 March 2015

From another perspective, Sergii Shcherbak[60] examined the classification of Bitcoin as a digital priced-commodity on basis of two governing codes/features: the limitation and deflationary rate. He examined these features in light of the statutory provisions of European Economic Area (EEA) Agreement and the Harmonised Commodity Descrpiton and Coding System (HS).

Theoretically speaking, Shcherbak assumed that the classification of Bitcoin as priced-commodity (material product) might be suited only on the essence (not the implication) of four assumptions:

1. The similarities between the Bitcoin mining process and products manufacturing process.

2. A conditional assumption that miners of Bitcoin would be known as the manufacturer of a product is known.

3. Bitcoin is a commodity, homogenous and fungible.

4. Bitcoin's value is determined by supply and demand basis. However practically speaking, he stated that "EU regulators have acknowledged that Bitcoin may be used as an article of commerce, both the EEA Agreement and (HS) perceive commodities and goods as tangible items and do not cover digital concepts such as Bitcoin".[61]

From the above discussion, we have tried to establish that the conception of Bitcoin's protocol in EU and US is closer to payment in cash than payment in kind such as barter, albeit the IRS has regarded Bitcoin as such for imposing taxes on the traders of Bitcoin as stock-market entity to undermine its widespread appeal.

---

[60] Sergii Shcherbak, "How Should Bitcoin be Regulated?', (LLM thesis, University of Stockholm 2014) 58-59
<http://www.ejls.eu/15/183UK.pdf> accessed 12 March 2015

[61] Ibid

2.1.3 Bitcoin protocol vis-à-vis barter in IBL

The precise classification of Bitcoin protocol in light of IBL requires an established examination of Bitcoin's protocol on basis of the investigative methodology of reasoning (*usul al-fiqh*)[62] and the legal maxims (*al-qawaid al-fiqhiyyah*).[63] The applicable maxim beforehand is what is known as "*Matters are to be considered in light of their objectives*" (*al-umur bi-maqasidiha*).[64] According to this maxim, the essence in Bitcoin protocol will based on the actual usage of Bitcoin currency and the objective of the protocol as such. Similar to a case where a party gives another a gift (*hibah* contract) in return for a sum of money, in that case the transaction will be considered a sale not a gift, as the price is stipulated.[65]

In deciding whether the "actual use and objective of Bitcoin" is a bartering transaction, money transaction or normal trade, we have to explore the classical definitions of sale. It has been defined by the classical legal schools as "*the act of exchanging valuable things either determined or yet to be determined*".[66] This term "things" is the key to classify the payment scheme of Bitcoin protocol. It is divided into three forms of transaction: money exchange (money in exchange for money); barter exchange (a valuable commodity in exchange for a

---

[62] It is also known as the principles of jurisprudence and defined as the legal technique for driving and interpreting the rulings from the primary sources such as the Quran and the authentic narrations of the prophetic tradition. As an example; "*the studying of the words and their implications, distinguishing the general from the specific, the restricted from the unrestricted, etc.*" The first combination as an independent science in the field was the book "Al-Risala" by the scholar al-Shafi'(820). See also, <http://www.oxfordislamicstudies.com/article/opr/t125/e2444> accessed 23 March 2015

[63] The consolidated themes and patterns of the legal rulings which are derived from reading on the primary sources, particular principles dealing with a particular subject matter or the theory of analogy between the related circumstances of the subject matter. An example; "Which is established by certainty is not faded by doubt" or "In claims; the objective of the parties in the litigation shall be relied upon and not the apparent" The first combination in the field was the made by the scholar al-Karkhi(952AD)

[64] The maxim are d driven from prophetic tradition It is narrated on the authority of 'Umar bin al-Khattab who said: I heard the Messenger of Allah (peace be upon him), say: "Actions are according to intentions, and everyone will get what was intended

[65] Jalal al-Din al-Suyuti, 'Similarities in the Branches of the Law' (1505) 104

[66] Mansur Al-Buhuti, Al-Rawd Al-Murbi (1887) Vol 1 p. 8

valuable commodity); and sale proper (a valuable commodity in exchange of money).[67] As observed by Ibn Rushd (520/1126 - 595/1198):

> *When two commodities are exchanged, one may serve as a currency and the other as a priced commodity or both may serve as currencies. When a currency is exchanged for a currency the sale is called sarf [exchange], when a currency is exchanged for a priced commodity, the transaction is sale proper, similar is the sale of a priced commodity for another priced commodity (barter)...*[68]

In short, Bitcoin protocol can be classified as both money exchange and proper sale on the ground of the classical definition of "things". Therefore, the Bitcoin protocol is regulated according to the objective of the users and actual functioning on case-to-case basis. For example, if users are exchanging traditional money for Bitcoin, that case will be regarded as a *sarf* (money exchange). Similarly, if a user used Bitcoin currency in exchange for priced commodity, this would be classified as *bay* ("sale proper"). With regard to barter exchange, however, it is highly unimaginable in Bitcoin protocol since it has no intrinsic value per se; it is unimaginable that two users would exchange Bitcoin for Bitcoin simultaneously.

Apart from what has been discussed above, the classification of Bitcoin currency remains a puzzle. The conventional view is that Bitcoin currency and fiat currency share a common theme: both have no intrinsic value. Others view it as gold-like, since it resembles gold in its limitation and deflationary nature. Therefore, before we explore the legal positioning of Bitcoin currency, we will explore the conception, functioning and the types of money in order to explore the real functioning of Bitcoin currency.

---

[67] Ottoman civil code (1869), Sale, section 120-122

[68] Ibn Rushd, *Bidayat al-Mujtahid (The Distinguished Jurist's Primer)* (1198) translated in English (1996) Vol2, p. 154 <https://ia802703.us.archive.org/24/items/BidayatAl-mujtahidTheDistinguishedJuristsPrimerVol2/TheDistinguishedJuristsPrimerVol2.pdf > accessed 22 March 2015

2.2 Bitcoin currency vis-à-vis money

2.2.1 Concept of money in the ancient era

The idea of money as a means to transfer value was rooted in the earliest records of human civilization. Unlike bartering, they considered specific commodities as well as invented coins made by such commodities as a means to transfer value. Hence, traders were allocating value in such commodities or coins that were considered inherently valuable.

The earliest known monetary system was that of the Babylonian Empire. According to the English economist E. V. Morgan, there were two themes of the legal tender of the Babylon Empire. The first theme was private money, which was issued privately and accepted as legal tender without a formal decree, such as gold, silver, lead, bronze, copper, honey, sesame, cooking oil, wool, weapons, wine and beer, whereby the transacting parties determined the value of the exchanged goods or services according to the intrinsic value of these items. The other theme required more formalities and governmental intervention to be accepted as legal tender.[69] He also hinted that the various practices of money in different nations were determined by their need for a flexibility and ease, such as shells in coastal areas, precious metals in temperate lands, rice in Japan and tea in central Asia.

However, it is in the Mediterranean world that the real roots of modern monetary systems are found. In Egypt approximately 3100 years ago gold was used as legal tender on a considerable scale,[70] but because of the non-interchangeability of gold trade was relatively unstructured before the first issuance of interchangeable coinage attributed to the King of

---

[69] Victor Morgan, 'Tareekh Al-Noqood' [A History of Money](1965), translated to Arabic (1993)p. 13

[70] Martin Zhuwakinyu , 'Gold mining in ancient Egypt' (2012) <http://www.miningweekly.com/article/gold-mining-in-ancient-egypt-2012-06-08> accessed 11 February 12015

Lydia, Croesus (around 550 BCE).[71] The Lydian golden-coins were equal in weight and size, which facilitated their circulation widely in the Athenian markets and thus the maritime civilization around the Mediterranean.

The Athenian monetary system was a gold-based system until the Peloponnesian War (431–404 BCE), which was a turning point. The expenses for the war with Sparta were the grounds for the deficit spending, resulting in debasing the currency by mixing gold with copper in order to increase the monetary supply and raise the funds needed for the war. The deficit spending resulted in 1000 pure gold coins being levied from Athenian citizens for taxes, which were then mixed with 50% copper in order to double the money supply to 2000 coins, as shown in Figure 4.[72]

Figure 4: Deficit spending

---

[71] The British museum, 'Gold Coin of Croesus',
<http://www.britishmuseum.org/explore/highlights/highlight_objects/cm/g/gold_croesid_coin.aspx> accessed 11 February 2015

[72] *Seven Stages of Empire,* Dan Rubock, Hidden Secrets of Money, [2013]

25

As a result, the Athenians started to use the new debased currency, which had only face-value, for their daily needs, while hoarding the pure gold-based coin which had intrinsic value. Over time, the face-value (cheap) money drove the intrinsic-value money off the market; this phenomenon is called Gresham's law. The expansion of Gresham's law and hyperinflation which had hit the system was the reason behind the financial crisis of the Athenian market.[73]

Similar events occurred in the decline of the Roman Empire. Although it had a centralized coinage,[74] the pure silver-backed coin denarius was slowly replaced by the Antoninianu the "double denarius" coin, whereby Gresham's Law came into effect and inflation began.[75] In this regard, Alan W. Pense explored the legal tender stages of the Roman Empire thus:

> The basic silver coin of early Roman Empire was the denarius. By decree of Caesar Augustus in 15 B.C.E., it was nearly pure silver, 95%-98%, and had a "fixed weight"[76] and value in relationship to the rest of the Roman monetary system (store of value). Over the next 270 years, the silver content of the denarius declined gradually and then precipitously to about 2%... The final stage of the denarius was a duplex plated coin with a nearly copper core and a silver surface… By this time (280 C.E.), the silver coinage of the empire had almost totally lost its value and had to be reconstituted by Diocletian.[77]

Years later, the solidus of Byzantine also was formulated on a uniformed gold-base. In the West, the Carolingian and Anglo-Saxon coins (e.g. Athelstan's coin) were all silver-base in their early stages.

---

[73] ibid

[74] David Marsh, *The Euro; The Battle for the New Global Currency* (2d ed. 2011) 20

[75] Alan Pense, 'The Decline and Fall of the Roman Denarius' (1992) Lehigh University
220<http://www.lehigh.edu/~inarcmet/papers/pense%201992.pdf>accessed 23 March 2015

[76] Emphasis added

[77] ibid 213

In short, the societies of antiquity traded with two types of legal tender as a means of exchanging values (goods and services). The circulated legal tender of the ancient era was in two types: the first type was the pure precious metal such as gold or silver. They used to measure it with confidence as a medium of exchange and a store of value due to its inherent expensive features. The second type was the composite (debased) coins, generally gold or silver coins mixed with copper, which was commonly used for deficit spending (often linked to military commitments) by governments. These mixed-up coins used to have a face-value in the market and often had hit by Gresham's law and ended with hyperinflation and political chaos.

2.2.2 The concept of money in the modern era

As noted above, the patterns of money as a medium of exchange were an effective tool facilitating transactions and simplifying the allocation of values. Money was first formulated in coins made of precious metals such as gold or silver,[78] generally becoming debased over the lifespan of the issuing states, prior to the invention of fiat currency such as *choi* in China.[79] Paper notes backed by gold or silver (the gold standard) were the core of European (and thus, via imperialism, of world) monetary systems from the 17th century onwards. The paper certificate was functioning as a medium of exchange in the market, while maintaining its value according to the gold standard, as shown in Figure 5.

[78] The gold sovereign of Britain, the gold eagle of US and the new gold mark of Germany

[79] Usually understood as 'paper' money, *choi* was in fact silk (and thus of intrinsic value), backed by silver in the Chinese treasury

27

Figure 5: Gold certificate as paper note[80]

During the period 1880-1915 (including the Belle Epoch or Gilded Age), the gold standard established confidence as an economic standard on basis of the gold. This means that the bearer of such paper money was guaranteed that the issuing bank would redeem the certificate with the equivalent amount of physical gold on demand, as authorized by law. However, increasing discrepancies arose between the purported value of the certificate and the actual spot price of redeemable gold, which led to the Gold Exchange Standard (1916-1943). In 1944 a fixed exchange-rate system was agreed upon in the Bretton Woods Agreement, which "saw all currencies linked to the dollar, and the dollar linked to gold".[81]

Pursuant to the agreement, the dollar standard was established by the early 1960s. However, the dollar standard was not able to maintain its value for deficit spending as noted by IMF: "domestic spending on President Lyndon Johnson's Great Society programs and a rise in military spending caused by the Vietnam War gradually worsened the overvaluation of the dollar".[82] By the end of 1971, "U.S. President Richard Nixon announced the 'temporary'

---

[80]Gold certificate as paper currency < http://upload.wikimedia.org/wikipedia/commons/a/a7/US-%2410000-GC-1934-Fr.2412.jpg> accessed 25 March 2015

[81]Economist, What was decided at the Bretton Woods summit < http://www.economist.com/blogs/economist-explains/2014/06/economist-explains-20> accessed 25 March 2015

[82] IMF, The end of the Bretton Woods System (1972–81) < http://www.imf.org/external/about/histend.htm> accessed 25 March 2015

suspension of the dollar's convertibility into gold… and by March 1973 the major currencies began to float against each other".[83]

Evidently, the gold standard was based on the confidence of the intrinsic value of the precious commodities, famously reflected in the promise of the Governor of the Bank of England still ceremonially printed on GBP bank notes: "I promise to pay the bearer [of this note] on demand the sum of…". Increasing government debts, largely linked to the world wars, led to the replacement of the gold standard by IOUs or governmental debts, whereby currency has value based on trusting the authoritative power.

To some extent there are fundamental differences between the capitalist and Islamic monetary paradigms because the latter distinguishes between the functioning of money according to its objective into two functions. The first objective is functioning as medium of exchange, while the second objective is as an economic standard (value determination/store of value). Unlike capitalism[84], it does not view fiat money from the economic standard perspective, as explored further under the legal classification of IBL.

Unlike tangible (whether commodity, commodity-backed or even fiat) money, Bitcoin is intangible money created by decentralized miners and self-governed by computer codes, as noted earlier, hence the economic standard of Bitcoin currency has to be examined as well as its functional as a medium of exchange. Technically, Bitcoin is being considered as money in cyberspace since it can be purchased by in an open-flow network.

Nevertheless, the codes of Bitcoin are hard to define. In common with commodities and precious money it has a deflationary issuance rate and finite nature, while it is neither made

---

[83] Ibid

[84] Jodi Beggs, 'Types of Money' < http://economics.about.com/od/money/a/Types-Of-Money.htm> accessed 11 March 2015

nor backed by intrinsic value, which resembles fiat money. The conception of Bitcoin therefore has to be examined under a functional test i.e. as a medium of exchange and store of wealth, as well as in terms of the creation process of the money (mining) in order to precisely establish whether it may be a legal tender or not, and under which jurisdictions.

2.3 Concept of Bitcoin as legal tender

2.3.1 Concept of Bitcoin currency in the US Constitution

The use of precious metals as legal tender continued into the era of the US Founding Fathers. They wrote the US Constitution during a time of financial instability "in effort to protect individuals from spurious money creation by state governments-and, by implication, from the same activity of the federal government",[85] as observed in the following extract:

> No state shall enter into any treaty, alliance, or confederation; grant letters of marque and reprisal; coin money; emit bills of credit; make anything but gold and silver coin a tender in payment of debts; pass any bill of attainder, ex post facto law, or law impairing the obligation of contracts, or grant any title of nobility.[86]

This was honored until the Civil War, when for expediency the US Congress (the Union) passed the Legal Tender Act in 1862, granting the administration authority to increase the money supply without being restricted with relation to either gold or silver in such emergency cases.[87] During that period, the financial instability and volatility was witnessed after the

---

[85] Richard H. Timberlake, 'The Significance of Unaccounted Currencies',[1981]41 JEconHist 845

[86] US Const, art 1, § 10

[87] Encyclopædia Britannica, '*Legal Tender Cases'*, (21October 2014)<http://www.britannica.com/EBchecked/topic/334891/Legal-Tender-Cases#ref285279 > accessed 23 March 2015.

issuance of greenbacks, fuelling government-inspired inflation (deficit-spending) and suspension.[88]

The absolute interpretation on the gold clause (Article 1, section 10) is a controversial issue. It remains an unsettled and disputed issue. The first recorded disputes on its interpretation that between the two Supreme Court rulings, in *the Knox and Hepburn* cases. These are central in the functional definition of money, which is highly important for establishing the functional classification of digital cryptocurrency.

As recorded, *Knox v. Lee* Supreme Court case had restricted the interpretation of the prohibition to issue bills of credit (greenbacks) only at the state level. It reasonably argued that on basis of the plain text of the Constitution, especially in cases of emergencies. On the other hand, *Hepburn v. Griswold* had broadened the interpretation of bill of credit prohibition, to include not only states but any authority *inter alia* the Congress on the grounds of the economic policy rationale behind the text, as discussed below.

With regard to the argument of the first case, the majority of the Justices in the Supreme Court in the case of *Knox v. Lee*[89] held for the Legal Tender Act, as argued by J. Strong:

> If it be held by this court that Congress has no constitutional power, under any circumstances, or in any emergency… the government is without those means of self-preservation which, all must admit, may, in certain contingencies, become

---

88 Richard H. Timberlake, 'The Significance of Unaccounted Currencies',[1981] 41 J. Econ. Hist 847,

See also Bennett T. McCallum , 'The Future of Central Banking: A Lesson From United States History' (2010) 2 < http://www.imes.boj.or.jp/research/papers/english/10-E-14.pdf> 23 March 2015, he mentioned that ((*The occasion upon which fiat money made its appearance in the U.S., for the first time since the adoption of the Constitution, was the Civil War of 1861-1865, with three issues of the infamous "Greenbacks" occurring in 1862, 1863, and 1864. The total Greenback emission was $450 million, which alone would have represented a near doubling of the money supply relative to its magnitude in 1860*)).

89 Knox v. Lee, 79 U.S. 457 (1871)

indispensable… if, contrary to the expectation of all parties to these contracts, legal tender notes are rendered unavailable, the government has become an instrument of the grossest injustice.

It should be noted, however, that this Act was (predictably) later extended to include not only emergency cases but also peace-time scenarios, as upheld in the Supreme Court case *Julliard v. Greenman*.[90]

Conversely, the judges who opposed the issuance of bills of credit upheld this position in the case of *Hepburn v. Griswold*,[91] Led by the J. Ailing Grier, the majority reversed the Congress's power to issue greenback (fiat) money as legal tender at any time. The argument of the court was based on distinguishing the interstice value of the precious metal from the greenback fiat currency. The court stated:

The former possess intrinsic value determined by the weight and fineness of the metal; the latter have no intrinsic value, but a purchasing value, determined by the quantity in circulation, by general consent to its currency in payments, and by opinion as to the probability of redemption in coin… No Act making them a legal tender can change materially the operation of these laws. Their force has been strikingly exemplified in the history of the United States notes. Beginning with a very slight depreciation when first issued,[92] in March, 1862, they sank in July, 1864, to the rate of two dollars and eighty-five cents for a dollar in gold,

---

[90] Julliard v. Greenman, 110 U.S. 421 (1884)

[91] Hepburn v. Griswold, 75 U.S. 8 Wall. 603 (1869), this case is overruled by Knox v, Lee.

[92] Richard H. Timberlake, 'The Significance of Unaccounted Currencies',[1981] 41 J. Econ. Hist 857, the author said *(The general and rapid rise in prices in 1862 due to the first issue of greenbacks during the* Civil War was perhaps the most acute example of government-inspired paper money inflation and suspension. Commodity values of most metallic coins rose sharply above their monetary values, and coins then went out of circulation, leaving the North's economy with almost no currency denominations below $5.)

and then rose until recently a dollar and twenty cents in paper became equal to a gold dollar.

Likewise, Marshall, C. J., said in the case of *Craig v. The State of Missouri*[93], speaking about the greenback fiat currency (paper money):

> Such a medium has been always liable to considerable fluctuation. Its value is continually changing; and these changes, often great and sudden, expose individuals to immense loss; are the sources of ruinous speculations, and destroy all confidence between man and man. To cut up this mischief by the roots – a mischief which was felt through the United States, and which deeply affected the interest and prosperity of all – the people declared in their Constitution that no State should emit bills of credit.

Both perspectives are based on a valid reasoning that could collectively support a clear understanding of the legislative intent in the functioning of money. For example, the first case *Knox v. Lee* had valid concerns over the deflationary feature of commodity money, such as gold. This limitation of gold is highly risky for the social welfare and public concern when hoarded, as observed during the Great Depression, and can be understood from the context of the Gold Reserve Act of 1934. In contrast, the second case *Hepburn v. Griswold* focused on another functional aspect, the commodity money as an economic standard, which is the self-regulatory value-determination of intrinsic gold. As observed earlier, the gold standard plays a strong role in resisting the inflation or protecting the market from fluctuation, as described by

---

[93] Craig v. The State of Missouri 29 U.S. 4 Pet. 410 (1830)

Milton Friedman (1976), who observed that the gold standard is "thoroughly consistent with [classical] liberal principles".[94]

As a result, it seems from the functional definition of legal tender in light of the US Constitution (article 1, section 10) that the fundamental bottom line of the ideal legal tender has to be a medium of exchange, anti-hoarding and anti-inflation (intrinsic value), as implied from the unconstitutionality of bills of credits and their prohibition. Theoretically, we argue that the decentralization medium of exchange is not an issue *per se* if these referred patterns and features are available in the governing codes of Bitcoin. Hence, the key issues are mainly in the "intrinsic value" and "anti-hoarding" codes of Bitcoin.

It might be argued that Bitcoin is a gold-like standard; they both share a common theme, being inherently finite and deflationary. However, it seems that assumption is not precisely valid on basis that Bitcoin does not resemble gold/silver money either in its preciousness nor usefulness features, especially with the volatility risk associated with Bitcoin. This implies that Bitcoin does not resemble the gold standard and would rather fall under the bill of credit prohibition, unless proven otherwise.

To sum up, the above-mentioned features have to be parts of the self-regulatory governing codes of Bitcoin in cyberspace, albeit it remains a nebulous concept for both regulatory bodies and even its own users. Further examination in the policy rationale behind the gold clause and its implication in cyberspace is needed (as discussed in chapter 3).

---

94 Richard M. Ebeling , 'Monetary Central Planning and The State', (January 1999) at <http://fff.org/explore-freedom/article/monetary-central-planning-state-part-27-milton-friedmans-thoughts-costs-paper-money/> accessed 9 March 9, 2015

2.3.2 Concept of Bitcoin currency in EU regulation

The status of Bitcoin currency in Europe cannot be properly understood without the two monetary pillars of the Maastricht Treaty and monetary unification, based "on the residues of the nineteenth-century gold standard… The gold standard underpinned economic and social stability… linked to the strength and solidity of gold".[95]

Monetary unification was a core part of the European mission of prosperity, solidarity and unity, inspired by the devastation of the world wars.[96] This policy was the foundation of the single currency conception of the Eurozone in 1999, which was rooted in the Optimum Currency Areas theory. The European Commission (1991) intended to fully achieve market integration through a single currency. The "economic advantages of 1992 are certainly not fully achievable without a single currency, especially in the field of financial market integration".[97] This tentative observation of the European Commission was later embodied in the European Monetary System (EMS) rules, agreed in 1996 at the Dublin European Council meeting, which "requires all members of the European Union (including those that are not members of the monetary union) to pursue convergence policies with specific targets for budget balance and inflation [with the exception of the UK]".[98]

It has also been embodied in the second Exchange Rate Mechanism agreement between the European Central Bank (ECB) and non-euro, members aiming "to maintain stable exchange rates and to avoid excessive exchange rate fluctuations on the internal market… thereby

---

[95] David Marsh, *The Euro; The Battle for the New Global Currency* (2d ed. 2011) 21

[96] ibid 19-45

[97] Directorate-General for Economic and Financial Affairs, 'One Market, One Money; An Evaluation of the Potential Benefits and Costs of Forming an Economic and Monetary Union' (1990) EC 44, 17

<http://ec.europa.eu/economy_finance/publications/publication7454_en.pdf > accessed 11 March 2015

[98] Martin Feldstein, '*The Political Economy of the European Economic and Monetary Union: Political Sources of an Economic Liability*' (1997) 11 (4) JEP, 6

<http://www.econ.uba.ar/www/departamentos/economia/plan97/internacional/vanoli/bibliografia/FELDSTEIN.PDF>
accessed 23 March 2015

35

helping them in their efforts to adopt the euro".[99] The underlying rationale is to structure an effective legal platform for the Single Euro Payments Area (SEPA) in order to nurture competition, innovation and security as implied in the adopted legislative package in the field of the EU payments framework by the EC with regard to the Second Payment Services Directive (PSD2).[100] Similarly, the European Single Market is an objective in cyberspace as stated in Directive 2000/46/EC.

To formulate a single market in cyberspace on one hand, the Directive adopted a flexible technical-neutrality standard for the payment scheme and defined the E-money in broad sense on the other hand as "monetary value stored on an electronic device issued on receipt of funds and accepted as means of payment by third parties".[101] However, because the PayPal case questioned the technical-neutrality of digital money in the Directive, the EC perceived lack of regulation of such new payment scheme and considered the PayPal scheme to be closer to a credit token than to electronic money.[102]

Later, the EC amended the E-Money Directives to produce Directive 2009/110/EC, which is the last amendment on the subject. The preamble highlighted the true single market and user-friendly services as the reasons behind the amendments. It seems from the functional definition of the Directive 2009 that E-money has specific features. The first recognizable feature is the "centralized issuance" of the digital currency, which is expressly indicated by the limitation of the authorized payment service providers in the fifth recital of the referred

---

[99] Exchange rate mechanism II agreement [2006] C 73/08

[100] COUNCIL Directive, on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC

[101] Council Directive 2000/46/EC of 18 September on the taking up, pursuit of and prudential supervision of the business of electronic money institutions Art.1.3(b)

[102] Andres G. Gonzalez,' PAYPAL: The Legal Status of C2C Payment System' (2004) 11
<http://www.era.lib.ed.ac.uk/bitstream/handle/1842/2262/paypal.pdf?sequence=1&isAllowed=y> accessed 23 March 2015

Directive.[103] Hence, the decentralized peer-to-peer digital money is not covered by the regulatory framework of the Directive.

Conversely, it could be counter-argued for the competence of the 2009 E-Money Directive that the scope of the regulatory framework of the Directive also covers the decentralized payment scheme on the ground of the legislative intent as the legislator expressly stated in the fifth recital of the referred Directive:

> Where such a specific-purpose instrument develops into a general-purpose instrument, the exemption from the scope of this Directive should no longer apply. Instruments which can be used for purchases in stores of listed merchants should not be exempted from the scope of this Directive as such instruments are typically designed for a network of service providers which is continuously growing.[104]

There are two other features of E-money such as the importance of electronic money to be backed by state-money as well as broadly speaking[105] to be a "store of value".[106] According to the seventh recital, it conditionally covers all certified service providers as long as "the (authorized)[107] payment service provider issues a pre-paid stored value in exchange for

---

[103] Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC , Recital 5

[104] ibid

[105] Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC , Recital8 ((definition should be wide enough to avoid hampering technological innovation and to cover not only all the electronic money products available today in the market but also those products which could be developed in the future))

[106] ibid Article2.2

[107] ibid Article 1.1 & 10

funds".[108] The measurement of the value has to be regulated by a standardized arbiter either, gold or a central bank.

In February 2015 the ECB described Bitcoin as "inherently unstable" due to the referred drawbacks in addition to the anonymity of the users and the risk of fraud. According to the ECB, Bitcoin does not meet the status of legal tender in number of countries (such as Sweden and Finland). These countries do not classify Bitcoin as a currency, Germany in turn, classified it as a currency but not as a legal tender.[109] ECB further demonstrated the regulatory framework of the Bitcoin service provider in light of different member states. For instance, "In Germany, BaFin has stated that the use, sale and purchase, and mining of units of Bitcoin do not in themselves require an authorization, although additional services may be subject to authorization".[110]

In nutshell, the EU's position in general terms has regarded Bitcoin as medium of exchange but not as a legal tender as observed by the E-money Directive and implied from the ECB classification. The underlying reasoning is that the legal tender should only be manufactured by governments or their authorized representatives, who also drives and determine its value. Unlike in the US, money is a legal tender as long as it resembles the economic rationale as stated by some Supreme Court cases.

2.3.3 Concept of Bitcoin currency in IBL

The establishment of the IBL conception of Bitcoin as currency is based on the previous noted maxim *"Matters are considered according to their objectives"*. The functional categories of

---

[108] ibid Recital7

[109] European Central Bank, 'Virtual Currency Schemes-a Further Analysis' (2015) 30-31

<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 11 March 2015

[110]ibid

money are divided into two types: as a medium of exchange; and as a measure of value/economic standard.

With regard to the first referred category. It has been defined by several Muslim scholars, such as Ghazzali, Malik, Ibn Taymiyyah and others as "anything that gains general acceptance as a medium of exchange, whenever or wherever that occurs and in any way that it occurs".[111] In this regard, money is defined in broad sense; it includes commodity money, paper money and digital money. As implied, they insisted mainly on its objective as a mere medium of exchange, not as something to be profited from in itself (e.g. currency speculation), with the chief purpose of functioning by circulation in the market, and to facilitate the trade/services among the communities: "It becomes useful only when it is exchanged into a real asset or used to buy a service".[112] This was the conclusion reached by Ibn Taymiyyah in his legal verdicts:

> *As for dirhams (gold-coin) and dinars (silver-coin), there is no natural or legal definition for these; however, the matter returns to habit and terminology. This is because the basic principle is that the objective is not these coins in themselves; rather, the objective is that they should be a standard for mutual transactions. Dirhams and dinars are not sought for themselves. Rather, they are means by which mutual transactions are carried out, and this is why they*

---

[111] Abdullah Mani, 'Paper Money: Its Reality, History, Value and Legal Ruling' (1971) 5-6
<https://unity1.files.wordpress.com/2009/06/paper-money-islamic-legal-analysis.pdf > accessed 23 March 2015.
[112] Faruq Ahmad and M. Kabir Hassan, 'The Time Value of Money Concept in Islamic Finance' (2006) 23(1) AJISS 72 <
http://iefpedia.com/english/wp-content/uploads/2009/11/The-Time-Value-of-Money-Concept-in-Islamic-Finance.pdf>
accessed 23 March 2015 , The underlying reasoning according to the author (((a) Money has a technical property of yielding its owner's real income simply by holding it and not exchanging it with other goods. (b) Money is liquid, virtually no carrying or production costs are involved, and it has no substitute. (c) Demand for money is unreal, as it is derived from demands for goods that money can buy. (d) Money is exempt from the law of depreciation, to which all goods are subjected. (e) Money is the product of a social convention having a purchasing power that results mainly from sovereignty as against the inherent value of other goods)).

serve as money... A pure means, the substance or form of which is not an objective in itself, achieves the objective, whatever it may be. In this last sentence, there is an indication that money is whatever gains general acceptance as a medium of exchange, whatever its substance or form may be.[113]

As a result, Bitcoin shall be regarded as medium of exchange as long as the public practice considered it as such. Since the decentralized scheme is not an unlawful custom *per se*, this feature is considered to be lawful payment scheme as long as the other computer codes are in compliance with the governing IBL rules and regulations. That can also be deductive from the maxim "lawful[114] custom is the basis of determination".[115]

The second functional category of money is the functioning as economic standard and measurement of value. This objective is primarily based on the prophetic tradition that: "*Gold is to be paid for by gold, silver by silver, wheat by wheat, barley by barley, dates by dates, and salt by salt - like for like, equal for equal, payment being made on the spot. If the species differ, sell as you wish provided that payment is made on the spot*".[116]

Concerning these instruments as such, they can be divided collectively into two types: precious metals and foodstuffs. The IBL expressly widens the scope of the items that can be measured either intrinsically or extrinsically. This implies that the value determination in IBL

---

[113] Abdullah Mani, 'Paper Money: Its Reality, History, Value and Legal Ruling' (1971) 6

[114] See generally Sami Al-Suwaliem, 'The Tenets of The Islamic Economic System'(2014) <http://www.researchgate.net/publication/202351087_Tenets_of_the_Islamic_Economic_System> accessed 15 February 2015 , The lawful custom of any type of money either commodity money, commodity-backed money, fiat money or digital cryptocurrency should balance between wealth creation and wealth distribution by four governing rules. The first rule is Zakah which is the measure against hoarding. The second rule is the prohibtion on the Israf (non-productive spending) due to its impact on creating bubbles. Thirdly is the prohibition of Riba (usury) to combat the 'inverted debt pyramid' and the imbalanced growth of wealth. Lastly is the prohibition of gharar (ambiguity/insecurity) and maysr (speculation) to prevent the zero-sum game))

[115] Mishkah, 'Legal Maxims of Islamic Jurisprudence' (2013, 123 < http://islamhouse.com/en/books/729618/> accessed 23 March 2015

[116] The narrations and text combined by Imam Muslim, The Book of Transactions (Kiab Al-Buyu) N. 3853 (Died at 874)

does not stem from the limitation and scarcity as the conventional dominant view of gold-standard, but it should have an alternative rationale. The precise cause has been observed by Muslim scholars such as Ibn Qayyim, who states that: *"The preservation of moneyness (thamaniyah) of precious metals from volatility is the reason behind the prohibition of unequal exchange of the same kind. While the reason behind prohibition of unequal exchange of the same kind of foodstuffs is that it will disturb their purpose of serving as diet"*.[117]

In addition, the value determination is governed by a restriction on the equal exchange rate rule. The underlying wisdom is to ensure the fair exchange in transactions and eliminating any unjust enrichment that might occur. This precise cause (*illah*) is deduced by many scholars as well. For example, Al-Qurtubi (1273) referred to the wisdom as "the mathematical quality of measure produced by money", while Ibn al-Qayyim (1350) referred to it thus:

> *Price is the standard through which values of goods are known. So this standard should be fixed and stable. It should not fluctuate. For if the measure of prices rises or falls like other commodities, there would be no way to evaluate the goods; all would be commodities. It is people's inevitable common need to have a measure of prices through which they can measure the value of merchandises. And that is not possible without a standard that can define the value. Such a measuring rod should be stable and it should not be subject to evaluation by some other thing. If it were so, it would be like any commodity whose value rises*

---

[117] Ibn al-Qayyim, I'laam ul Muwaqqi'een 'an Rabb il 'Aalameen (Information for Those who Write on Behalf of the Lord of the Worlds) (1350) Vol1, p. 139

and falls. Consequently people's transactions will be deteriorated; disputes will arise and there will be tremendous injury...[118]

Similarly, in a case study concerning paper money, the issue was upheld in 1994 by Judge Abdul Razzaq 'Afifi as: *"The currency needs to be backed in principle by the resources of the country. It is not necessary that there be physical reserves of gold or silver, etc., as long as there are enough resources available within the country to produce items that have equivalent value of the gold, silver or other previous money"*.[119]

Overall, this indicates that the key legislative intent of the functional of money (as economic standard) is to maintain the purchasing power of the financial instrument, in order to establish the confidence as well as the economic incentive among the public. The precise cause of such objective is not through the scarcity of the items, but through the usefulness and effort exerted beyond the intrinsic values of the money either commodities or foodstuffs.

If we assumed that Bitcoin is analogous to the gold and its precise cause is moneyness, then Bitcoin is definitely not eligible to resemble gold/silver in cyberspace on basis of a mere limitation or deflationary nature, especially that these two features have not established the precise cause which is the public confidence, but rather created an injury for the holders and the users alike due to high volatility.

---

[118] Faruq Ahmad and M. Kabir Hassan, 'The Time Value of Money Concept in Islamic Finance' (2006) 23(1) AJISS 81 < http://iefpedia.com/english/wp-content/uploads/2009/11/The-Time-Value-of-Money-Concept-in-Islamic-Finance.pdf> accessed 23 March 2015

[119] Abdullah Mani, 'PAPER MONEY:Its reality, history, value and legal ruling', (1971) 33

42

2.4 The drawbacks of Bitcoin protocol and currency

Historically, the public confidence has been established independently by the gold standard. The gold as an economic standard has many *sui generis* features that enable such precious commodity money to be a self-regulated measurement of value.

The building blocks of Bitcoin, in turn, consist of numerous codes. Some of these codes are well-governed in the decentralized digital community, such as proof-of-work to ensure the legitimacy of ownership and secure the network, as well as the unlocking of advanced electronic signatures (public-private key), which proves ownership and strongly preserves it in the digital wallet. Others remain flaws *inter alia* volatility and money laundering.

In other words, Bitcoin could be successful money as a medium of exchanges as the traditional money in couples of properties such as being a unit of account, durability and interchangeability, but its flaws remain on losing the public confidence. Although it is coded to be anti-inflation, it remains to be so volatile. The volatility is a serious drawback to the referred chosen legal jurisdictions such as US, EU and IBL. Solving out this issue is indeed a key factor to be considered as legal tender in some legal jurisdictions where centralized issuance is not required. Hence, the research will focus on this examination further in the next chapter.

43

CHAPTER 3: THE ISSUE OF BITCOIN'S VOLATILITY

3.1 The dilemma of volatility

The precise cause of volatility in Bitcoin is better examined through an exemplary decentralized case. As previously discussed in chapter 1, the transacting parties were operating in a decentralized trust network, however they later detected that some counterfeited money was circulating in the market. The network was outnumbered. Albeit they were not able to identify the alleged party, they consensually agreed to secure the market from any similar incident might occur. They invented a governing code, so as any party (e.g. Alice, John, Mary, Adam or others) would have the ability to print/issue a note, but to be accepted as legal tender it would have to be stamped by a secured stamping machine.

The stamping machine was publically owned. It was stamping with a distinctive watermark throughout a complex process. The complexity of the process was due to the random function of the stamping-machine. The only way that the issuer had to follow (for note-stamping at the machine) was to repeatedly trying to stamp it again and again, which would take approximately five to seven hours per note. Besides, the machine randomly functioned; thus the more notes were stamped, the less potential there was for other notes to be stamped.

In fact, Bitcoin mining is designed in a similar way. As Antonopoulos (2014) illustrated, it is "a giant Sudoku puzzle… the 'puzzle' used in Bitcoin is based on a cryptographic hash and exhibits similar characteristics: it is asymmetrically hard to solve but easy to verify, and its difficulty can be adjusted".[120] The difficulty, as shown in Figure 6[121] is connected to the diminishing nature of Bitcoin (every four years approximately) to resist inflation.

---

[120] Andreas Antonopoulos, 'ch2', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014).

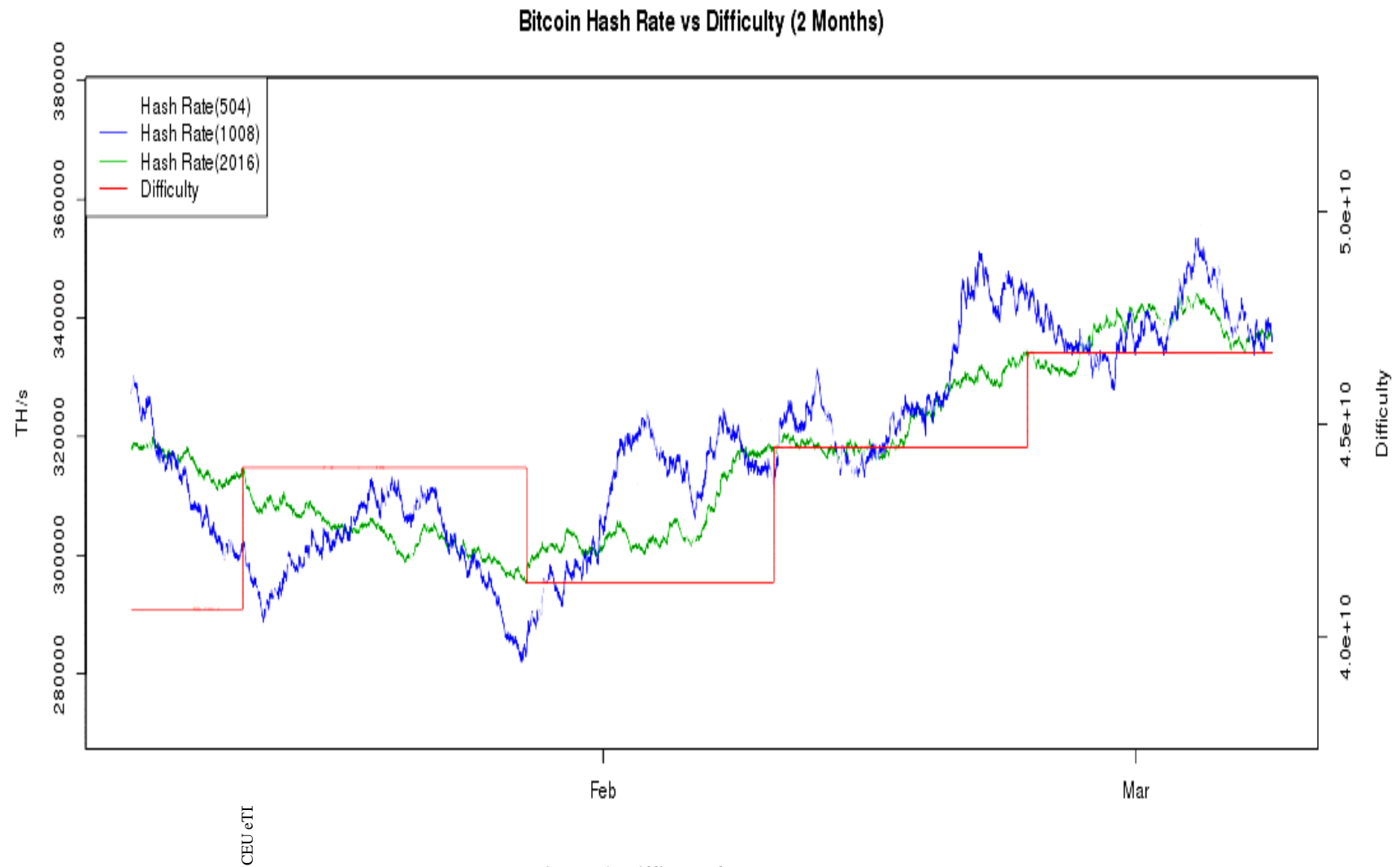[121] Bitcoinwisdom.com < http://bitcoinwisdom.com/bitcoin/difficulty> accessed 7 March 2015.

Figure 6: Difficulty for the late comers

Under difficult conditions, a party would presumably act in his/her own self-interest by maximizing their own wealth, albeit at the expense of others. That is, a situation in which every party cannot be better off without someone else being made worse off.

To explore further, we can imagine that the working hours (in the explanatory case) were eight hours per-day. Each party used to compete and consume his/her economic energy in a useful performance, which increases economic activity. However, if the free-competition was shifted from the substantial, useful and client-centric efforts to be rather consumed in stamping chance-based deflationary notes, in this case the market would not be aligned with the economic equilibrium standard.

On the contrary, if the holder/miners treated the money as a priced-commodity (even though it has zero intrinsic value) to sell it on auction and earn profit, then exploitation, corruption and injustice would prevail simultaneously with an economic incentive loose and volatility in values.

3.2 The root of Bitcoin's volatility

The price of Bitcoin is prone to significant fluctuations up and down over short periods of time. Theses fluctuations are not foreseeable beforehand. It could be bearable at some points in time or extremely unbearable at other points in time. For example, in 2013 Bitcoins dropped about 50%, from $1,155 to $576.29; its volatility was 142%, compared to the USD's of 10%.[122] Hence, the prices of merchandise as measurable by Bitcoin are highly uncertain, which undermines the purchasing power of Bitcoin as a medium of exchange, a phenomenon widely known as volatility risk.

---

[122] Nicole D. Swartz, 'Bursting the Bitcoin Bubble: The Case To Regulate Digital Currency as a Security or Commodity' (2014) 17 Tul. J Tech& Intell Prop 5

The dominant view is that Bitcoin is inherently unstable because of volatility arising from such features of the decentralized payment scheme.[123] Hence, it shall not be classified as legal tender[124] and it is prone to failures and lead to bubbles unless it is regulated by intermediaries. This view insists that stability and the confidence have caused by the centralized regulatory power (e.g. the Federal Reserve) to adjust the monetary policy and the purchasing power of the currency.[125] As suggested by the ECB: "Some aspects of these risks are inherent to the VCS concept and the risks mostly remain unmitigated by legislation, regulation or supervision".[126]

However, it should be noted that these are debatable issues; intermediaries are not necessarily more effective or efficient than self-regulation, and it could be argued that Bitcoin as a decentralized payment scheme is not inherently volatile. In fact, the excess volatility and the inefficiency have long been observed in the regulated financial institutions in the banking sector and stock markets: "Robert Shiller (1989) finds that volatility of stock market (S&P 500) is much higher than would have been predicted by efficient market hypothesis, particularly for the latest part of the twentieth century".[127]

In addition to that, an empirical examination made on the decentralized banking era also known as the free banking. It was accepted in some states, conditionally accepted in others

[123] Craig Elwell and M. Maureen Murphy and Michael Seitzinger , 'Bitcoin; Questions, Answers and Analysis of Legal Issues' (2015) Congressional Research Service 9 < http://www.fas.org/sgp/crs/misc/R43339.pdf> accessed 22 March 2015

[124]ibid 5, 11-12 , see also Cara R. Baros, 'Barter, Bearer, and Bitcoin: The Likely Future of Stateless Virtual Money' (2014) U Miami Bus. L. Rev. 23 (201) 15. <http://repository.law.miami.edu/cgi/viewcontent.cgi?article=1018&context=umblr>23 March 2015 , see also Andrei Dinu, 'The Scarcity of Money: The Case of Cryptocurrency' (2014) 19.

[125] Joseph Haubrich, 'Bitcoin versus the Dollar' (2014) <http://www.clevelandfed.org/Newsroom%20and%20Events/Publications/Economic%20Trends/2014/Bitcoin%20Versus%20the%20Dollar > accessed 8 March 2015

[126]European Central Bank, 'Virtual Currency Schemes-a Further Analysis' (2015) 32, <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 11 March 2015

[127] Sami Al-Suwailem, 'Complexity and Endogenous instability' (2012) Dipartimento di Economia, Facoltà di Economia 6 < http://www.assru.economia.unitn.it/files/DP_3_2012_I.pdf> accessed 23 March 2015

and totally prohibited in the remainder. In fact, the banking sector as well was viewed as inherently volatile (similarly to Bitcoin). During the free-banking era, it was governed by states' laws which "essentially allowed anyone to open a bank, issue their own currency (bank notes), take deposits, and make loans."[128] Findings based on couple of comparative examinations between the regulated banking system vis-à-vis the free-banking systems show a significant result. The result not only shows that the cause of instability and volatility is not due to the decentralization scheme of "free-banking" *per se*, but also shows that the moral hazard hypothesis played a role in the instability of the regulated banks in that era.[129] Adrian Turner (2009), ex-governor of Financial Services Authority, UK, remarks:

> Indeed, there are good reasons for believing that the financial industry, more than any other sector of the economy, has an ability to generate unnecessary demand for its own services—that more trading and more financial innovation can under some circumstances create harmful volatility against which customers have to hedge, creating more demand for trading liquidity and innovative products; that parts of the financial services industry have a unique ability to attract to themselves unnecessarily high returns and create instability which harms the rest of community.[130]

This insight could also be the basis for Bitcoin regulatory framework. By examining the technical relationship between Bitcoin and the banking sectors, the decentralization payment scheme is neither a legal issue nor inherently unstable. Rather, the fundamental cause of instability and volatility in both financial systems are the greed and the lack of honesty in the

---

[128] ArthurJ. Rolnick and Warren E. Weber, 'Inherent Instability in Banking; The Free Banking Experience' [1985-1986] 5 Cato J. 877

[129] See generally ibid, see also Kam Hon Chu, ' Is Free Banking More Prone to Bank Failures Than Regulated Banking?' [1996-1997] 16 Cato J. 47, 58-59

[130] Charles J.Whalen, Financial Instability and Economic Security After The Great Recession (2011) 132

human behaviors, namely the tendency of one party to unjustly enrich at the expense of the other party. This phenomena could be encapsulated in moral hazard, hoarding and selfish utilization. The elimination of such drawbacks has to be regulated by anti-deflation/anti-hoarding policy as well as the value has to be decided fairly either by sufficient governmental intervene or by self-regulatory built-in arbiter computer-codes.

Considering Bitcoin is self-regulated, limited, decreasing and rewarded by early come-early hoarded basis, there tends to be important gaps in the governing codes. As noted earlier, the early holder can manipulate and control the market and the prices will be so volatile up and down which will be a disaster without intermediary to regulate such fluctuations risk.

Indeed, "Gold was the world's arbiter, bringing in automatic adjustment for countries which over-extended themselves by importing more than they exported and thus suffering balance of payment deficits."[131] But, the value decider of gold on basis of mere scarcity is impractical with the self-regulated digital crypto-currency such as Bitcoin. But the question arose as whether the value decider of precious metal is the mere scarcity?

3.3 The value decider of precious metals and Bitcoin

Wei Dai (1993) referred to the money creation aspect as the most problematic part of virtual currencies, but he proposed the auction as the basis for deciding value.[132] Satoshi (Bitcoin 2008) suggested that the common theme between Bitcoin and gold is the cost production in context of the incentive for the issuers due to their "time and electricity that is expended".[133] Our assumption that the key value decider of gold is the monyness, defined as "the amount of intrinsic value an asset has which is true, inherent, and essential value, not depending upon

[131] David Marsh, *The Euro; The Battle for the New Global Currency* (2d ed. 2011) 22

[132] Wei Dai, 'B-Money' < http://www.weidai.com/bmoney.txt, 1998> accessed 10 February 2015

[133] Nakamoto Satoshi, 'Bitcoin: A Peer-to-Peer Electronic Cash System' 4 (2008)

accident, place, or person, but the same everywhere and to everyone".[134] This monyness of the gold is driven by the high cost of production, difficulty of extracting[135] and usefulness. Hence, the rarity of gold is a result of such hardship and not a main intended feature.

For Bitcoin, however, to have an intrinsic value it has to resemble the gold in these features (cost of production and usefulness) and not merely the result (hardship). The digital mining has to be aligned with the economic incentive, valuable efforts and usefulness. As noted above, the financial disaster is linked to moral hazard and exploitation, whereas the economic equilibrium is linked to the valuable efforts and fairness. At this point, Bitcoin would resemble the solid gold standard which "thoroughly consistent with [classical] liberal principles" as stated by Milton Friedman.

The digital intrinsic value as governing code is not just a theory, it is also practice. The dual-purpose code has proven the possibility of monyness in cyberspace. The mining process has developed on the basis of the dual-purpose governing-code to alternatively resemble the gold in its usefulness and monyness. The programmer Antonopoulos stated that although mining is relatively cheap, it has "been criticized by many as being 'wasteful.' The next generation of alt coins attempt to address this concern. Dual-purpose proof-of-work algorithms solve a specific 'useful' problem, while producing proof of work to secure the network".[136]

In a nutshell, the main risky dilemma of Bitcoin is volatility. Some opinions considered Bitcoin to be inherently risky and suggested the preventive approach as a regulatory tool. However, by examining the main cause of volatility on the ground of a clinical approach, it

---

[134] Black's law dictionary <http://thelawdictionary.org/moneyness/> accessed 10 March 2015

[135] Sellgoldhg <http://www.sellgoldhq.com/why-is-silver-cheaper-than-gold/> accessed 10 March 2015 ((Aluminum, for example, is a relatively cheap metal because it is abundant, but it is also a little difficult to extract. Much of the silver and gold discovered is actually alloyed with other metals, which usually requires separation of the two metals in order to produce pure silver or pure gold))

[136] Andreas Antonopoulos, 'ch9', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014)

seems that the middle-man regulations are not necessarily more effective and efficient than self-regulation unless it regulates the hoarding and exchange rate fairly.

Furthermore, the findings show that the volatility attributable to Bitcoin is caused by moral hazard and exploitation due to the lack of the built-in governance of the behavior of the miners (easy for early miners, difficult for later-comers), which is rooted in the lottery-like mechanism of current Bitcoin mining process. As a result, it opens a window of gaining Bitcoin without risk, to be exploited, hoarded and manipulated in terms of market price, which turns Bitcoin from the function of money to become a stock traded at auction. However, if Bitcoin would resemble the functioning components of the precious metals in cyberspace, such as re-designed with dual-purpose (DP) model, it could be a workable solution for mitigating volatility and moral hazards with conditional to be under the supervision of the administrative power to regulate exchange rate and hoarding. The remaining questioning as to what extent the chosen jurisdictions may survey such a DP mining model.

3.4 The legal analysis of dual-purpose (DP) model

The DP model is a new mechanism for rewarding-based the minors and a necessary feature to be legitimate governing computer code in cyberspace according to some jurisdictions, while not an add-in for its legitimacy in others. The test is the time-value of money and its application in cyberspace. Some jurisdictions views that money per-se has time-value, so the DP model is not an add-in governing-code. While other jurisdictions views money has no time-value unless it is utilized efficiently with useful and valuable utilization, therefore the DP model would be a necessary add-in governing code for such jurisdictions.

51

3.4.1 The legislative intent of US law

As noted previously, the Founding Fathers wrote the US Constitution at a time of financial volatility and instability, which was the reason behind the gold clause. Indeed, it is hardly imaginable that the Founding Fathers would have referred to such an arcane financial caveat without a pragmatic reason for doing so. The observation of the public policy rationale could be determined from the legislative history, legislator intent and Supreme Court law case studies. As noted in the *Hepburn v. Griswold and Craig v. The State of Missouri* Supreme Court cases, the reasoning of the judges focused on the substantial effects on the market. They reasonably referred to the monyness of the gold and its impact on preserving the economic incentive in the market. Accordingly, the link between monyness and economic incentive is the functional key for any money-like such (as Bitcoin) in order to practically establish the public confidence as observed by the economist Richard H. Timberlake, Jr:

> Private money (decentralized)[137] would need to offer an economic incentive. The only possible incentive for such issues is an operational ongoing redemption practice in some commonly demanded merchandise, property, or service. The records of unaccounted currency issued in the nineteenth century offer evidence that money of this description is practicable.[138]

The underlying reasoning behind the economic incentive is linked to the progress of science, useful arts, commerce and society's welfare. For instance, the legislator intended to protect the incentive of the authors and inventors in the Copyright Clause of the United States Constitution[139] in order to protect the time and resources invested in intellectual property by

---

[137] (decentralized) added

[138] Richard H. Timberlake, 'The Significance of Unaccounted Currencies',[1981] 41 J. Econ. Hist 866

[139] U.S. Const. art. 1, § 8

its owners. This interpretation is clearly stated on the Supreme Court case of *Stewart v. Abend*: "to obtain fair remuneration for his creative efforts".[140]

As implied by the creative efforts, the authors significantly utilized their time. Such monetary value is also defined in broader sense as noted in the Supreme Court case of *Marine Midland Bank*: "As the bricklayer and mason must account for time and effort, so, too, must the attorney. His remuneration must be measured by his efforts… a standard of reasonableness must at all times reflect fair dealing and strict accountability".[141]

Moreover, in Supreme Court case *SEC v. W. J. Howey Co[142]*, the court held for the general applicability of the Securities Act of 1933 and included the offer of a land sales and service contract within the definition of the "investment contract". In applying so, the court relied on test strands of many factors, as noted by justice Murphy: - "The test is whether the scheme involves an investment of money in a common enterprise with profits to come solely from the "efforts"[143] of others".[144] While the factual basis of the case is irrelevant, but the case implies that the efforts are an important element for the legal determination. In addition, the researchers in the corporate governance fields have strongly recommended the link between the executive performance and compensation. In addition, they recommended tying bonuses to long-term performance and proposed to SEC a more transparent mechanism for public companies "to make the amount and structure of their executive pay packages more transparent".[145]

---

[140] Stewart v. Abend, 495 U.S. 207 (1990)

[141] Wasserbauer v. Marine Bank, 92 Misc.2d 388 (1977)

[142] SEC v. W. J. Howey Co., 328 U.S. 293 (1946)

[143] Emphasis added

[144] ibid

[145] See generally Lucian A. Bebchunk, Jesse M. Fried, 'Executive compensation' (2005), 17 (14) Journal of applied corporate finance

If so, then the useful and valuable efforts of the miners in cyberspace will be a necessary add-in feature. In other words, the dual-purpose (DP) mining as governing-code which has linkage between pay and performance, economic incentive and monyness similar to gold is indeed a strengthening input to be surveyed to the gold clause and legislative history and intent.

3.4.2 The legislative intent of EU law

In contrast to the US economic approach, the conception of decentralized cryptocurrency as such is a challenging issue to the legislative intent behind the European single currency, notwithstanding the re-design of Bitcoin with DP model. If we examined the DP model theoretically speaking, we could assume that it falls under the legislative intent on the basis of the 'sweat of the brow' doctrine. This doctrine implies the monetary value of the mere economic energy, time and efforts by the authors, even though it is not creative work, as expressly stated in the Databases Directive 96/9/EC:

> Whereas the object of this sui generis right is to ensure protection of any investment in obtaining, verifying or presenting the contents of a database for the limited duration of the right; whereas such investment may consist in the deployment of financial resources and/or the expending of time, effort and energy.[146]

However, it could be counter-argued that the plain text of the legislator did not interpret the terms "time, effort and energy" in a narrow sense connected to the usefulness and valuableness of the effort. Rather, the legislative intent is presumably going to protect any efforts or time regardless whether it is valuable or useful, hence the "mere time" has a monetary value. Unlike the associated features of gold, it could be sufficient for the miners to

---

[146]Datab Council Directive 96/9/EC of 11 March 1996 on the legal protection of databases, recital (40). ases Directive 96/9/EC, recital (40)

54

be rewarded with the mere-time invested, as it is currently built-in with Bitcoin protocol. This argument is also supported by the rationale behind the EU's Late Payment Directive, which entitles the business to be paid an interest against the mere-time passed as a compensation for recovery costs.

As the wording of the fourth indent of Article 121(1) of the EC Treaty requirement indicates that the money has a value over long-time: "the durability of convergence achieved by the Member State and of its participation in the exchange-rate mechanism of the European Monetary System being reflected in the long-term interstate levels".[147]

To conclude, the EU is trust-based in terms of centralized money. The issuance of currency is a loan-based system connected to member states' GDB-debts. As a result, the dual-purpose code is unnecessary add-on feature as an economic standard of the digital cryptocurrency.[148]

3.4.3 The legislative intent of IBL law

The time-value of money in IBL considers the time investment in terms of risk and the maxim: "no reward without risk"*(al-ghorm bil ghonm)*. It could be argued that risk is inherent in the mining process of Bitcoin, but the reality is that the differences are significant. The mining as observed is based on zero-sum game and it is a chance-based system. These bases cannot build public confidence as intended by the legislator. As observed by Ibn Taymiyyah:-

> *Reward of deeds is based on their usefulness, not their hardness; a good deed*
> *might be hard, but its goodness is for a reason other than being hard. Reward*
> *may be larger if involved hardship is larger, not because hardship is the*

147Hanspeter K. Scheller,' History, Role and Functions' (2ed REV 2006) 36
<http://www.ecb.europa.eu/pub/pdf/other/ecbhistoryrolefunctions2006en.pdf> 24 March 2015
148Council Directive 2011/7/EU of 16 February 2011 on combating late payment in commercial transactions Text with EEA relevance

55

objective of the deed, but because the deed implies hardship. In other words,

hardship is secondary in determining the value of the deed. The primary factor

is its usefulness. Accordingly, value would reflect its hardness, but only to the

extent that it is useful.[149]

The Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI) in 2008 issued a standard named "trade in currencies". They expressly stated the restriction of the monopoly (*ihtikaar*) on currency: "The dealing in currencies shall not aim at establishing a monopoly position, nor should it entail any evil consequences to the interest of individuals or societies".[150]

As the preceding analysis has shown, the cost production of extracting the commodity money is usually pre-determined. If the commodity money is inherently valuable, it would connect the qualitative efforts to the real economy. This phenomenon would allow the community to have confidence on the commodity money as value decider, since they will be assured that it is a result of a real and useful effort for the welfare, and not a result of exploitation and speculative method. As such, the DP model of digital cryptocurrency would definitely be a necessary code for IBL, which will create confidence in the networks, since it provides value-adding and wealth-creating activities.

Under the above analysis, we can conclude, that the regulatory framework of Bitcoin is formulated in computer codes that do not efficiently manage risks or controlling them (e.g. compared to the gold standard). Greater confidence is needed to maintain the function of the currency's purchasing power as a measure of value. Hence, the DP model may be the missing

---

[149] Sami Al-Suwailem, 'Islamic Approach to Risk' (2011) 3
[150]AAOIFI, Shariah Standard No.1 (trade in currencies) art. 2/1 d, p. 5

block which could meet the needed criteria in some jurisdictions such as US's gold clause and IBL, but not the EU.

In this case, Bitcoin has sorted out the double-spending problem through its input/output chain of signatures mechanism (as observed in chapter 1). However, it has raised another concern over the inability for reimbursement or being charged back. As such, it creates a consumer risk in cyberspace, as discussed in the next chapter.

57

CHAPTER 4: THE ISSUE OF BITCOIN'S IRREVOCABILITY

4.1 The dilemma of Bitcoin's irrevocability

In the case of traditional payment, consumers are eligible to chargeback their money, either from the merchants or from the banks. This chargeback mechanism provides a strong protection for consumers against fraudulent transfer in banking service, or misrepresentation (as an example) in any commercial services.

Bitcoin, in turn, is designed to be irrevocable, as noted earlier; each precedent transaction authorizes the following transactions up to the moment when Bitcoin currency is paid by a buyer and so on and so forth. This design endangers consumer protection concerns in cyberspace: is the seller liable to reimburse a buyer? If so, what rate should the buyer be reimbursed with, especially in case of volatility? Besides, who is going to be liable in case of fraudulent transaction or fraudulent transfer?

For the purpose of legal determination in light of the chosen jurisdiction, the relation of Bitcoin clients to the Bitcoin protocol should be analyzed with an understanding of client categories and securities tools.

4.2 The technical aspect of Bitcoin's contractual relationship

4.2.1 The technical aspect of Bitcoin clients

The contractual relationship of Bitcoin starts with the registration process of both Bitcoin clients (users and merchants) in the Bitcoin network.

Initially, the Bitcoin clients have to register in the network online by installing Bitcoin software. In this stage, Bitcoin clients are shaping their wallet forms by choosing to be alternatively, (a) full client user (similar to a standalone email server) who handles their own protocol by themselves, manages their own wallet and verifies their own transactions without

relying on third party services; (b); a lightweight client user (similar to standalone email client) who relies on third-party services to verify their transaction and interactions within the network, storing his wallet by himself; (c) a web client user (similar to a Gmail/Yahoo client) who relies merely on third party services for verifying transactions as well as the storage of the wallet.[151]

In case of data loss or fraudulent transfer, these referred categories are necessary to apportion the liability between users, service-providers and the merchants. These differences have been observed by the programmer Antonopoulos, who notes that:

> The choice of Bitcoin client depends on how much control the user wants over funds. A full client will offer the highest level of control and independence for the user, but in turn puts the burden of backups and security on the user… a web client is the easiest to set up and use, but… security and control is shared with the user and the owner of the web service. If a web-wallet service is compromised, as many have been, the users can lose all their funds. Conversely, if users have a full client without adequate backups, they might lose their funds through a computer mishap.[152]

After the registration, the Bitcoin clients have to set up a private key (password) for their wallet, regardless of the forms. They have a technical liability to protect their password by being completely random and hard to break.[153] Afterwards, the Bitcoin clients can create their own public key (like an email address) where they can store, buy, send or receive the

---

[151]Andreas Antonopoulos, 'ch1', *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st, O'Reilly Media, 2014)

[152] Ibid

[153] ibid ((Use a combination of upper and lowercase characters, numbers, and symbols. Avoid personal information such as birth dates or names of sports teams. Avoid any words commonly found in dictionaries, in any language. If you can, use a password generator to create a completely random password that is at least 12 characters in length. Remember: bitcoin is money and can be instantly moved anywhere in the world. If it is not well protected, it can be easily stolen))

payments. This address can also be shaped in a barcode format called QR code, which simplifies the process of payment simply by scanning the code through smartphone camera.[154]

As implied, the public key (either numerically or as a QR code) manifests the digital signatures of the clients. They are also convertible, printable (in coin/paper) and useable in a physical form as well. As such, it should strengthen the privacy mechanism of the clients[155] by enabling them to keep their private-public keys in their custody.

4.2.2 The technical aspect of the Bitcoin transaction

In this stage, we can imagine the contractual relationship between the two transacting parties/clients of Bitcoin; the users and the merchants. Similar to the traditional transaction, Bitcoin user is a buyer who acquires a certain property/service for a certain amount of payment in Bitcoin (BTC price). In turn, the Bitcoin merchant is the seller who transfers such value to the Bitcoin user.

Unlike traditional payment, Bitcoin transaction could be paid by several methods, such as by scanning the QR code of the merchant or handling the physical printed Bitcoin or traditional money after being exchanged from Bitcoin beforehand. At this point, the resulted transaction appears on the blockchain as unconfirmed as shown in Figure7[156]. Here, the decentralized verifying-miners are liable to secure the network from any fraud. Before the validation of the transactions as confirmed, the verifiers would filter every transaction against a long checklist

---

[154] Ibid

[155] ibid chapter 10, the author mentioned a personal experience for securing his Bitcoin ((I personally keep the vast majority of my bitcoins (99% or more) stored on paper wallets, encrypted with BIP0038, with multiple copies locked in safes. Keeping bitcoin offline is called *cold storage* and it is one of the most effective security techniques. A cold storage system is one where the keys are generated on an offline system (one never connected to the Internet) and stored offline either on paper or on digital media, such as a USB memory stick))

[156] Blockchain.info < https://blockchain.info/tx/55c6bfbdf1f78da66abb22deff06b5e942f52b60a28ce5299bdf5daf08609977 > accessed 26 March 2015

60

of criteria and discarded the invalid transactions. As a result, the confirmation will be propagated at the blockchain, as in the screenshot in Figure 8.[157]

---

[157]Blockchain.info <http://blockchain.info/tx/0923241e6f251dbf8804d4b492480a8f7d0e55f8f597c30d6b04b3429a38af5a > accessed 16 March 2015

Figure 7: Unconfirmed transaction

Figure 8: Confirmed transaction

As illustrated (in Figure 8), the output is a buyer resident in US. This buyer transacted with a seller at an estimated price of 0.407631 BTC ($118.42). This transaction was later verified and confirmed by a miner, who was rewarded with an estimated 0.0005 BTC ($0.15) transaction fee. It might be assumed that the system might be attacked by fraud and lead to market failure, but it seems resilient. BitPay, a Bitcoin processing company, has experienced zero fraudulent orders in more than 10,000 Bitcoin transactions.[158] In contrast, the centralized digital payment had experienced an increase in fraud by order rate from 0.6% in 2011 to 0.8% in 2012.[159]

Notwithstanding that the Bitcoin clients have a wide range of available procedural techniques concerning their storage, security and control, in addition to online-accessing and screen-shooting the transaction from the cyberspace, the irrevocability code of Bitcoin may rise up the allocation of risk disputes between the Bitcoin clients.

4.3 The legal aspect of Bitcoin's contractual relationship

The transaction in Bitcoin is usually made between two types of clients, as observed earlier. If we assume that the two clients are web-clients, they rely on the services provided by an agency service-provider.[160]

---

[158]Bitpay, BitPay Surpasses 10,000 Bitcoin Merchant Transactions, Zero Cases of Payment Fraud <http://blog.bitpay.com/2013/01/22/bitpay-surpasses-10-000-bitcoin-merchant-transactions-zero-cases-of-payment-fraud.html> accessed 17 March 2015

[159]CyberSource Corporation, Online Fraud Report Online Payment Fraud Trends, Merchant Practices, and Benchmarks 14TH Annual edition (2013) at 4

[160] In practice, some agents (service providers) declare an exemption from any liability, which might be caused by their principles; either merchants or users. As such, the merchants would be contractually responsible for any strict or product liability. And the users' refunds, in turn, are subjected to the fluctuation risk, which might be fewer amounts than what initially paid with. In addition, some agents (service providers) require from merchants to provide a disclosure-refunds policy for its users. They recommend, therein, merchants to refund their consumers with the purchase price of the item, instead of being uncertain

Considering the nature of Bitcoin currency and transactions, it is reasonable to assume that the (user) buyer may ask to recourse his/her Bitcoin currency from the seller (merchant), because of a specific deficiency in the merchandise; the seller also might ask for chargeback for damages, because of a defraud caused by the buyer; or both of the parties might conflict over the refund rate because of the fluctuation risk. However, all of these actions share a similar refunding process.

The refunding process is dominantly viewed as "a new separate Bitcoin transaction" *per se*, yet we respectively disagree. Our assumption is based on the mere fact that the exercise of payment from one wallet to another in Bitcoin is actually similar to the exercise of payment in traditional money from one hand to another. Thus, it should not differ from the typical mechanism, but the legal aspect would vary from case to case basis according to the factual basis of each case; refund, withdrawal or new bid, the same as the mere exercising of traditional withdrawal of the refund; by reversing the possession of money from one hand to another.

However, the differences are mainly in the allocation of the fluctuations risks and the transaction fees which could be adjusted or allocated between the concerning parties.[161] As a result, the concerning issues beforehand concern under what circumstances the merchants should be bound by law to refund the user and what exchange rate should be used (e.g. the rate at the time of the original transaction or the rate at the time of refund).

The aim of the contract law as a private law is to dispense the balanced justice between the private transacting parties. To comprehend Bitcoin's consumer protection, further

---

[161] Another side concern might arose is the impossibility to cancel a mistaken payment, thus the payer would lose his payment. Indeed, the more the transaction is counted as input in the chain, the more difficult to be cancelled. The possible cancelation scenario, in turn, is prior to the transmitting time in the network or through double-spending to be rejected by the verifiers, and it is generally advisable for the users to be fully aware before the payment

consideration is needed by examining both the legal effect of the contract's formation as well as the consumer protection rules-within the selected legal frameworks (US/EU/IBL).

4.3.1 Bitcoin's consumer protection in US regulation

Albeit they are not legally binding, the Uniform Commercial Code (UCC) and the Uniform Electronic Transaction Act (UETA) have been widely adopted by almost all States in the US. Regarding the UETA, it validates any electronic medium as long as its circumstances and procedurals are reasonable, and the UCC insists on the validity of any manner of contracts so far as sufficiently show agreement.[162] In addition, it sets out a framework to govern commercial related issues. As an example, it sets out the framework of the contract's related issues *inter alia* express warranties,[163] implied warranties,[164] doctrine of unconscionability[165] and frustrations.[166]

A quick analysis of the factual basis of Common Law[167] suggests that these rules are applicable to the transactions held on distance such as Bitcoin's transaction. As an example, the case of *Hill v. Gateway 2000,* In this case, the transaction was concluded over the phone (on distance), however the buyer was not aware of some additional terms in the contract except in later time. The holding of the court was on the effectiveness of the contract even without being informed of what it contains therein. Meaning, the contract will be enforceable on the same grounds as any other contractual terms. Similarly, the court held in the *ProCD, Inc. v. Zeidenberg*. It was an issue of the enforceability of the shrink wrap license. The issue

---

[162] UCC section 2-204, 2-206 do not require formal rules for offer and acceptance. Thus parties may contract entirely over the internet

[163] Affirmation, promise, description or sample

[164] Fit for the ordinary purpose for which they are to be used

[165] UCC Section 2-302

[166] UCC Section 2-615

[167] ProCD v. Zeidenberg (86 F.3d 1447 [7th Cir. 1996]) and Hill v. Gateway 2000, Inc. (105 F.3d 1147 [7th Cir. 1997] Specht v. Netscape (306 F.3d 17 (2d Cir. 2002))

was hold by Justice Easterbrook who primarily held on the validity of the contract on the ground of 2-206 (describing acceptance of a contract) and (UCC) sections 2-204 (describing a valid contract). The reasoning of Justice Easterbrook was more grounded on the market practice, he examined the question of acceptance and noted that Zeidenberg could have rejected the terms of the contract and returned the software. That means, the US courts would not generally interfere in normal market practices, but would rather focus on the consent matters between the parties. It measures the consent through the reasonable prudence standard in the contractual context at cyberspace, which mainly measures the awareness of the contract's existence and not what contained therein. However, if we assumed that the Bitcoin transaction is endowed with a warranty (either expressed or implied), the parties would be governed by its terms.

Conversely, Omri Ben-Shahar and Eric A. Posner (2011) criticized the measure standard behind the referred cases. They argued for the importance of imposing the right of withdrawal for consumers, they stated that the holding of the courts "rely on offer-and-acceptance doctrine, which is poorly suited to the problem… in fact the policy concerns apply more generally to all the characteristics of a product or service… By contrast, we describe the right to withdraw as an aspect of the optimal contract between sellers and buyers regardless of relative bargaining power".[168]

In the federal level, the right of withdrawal is not recognizable for consumers except in narrow exceptions *inter alia* "doorstep sales tactics, telemarketing, and other situations in which consumers are vulnerable to 'seduction,' such as purchases of time-shares made during vacations",[169] but no right of withdrawal is granted in case of the complex contracts.[170]

---

[168] Omri Ben-Shahar and Eric A. Posner Source, 'The Right to Withdraw in Contract Law' (2011) 40 UChiLRev 116-17
[169] ibid 120

At the state level, in turn, the regulation varies. New York[171] and California[172] codification recognizes the right of withdrawal that applies in wide scope of sales, but this could be easily wiped out by either a disclosed policy or a posted sign. On the other side, other states further restricted and limited transactions involving high-pressure tactics.[173]

If we assume that the parties have concluded a contract with a clear refunding policy, the fluctuation risks still remain an issue. As noted earlier, the refunding case is not a new bid, but rather a mere reversed-performance to chargeback the other party. Hence, the commercial impracticably UCC Section 2-615 would govern. The bottom-line as observed by Common Law is the reasonable foreseeability standard between the parties, which distinguishes between the normal risks of contracting such as the fluctuation in the price and market changes, from the abnormal risks such as a financial collapse or governmental prohibition.

The case *Ner Tanrid Congregation of North Town v. Krivoruchko*[174] is neither a Bitcoin case nor UCC case, but the arguments could be applicable to UCC section 2-615. The court reasoned that financing is a standard risk in almost every real estate transaction and that the problems associated with the real estate "bubble" were reasonably foreseeable. Likewise, the standard of fluctuation of Bitcoin is foreseeable, which obliges each party to chargeback the other according to their agreement.

To sum up, the US regulation has adopted the market-oriented approach in regulating the consumer protection issues. The common theme of the Bitcoin and traditional commercial transactions are similar, they both are held normally in physical premises and online distance.

---

[170] Ibid

[171] New York Code, General Business, sec. 218-a

[172] California Civil Code, sec. 1723

[173] ibid at 143

[174] Ner Tanrid Congregation of North Town v. Krivoruchko, 2009 WL 1930191 (NDIll 2009)

Thus, courts will not interfere in the market practices; the parties shall be obliged to reverse back the deal within the agreed terms of the contracts and foreseeability standard.

4.3.2 Bitcoin's consumer protection in EU regulation

Unlike the market-oriented approach of US jurisdiction, the EU has adopted a social-oriented approach in laying down the regulatory framework of the consumer-protection matters. These matters are *inter alia* the legal certainty by harmonizing certain aspects of consumer distance and off-premises contracts and the right of withdrawal.

Considering the nature of Bitcoin transaction, it is an internet-connected transaction concluded between its clients. As noted previously, the Bitcoin clients are categorized according to the level of relying on an intermediary's services, primarily for either verifying and/or storing services. In addition, Bitcoin clients might depend on an agent who provides a mere agency-service, within the user-merchant contractual relationship. These inputs are inherently important to determine whether the Bitcoin transaction meets the required definition of the examining directives in the sense of the information to be provided aspect, which is generally regulated by Directive 2000/31/EC (E-Commerce Directive) and the right of withdrawal, which is generally regulated by Directive 2011/83/EU (Consumers Rights Directive).

Pursuant to the *acquis communautaire* nature of the EU,[175] both of the Directives have been established. The applicability of E-Commerce Directive has been examined by Sergii Shcherbak. Comparing the criteria of Bitcoin vis-à-vis the criteria of service-provider[176],

---

[175] Consolidated version of the Treaty on the Functioning of the European Union [2012] 326/01, Article 169(1) (a), Article 169(2)

[176] Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, The Directive defined "service-provider" as: - " For the purposes of this definition:– at a distance, means that the service is provided without the parties being simultaneously present,– by electronic means, means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital

Scherback argued that Bitcoin does not match with criteria defined in Article 2, particularly that the service provider should normally be remunerated, whereas "Bitcoin is publicly accessible and is not provided by any entity which could implement the relevant remuneration policy".[177]

Secondly, the service provider should be at the individual request of a recipient of services, which means, that the service is provided through the transmission of data on individual request. By analyzing the relationship between Bitcoin users and the Bitcoin network, he concluded that the Bitcoin scheme is a multi-point-to-point platform, which does not fall under this definition:

> The legal presence or absence of an individual request within the provision of a certain service both depend on whether the service is transmitted to the user via a somewhat shielded point-to-point channel or is transmitted to the public through a generally accessible point-to multi- point connection. In the case of Bitcoin, there is no point-to-point channel of the transmission of the service, since the user receives the service from the Bitcoin network supported by the community of Bitcoin miners. From the other perspective, a point-to-multi-point transmission also does not take place in the Bitcoin scheme, since the service is not centralized. It can be argued that Bitcoin as a service is transmitted to the

---

compression) and storage of data, and entirely trans-mitted, conveyed and received by wire, by radio, by optical means or by other electro-magnetic means,– at the individual request of a recipient of services means that the service is provided through the transmission of data on individual request received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely trans-mitted, conveyed and received by wire, by radio, by optical means or by other electro-magnetic means,– at the individual request of a recipient of services means that the service is provided through the transmission of data on individual request.

[177] Sergii Shcherbak, "How Should Bitcoin be Regulated?', (LLM thesis, University of Stockholm 2014) 75 <http://www.ejls.eu/15/183UK.pdf> accessed 12 March 2015

user through a kind of multi-point-to-point platform, whose concept is not considered by the ISS Directive.[178]

Moreover, the E-Commerce Directive and the information society service Directive, have both defined service provider as "natural or legal persons" on the grounds that Bitcoin is neither controlled nor owned by anyone, but rather a decentralized in a network. As a supportive argument, the research quoted that the ECB has also highlighted the inapplicability of the E-commerce Directive on Bitcoin transactions.[179]

Although we agree on the analysis of the research, we assume that the services transmitted are shaped and designed according to the level of Bitcoin's clients as observed earlier, which are full-client, lightweight-client or web-client.

Hence, the applicability of "service-provider" should rather be decided on case-to-case basis. If we assumed an applicable case, the Bitcoin service provider should be obliged to indicate the price of goods/service clearly and unambiguously, inclusive of tax and delivery costs, as stated by the Article 7 of E-Commerce Directive. It might be argued that if the prices in Bitcoin are speculative and volatile, is it appropriate for a consumer to withdraw? If so, one at what standard should the price be determined?

Notwithstanding the right of withdrawal being granted by the Consumers' Rights Directive, as indicated by the plain text of the Directive it is widely applicable to any contract either made through distance/online communication or in physical premises, pursuant to Article 2 and Article 3. Accordingly, Bitcoin transactions would be covered within the scope to "any contract concluded between a trader and a consumer", yet the Directive expressly excluded

---

[178] ibid 76
[179] ibid 77

the contract of a speculative nature from being reversed or refunded in accordance to the recital (49) and Article 16, point (b) of the Directive. Recital (49) states that:

> Certain exceptions from the right of withdrawal should exist, both for distance and off-premises contracts. A right of withdrawal could be inappropriate for example given the nature of particular goods or services. That is the case for example with wine supplied a long time after the conclusion of a contract of a speculative nature where the value is dependent on fluctuations in the market ('vin en primeur').

Article 16 states that "(b) the supply of goods or services for which the price is dependent on fluctuations in the financial market which cannot be controlled by the trader and which may occur within the withdrawal period". As a result, the right to withdraw in the Bitcoin transactions of various speculative goods/services is not recognizable pursuant to the analogy of Article 16, point (b).

Under the above analysis, we could conclude that the EU jurisdiction in the field of contract law has established a regulatory framework concentrates mainly on the certainty and consumer-market-balance within the internal market. Unless the measurable goods/services by Bitcoin are volatile, the Consumer Rights Directive[180] would cover such contractual relationships between Bitcoin clients. The variants of Bitcoin clients are considered a new scheme, which is not entirely covered by the E-Commerce Directive. For practical consideration for the irreversibility issue within cross-border cases, it is advisable to opt-in the foreseeability standard with accordance to Article 79 of CISG which states that:

---

[180] Council Directive 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance

(1) A party is not liable for a failure to perform any of his obligations if he proves that the failure was due to an impediment beyond his control and that he could not reasonably be expected to have taken the impediment into account at the time of the conclusion of the contract or to have avoided or overcome it or its consequences.

(2) If the party's failure is due to the failure by a third person whom he has engaged to perform the whole or a part of the contract, that party is exempt from liability only if:

(a) he is exempt under the preceding paragraph; and

(b) the person whom he has so engaged would be so exempt if the provisions of that paragraph were applied to him.

(3) The exemption provided by this article has effect for the period during which the impediment exists.

(4) The party who fails to perform must give notice to the other party of the impediment and its effect on his ability to perform. If the notice is not received by the other party within a reasonable time after the party who fails to perform knew or ought to have known of the impediment, he is liable for damages resulting from such non-receipt.

4.3.3 Bitcoin's consumer protection in IBL regulation

The contractual relationship in IBL, like other legal jurisdictions, has certain elements in formalities or in substantive nature that are necessary to produce legal effects on the transacting parties.

73

The formulation of offer-acceptance is one of these elements. As observed earlier, Bitcoin's offer and acceptance is made electronically, either physically through scanning the bar (QR) code of the counterparty; or by distance payment through entering the public address and amounts of the counter-party. These criteria of "offer-acceptance" mechanism have to be matched with the applicable scope of IBL. The formulation of the offer-acceptance mechanism is based on the doctrine of "mutual consent between the transacting parties", as in the Qur'anic verse (4: 29): "*O you who have believed, do not consume one another's wealth unjustly but only [in lawful] business by mutual consent…*"

The term "mutual consent" was not elaborated in further terms or specified by special practices, which implies that the legislator meant that the scope of "mutual consent" mechanism should be broadly applied. This conclusion is based on one of the principles of the investigative methodology of reasoning (*Usul al-Fiqh*) translated as: "*The fact that was not clarified in further terms, shall be interpreted as applicable in general terms*"[181].

The applicability of this standard has been further elaborated by several jurists, such as Al-Uthaymin, who said:

> *It is necessary that we act on the general (interpretation) until it is proven (to be) specific; this is because the texts of the Quran and Sunnah (primary resources) require we act on what they signify until evidence to the contrary become(s) apparent. So when we find something general that has come about due to a special reason then we must act upon the general (text); because what counts is the generality of the wording and not the specifics of the reason (that*

---

[181] Imam al-Shafi , Al-Risala" (820) p. 96-108

74

text of Quran was revealed), except when an evidence indicates the specific nature of that text, thereby making it specific to whatever is similar to it.[182]

Under the above premises, this standard is applicable to the mutual consent element of IBL's private contract law, which could be concluded by *inter alia* oral, writing, conduct, sign-language, computer-button or Mobile-application.

On the other hand, the same referred Qur'anic verse cited previously (4: 29) referred to another fundamental ruling on contract law, which is consumer protection. The verse has referred to the prohibition of "consuming one another's wealth unjustly". The eating up one's wealth has been elaborated as *inter alia* in the deceptive uncertainty sale (*gharar* - insecure or ambiguous)[183]. Technically, the *gharar* contract is understood as one in which a result is concealed or the terms of the contract are open-ended in nature. It is therefore a type of transaction that has ambiguous terms/descriptions of the subject matter/price, which usually ends in enmity and hatred between the transacting parties (as discussed in detail in Standard No. 31 of AAOIFI).[184]

The primary resources, in turn, insist on the transparency in the commercial communication. Similar to the Article 6 of E-commerce Directive, the transacting parties are obliged to clearly identify *inter alia* the contractual terms; subject matters; quantity; deferred period and attributes of the prices of the commercial activates[185] pursuant to the prophetic tradition: "*The two parties to a transaction have the option (of cancelling it) until they part. If they are honest and disclose any defects, their transaction will be blessed, but if they lie and conceal defects*

---

[182] Muhammad Bin Salih Al-Uthaymin, The Foundations of The knowledge of Usual (1970) p. 49

[183] AAOIFI, Shariah Standard No.31 (Controls on Gharar in Financial Transaction) appendix, p. 547

[184] Ibid 537-544

[185] Ibn Rushd, Bidayat al-Mujtahid (The Distinguished Jurist's Primer) (1198) translated in English (1996) Vol2, p. 179-187

75

the blessing will be erased".[186] As a result, the validity of Bitcoin transaction needs to be based on full consent, full knowledge and transparency. Albeit, the transactions are not only concluded on an item which is visible, present and examinable, but it could be concluded on unexaminable items.

Likewise, Bitcoin transaction is not only concluded in physical premises, but also on distance-payment, which might contains a partial awareness of the subject matter. In this case, the elimination of uncertainty in light of IBL is grounded on the option modes. The option modes are types of mutual agreement between the parties to eliminate the uncertainty of either subject-matter or price. These modes are categorized as follows; the option by description/examination (*khiyar al-ru'ya/wasf*), which constitutes the validity of a transaction on conditional, to be in conformity with the provided description.[187] The option during the meeting (*khiyar al-majlis*) is "conferred on each of the parties to a contract allowing them to rescind it or not to proceed with concluding the contract (usually of sale) before they leave the contract assembly (session), i.e., before they physically or constructively part or separate".[188]

The option by stipulation/condition (*khiyar al-shart*), which is a conditional covenant that "confers on the parties the right to proceed with contract by confirming it or to cancel it, all within a pre-agreed period of time…"[189] The option of defect (*khiyar 'aib*) is the option established for the buyer to return the sold commodity on the basis of a defect.[190]

The cash price option (*khiyar al-shart*) comes into effect when the transacting parties mutually agree on deferred payment within a certain period of time (usually three days),

186 Al-Bukhaari (2079) and Muslim (1532)

187 Ibn Rushd, Bidayat al-Mujtahid (The Distinguished Jurist's Primer) (1198) translated in English (1996) Vol2, p. 187

188 investment-and-finance.net < http://www.investment-and-finance.net/islamic-finance/k/khiyar-al-majlis.html> accessed 22 March 2015

189 Ibid< http://www.investment-and-finance.net/islamic-finance/k/khiyar-al-shart.html> accessed 22 March 2015

190 Ibid<http://www.investment-and-finance.net/islamic-finance/k/khiyar-al-ayb.html> accessed March 22, 2015

otherwise the seller shall terminate the contract. This rule was referred in the Article 313 of the Ottoman Civil Code (*Majallat al-Ahkam al-'Adliyah*): "*If the buyer and seller agree that the price shall be paid at such a time, and that if it is not paid, there is not to be any sale between them, this is a valid agreement. This is called 'money option*".[191]

This is alongside the post-contractual option to terminate the contract subject to the parties' agreement *(Iqalah)*. Consequently, the Bitcoin clients are conferred with these rights to ensure the full consent and transparency in their transaction.

Hence, the refunding policy shall be structured accordingly, meaning, it shall not consider the technicality of the recharging back mechanism in Bitcoin as a new separate transaction, but rather, the Bitcoin user in context of option by defects, as an example, will be entitled to reimburse the full initial (purchase) price and return the goods to the Bitcoin merchant as long as the subject matter has not altered in the position of the user. However, if the defect is slight, some judges are on the opinion that the return of the goods is not necessitated, but the value of the defect (*arsh*) is to be compensated.[192] From the perspective of Bitcoin merchant, in turn, the refunding policy of Bitcoin transaction should distinguish between "stated sale"*(ain)* and "described sale" *(wasf)*. The "stated sale" is that in which the sold item is meant *per se*, while in the "described sale" the sold item is meant by description. In case of the former, the merchant has no right to substitute an alternative for the user, while in the latter case the merchant would have the right to do so.[193]

Apart from the certainty in the subject-matter, the certainty and fixation of the price has to be established and agreed upon by the Bitcoin clients, even though the price is fluctuating. This

---

[191] Muhammad Wohidul Islam, 'Dissolution of Contract in Islamic Law' (1998) 4 (13) Arab Law Quarterly 340

[192] Ibn Rushd, Bidayat al-Mujtahid (The Distinguished Jurist's Primer) (1198) translated in English (1996) Vol2, p. 212-213

[193] Mansur Al-Buhuti, Al-Rawd Al-Murbi (1887) Vol 1 p. 8

means that the refunding has to be paid back fully without being subject to any post-incident or volatility, as such, the consensus between all classical judges from different regions are held.[194]

4.3.4 Conclusion

To sum up, the applicability of Bitcoin transaction by and large, are applicable in the selected examining legal jurisdictions. These jurisdictions have adopted various approaches, from market-oriented to consumer-oriented. The irrevocability feature seems not violating the consumer-protection regulation of the different jurisdictions in cyberspace, since the right of withdrawal is granted in the US (State Law), the EU Consumer's Right Directive and Qur'an 4: 27 in IBL.

Besides, the fluctuation risk could either be regulated by fixing rate standard as in IBL, or by the foreseeability standard as in UCC section 2-615 and Article 79 of the CISG, which has been adopted by many countries, including EU member states.

---

[194] Ibn Abdin, *collection of messages* (Majmuat Rassayal)(1884) volume(2), p. 60, see also *Sahnun, The bloggers (Al-Mudawwana) (854) p. 1160, see also* Ibn Qudama al-Maqdisi, Al-Muqni (1223) p. 434.

THE LEGAL STATUS OF THE UNWRAPPED BITCOIN

Our study attempted to outline for the reader the root of the challenging regulatory framework of Bitcoin from a comparative perspective. In doing so, the thesis initially split up the components of Bitcoin and analyzed it separately as a currency, protocol and a transaction from both technical and legal perspectives. The technical analysis has shown that Bitcoin as a protocol of payment is closer to cash (i.e. an indirect medium of exchange) than barter (direct medium of exchange). Likewise, the legal analysis has shown that the express legal terms of EU, IBL and even the US support this classification.

On the other hand, Bitcoin as a currency is framed to function as self-regulatory commodity money such as gold/silver in cyberspace on the basis of its rarity. Despite this fact, it is volatile due to moral hazard and exploitation, as with the traditional banking sectors and stock markets. At the same time, the implementation of rarity in Bitcoin currency is a mistaken rationale from the framers of Bitcoin, since public confidence is ultimately derived from the preciousness and usefulness of gold. The historical and legal analysis has shown that precious money used to function as a value decider due to various parameters pertaining to usefulness and cash-production. These parameters are manifested in the dual purpose of mining.

In fact, we discovered that the legal tender of Bitcoin cryptocurrency, whether in light of the US Constitution or IBL rulings, would be supported by the DP module of Bitcoin, subjected to conformity with public policy rulings and criminal law. In contrast, the EU single currency conception would not be in conformity with the decentralized cryptocurrency *per se*.

Meanwhile, we examined the wide view of Bitcoin transaction as irreversible which would violate the consumer protections rights. But, we discovered that the technical aspect of Bitcoin is similar to any traditional payment. Moreover, the consumer protection regulations

79

in the comparable jurisdictions are applicable to the Bitcoin transaction, since it is either physical premises or online distance. Consumers have rights under the EU and IBL to be provided with the information either terms or a contract, with the exception of the US, which insists only on the awareness of contracts and not their contents, namely, it is considered to be market practices which the court will not intervene in.

In addition, the warranties contracts are provided by the three chosen jurisdictions in Bitcoin with an exception to the price volatility. In this case, the IBL insists on the initial price to be refunded, while the US and EU in the view to be regulated under the foreseeability standard.

Under the above premises, we could conclude that the volatility is one of the key issues surrounding Bitcoin as legal tender. Since the establishment of public confidence is a sui generis feature of the legal tender as observed from historical human civilization, economic theories and legal policy rationales, it is reasonable to assume that Bitcoin could be self-regulated legal tender as long as it creates public confidence and maintains the economic incentive, which is the aim for any monetary standard, especially for an era "wherein half of global (traditional) wealth is held by 1% of the total population".[195]

---

[195] The Guardian, 'New Oxfam report says half of global wealth held by the 1%'
<http://www.theguardian.com/business/2015/jan/19/global-wealth-oxfam-inequality-davos-economic-summit-switzerland>
26 March 2015

BIBLIOGRAPHY

Primary resources

1. US Const, art 1, § 10
2. State v. Albarty, 76 S.E.2d 381 (1953)
3. Speigle v. Meredith, 22 F. Cas. 910 (1868).
4. Knox v. Lee, 79 U.S. 457 (1871)
5. Stewart v. Abend, 495 U.S. 207 (1990)
6. Wasserbauer v. Marine Bank, 92 Misc.2d 388 (1977)
7. Julliard v. Greenman, 110 U.S. 421 (1884)
8. ProCD v. Zeidenberg (86 F.3d 1447 [7th Cir. 1996]) and Hill v. Gateway 2000, Inc. (105 F.3d 1147 [7th Cir. 1997] Specht v. Netscape (306 F.3d 17 (2d Cir. 2002))
9. Hepburn v. Griswold, 75 U.S. 8 Wall. 603 (1869)
10. SEC v. W. J. Howey Co. , 328 U.S. 293 (1946).
11. Craig v. The State of Missouri 29 U.S. 4 Pet. 410 (1830)
12. Topic 420 – Bartering Income, I.R.S. (2015) < http://www.irs.gov/taxtopics/tc420.html > accessed 11 February 2015
13. UCC section 2-204, 2-206
14. UCC Section 2-302
15. UCC Section 2-615
16. New York Code, General Business, sec. 218-a
17. California Civil Code, sec. 1723
18. Directorate-General for Economic and Financial Affairs, 'One Market, One Money; An Evaluation of the Potential Benefits and Costs of Forming an Economic and Monetary Union' (1990) EC 44, 17 <http://ec.europa.eu/economy_finance/publications/publication7454_en.pdf > accessed 11 March 2015
19. Exchange rate mechanism II agreement [2006] C 73/08
20. COUNCIL Directive, on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC
21. Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC
22. Council Directive 2000/46/EC of 18 September on the taking up, pursuit of and prudential supervision of the business of electronic money institutions

23. European Central Bank, 'Virtual Currency Schemes-a Further Analysis' (2015) 30-31, <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 11 March 2015

24. Council Directive 96/9/EC of 11 March 1996 on the legal protection of databases, recital (40)

25. Consolidated version of the Treaty on the Functioning of the European Union [2012] 326/01, Article 169(1) (a), Article 169(2)

26. Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

27. Council Directive 2011/7/EU of 16 February 2011 on combating late payment in commercial transactions Text with EEA relevance.

28. Council Directive 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance.

29. Ottoman civil code (1869), Sale, section 120-122

30. Hadith, compiled by Imam Muslim, The Book of Transactions (Kiab Al-Buyu) N. 3853

31. Mishkah, 'Legal Maxims of Islamic Jurisprudence' (2013) 123 < http://islamhouse.com/en/books/729618/> accessed 23 March 2015

32. AAOIFI, Shariah Standard No.1 (trade in currencies) art. 2/1 d, at 5

Secondary resources

33. Antonopoulos A, Mastering Bitcoin: Unlocking Digital Cryptocurrencies (1st, O'Reilly Media, 2014)

34. Glaser F 'and others, 'Bitcoin-Asset or Currency? Revealing Users Hidden Intentions' (2014) < http://ecis2014.eu/E-poster/files/0917-file1.pdf > accessed 22 March 2015

35. Jansen, K and Demeester,T 'The Gold Repatriation Movement' < http://www.bullionstar.com/blogs/koos-jansen/tag/bitcoin/ > accessed 5 March 2015

36. Coindesk <http://www.coindesk.com/bitcoin-atm-map/ > accessed 7 February 2015

37. Isidore C 'First U.S.-Based Bitcoin Exchange Opens' CNN (26 January 2015), <http://money.cnn.com/2015/01/26/investing/bitcoin-exchange-coinbase/> accessed 7 February 2015

38. Macheel ,T 'Coinbase Expands European Service to 5 More Markets' Coindesk (October 2, 2014) < http://www.coindesk.com/coinbase-expands-european-service/ > accessed 5 March 2015

39. Thomson Reuters, 'Global Islamic Economy Report (2013)' < http://www.dinarstandard.com/state-global-islamic-economy-report-2013/> accessed 7 February 2015

40. Singhal,A and Rafiuddin,A 'Role of Bitcoin on Economy' (2014) 2(1) WCECS 4 <http://www.iaeng.org/publication/WCECS2014/WCECS2014_pp1028-1033.pdf>accessed 22 March 2015

41. CNBC <http://www.cnbc.com/id/101515483> accessed 7 February 2015

42. Elwell, C and Murphy, M and Seitzinger, M, 'Bitcoin; Questions, Answers and Analysis of Legal Issues' (2015) Congressional Research Service 2 < http://www.fas.org/sgp/crs/misc/R43339.pdf>22 March 2015

43. Europarl < http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-003807&language=EN > accessed: 7 February 2015

44. Clinch M, ' Bitcoin Recognized by Germany as 'Private money' (2013) < http://www.cnbc.com/id/100971898> accessed: 7 February 2015

45. Wei Dai, 'B-Money' < http://www.weidai.com/bmoney.txt, 1998> accessed 10 February 2015

46. Satoshi N, 'Bitcoin: A Peer-to-Peer Electronic Cash System'(2008), < https://bitcoin.org/bitcoin.pdf > accessed 22 March 2015

47. Csirmaz L, 'Secret of Bitcoin', CEU Net workshop 4 (2014)

48. Bitcoin magazine <https://bitcoinmagazine.com/wp-content/uploads/2013/08/bitcoin-volatility-compared.png> accessed 4 March 2015

49. Miers I 'and others', 'Anonymous Distributed E-cash from Bitcoin' 12 (2013) <http://isi.jhu.edu/~mgreen/ZerocoinOakland.pdf> accessed 22 March 2015

50. Miers I 'and others', 'Decentralized Anonymous Payments from Bitcoin', (Extended version) (2014) <http://zerocash-project.org/media/pdf/zerocash-oakland2014.pdf>accessed 22 March 2015

51. Angel, J and McCabe, D ,'The Ethics of Payments' (2014) MSB 20057, 4 < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379233> accessed 22 March 2015

52. Roth A 'and others', 'Efficient Kidney Exchange: Coincidence of Wants in a Markets with Compatibility-Based Preferences' (2007) American Economic Review 97(3) 829<http://dash.harvard.edu/bitstream/handle/1/2562809/Roth_Kidney3way.pdf> accessed 22 March 2015

53. De Filippi, P, 'Bitcoin: a regulatory nightmare to a libertarian dream', Internet Policy Review 3 (2) (2014) 7 <http://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream> accessed 22 March 2015

54. Baros C, 'Barter, Bearer, and Bitcoin: The Likely Future of Stateless Virtual Money' (2014) U. Miami Bus. L. Rev. 23 (201) 4 <http://repository.law.miami.edu/cgi/viewcontent.cgi?article=1018&context=umblr>23 March 2015

55. European Central Bank, 'Virtual currency schemes' (2012) 5 <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 11 March 2015

56. European banking authority, 'EBA Opinion on virtual currencies', (2013) EBA/WRG(1) 1 <http://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies .pdf> accessed 11 March 2015

57. European banking authority, 'EBA Opinion on virtual currencies', (2014) EBA/Op (8) 12 < http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 11 March 2015

58. Shcherbak S, ''How Should Bitcoin be Regulated?', (LLM thesis, University of Stockholm 2014) 58-59 <http://www.ejls.eu/15/183UK.pdf> accessed 12 March 2015

59. Al-Buhuti M, Al-Rawd Al-Murbi (1887) 8

60. Ibn Rushd, Bidayat al-Mujtahid (The Distinguished Jurist's Primer) (1198) translated in English (1996) Vol2, p. 154 <https://ia802703.us.archive.org/24/items/BidayatAl-mujtahidTheDistinguishedJuristsPrimerVol2/TheDistinguishedJuristsPrimerVol2.pdf > accessed 22 March 2015

61. Morgan,V , 'Tareekh Al-Noqood' [A History of Money](1965), translated to Arabic (1993)p. 13

62. Zhuwakinyu M, 'Gold mining in ancient Egypt' (2012) <http://www.miningweekly.com/article/gold-mining-in-ancient-egypt-2012-06-08> accessed 11 February 12015

63. Marsh,D, 'The Euro; The Battle for the New Global Currency' (2d ed. 2011) 20.

64. The British museum, 'Gold Coin of Croesus', <http://www.britishmuseum.org/explore/highlights/highlight_objects/cm/g/gold_croesid_coin. aspx> accessed 11 February 2015

65. Seven Stages of Empire , Dan Rubock, Hidden Secrets Of Money, [2013]

66. Pense,A, 'The Decline and Fall of the Roman Denarius' (1992) Lehigh University 220<http://www.lehigh.edu/~inarcmet/papers/pense%201992.pdf>accessed 23 March 2015

67. Ahmad F and Hassan MK, 'The Time Value of Money Concept in Islamic Finance' (2006) 23(1) AJISS < http://iefpedia.com/english/wp-content/uploads/2009/11/The-Time-Value-of-Money-Concept-in-Islamic-Finance.pdf> accessed 23 March 2015

68. Beggs J, 'Types of Money' < http://economics.about.com/od/money/a/Types-Of-Money.htm> accessed 11 March 2015

69. Timberlake R, 'The Significance of Unaccounted Currencies',[1981] 41 J. Econ. Hist 845

70. Encyclopædia Britannica, 'Legal Tender Cases', (21October 2014)<http://www.britannica.com/EBchecked/topic/334891/Legal-Tender-Cases#ref285279 > accessed 23 March 2015

71. Ebeling R , 'Monetary Central Planning and The State', (January 1999) at <http://fff.org/explore-freedom/article/monetary-central-planning-state-part-27-milton-friedmans-thoughts-costs-paper-money/> accessed 9 March 9, 2015

72. Martin Feldstein, 'The Political Economy of the European Economic and Monetary Union: Political Sources of an Economic Liability' (1997) 11 (4) JEP, 6 <http://www.econ.uba.ar/www/departamentos/economia/plan97/internacional/vanoli/bibliografia/FELDSTEIN.PDF> 23 March 2015

73. Mani A, 'Paper Money: Its Reality, History, Value and Legal Ruling', (1971) 5-6 <https://unity1.files.wordpress.com/2009/06/paper-money-islamic-legal-analysis.pdf > accessed 23 March 2015

74. Bebchunk L, Fried J, 'Executive compensation' (2005), 17 (14) Journal of applied corporate finance.

75. Ibn Abdin, collection of messages (Majmuat Rassayal)(1884) volume(2), p. 60, see also Sahnun, The bloggers (Al-Mudawwana) (854) p. 1160, see also Ibn Qudama al-Maqdisi, Al-Muqni (1223) p. 434

76. Ibn al-Qayyim, I'laam ul Muwaqqi'een 'an Rabb il 'Aalameen (Information for Those who Write on Behalf of the Lord of the Worlds) (1350) Volume 1, p. 139

77. Bitcoinwisdom.com < http://bitcoinwisdom.com/bitcoin/difficulty> accessed 7 March 2015

78. Swartz N, 'Bursting the Bitcoin Bubble: The Case To Regulate Digital Currency as a Security or Commodity' (2014) 17 Tul. J Tech& Intell Prop 5

79. Haubrich J, 'Bitcoin versus the Dollar' (2014) <http://www.clevelandfed.org/Newsroom%20and%20Events/Publications/Economic%20Trends/2014/Bitcoin%20Versus%20the%20Dollar > accessed 8 March 2015

80. Suwailem S, 'Complexity and Endogenous instability' (2012) Dipartimento di Economia, Facoltà di Economia 6 < http://www.assru.economia.unitn.it/files/DP_3_2012_I.pdf> accessed 23 March 2015

81. Suwailem S, 'Islamic Approach to Risk' (2011) 3.

82. Rolnick A and Weber W, 'Inherent Instability in Banking; The Free Banking Experience' [1985-1986] 5 Cato J. 877

83. Kam Hon Chu, ' Is Free Banking More Prone to Bank Failures Than Regulated Banking?' [1996-1997] 16 Cato J. 47, 58-59

84. Whalen C, Financial Instability and Economic Security After The Great Recession (2011) 132

85. Blockchain.info <http://blockchain.info/tx/0923241e6f251dbf8804d4b492480a8f7d0e55f8f597c30d6b04b3429a38af5a > accessed 16 March 2015 , 7:47 PM

85

86. Bitpay, BitPay Surpasses 10,000 Bitcoin Merchant Transactions, Zero Cases of Payment Fraud <http://blog.bitpay.com/2013/01/22/bitpay-surpasses-10-000-bitcoin-merchant-transactions-zero-cases-of-payment-fraud.html> accessed 17 March 2015

87. Shahar O and Posner E, 'The Right to Withdraw in Contract Law' (2011) 40 UChiLRev 116-17

88. Imam al-Shafi , Al-Risala" (820) 96-108

89. Ibn Rushd, Bidayat al-Mujtahid (The Distinguished Jurist's Primer) (1198) translated in English (1996) Vol2, p. 187

90. Investment-and-finance.net

91. Islam M, 'Dissolution of Contract in Islamic Law' (1998) 4 (13) Arab Law Quarterly 340

92. Forbes, < http://www.forbes.com/sites/investopedia/2014/04/21/everything-you-ever-wanted-to-know-about-the-gold-standard/> accessed 25 March 2015

93. Gold certificate as paper currency < http://upload.wikimedia.org/wikipedia/commons/a/a7/US-%2410000-GC-1934-Fr.2412.jpg> accessed 25 March 2015

94. Economist, What was decided at the Bretton Woods summit < http://www.economist.com/blogs/economist-explains/2014/06/economist-explains-20> accessed 25 March 2015

95. IMF, The end of the Bretton Woods System (1972–81) < http://www.imf.org/external/about/histend.htm> accessed 25 March 2015.

96. Gonzalez A,' PAYPAL: The Legal Status of C2C Payment System' (2004) 11 <http://www.era.lib.ed.ac.uk/bitstream/handle/1842/2262/paypal.pdf?sequence=1&isAllowed=y> accessed 23 March 2015.

97. Rubin R and Dougherty C, 'Bitcoin Is Property Not Currency in Tax System, IRS Says' < http://www.bloomberg.com/news/articles/2014-03-25/bitcoin-is-property-not-currency-in-tax-system-irs-says> accessed 26 March 2015.

98. Blockchain, ' Total Bitcoins in Circulation' < http://blockchain.info/charts/total-bitcoins> accessed 10 February 2015

99. Blockchain, ' Currency Stats' < https://blockchain.info/stats > accessed 10 February 2015