

Cryptocurrency: The Emerging or Engulfing Currency

Astha Rai¹, Devendra Bhavsar², Yash Saraswat³

^{1,2,3}*Department of Computer Science Engineering, JK LakshmiPat University Jaipur Rajasthan, India*

Abstract- Recently, cryptocurrencies have become the utmost talked about topics in the financial industry. A cryptocurrency is a digital or virtual currency that uses cryptography for security. A cryptocurrency is difficult to trace because of its security feature. A defining feature of a cryptocurrency is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation. Cryptocurrencies have their benefits and drawbacks. The paper elaborates different aspects of cryptocurrencies, starting with their early development, challenges and risks, advantages and disadvantages, and their future dealing with issues related to the practical function of cryptocurrencies. It was concluded that it is not easy to predict the future of cryptocurrencies, since it is still developing. However, the banks and other financial institutions should see and consider cryptocurrencies as an alternative for the financial transactions in the future.

Keywords- cryptocurrencies, development, advantages disadvantages, financial transactions

I. INTRODUCTION

In a historical retrospective, markets have experienced a huge development and so have the exchange instruments aiming to make trade transactions as easy as possible. Money being the earliest is a unit of accounting providing a simple device for identifying and communicating value [4]. From the era of barter to metal and coins, to gold and silver, continuing by modern monetary systems and checks and ending with the latest global currency developments, such as introduction of cryptocurrencies known as bitcoin and Ethereum and alike, we have come along a long way. Each type of the money has played its indispensable role in transaction activities for the respective time period. However, with the emerging digital era there was a need for more sophisticated goods exchange instruments. In this regard the introduction of cryptocurrencies has revolutionized the international payment system to an unimaginable scale. A cryptocurrency is a digital or virtual currency that uses cryptography for security. Cryptocurrencies have their benefits and drawbacks. The main benefits of cryptocurrencies use are that they make it easier to transfer funds between two parties in a transaction; these transactions are facilitated through the use of public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks for internet online based transactions. The threat of hacking is the biggest threat of cryptocurrency system of payments [1]. For example, In Bitcoins short history, the company has been subject to over 40 thefts. However, despite the potential risks, still, many observers look at cryptocurrencies as a revolutionary tool in the modern world. There are approximately 856 and still counting cryptocurrencies. In regard of market capitalization Bitcoin is the leader in the long list of crypto currencies, followed by Ethereum and Ripple.

II. EVOLUTION AND MAJOR CONTRIBUTIONS

Historically, cryptography was mainly used by military, secret services and other intelligence agencies as a protection from the information leakage. An emerging belief is that an autonomous decentralized digital currency is appealing because of the anonymity and liberty that it affords. Transfer of money across geographic regions be it domestic and international can be quickly accomplished without worrying about governmental regulations.[3] A major development that contributed in cryptocurrency creation is the Cypherpunk movement that “formally” emerged in the early 1990s. The Cypherpunk movement is an activist movement whose participants seek to engineer social and political change and enhanced security and privacy through cryptographic techniques. The founders of the Cypherpunk group were Eric Hughes, a UC Berkeley mathematician, Timothy C. May, a former chief scientist at Intel, and John Gilmore, an employee at Sun Microsystems and founder of Cygnus Support as well as the Electronic Frontier Foundation. All three were wealthy and shared a strong libertarian streak. Another major contributor to creation of cryptocurrency is David Chaum, a cryptologist who got his doctoral degree from the University of California Berkeley. As a doctoral student in the 1980s,[2] Chaum explored several concepts and developed several methods focusing on anonymous communication and anonymous financial transactions. In 1981 Chaum published the article “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms” which described a method, using public key cryptography, to hide the identity of a participant in an email communication,

as well as the contents themselves. He explained one of its uses in elections where an examiner could verify that all the votes have been correctly counted without revealing the identity of the voters[1]. A huge contribution of Chaum in this field is creation of a digital currency based on cryptography that he called E-Cash, and in 1990 founded a company called Digi-Cash, an electronic money corporation. The world's first electronic cash payment took place in May 1, 1994. However, most attempts at creating a workable cryptocurrency have failed to gain consumer acceptance[4], until bitcoin was introduced in January 2009 when Satoshi Nakamoto who is believed to use this name as a pseudonym mined the first block of bitcoins, known as the genesis block, gaining a reward of 50 bitcoins.

III. THE TRAILING FUTURE

There are different and confronting opinions regarding the future of cryptocurrencies in general and bitcoins in particular. While, those with libertarian views of life are optimistic and embrace the cryptocurrency system, other authors, economists, and scholars from this field are not enthusiastic about the use of cryptocurrency in the system of payments and financial transactions. The optimistic view of cryptocurrencies use is backed by the fact that they make it easier to transfer funds between two parties in a transaction; these transactions are facilitated through the use of public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks. In addition, many countries have started to accept bitcoin as a valid currency. Especially, countries that aim to get rid of cash have a very friendly approach to cryptocurrencies. An argument that promoters of bitcoin use is Market capitalization of bitcoin, Ethereum and other cryptocurrencies, claiming that cryptocurrency market has become very large and powerful, so banning it would be too costly for any country.

On the other side some claim that cryptocurrencies are very volatile, can be used for money laundry or financing illegal activities.

3.1 Advantages

Payments made in this system are impossible to cancel. The coins cannot be faked, copied or spent twice. These capabilities guarantee the integrity of the entire system.

Decentralization: There is no central control authority in the network; the network is distributed to all participants. And even if some part of the network goes offline, the payment system will continue to operate stable.

Anonymity: It is completely anonymous and at the same time fully transparent as the information of transaction and owner is stored on separate block chains.

Speed of transaction: The ability to send money anywhere and to anyone in a matter of minutes after the associated network processes the payment.

No chances of fraud: These transactions do not require disclosure of any personal data. Instead, it uses two keys: public and private. The public one is available to all but the private key is known only to the owner. The transaction needs to be signed by interacting private keys and applying a mathematical function. This creates evidence that the transaction is performed by the owner.

3.2 Disadvantages

Strong volatility: almost all of the ups and downs of their value depend directly on the declared statements of the governments of different countries. This volatility creates the problem in the short term.

Large risks of investing in cryptocurrency that should be considered in the medium and long term.

Lack of understanding the concept of cryptocurrency since not a many are aware of it and don't even know the existence of such term.

Under development: since it is still developing, it is prone to many risks and especially because it has no physical form it is a bit difficult to improve its existing features.

IV. CONCLUSION

The paper aimed to provide a basic analysis of cryptocurrency. It is found that the future of cryptocurrencies could be bright if some conditions are fulfilled. Bitcoin and other cryptocurrencies have the potential to replace traditional and new payment methods. But to achieve that and become a dominant power in system of payments, they must overcome a number of critical challenges. That is unlikely to happen in the short time period but where there is a will there is a way and time anyway flies.

V. REFERENCES

- [1] Ivaschenko, A.I. (2016). Using Cryptocurrency in the Activities of Ukrainian Small and Medium Enterprises to Improve their Investment Attractiveness. *Problems of economy*, (3), p. 267-273.
- [2] Tymoigne (2015). Do Cryptocurrencies Such as Bitcoin Have a Future? No: As a Currency, Bitcoin Violates All The Rules of Finance. *Wall street journal – Eastern edition*, 265(49), p. 1-2.
- [3] Cryptocurrencies: A Brief Thematic Review Archived 2017-12-25 at the Wayback Machine.. *Economics of Networks Journal*. Social Science Research Network (SSRN).
- [4] Greenberg, Andy (2012). *This Machine Kills Secrets: How WikiLeaks, Cypherpunks, and Hacktivists Aim to Free the World's Information*.