An Empirical Evidences on Cryptocurrencies: Emerging Digital Money in the World.

Nischal Risal
Lecturer, Nepal Commerce Campus

Abstract

This paper aims toward amplifying the concept of cryptocurrency as emerging digital money in the world and its practices in Nepal. The paper is based on review of various articles, books and relevant websites that provide information regarding cryptocurrencies. The paper highlighted the conceptual part and types of cryptocurrencies in the first section, the major literature review in the context of world in the second section, and the practices of cryptocurrency in Nepal in third section followed by conclusion in final section. An exploratory research design has been adopted in the study. The primary survey has been done to collect the data with self administered questionnaire. The paper reveals the importance of cryptocurrencies in the present context of digital world. The paper concluded that the majority of the respondents are not well known about cryptocurrency in Nepal. The respondents are found interested to invest with knowledge, policy and security on cryptocurrency in Nepal. This thematic based research paper will create a platform for the researcher to study the practical scenario of cryptocurrency.

Keywords*; Cryptocurrency, Block-chain, Bitcoin, Digital money*

Section I

Conceptual Review

A form of digital money that uses codes is a cryptocurrency. A universal ledger called a blockchain store the details of each transaction of these electronic coins. To hold access to the database, a user must realize some specific conditions called a private and a public key. The bank account, money, and the transactions are spreadsheet of a database on the internet. The data is stored in a ledger that has a network of servers called nodes, to keep track of your money. The blockchain preserves every transaction in the ledger and shares the details with several other users. It renders the Bitcoin users a form of proof-of-work or simply they trust their counterpart. When people talk about cryptocurrencies, they usually refer to Bitcoins. Bitcoins are one of the many forms of electronic currency. There are Ethereum, Ripple, Litecoin, Monero and many other cryptocurrencies. Till date, there are about 700 Bitcoin-like currencies and they all hold different monetary values.

Digital cash needs a payment network with account, balances, and transaction. A central authority like banks, take control over these transactions. The problem with this type of payment network is that customers had free will to double-spend. This means that one can spend the same amount twice or conduct any type of fraud. Therefore, a central server keeps the record of the balances and prevents the entities from double-spending.

Cryptocurrency allows money to transfer faster and costs much cheaper compared to other conventional methods. A blockchain contains all the accounting data of economic transactions, property and the record of every single trade that have occurred among users. It is a universal digital book or an online ledger. Users can also check whether a future transaction is valid or not through the blockchain. Since a blockchain technology does not have an imprint or physical validation of the transaction, the Internet stores this information. The information inside the block chain database is truly public and shared all over the internet. They exist as a shared and continually updated string of data, and these data are consistent with one another. Only the parties involving in the transactions can access and view the details. Consequently, duplicating or counterfeiting these data is impossible for some hackers.

A global network of computers that use blockchain technology manages the directory for each Bitcoin transaction and operates on a peer-to-peer basis, also known as a node. A node is a network of computers that create a blockchain. These networks use clients that perform the task of validation and record the transfer of coins from user-to-user. These nodes circulate the documentations throughout the Internet. Every computer in a node is an administrator of a blockchain that can join the network freely. Each of these administrators has a chance of winning Bitcoins.

Cryptocurrencies like Bitcoin use an SHA 256 Hash algorithm which stands for Secured Hash Algorithm 256-bit. A Hash is a string of strong cryptographic codes or functions (similar to binary 1's and 0's) that use hexadecimal codes. Miners decrypt the SHA code using high-powered computers and strong mathematical calculations. The transaction adds to the blockchain after the miners decode the hash. Coinbase then provides the miners with a specific number of Bitcoin as a reward. This is how miners create valid Bitcoins. The number of people who use these coins for their daily administration set the value of Bitcoins. But for those who do not use these powerful processing chips, they can buy or sell Bitcoins through online exchanges like Coinbase or Local Bitcoins. These bitcoins do not have an intrinsic value or any physical form. They just exist and possess a certain value. In late 2008, Satoshi Nakamoto, the unknown brain behind cryptocurrency, developed 'A Peer-to-Peer Electronic Cash System' also known as Bitcoin. A peer-to-peer network is a hub of computers for sharing files, videos or any other information (just like bit-torrent). In previous years, digital cash took rapid economic growth since its evolution in the late 2000s. People started to use electronic card systems that provided more security than carrying paper currency. Banks, shopping malls, money exchange, and many other sectors use digital cash such as credit and debit cards for their daily transactions. But still, digital cash have their inadequacy.

The famous cryptocurrencies found at present are explained as;

Bitcoin

The first and the most famous cryptocurrency Bitcoin has a market cap that exceeds over $7billion. A single bitcoin is worth $2,570. Its transaction volume has reached more than 200,000 daily transactions. Some Cyber-crime agency like DarkNet uses Bitcoins as a global means of payment for illegal transactions.

Ethereum

Ethereum has ascended to the second position below Bitcoin in the hierarchy of cryptocurrencies. Other than Bitcoins, Ethereum not only allows transactions for existing accounts and balances but they also validate complex contracts and programs for corporate banks. Besides Ethereum, there is a host of cryptocurrencies like DigixDAO and Augur. They belong to a family of cryptocurrency of Ethereum. A single Ethereum coin is worth $250 in the current market.

Litecoin

Litecoin is one of the first cryptocurrencies after Bitcoin. They are faster than Bitcoins and take a larger amount of token with new mining algorithm. Users trade Litecoins excessively with one another. They use Litecoins as a backup for Bitcoins.

Monero

Monero uses a new type of algorithm (a cryptonite algorithm) that adds privacy features which were missing in Bitcoins. This type of algorithm introduced a concept of ring signatures. The ring signatures were able to pierce through the blockchain and secure the transactions. It was famous for the darknet marketers when the internet felons decided to use it as a currency. The best cryptocurrency apps those are free on android market are; Bitcoin Checker, Bitcoin Price IQ, Bitcoin Wallet by Coinbase, Cryptonator, and zTrader.

On the basis of the information available and existing literature the paper is focused on exploring the existing knowledge on cryptocurrencies in the world of digital money.

Section II

Review of Literature

Andriole (2017) explained that most people, who bought a house or a car, or bought things on Amazon, never thought about paying with cryptocurrency. Most people had no idea how many cryptocurrencies there were (over 1,000), though a lot of people had heard something about Bitcoin. The major significance of cryptocurrencies as explained by Andriole (2017) were;

The theft was essentially impossible with cryptocurrency.

It was potentially nefarious: money laundering, among other transactions, was easy.

Governments could not control it though they could and would regulate and tax it (principally through investment instruments).

An investor could play with cryptocurrency and had created their own digital wallet. They could convert some conventional money into Bitcoin, Ethereum, Litecoin or Ripple, and experiment with how it had worked. They could assess the industry's appetite for change, experimentation and alternative payment systems; track industry progress as well as the technological infrastructure required to expand the use of cryptocurrency (Gao, 2017).

Kim, et, al. (2016) analyzed the user comments in online cryptocurrency communities to predict fluctuations in the prices of cryptocurrencies and the number of transactions. By focusing on three cryptocurrencies, each with a large market size and user base, the researcher attempted to predict such fluctuations by using a simple and efficient method. Furthermore, the simulated investment demonstrated that the proposed method was applicable to cryptocurrency trading. In addition, the rich information in online communities could contribute to understand the cryptocurrencies from different perspectives. Cryptocurrencies were increasingly being used, and their usability had drawn attention from different perspectives.

Narayanan, et, al. (2016) concluded that the given bitcoin's cypherpunk roots, its scattered documentation, and its lack of a formal specifications, Bonneau, Miller, Clark, Narayanan, Kroll and Felten had completed the monumental tasks of producing the first systematic exposition of bitcoin. The researcher had identified three components of bitcoin's design that could be decoupled and analyzed individually: (1) transactions and scripts, (2) consensus and mining, and (3) the peer-to-peer communication network.

Heilman (2015) was eager to identify new attack vectors against the bitcoin network since the authors of the selfish mining paper garnered praise and publicity in 2013. The researcher had revealed the eclipse attack, in which the attacker had monopolized all of the victim's incoming and outgoing connections, thus isolating the victim from the rest of its peers in the network. The attacker could then trick the victim by feeding him misinformation about the state of the ledger, or coopt the victim's computing power for its own nefarious purposes.

Noether, et, al. (2016) concluded that a strong desire for financial privacy in bitcoin had come as no surprise, given the community's historically libertarian leanings. Viglione (2015) had proved an inverse relationship between economic freedom and bitcoin price premiums.

The researcher also concluded that even at this early, volatile stage, bitcoin was generating useful macroeconomic data. Evans (2015) had argued that the overlap between hard-money advocacy and Sharia compliant finance was large enough for these two communities to build intellectual bridges. The paper had put bitcoin on the radar of many people previously far removed from cryptocurrency, resulted in a surprising amount of attention from Muslims worldwide.

Eyal (2016) had explained the Bitcoin-NG as a radical scalability proposal that employs micro blocks and key blocks to bypass the tradeoff between transactional throughput and latency in bitcoin's present peer-to-peer communication network. In addition to benchmarking the performance of their proposal using a large-scale bitcoin-network simulator, the authors had introduced several novel metrics such as consensus delay and mining power utilization for quantifying the security and efficiency of blockchain protocols.

Stephen and Moore (2015) had concluded that holding a small portion of reserve assets in bitcoin could be beneficial to the small island nation. The appropriate portfolio allocation could both improve returns and increase diversity against speculative attacks, without significantly affecting the volatility of the reserve balance. The authors had recognized that digital currency could become a key currency for settling transactions and that it was necessary for central banks to evaluate their potential impact. The paper had revealed that the emerging worldwide recognition of bitcoin as a useful store of value among central bank authorities. Garay, Kiayias and Leonardos (2015) result was aligned with those from Eyal and Sirer (selfish mining) and in fact broadly generalized the underlying concepts.

Poon and Dryja (2016) had presented their invention: the Bitcoin Lightning Network, which was an extension of two-party payment channels applied in such a way as to permit instant transactions between any numbers of participants. Lightning transactions were normal bitcoin transactions, but except for rare cases were not actually posted to the Blockchain.

Brown (2016) explained that the bitcoin had become the currency of choice for cybercriminals. Its distinctive characteristics of decentralisation and pseudo-anonymity were also attractive to criminal actors in general, and yet Bitcoin had been assessed as representing only a low money laundering risk. In many respects, cryptocurrencies were still viewed as an unfamiliar, marginal phenomenon restricted to the purview of specialists. Bitcoin constituted a substantial danger in terms of criminal enterprise; and to promote the case for greater awareness among criminal justice professionals and law enforcement officers in particular. Dallyn (2017) had explored the libertarian political belief system that surrounds Bitcoin's status as a financial asset.

Section III

Cryptocurrency in Nepal

According to NRB Act, 2058, Foreign Exchange Act, 2019, with the notice dated 2074 Shrawan 29, Nepal Rastra Bank officially had declared the Bitcoin as an illegal financial mechanisms in Nepal taking strict measures such as arresting Bitcoin exchange operators. Bitsewa, Nepals Bitcoin and Blockchain Company was found with its inception in 13, October, 2016. E-Sewa had also worked for Bitcoin. Due to notice of NRB, the company had been shut now. The public, students, investors and other practitioners are not found aware and active in cryptocurrency bitcoin in Nepal.

Section IV

Research Methodology

The research paper is based on thematic review of existing literature. The descriptive and exploratory research designs have been adopted in the study. The purposive and convenience sampling method have been used in the study. The primary data has been collected from investors, investment company professionals, academicians, students, PhD and MPhil Scholars, and finance associates. The instrument used is interview method. The process of interview is self presence interview. The interview is based on self prepared primary questionnaire dealt with concept, practice and interest in cryptocurrency. The interview has been taken until the usable response become equal to male and female. The study is confined to 100 usable questionnaires. The recorded data are tabulated and analyzed using SPSS software. The measures of central tendency are the major statistical tools used in the study.

Section V

Results

SN	Questions/ Respondents	Response	Results
1.	Male Female	50% 50%	Equal
2.	Number of respondents	100	
3.	Do you have any idea on Cryptocurrency ? Male Female	 40% No 46% No	Majority of the respondents do not have an idea on cryptocurrency.
4.	Do you think cryptocurrency may have contribution in the economic development? Male Female	 45 % Yes 47% Yes	Respondents think that new emerging concept may help in boosting the economy. It is now known as an emerging concept in the world.
5.	Why government in Nepal does prohibit the use of cryptocurrency?	100 %	Respondents view it due to lack of system and mechanisms to use cryptocurrency. They revealed that it might lead to negative impact on developing economy.
6.	If you get an opportunity to learn about cryptocurrency, Will you participate and invest in cryptocurrency ? Male Female	 100 % Yes 100% Yes	Respondents are found active to learn and participate in cryptocurrency with proper system, knowledge, security in Nepal

Section VI

Conclusions and Discussions

Cryptocurrency is becoming popular in developing world but lacking behind in developing countries. The response view of male and female could not be distinguished in this paper. The generalizations of the results need validation from respective concerned personnel and the organizations. People do not have an idea on cryptocurrency even they heard about it. The finding from the primary analysis is consistent with the findings of Andriole (2017). The government had prohibited the use of cryptocurrency in Nepal. The reality is contradictory with the conclusion of Andriole (2017). Nepalese investors are not interested in the investment in cryptocurrency.

The findings are contradictory with Andriole (2017); Gao (2017); Kim, et,al. (2016); Noether,et,al.(2016); Viglione (2015); Stephan and Moore (2015); Eyal (2015); Garay, et,al.(2015). Whereas consistent with the findings from Brown (2016) and Heilman (2015). The thematic review explained about security problem in rendering the Bitcoin. It might be the major reason for prohibition for Bitcoin in Nepal. Brown (2016) concluded Bitcoin feature as change feature that may promote criminal activities. The problem with digital payment network is that customer had free will to double spend which mean that one could spend same amount twice. The study concluded that the use of Bitcoin and/or cryptocurrency might have impact on economic development. The research findings have opened the platform for the researchers to work on it. So that, it may provide the new insight and possibilities of Bitcoin in Nepal.

References

American Psychological Association. (2009). Publication manual of the American Psychological Association. Washington, USA: APA Service Center.

Andriole, S. (2017). Cryptocurrency is here and it's frightening. https://www.forbes.com/sites/steveandriole/2017/08/11/cryptocurrency-is-here-its-frightening.

Best, J.W., & Kahn, J.V. (1995). Research in education. Englewood Cliffs, USA: Prentice-Hall Incorporation.

Bonneau, et, al. (2015). Research perspectives and challenges for bitcoin and cryptocurrencies; Security and Privacy (SP), IEEE Symposium. doi: 10.1109/SP.2015.14.

Brown, S.D. (2016). Cryptocurrency and criminality. The Policy Journal, Vol.89 (4).

Creswell, J.W. (1998). Qualitative inquiry and research design: choosing among five traditions. London: Sage Publications.

Dallyn, S. (2017). Cryptocurrencies as market singularities: the strange case of bitcoin.

Journal of Cultural Economy, Vol-10(5), 462-473, http://dx.doi.org/10.1080/17530350.2017.1315541

Denzin, N.K., & Lincoln, Y.S. (2005). Qualitative research. India: Sage Publication.

Evans, W. (2015). Bitcoin in Islamic banking and finance. Journal of Islamic Banking and Finance, Vol. 3(1), 1-11,doi: 10.15640/jibf.v3n1a1 URL: http://dx.doi.org/10.15640/jibf.v3n1a1

Eyal, et, al. (2016). Bitcoin-NG: a scalable blockchain protocol. 13th Usinix Symposium.

Flyvbjerg, B. (2006). Five misunderstandings about case study research. Qualitative Inquiry, Vol. 12(2), 219-245.

Gao, K. (2017). The cryptocurrency funds have arrived, and they're bringing wall street money. Long only, ETF investing, commodities, tech.

Garay, et,al. (2015). The bitcoin backbone protocol: analysis and applications. doi: 10.1007/978-3-662-46803-6-10. Advances in Cryptology – EUROCRYPT, 281-310.

Heilman, et,al. (2015). Eclipse attacks on bitcoin's peer-to-peer network. 24th Usenix Security Symposioum, USA: Wasinghton.

Kim, et,al. (2016). Predicting fluctuations in cryptocurrency transactions based on user comments and replies. PLOS One Tenth Anniversary, https://doi.org/10.1371/journal.pone.0161197

Narayanan, et,al. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Boston University.doi:10.5195/LEDGER.2016.34

Poon, J., & Dryja, T. (2016). The Bitcoin lightning network: scalable off-chain instant payments.

DRAFT Version 0.5.9.2

Sekeran, U. (2003). Research methods for business. River Street, NJ: John Wiley & Sons.

Shaw, I., & Gould, N.(2001). Qualitative research in social work. Greater Kailash-I, India: Sage Publication.

Stake, R. (1995). The art of case research. Thousand Oaks, CA: Sage Publications.

Stephen, J.,& Moore, W. (2015). Should cryptocurrencies be included in the portfolio of international reserves held by the central bank of Barbados? Central Bank of Barbados.

Viglione, R. (2015). Does governance have a role in pricing? Cross-country evidence from bitcoin markets. University of South Carolina: Department of Finance.

Yin, R. (1994). Case study research: design and methods. Beverly Hills, CA: Sage Publishing.