International Academic Institute for Science and Technology

International Academic Journal of Business Management
Vol. 6, No. 1, 2019, pp. 32-37.

ISSN 2454-2768

International Academic Journal of Business Management

Bitcoin: The Future Investment

Manoj V. Thomas [a], Ashitha Babu P.[b]

[a] *Dept. of Computer Science and Engineering, Vimal Jyothi Engineering College, Chemperi, Kannur*.

[b] *Dept. of Computer Science and Engineering, Vimal Jyothi Engineering College, Chemperi, Kannur.*

Abstract

In this paper, we discuss the Bitcoin, the leader among the existing cryptocurrencies including its trends, success factors, current challenges and possible scope of investing in the Bitcoin market. In this paper, the evolution of Bitcoin including its working mechanism is discussed. We also analyse the unique features of Bitcoin and how they lead other cryptocurrencies. The trends in investing Bitcoin market is explained. Also, the success factors and the current challenges faced by Bitcoin and how they overcome to lead the present market are presented.

Keywords: Bitcoin, Blockchain, Cryptocurrencies, Digital Currencies, Survey, Investment

DOI: 10.9756/IAJBM/V6I1/1910004
Received:24 January 2019/Accepted:18 April 2019/Published:18 June 2019

I. INTRODUCTION

The advancement in technology is amazing us in every sector. Also, the change from paper cash to electronic cash is not a one day process. Among the available digital cash, cryptocurrencies are the leading virtual money provider. They are distinct in their every behavior with an identity. They have separate encryption and decryption mechanism which are similar to lock and unlock mechanism. At the time of writing this report, there are about 1,658 cryptocurrencies over the world. It may be seen that a new cryptocurrency can be created at any time. By market capitalization [6], it is clear that Bitcoin is currently the largest blockchain network, followed by others which are Ethereum, Ripple, Bitcoin Cash, Litecoin, and EOS. The rest of the paper is organized as follows. Section II talks about the evolution of bitcoin, and section III discusses how the bitcoin works. Section IV explains the unique features of the crypto-currency and section V details the success factors. Section VI details the current challenges and finally, section VII concludes the paper.

II. EVOLUTION OF BITCOIN

Satoshi Nakamoto created Bitcoin and was in the year 2009 [1]. The decentralized currency Bitcoin was designed to be intended to eliminate the "middleman" from financial transactions. Here payments with no transaction fees and no need to exchange any personal information are main attraction and are sent peer-to-peer from the payee to the recipient [4]. The currency is completely virtual and is not controlled by any central authority. Mining is the process through which new Bitcoins are created. Mining requires computing equipment solving complex mathematical problems, and the reward is a newly created block of Bitcoins. The readily available software programs also allow users to either mine for Bitcoins on their own or join which essentially allow participants to combine the power of their mining hardware and then share any blocks of coins that they receive [2].

III. HOW THE BITCOIN SYSTEM WORKS

A global, distributed cryptographic ledger of transactions, or blockchain, through a consensus algorithm running on hardware scattered across the world is maintained by the Bitcoin system [1][8]. A computationally intense proof-of-work function called mining, which integrates BTC transactions into the blockchain is performed by the system. Each transaction debits a sender's account and is credited in the receiver's account which is aggregated with other pending transactions into a block by a single machine and posted to the blockchain's head. The hash of the previous head block is contained in every block, creating a total order. Upon receiving notice of a block's posting, other nodes in the system will verify that the transaction is in order—for instance, not improperly creating, moving, or destroying BTCs— and then use the new block as the head block for future blockchain updates.
The proof-of-work is shown in the figure.1 [1]

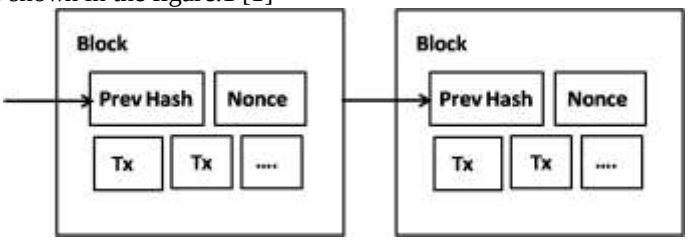


Figure 1. Proof-of-work

The transactions hashed in a Merkle Tree is shown in the Figure.2 [1][5]

DOI: 10.9756/IAJBM/V6I1/1910004
Received:24 January 2019/Accepted:18 April 2019/Published:18 June 2019

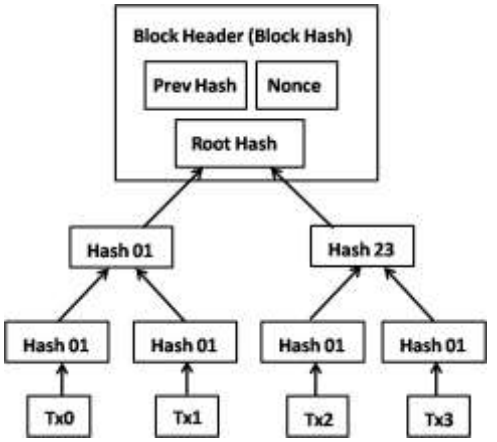


Figure 2. Transactions Hashed in a Merkle Tree

IV. WHAT MAKES BITCOIN UNIQUE

Bitcoin is different from other currencies in numerous ways, the first and important is they have no central authority, unlike other currencies which are backed by the government. They can subject to inflation due to scarcity caused by an artificial limit. Country backed currencies are subject to deflation as well. The transactions are registered in the Bitcoin blockchain [1]. This acts as a ledger, whereas cash transactions may or may not be recorded. Here the transactions are immutable**,** whereas the majority of digital records can be duplicated. But transaction requires fees to be paid to miners. This is quite similar to taxes we pay the government, except taxes can be evaded quite easily compared to having a transaction registered in the blockchain without paying fees. Bitcoin transactions are made over the internet and are public, which includes Bitcoin addresses being known, whereas cash transactions are pretty much anonymous and do not leave behind a trail. Bitcoin is also known as the internet's currency because it is resident on the internet with scores of people (miners) keeping track of each transaction happening by recording it within the Blockchain.

4.1 A look into recent Bitoin crashes [3]

Bitcoin has spectacularly 'died' several times :
94% June-November 2011 from $32 to $2 because of MtGox hack
36% June 2012 from $7 to $4 Linod hack
79% April 2013 from $266 to $54. MTGox stopped trading
Dec 2013 to March 2015 from $1300 to $180
87% from $1166 to $170 November 2013 to January 2015
49% Feb 2014 MTGox tanks
40% September 2017 from $5000 to $2972 China ban
55% January 2018 Bitcoin ban FUD. from $19000 to 8500

4.2 Bitcoin rise reasons

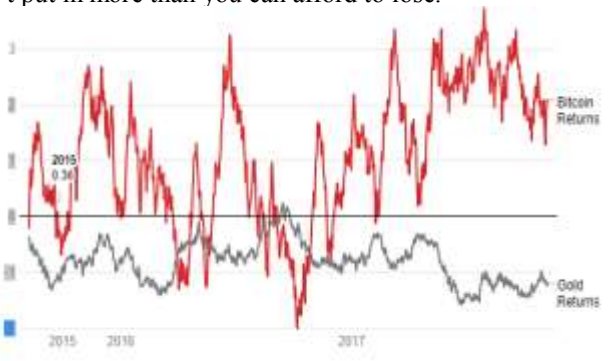
Animal Spirit which refers to investors making decisions based on the behaviour of other market participants and their own intuitions, rather than hard analysis.
Political risk around national currencies can also affect the price of Bitcoin as people use it to hedge against price movements in a particular currency, or they need to quickly move large amounts of value out a country or currency.
Regulators around the world have had to catch up to the rise of Bitcoin. They must decide, for instance, how it will be treated by the tax system, or whether and what regulation applies to its use.

DOI: 10.9756/IAJBM/V6I1/1910004
Received:24 January 2019/Accepted:18 April 2019/Published:18 June 2019

Bitcoin's governance, although Bitcoin is a decentralized currency, some decisions about how it will work or evolve need to be made from time to time. These also have an impact on the price.

4.3 Investment in Bitcoin Market [3]

Bitcoin can also be a long-term investment due to it being unregulated in supply and having some huge benefits over some national currencies: it is global, untied to supply of currencies by central banks, easily transferable across borders, and doesn't suffer from the considerable transaction and administration costs paid to banks, currency markets and financial traders. Being a relative new market, however, with no mathematical mechanism to predict how it will act in the future, it really it is a case of buyer beware. Our only tip would be – don't put in more than you can afford to lose.



Comparing the return for Bitcoin to the return from gold

I. The volatility of gold and Bitcoin

V. SUCCESS FACTORS OF BITCOIN

From the previous section we clearly see that Bitcoin with the unsaid advantage of being the oldest digital currency deployed, being the global market winner. In this section we analyze some of the factors that influenced the success of the Bitcoin [1]

- *No need for trusted third party(Bank) or central point*: Bitcoin system does not need a bank or central authority to keep track of the transaction ledger, instead it relies on the trusted peer-to-peer network to do the same. Everyone in the network keeps a copy of the public ledger and this ledger is updated every 10 minutes on an average. Bitcoins system depends on a voting mechanism (for the next block to be on the top of the stack) from the peer-to-peer network users to avoid double-spending and resolve disputes.
- *Incentives for participation*: Every Bitcoin user gets the Bitcoin which he successfully mines and adds to the public block-chain by exploiting his computer resource to solve the cryptographic puzzle. Miners receive the optional transaction fee which is very low at the moment. Unlike any other hard currency resource such as gold, Bitcoin mining cannot be done once there are 21 Million Bitcoins in the global network.
- *Bitcoin money supply which is predictable*: As the number of Bitcoin users increases, the difficulty of computational puzzle that they have to solve for the mining of Bitcoin increases. This ensures that the new coins are mined at a fixed rate with the growth of Bitcoin users. Hence early miners have an unstated advantage of mining the coins easily.
- *Open Source code and Easily implementable modules*: Bitcoin is launched as an open source project which increased its flexibility with the users from various backgrounds. Because of its open source nature, more people indulged themselves to test, attest and participate in the Bitcoin community by creating various readily available implementation modules or applications for desktop and mobile computers.

DOI: 10.9756/IAJBM/V6I1/1910004
Received:24 January 2019/Accepted:18 April 2019/Published:18 June 2019

- *Irreversibility of transactions*: Once the Bitcoin block is added to the block-chain, the transaction becomes irreversible. This is preferable for vendors who are hesitant to make business because of credit card fraud scams and charge backs. This feature helps many vendors to extend their business without the hesitation of usual monitory scams in the digital world. Linking the previous transactions in the Bitcoin system is inevitable which makes it resistant to double-spending without harming the anonymity of the end customer.
- *Low fees of transaction*: At the moment there is an optional transaction fee for verifying the Bitcoin blocks through voting. But its optional and chosen by the payer. But after certain point the transaction fees will be as profitable as the mining once the number of Bitcoins in circulation is reaching its upper limit.

VI. CURRENT CHALLENGES

Some of the challenges are [9]:

- *No intrinsic value*: Since there are no intrinsic value a number of people are dissatisfied. Also Bitcoin's price are highly depending on the demand and the buyer's willingness to pay.
- *Taxation and legal challenges for regulators:* It presents a whole new system of unexpected opportunities and challenges. The current regulatory state is uncertain, with various governments taking stands towards Bitcoin.
- *It has created huge hardware competition:* The procedure of verifying and authentication transactions has been greatly criticized for creating an artificial hardware competition and for consuming such huge amounts of energy to maintain its network.
- *Economic effects:* There has been a lot of great concern about the various economic effects when Bitcoin reaches its final supply and also the detrimental effect of it ending in inflation
- *Slow transactions:* A 10 minute confirmation is very cumbersome and clumsy for merchants who are in need of quick transactions.
- *Long-term security of its hashing algorithm:* Some experts are apprehensive about the long-term implications of the hashing algorithm.
- *No mechanism to recover stolen or lost Bitcoins:* With Bitcoin, it you lose it you lost it. There is no mechanism to recover stolen or lost Bitcoin.
- *It's not user friendly for users who are technologically challenged:* A lot of people struggle with fact Bitcoin is not a currency that you can hold in your hands and neither it comes from the bank or the government.

VII. CONCLUSION

The concept of Bitcoins has revolutionized the whole technology and financial world. Analyzing the current market trends in the digital currency world revealed that Bitcoin is the winner among all existing and newly forking digital currencies [7]. The success attained by Bitcoin on various factors makes it as the market leader among the digital currencies. Currently bitcoin is capable of handling a maximum of around 3.5 transactions every second which are published to the blockchain roughly every 10 minutes. Bitcoin will be capable of handling more transactions than Paypal (assuming Paypal experiences growth of around 7% per year) in the year 2027. Bitcoin will overtake VISA's transaction capability by the year 2035 and at the end of the growth cycle in 2039 it will be able to handle close to 50% of the total global non-cash transactions. Assuming that when solutions to current challenges are implemented successfully, it gives a positive hope about Bitcoin revolution to be continuing for a long run, providing economical benefits like future investment preserving the privacy of people around the globe without depending on any government or third party authorities.

DOI: 10.9756/IAJBM/V6I1/1910004
Received:24 January 2019/Accepted:18 April 2019/Published:18 June 2019

REFERENCES

[1] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash systems: https://bitcoin.org/bitcoin.pdf
[2] "Turning Bitcoin into Best coins" - Siddharth Rao https://arxiv.org/ftp/arxiv/papers/1412/1412.7424.pdf
[3] "Complete List of Digital Currency Exchanges from Around the World" http://planetbtc.com/complete-list-of-bitcoin-exchanges/
[4] Tatsuaki Okamoto and Kazuo Ohta. Universal Electronic Cash. In: Proc. of Advances in Cryptology - CRYPTO' 91, pp. 324-337, LNCS 576, Springer-Verlag, 1991.
[5] Bruce Schneier. Applied Cryptography, Protocols, Algorithms, and Source Code in C, Section 6.1: Digital Cash. John Wiley & Sons, Inc, 1993.
[6] Cryptocurrency Market Capitalizations based on available supply http://coinmarketcap.com/#USD
[7] Bitcoin Competitors: What You Should Know About 6 Alternative Cryptocurrencies http://www.ibtimes.com/bitcoin-competitors-what-you-should-know-about-6-alternative-cryptocurrencies-15 40168
[8] Scripting in Bitcoin systems : https://en.bitcoin.it/wiki/Script
[9] Bitcoin Problems: Full Analysis https://www.abitgreedy.com/bitcoin-problems

DOI: 10.9756/IAJBM/V6I1/1910004
Received:24 January 2019/Accepted:18 April 2019/Published:18 June 2019