Cryptocurrencies: A Comparative Study

Amey Mahajan
1601DMTCS00840
SVVV, Indore
iameymahajan5@gmail.com

Abhishek Jain
1601DMTCS00834
SVVV, Indore
abhijain451@gmail.com

Shruti Sharma
16010BTCC00316
SVVV, Indore
shrutisharma1827@gmail.com

ABSTRACT:

The world of cryptographic money is becoming popular day by day. A cryptocurrency is a virtual currency that uses cryptography for security. It operates without a single administration hence it is a decentralized currency. The transaction of cryptographic currency takes place directly users and intermediates. The prices of bitcoins are volatile i.e. they can unpredictably increase or decrease over a period of time. Bitcoins are considered high-risk assets whose transactions can only be refunded and not reversed. Countries across the world has started accepting cryptocurrency as a legitimate way of currency. However, India hasn't legalized cryptocurrency. The prices of cryptocurrency are volatile i.e. they can unpredictably increase or decrease over a period of time. Cryptographic money is considered high-risk assets whose transactions can only be refunded and not reversed. The objective of this paper is the comparative study between bitcoin, Litecoin.

BITCOIN:

Bitcoin is one of the most prominent cryptocurrency, which hit the news headlines in between 2018 as the price of one unit of the cryptocurrency passed $11,500 for the first time. It h is a subset of what is generally known as a digital currency. Bitcoin is a unique cryptocurrency that is widely considered to be the first of its kind. Like many created after it, Bitcoin uses the power of the Internet to process its transactions. Satoshi Nakamoto published a paper on the Web in 2008 for a peer-to-peer electronic cash system. Despite many efforts, the identity of Satoshi remains unknown to the public and it is not known whether Satoshi is a group or a person. The cryptocurrency invented by Satoshi Nakamoto, called bitcoins, is run using open-source software. It can be downloaded by anyone, and the system runs on a decentralized peer-to-peer network. It is not only decentralized but also supposedly fully distributed. That means that every node or computer terminal is connected to each other. Every node can leave and rejoin the network at will and will later accept the longest proof of work known as the blockchain as the authoritative record.

GENERAL FEATURES OF BITCOIN

➢ **Network and digital currency**

Bitcoin is a decentralized network and a digital currency that uses a peer-to-peer system to verify and process transactions. Instead of relying on trusted third parties, like banks and card processors, to process payments, the Bitcoin technology uses cryptographic proof in its computer software to process transactions and to verify the legitimacy of Bitcoins (Nakamoto, 2008) and spreads the processing work among the network. We make a clear distinction between the Bitcoin system where a capital B is used for the word Bitcoin and that of a Bitcoin, which is a unit of the currency or a digital address created by the Bitcoin system. With the invention of Bitcoin, payments can be made over the Internet without the control and costs of a central authority (Bitcoin Project) for the first time.

- **Genesis and decentralized control**

The first bitcoin was mined, or created, in 2009, following the online publication of a paper by a Satoshi Nakamoto describing the proof of concept for a currency that uses cryptography, rather than trust in a central authority (Nakamoto, 2008), to manage its creation and transactions. Nakamoto left the project in 2010 and his identity largely remains unknown. However, with the open-source nature of the Bitcoin software protocol, other developers have continued working on it and the Bitcoin community flourishes today.

- **How Bitcoin works**

To a layperson, bitcoin is a digital currency that is created and held electronically. These bitcoins are sent and received using a mobile app, computer software, or service provider that provides a bitcoin wallet. The wallet generates an address, akin to a bank account number, except that a Bitcoin address is a unique alphanumeric sequence of characters where the user can start to receive payments. Usually, bitcoins may be obtained by buying them at a Bitcoin exchange or vending machine or as payment for goods and services. However, Bitcoin is revolutionary because the double-spending problem can be solved without needing a third party.

- **Buying and storing bitcoins**

Against this technical backdrop, bitcoins are often used simply as payment in exchange for goods and services (Kaplanov, 2012). While the numbers of brick-and-mortar merchants who accept payments in bitcoins remain low, there are many more online merchants who accept bitcoins for both digital and physical goods and services. The price of these goods and services is usually based on the exchange rate between Bitcoin and a real-world currency, which can be found easily online.

- **Mining to create new bitcoins and process transactions**

Bitcoin is designed with a hard limit of 21 million bitcoins, which are expected to be created by 2040 for now, these bitcoins are generated through mining, during which miners, who are Bitcoin users running software on specialized hardware, process transactions and are rewarded with new bitcoins for contributing their computer power to maintain the network. Mining is important not only for new bitcoins to be issued but also because it is a necessary process for transactions to be added onto the blockchain and be subsequently confirmed. The verification process is a computationally intensive process that ensures that only legitimate transactions are verified and recorded onto the blockchain. It is the network that provides the computing power for the transactions to take place and for the transactions to be recorded.

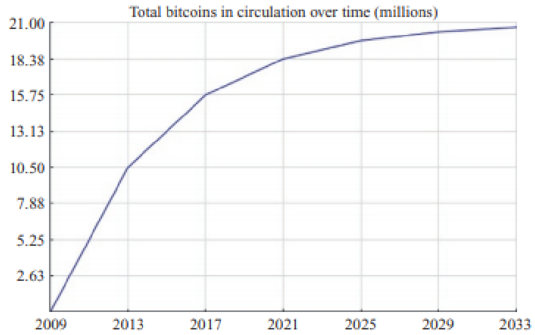


Fig 1: Bitcoin Supply

- **Security and cryptography**

The security of the technology used is supported using secure hash algorithms and has a good track record. The Bitcoin protocol is an open-source and is continuously improved by the developer community subject to consensus among all network users. The hash 20 Handbook of Digital Currency function mainly used in Bitcoin is SHA-256 (Pacia, 2013), which was incidentally originally designed by the NSA in the United States. There is no need for suspicion against the NSA because the SHA algorithm is part of the public domain and has been extensively analyzedto be secure (Pacia, 2013). SHA-256 is an upgrade from the SHA-1 series and is presently used in Bitcoin for the digital signatures that secure the transactions and blockchain and it forms the basis of the proof-of-work mathematical problem.

Central to Bitcoin technology is public-key cryptography, which with the SHA-25 hash function is used to generate Bitcoin addresses, sign transactions, and verify payments. Public-key cryptography is a technique of reliably determining the authenticity of Bitcoin transactions using digital signatures. It uses an asymmetrical algorithm that generates two separate but asymmetrically linked keys: a public key and a private key.

- **Pseudoanonymity**

A Bitcoin address is an alphanumeric sequence of characters. There is no other information that can identify the sender and recipient of the bitcoins. However, it is a common misconception to say that bitcoin is an anonymous currency. This misconception often arises from a lack of understanding of the technology.

BENEFITS AND RISKS

Bitcoin as a novel technology brings a range of benefits and risks to the table. This section outlines some of the most well-known benefits and risks.

- **Freedom of payments**

Bitcoin was specifically designed for fast transactions at low costs (Nakamoto, 2008). Payments can be processed with little or no fees, with the sender having the option to include 22 Handbook of Digital Currency a transaction fee for faster confirmations. A low transaction cost is possible because there is no single third-party intermediary. In addition to the lack of restrictions on transactions, users have full control of their bitcoins and the freedom to send and receive bitcoins anytime, anywhere, and to and from anyone.

- **Merchant benefits**

Bitcoin presents an alternative to the other methods of electronic payments accepted by businesses. Traditional credit card acceptance is expensive for merchants, with customers often having to pay for a merchant account and various fees for transactions, including but not limited to transaction fees, interchange fees, and statement fees. These fees add up and increase the costs of accepting credit cards for payments. Yet, merchants who forgo credit card payments may lose business from customers used to the ease of paying with credit cards. Not having to pay these expensive fees may allow businesses to pass on the cost savings to consumers, benefiting everyone.

- **User control**

Each Bitcoin transaction can only be effected by the user who has the private key, putting the user in full control of his bitcoins. Merchants cannot slip in unwanted charges later, unlike credit cards that offer limited protection against such charges once an unethical merchant has the card details. Transactions also do not contain substantial personal information, which is at risk of leakage and theft. However, the converse effect of full user control is the point that the private key controls the access to one's bitcoins. Bitcoin, being a digital currency, brings specific security challenges. Perhaps the most important risk to end users is that if the private key is lost, access to the bitcoins is irrecoverable. Poor wallet protection may leave users vulnerable to thefts, especially by specially crafted malicious software designed to steal bitcoins. Bitcoin users should therefore be security conscious with Bitcoin, just as they do for other financial activities.

- **Platform for further innovation**

The Bitcoin protocol may, in its original form, work as a payment network, but it has the potential for further innovation. What actually happens in the Bitcoin network is that data in the form of Bitcoin transactions are broadcasted and verified before being kept on the blockchain. Bitcoin technology may therefore be adapted for the transfer of other types of data, like stocks or bets. Feature layers are beginning to be built on top of Bitcoin, which include smart property and assurance contracts. Being an open-source technology, alternative digital currencies like Litecoin and Dogecoin, among others, have also emerged to suit different objectives.

- **Economic risk**

Bitcoin is something that is very different from the existing financial system for which country regulators have experience regulating. The innovative use of Bitcoin may be disruptive to the financial and payment markets in that Bitcoin, for example, can scale up to replace money transmission and card payment services, or even stock exchanges, which renders the incumbent service providers obsolete. If these changes occur rapidly, there is a risk that this will destabilize the financial and payment markets and ultimately price stability in a market.

LITECOIN:

Litecoin was created in late 2011 as a fork of Bitcoin, by then Google employee Charlie Lee. Litecoin is treated as a leading rival for Bitcoin currently and the main purpose of designing Litecoin was to process smaller value transactions fast. The difference between Bitcoin and Litecoin is that for mining Bitcoin heavy processing and fast computing is required unlike, Litecoin which can be mined by a normal desktop computer with comparatively lesser processing power. About 84 million Litecoin are there in circulation in comparison with 21 million Bitcoins and Litecoin transaction processing time is about 2.5 minutes compared to about 10 minutes for that of Bitcoin.

How does Litecoin work?

Vision

Litecoin was created by ex-Google engineer Charlie Lee in 2011 with the intent to improve the speed of transactions handled by a blockchain. He launched litecoin using code that was very similar to bitcoin, save for a few key differences that aimed to solve the transaction speed and scalability of bitcoin.

The main differences are that Litecoin will have a maximum of 84 million coins, as opposed to bitcoin's 21 million, and that it incorporates Scrypt proof-of-work mining algorithm, as opposed to bitcoin's SHA-256. The goal was for people to be able to use computer-grade hardware to mine Litecoin and thus making mining more democratic. Lee engineered Litecoin to complement to bitcoin as a means of payment.

Network Design & Security Model

Litecoin, similar to bitcoin uses a proof-of-work algorithm, rewarding the miners for processing each block. While bitcoin uses the SHA-256 mining algorithm, Litecoin uses Scrypt, an algorithm that allows users to make it possible for the average consumer to mine the coin using consumer grade hardware, as opposed to the specialized mining hardware that bitcoin utilizes. In May 2017, Litecoin conducted a “soft fork” to enable segregated witness (SegWit), a change which allowed a greater number of transactions per block to be created. This was done by putting less weight on each transaction via removing the signature information. This was done to solve the long-term scaling debate that originally started with bitcoin and trickled down to Litecoin.

Transaction Processing

The average time for Litecoin to produce a block is 2.5 minutes compared to bitcoin’s 10-minute block time. The transactions for Litecoin, similarly to bitcoin, are all produced on-chain.

Coding

Litecoin was written in C++ and was based on the bitcoin protocol. Litecoin was created and is used as an open source, peer-to-peer digital currency.

Ethereum (ETH)

Propelled in 2015, Ethereum is a decentralized programming stage that empowers Smart Contracts and Distributed Applications (ĐApps) to be assembled and kept running with no downtime, misrepresentation, control or impedance from an outsider. During2014, Ethereum had propelled a pre-deal for ether which had gotten a staggering reaction. The applications on Ethereum are kept running on its stage particular cryptographic token, ether. Ether resembles a vehicle for moving around on the Ethereum stage, and is looked for by for the most part designers hoping to create and run applications inside Ethereum. As indicated by Ethereum, it can be utilized to "classify, decentralize, secure and exchange pretty much anything." Following the assault on the DAO in 2016, Ethereum was part into Ethereum (ETH) and Ethereum Classic (ETC). Ethereum (ETH) has a market capitalization of $41.4 billion, second after Bitcoin among all cryptographic forms of money.

Ether

Ether is a fundamental token for operation of Ethereum, which thereby provides a public distributed ledger for transactions. It is used to pay for gas, a unit of computation used in transactions and other state transitions. Mistakenly, this currency is also referred to as Ethereum.

Supply

The total supply of ether was around Ξ106.7 million as of July 5, 2019. In 2017, mining generated 9.2 million new ether, corresponding to a 10% increase in its total supply. Casper FFG and CBC are expected to reduce the inflation rate to between 0.5% to 2%.· There is no currently implemented hard cap on the total supply of ETH.

Performance

In Ethereum all smart contracts are stored publicly on every node of the blockchain, which has costs. Being a blockchain means it is secure by design and is an example of a distributed computing system with high Byzantine fault tolerance. The downside is that performance issues arise in that every node is calculating all the smart contracts in real time, resulting in lower speeds. As of January 2016, the Ethereum protocol could process about 25 transactions per second. In comparison, the Visa payment platform processes 45,000 payments per second leading some to question the scalability of Ethereum. On 19 December 2016, Ethereum exceeded one million transactions in a single day for the first time.

Ethereum engineers have been working on sharding the calculations, and the next step (called Ethereum 2) was presented at Ethereum's Devcon 3 in November 2017. Ethereum's blockchain uses Merkle trees, for security reasons, to improve scalability, and to optimize transaction hashing.As with any Merkle tree implementation, it allows for storage savings, set membership proofs (called "Merkle proofs"), and light client synchronization.

Comparative Study

Objective

To study the performance of different cryptocurrencies mainly Bitcoin, Ethereum and Litecoin.

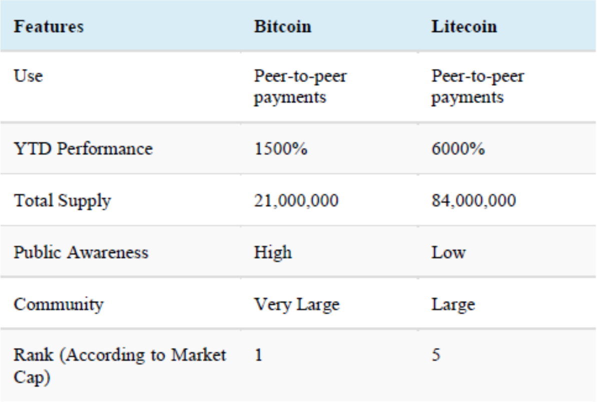
Methodology

The closing prices for major cryptocurrencies Bitcoin, Ethereum and Litecoin were compared for December 2017 and January 2018 as this was the time when the volatility of crypto-currencies was very high. The secondary data collected for the analysis purpose was selected from Coin desk website. It was seen from the chart that there is a highest volatility of Bitcoin and the prices for the Bitcoins show a declining trend but at the same time Ethereum and Litecoin comparatively showing increasing trend as they are newly introduced coins into the market.

Bitcoin Vs Litecoin (Ltc)

At the point when Litecoin first propelled in 2011, it was said that "if bitcoin is advanced gold, at that point litecoin is computerized silver". For quite a while, that was the situation. Litecoin immediately rose as the second biggest computerized money after bitcoin, as estimated by showcase capitalization. The altcoin even encountered a level of shipper reception in its initial years. Its notoriety blurred to some degree as the Ethereum task and its local advanced cash, ether, turned into the second biggest computerized money in 2016. In any case, when it was reported in mid 2017 that litecoin would embrace the purported "SegWit" overhaul for its blockchain, which addresses blockchain scaling issues, the cost of litecoin shot up from its 2-year exchanging scope of $3 to $5 to achieve another untouched high of over $366 on December 19, 2017.

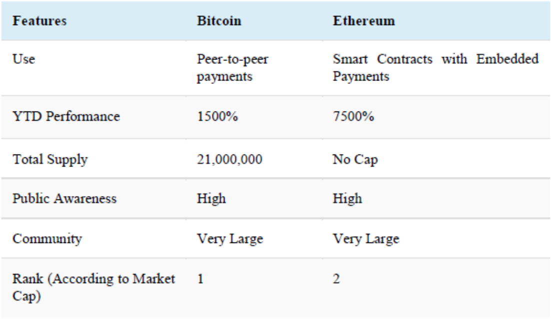
Litecoin has turned into an extremely prominent advanced money since it has every one of the advantages of bitcoin however has quicker exchange times and lower exchange expenses. This is the reason numerous computerized cash specialists trust it can possibly challenge bitcoin as the go-to advanced money without bounds. This conviction is shared by numerous advanced cash speculators, which may clarify why the cost of litecoin has revived by more than 6000 percent year-to-date. On the off chance that you trust that worldwide selection of litecoin (LTC) will surge since its exchanges are quicker and less expensive than bitcoin, at that point adding litecoin presentation to your portfolio could be the correct move



Features	Bitcoin	Litecoin
Use	Peer-to-peer payments	Peer-to-peer payments
YTD Performance	1500%	6000%
Total Supply	21,000,000	84,000,000
Public Awareness	High	Low
Community	Very Large	Large
Rank (According to Market Cap)	1	5

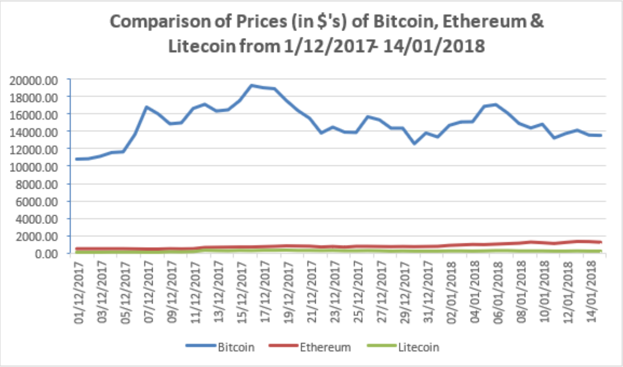
Bitcoin Vs Ethereum (Eth)

Ethereum's ether is the second greatest advanced money in the market with a market capitalization of over $75 billion. Ether is the advanced cash of the Ethereumblockchain, which is an open source blockchain stage that considers the formation of alleged "savvy contracts". Keen contracts are PC conventions that make computerized contracts which are expected to encourage, check, and authorize legally binding understandings between two gatherings.



Features	Bitcoin	Ethereum
Use	Peer-to-peer payments	Smart Contracts with Embedded Payments
YTD Performance	1500%	7500%
Total Supply	21,000,000	No Cap
Public Awareness	High	High
Community	Very Large	Very Large
Rank (According to Market Cap)	1	2

The Ethereumblockchain has accumulated significant enthusiasm from money related establishments and enterprises that trust that the capacity to safely store and exchange information utilizing blockchain innovation joined with self-executing keen contracts will diminish operational expenses and streamline business forms later on.



References

[1]. https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

[2]. https://www.bitcoinmarketjournal.com/bitcoin-vs/

[3]. Young, J. (2018, January 26). How Chinese Bitcoin Buyers Are Getting Around Government Ban. Retrieved from https://cointelegraph.com/news/how-chinese-bitcoin-buyers-are-getting-around-government-ban#

[4]. Jankinson, G. (2018, Jan 26). Twitter Reacts to Crypto Fear-Mongering at Davos WEF. Retrieved from https://cointelegraph.com/news/twitter-reacts-to-crypto-fear-mongering-at-davos-wef

[5]. Budget 2018: Bitcoins, crypto-currencies illegal, but govt to explore Blockchain. (2018, February 01).