Cryptocurrencies: The Revolution in the World Finance

Sanjeev Kumar Joshi, Nitesh Khatiwada, Jyoti Giri
MBM, Nepal Commerce Campus

Abstract

The cryptocurrency is thought to be the next internet revolution, where transactions are done utilizing peer-to-peer network creating a block-chain of the participants involved. Therefore, it is in totality creating a new virtual world, which might change the course of the foreseeable future finance.

The reaction to the block chain and cryptocurrency is synonymous to the reaction to the internet when for the first time it emerged. While it is widely accepted for transactions in some countries; for instance in Nepal, it is illegal.

Where the basic knowledge about the cryptocurrency is scarce in terms of Nepal, this article attempt to connote the grass root construct on cryptography, cryptocurrency and its practices across the globe to its readers.

***Key Words**: Cryptocurrency, Bitcoin, Block Chain, Cryptology, Peer-to-peer network.*

INTRODUCTION

Background

While cryptocurrency has been studied since the 1980s (Heilman, Kendler, Zohar, & Goldberg, 2015), Satoshi Nakamoto (a presumed pseudonym) in 2009 introduced the first 'open' virtual cryptocurrency entitled 'Bitcoin'. The notable fact about the currency is it do not require banks to process payments (Grinberg, 2011) and is self-regulatory – not requiring any central regulatory authority (Reynolds & Irwin, 2017).

Cryptocurrencies are digital token produced from cryptographic algorithms, transported across cyberspace using protocols such aspeer-to-peer networking differently distinguishable thru three key characteristics-electronic, not the liability of anyone (Harvey, 2015) and feature of peer-to-peer exchange(Bech & Garratt, 2017). Doc Searls Weblog, 2017, refers cryptocurrencies are as a digital asset designed to work as a medium of exchange using cryptography to secure the transaction and to control the creation of additional units of the currency. The regulation of the currency is

possible through a digital record-keeping device that uses balances to keep track of the obligations from trading among peers and that is publicly known to all traders (Chiu & Koeppl, 2017). There is no central authority that governs the system; instead the rules governing the system (e.g., defining what constitutes a valid transaction, specifying the total supply of the digital token and its issuance scheme, etc.) are enforced by all network participants (also called 'nodes') (Rauchs, 2017).

With crucial benefit of the security features; ease of use on mobile devices; relatively cheaper costs of production and transmission via the block-chain transmission protocol; and low long-term inflation risks (Harvey, 2015). In the recent years, cryptocurrencies have been increasingly utilized for international transactions, and it is possible their use might expand in the future. However, the innovation in cryptocurrency is still very much in the early stages of adoption. As a result, there are much more issues to be surpassed, particularly for if a central bank will legitimately look at including Bitcoin, for instance, in its reserve mix (Moore & Stephen, 2015). Evidences from most early adopting jurisdictions suggests cryptocurrencies as an asset and hence comprises the subject of capital tax implications on the sale and purchase (Moore & Stephen, 2015). Per se, being very innovative, unconventional and somewhat mysterious phenomena in a modern financial system, it is sometimes presented for as a mode of future of payments and a sign of new emerging economy shaped by centuries of money evolution, evolving regulations and social interactions that are not confined to virtual world(Dostov & Shust, Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?, 2016).

(Dandapani, 2017) Notes peer coin is the first scientific computing cryptocurrency. Such currencies are usually aimed at issues broader than just payments: both bitcoin and Digi cash (Brown & Duguid, 2002) , have certain political connotations(Dostov & Shust, Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?, 2016). Unlike most other currencies generic held by the central bank in their international reserves, the supply of those currencies is not controlled by a central bank but by a highly complex iteration of a mathematical proof (Moore & Stephen, 2015) . Similarly, counterfactual simulations done over the period 2009 to present suggests that adding Bitcoin to the reserve portfolio of the central bank would not significantly increase volatility but could provide opportunities to offset exchange rate depreciations against major currencies such as the Pound and the Euro (Moore & Stephen, 2015)

Besides, there has been a proliferation of virtual currencies across the globe, includes Facebook Credits, Microsoft Points and Amazon coins (Moore & Stephen, 2015) amongst others. With facts that global financial corporations such as Citibank are developing their own cryptocurrency due to these perceived benefits of utilizing the aforementioned protocols (Madore, 2015). Unlike cash, a cryptocurrency keeps track of the history of all transactions. This is done by forming a block-chain.

The existence and development of cryptocurrency are so bold, inevitable and futuristic that a number of central banks recently started to explore the adoption of cryptocurrency and block-chain technologies for retail and large-value payments, for instance, the People's Bank of China and Bank of England aims to develop a nationwide digital currency based on block-chain technology; the Bank of Canada, Monetary

Authority of Singapore are studying its usage for interbank payment systems (Chiu & Koeppl, 2017). Though cryptocurrencies are an area of heightened pecuniary, numismatic, technological, and investment interest, a comprehensive understanding of the theories and foundations is still left wanting among many practitioners and stakeholders (Chohan, 2017).

Since 2009, numerous cryptocurrencies have been developed, with, as of February 2017, 720 in existence (Chen, Chu, Nadarajah, & Osterrieder, 2017), Bitcoin is the largest and most popular representing over 81% of the total market of cryptocurrencies (Chen, Chu, Nadarajah, & Osterrieder, 2017). By 2013 Bitcoin's valuation exceeded US $2 Billion, the only cryptocurrency to achieve such a high valuation (Dandapani, 2017), has on 10th November, 2017 recorded at $ 6575 shows a decline by 9.59% and $ 693.0303 in currency denominations (Russo, 2017). The combined market capitalization of all cryptocurrencies is approximately USD $19 billion (as of February 2017), with the top 15 currencies representing over 97% of the market, and seven of these accounting for 90% of the total market capitalization. Each cryptocurrency is riskier than the Euro (Chen, Chu, Nadarajah, & Osterrieder, 2017).

A notable study suggests that the main issues with the adoption of cryptocurrencies include an early track record of illiquidity, high volatility and potentially nebulous uses.

Purpose of the Study

The major purpose of the study is to give a brief introduction of cryptocurrency to the readers.

The specific purpose of the study is streamlined as under

- To know about the existence and use of cryptocurrency.
- To understand the working mechanism of the cryptocurrency.
- To examine the current development in the field of cryptography.
- To understand the implication of cryptocurrency.
- To path a way forward for the like studies in the future.

Limitations of study

The study was primarily designed to include interviews and opinion survey of the experts pertaining to banking, capital market, Information Technology (IT) experts, and financial experts including professionals backed by the article reviews of the pertinent field. However, due to lack of in-depth knowledge and understanding in the field andquestion posed on its legality put constrains for this article to be portrayed as more realistic and practical.And hence only review of article could be incorporated under the study.

Put differently, the reviewed articles originate from the developed nations. Hence, unavailability of adequate literature at Home County has imparted its effect on the analysis, comparison and conclusion of the study.

Definition of the Terms

Cryptography

Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. Cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing (Kumari, 2017).

Cryptocurrency

A cryptocurrency is a digital or virtual currency that uses cryptography for security. A cryptocurrency is difficult to counterfeit because of this security feature. A defining feature of a cryptocurrency, and arguably its most endearing allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation (Silver, 2017).

Cryptology

The study of secret codes or ciphers and the device used to create and decipher them is termed as cryptology(Collins, n.d.). Such study is based on the fundamental assumption of encryption and decryption.

Block Chain

A block-chain is a digitized, decentralized, public ledger of all cryptocurrency transactions. Constantly growing as 'completed' blocks (the most recent transactions) are recorded and added to it in chronological order.It allows market participants to keep track of digital currency transactions without central recordkeeping. Each node (a computer connected to the network) gets a copy of the block-chain, which is downloaded automatically (Silver, 2017).

Peer to Peer Network

A network of computers configured to allow certain files and folders to be shared with everyone or with selected users. Peer-to-peer networks are quite common in small offices that do not use a dedicated file server. All client versions of Windows, Mac and Linux can function as nodes in a peer-to-peer network and allow their files to be shared (Giles, 2006).

LITERATURE REVIEW

Cryptocurrencies are physical precomputed files utilizing a public key /private key pairs generated around a specific encryption algorithm. The key assigns ownership of each key pair, or 'coin,' to the person who is in possession of the private key. These key pairs are stored in a file named 'wallet.dat,' which resides in a default hidden directory on the owner's hard drive (Heid, 2013). Cryptocurrency is neither commodity money nor fiat money. It offers a new mix of technical and monetary characteristics that raise different economic questions than other kinds of currencies (Blume, 2014). It has many of the characteristics of a precious metal based coinage with a form of

inherent value, rather than a government-backed currency used for trading of value. The decentralized model for the creation and control of the cryptocurrencies means that they are a disruptive influence on traditional currencies as they are not easily subject to central control (Taylor, 2015), and since they are encrypted and facilitate digital barter, may revolutionize digital trade markets by creating a free flowing trading system without fees (DeVries, 2016). Further, since they are payment instrument rather than private currencies, their embeddedness' in the financial system minimizes the ML/FT risks (Dostov & Shust, Cryptocurrencies: an unconventional challenge ti the AML/CFT regulators?, 2016).

Cryptocurrencies offer confidentiality and privacy of transection as well. It uses complex hashing and time stamping methodologies to uniquely identify each coin within that currency. Crypto currency systems generally claim to provide anonymous, decentralized processing of transactions (Sufian Hameed, 2016). In a political economy sense too, it may be valuable to have a cryptocurrency with a stable purchasing power to allay fears of adoption, even if the currency would nevertheless not sustain widespread growth until the regulations preventing intermediation are relaxed (Harwick, 2016).

These currencies might be prone to double spending attacks (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016) which depends on individual incentives to reverse a particular transaction (Chiu & Koeppl, 2017). This can be mitigated through designing alternate cryptocurrency called Scrooge-Coin (Chiu & Koeppl, 2017).

(Reynolds & Irwin, 2017) Found that to keep up with a rapidly expanding global environment, and with the gap between the 'global' and the 'local' becoming smaller, criminals are adopting new forms of currency, such as cryptocurrency, to increase the level of anonymity afforded to their illicit activities. Further, the compliance and implementation of anti-money laundering legislation and customer identification security standards are insufficiently utilized within some exchange services, resulting in more technologically adept, or well-funded, criminals being able to circumvent identification controls and continue to transact without revealing their identities.

RESEARCH METHODOLOGY

This article is based on secondary data. Various articles and research papers published in different form were consulted upon as per the objective of review. The study follows an exploratory design.

FINDINGS

Many of the technologies we now take for as granted were quiet revolutions in their times. Be it internet, smartphones or smart technologies, they have changed the way we live and work. These thing has been around for merely a decade and they have changed the whole business and living style landscape around the world.

Another revolutionary digital phenomenon is block-chain/crypto currency. The following is an insight on the technological development (Gupta, 2017):

- The first major block-chain innovation was bitcoin, a digital currency experiment. It is used by millions of people for payments, including a large and growing remittances market.

- The second innovation was called block-chain, which was essentially the realization that the underlying technology that operated bitcoin could be separated from the currency and used for all kinds of otherinter-organizational cooperation. Almost every major financial institution in the world is doing block-chain research at the moment, and 15% of banks are expected to be using block-chain in 2017.
- The third innovation was called the "smart contract," embodied in a second-generation block-chain system called ethereum, which built little computer programs directly into block-chain that allowed financial instruments, like loans or bonds, to be represented, rather than only the cash-like tokens of the bitcoin. The ethereum smart contract platform now has a market cap of around a billion dollars, with hundreds of projects headed toward the market.
- The fourth major innovation, the current cutting edge of block-chain thinking, is called "proof of stake." Current generation block-chains are secured by "proof of work," in which the group with the largest total computing power makes the decisions. These groups are called "miners" and operate vast data centers to provide this security, in exchange for cryptocurrency payments. The new systems do away with these data centers, replacing them with complex financial instruments, for a similar or even higher degree of security. Proof-of-stake systems are expected to go live later this year.
- The fifth major innovation on the horizon is called block-chain scaling. Right now, in the block-chain world, every computer in the network processes every transaction. This is slow. A scaled block-chain accelerates the process, without sacrificing security, by figuring out how many computers are necessary to validate each transaction and dividing up the work efficiently. To manage this without compromising the legendary security and robustness of block-chain is a difficult problem, but not an intractable one. A scaled block-chain is expected to be fast enough to power the internet of things and go head-to-head with the major payment middlemen (VISA and SWIFT) of the banking world.

On 5th of December, 2013 a proposal was made by few members of the Swiss parliament calling Swiss government for assessing the utilization of bitcoin currency by the financial sector shedding light on bitcoins and other cryptocurrencies from legal standpoint(Yeghiazaryan). Swiss government stated to be neutral to usability of virtual currencies like bitcoin. While cryptocurrencies are legal in 96 countries of the world (including USA, Canada, Australia, European Union), in many of the countries it is illegal (example Nepal) for the fact that bitcoin can be anonymously used to conduct transactions between any account holders, anywhere and anytime across the globe, makes it attractive to criminal elements. They may use bitcoins to buy or sell illegal goods like drugs or weapons. Most countries have not clearly made determinations on the legality of bitcoin, preferring instead to take a wait-and-see approach (example Russia). While some countries are developing cryptocurrencies of their own (example

China, Britain). Some countries have indirectly assented to the legal usage of bitcoins by enacting some regulatory oversight. However, bitcoin is not legally acceptable as a substitute for a country's legal tender.

The cryptocurrency world is evolving at such a dizzying pace that it can be hard to take in the magnitude of everything that's happening in bitcoin. 2017 has been a record-breaking year for bitcoin. From transactions to trading volume, and from wallet installations to market cap, every possible metric has been surpassed, shattered, and then shattered again (Sedgwik, 2017).

The Statistics about Bitcoin

Overview	
Current Bitcoin Supply	16.67 Million
Crypto Market Dominance	58%
24 Hour Trade Volume	$ 4.9 Billion
Transaction	
Countries where bitcoin usage is unrestricted.	96
Transactions per hour.	12,000
BTC sent per hour.	99,000
Average transaction value.	0.103 BTC
Mining	
Network hash rate in TH/s.	11 million
Block chain size.	166 GB
Mining rewards in the last 24 hours.	$12.8 million
Blocks mined in the last 24 hours.	129
Bitcoin transactions confirmed in the past 24 hours.	326,000
Ownership	
Amount of bitcoin owned by just 4% of addresses (containing 2.9 million BTC).	96%
Number of addresses richer than $10,000.	457,000
Number of active addresses in the last 24 hours.	715,000
Value of the 100 richest bitcoin addresses.	$19 billion
Number of Bitcoin wallets downloaded.	500,000
Popularity	
Number of subscribers on r/Bitcoin.	400,000
Number of bitcoin tweets sent per day.	80,000

Source: Bitcoin by numbers: news.bitcoin.com

Cryptocurrencies are also prone to the financial bubbles.Its price is up 600% over the past 12 months, and 1,600% in the past 24 months. At over $4,200 (as of 5 October), a single unit of the virtual currency is now worth more than three times an ounce of gold. Some bitcoin evangelists see it going far higher in the next few years (Rogoff, 2017). The price of a single bitcoin has gone up parabolically and at a faster pace than any other speculative vehicle in market history, as investor enthusiasm for the new medium has reached a fever pitch(Insana, 2017).

CONCLUSIONS AND IMPLICATIONS

The cryptocurrency is a virtual currency that is revolutionizing the payment system across the globe. Though there are mixed reactions, with its development it will possibly be used as the major means of payment in the future. More financial institutions and government adopting cryptocurrencies could contribute to their growth. Not only that, the concept behind the cryptocurrency namely block-chain and peer-to-peer network, is also making an impact in other fields such as smart contracts.

Ease in the use of cryptocurrency, its use in terrorism financing, impact of making it illegal and/or legal in any economy, psychological factors guiding the bubble and bursts, the application of efficient market hypothesis, its usability in crowd funding, and many more topic in relation to the cryptocurrency still remains to be explored forfuture researcher.

References

Bech, M. L., & Garratt, R. (2017, September 17). Central bank cryptocurrencies. Retrieved 2017, from https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf

Blume, S. N. (2014). cryptocurrency. The New Palgrave Dictionary of Economics.

Brown, J., & Duguid, P. (2002). The Social Life of Informaton. Havard Business. Retrieved 2017

Chen, S., Chu, J., Nadarajah, S., & Osterrieder, J. (2017). A Statistical Analysis of Cryptocurrencies. (C. S. Tapiero, Ed.) Journal of Risk and Financial Management, 10(2). doi:10.3390/jrfm10020012

Chiu, J., & Koeppl, T. (2017, November). The Economics of Cryptocurrencies- Bitcoin and Beyond. Retrieved 2017, from http://qed.econ.queensu.ca/working_papers/papers/qed_wp_1389.pdf

Chohan, U. W. (2017, August 25). SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024330

Collins. (n.d.). Retrieved November 18, 2017, from Collins Website: https://www.collinsdictionary.com/dictionary/english/cryptology

Dandapani, K. (2017). E-Finance II. Managerial Finance, 43(5). Retrieved 2017

DeVries, P. D. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. International Journal of Business Management and Commerce .

Dostov, V., & Shust, P. (2016). Cryptocurrencies: an unconventional challenge to the AML/CFT regulators? Journal of Financial Crime, 21(3), 249-263. Retrieved 2017

Giles, L. M. (2006). Introduction to Windows Peer-to-Peer Networking.

Grinberg, R. (2011, December 9). Bitcoin:An Innovative Alternative Digital Currency. Hastings Science and Technology Law Journal, 4.

Gupta, V. (2017, February 28). A Brief History of Blockchain. Retrieved from Harvard Business Review: https://hbr.org/2017/02/a-brief-history-of-blockchain

Harvey, C. R. (2015, March 1). Do Cryptocurrencies Such as bitcoins Have a Future? The Wall Street Journal. Retrieved from https://www.wsj.com/articles/do-cryptocurrencies-such-as-bitcoin-have-a-future-1425269375

Harwick, C. (2016). Cryptocurrency and the Problem of Intermediation. The Independent Review, 20(4). Retrieved 2017

Heid, A. (2013, June). Hackmiami. Retrieved from Hackmiami.org: http :// www. HackMiami. org

Heilman, E., Kendler, A., Zohar, A., & Goldberg, s. (2015, August). Eclipse Attacks on Bitcoin's Peer-

to-Peer Network. WashingtonD.C: USENIX Security symposium.

Insana, R. (2017, 09 13). Bitcoin is in a Bubble, and Here'S How It'S Going to Crash. Retrieved from CNBC: https://www.cnbc.com/2017/09/13/bitcoin-is-in-a-bubble-and-heres-how-its-going-to-crash-ron-insana.html

Kumari, S. (2017, April 4). A research Paper on Cryptography Encryption and Compression Techniques. International Journal Of Engineering And Computer Science, 6(4), 20915-20919. doi: 10.18535/ijecs/v6i4.20

Madore, P. (2015, July 7). cryptocoinsnew. Retrieved from cryptocoinsnew website: https://www.cryptocoinsnews.com/citibank-developing-cryptocurrency/

Moore, W., & Stephen, J. (2015). Should Cryptocurrencies be included in the portfolio of International Reserves held by central Banks? Department of Economics Working Paper Series. Barbados: The University of West Indies. Retrieved 2017, from http://www.centralbank.org.bb/Portals/0/Files/Working_Papers/2015/Should%20Cryptocurrencies%20be%20included%20in%20the%20Portfolio%20of%20International%20Reserves%20held%20by%20the%20Central%20Bank%20of%20Barbados.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press. Retrieved 2017, from http://bitcoinbook.cs.princeton.edu

Rankin, M. D. (2017, Oct). Moneytreade.com. Retrieved from Moneytreade.com: https://www.facebook.com/moneytradecoin/posts/1509167222540123

Rauchs, D. G. (2017). GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY. Cambridge Center for alternative Finance.

Reynolds, P., & Irwin, A. S. (2017). Tracking digital footprints: anonymity within the bitcoin system. Emerald Insight, 19(4), 407-425. Retrieved 2017

Rogoff, K. (2017, 10 9). Bitcoin's Price Bubble Will Burst Under Government Pressure. Retrieved from The Guardian: https://www.theguardian.com/technology/news-blog/2017/oct/09/bitcoin-price-bubble-government-cryptocurrency

Russo, C. (2017, November 11). Bloomberg Technology. Bitcoin Plunges After Plans for Split Called Off. Retrieved 2017, from Bloomberg Markets website: https://www.bloomberg.com/news/articles/2017-11-10/bitcoin-slumps-as-developer-community-remains-divided

Silver, C. (2017, November). Cryptocurrency. Retrieved from Investopedia: https://www.investopedia.com

Sufian Hameed, S. F. (2016). The Art of Crypto Currencies. (IJACSA) International Journal of Advanced Computer Science and Applications.

Taylor, M. (2015, march). Cryptocurrency has it come? Retrieved from Capegimini: https://www.capgemini.com/wp-content/uploads/2017/07/cryptocurrency-has_its_time_come.pdf

Yeghiazaryan, A. (n.d.). LEGALITY OF CRYPTOCURRENCIES: WHERE, HOW, AND WHY? BLOCKCHAIN RESEARCH & DEVELOPMENT HUB. Retrieved 2017, from https://blockchainrndhub.com/en/887Z4HHV