International Journal of Research in Economics and Social Sciences (IJRESS)
Available online at: http://euroasiapub.org
Vol. 7 Issue 8, August- 2017, pp. 51~61
ISSN(o): 2249-7382 | Impact Factor: 6.939

CRYPTOCURRENCY

Saving Privacy in Digital Age

(Special Reference to Thane Region)

Ruchi Nityanand Prabhu
MMS (Finance)
Dr. VN Bedekar Institute of Management Studies, Thane
Mumbai University
Email Id: ruchi.prabhu18@gmail.com

Do Not Invest; If You Can't Afford to Lose

Abstract: *The world of money and finance is transforming before our eyes. Digitised assets and innovative financial channels, instruments and systems are creating new paradigms for financial transaction and forging alternative conduits of capital. Cryptocurrencies have emerged as important financial software systems. They rely on a secure distributed ledger data structure; mining is an integral part of such systems. Mining adds records of past transactions to the distributed ledger known as Blockchain, allowing users to reach secure, robust consensus for each transaction. Mining also introduces wealth in the form of new units of currency. Cryptocurrencies lack a central authority to mediate transactions because they were designed as peer-to-peer systems. They rely on miners to validate transactions. Cryptocurrencies require strong, secure mining algorithms. In this paper, I survey and compare and contrast current mining techniques as used by major Cryptocurrencies. I evaluated the strengths, weaknesses, and possible threats to each mining strategy. Overall, a perspective on how Cryptocurrencies mine, where they have comparable performance and assurance, and where they have unique threats and strengths are outlined.*

Keywords: Cryptocurrency, Bitcoins, Mining, Distributed Ledgers, Blockchains.

Introduction

Cryptocurrency

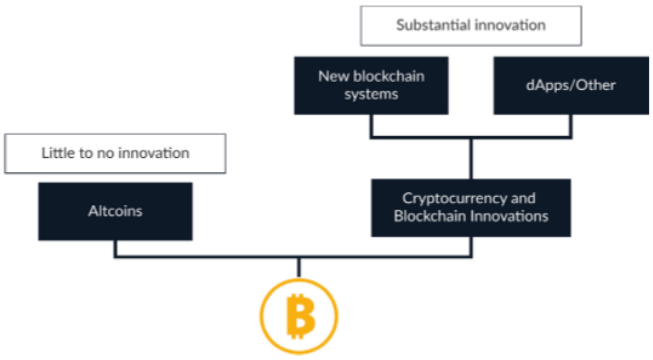
A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. Cryptocurrencies are classified as a subset of digital currencies and are also classified as a subset of alternative currencies and virtual currencies

Bitcoin became the first decentralized cryptocurrency in 2009. Since then, numerous cryptocurrencies have been created. These are frequently called *altcoins*, as a blend of *bitcoin alternative*. Bitcoin and its derivatives use decentralized control as opposed to centralized electronic money/centralized banking systems. The decentralized control is related to the use of bitcoin's blockchain transaction database in the role of a distributed ledger.

BITCOIN, ALTCOINS, AND INNOVATION

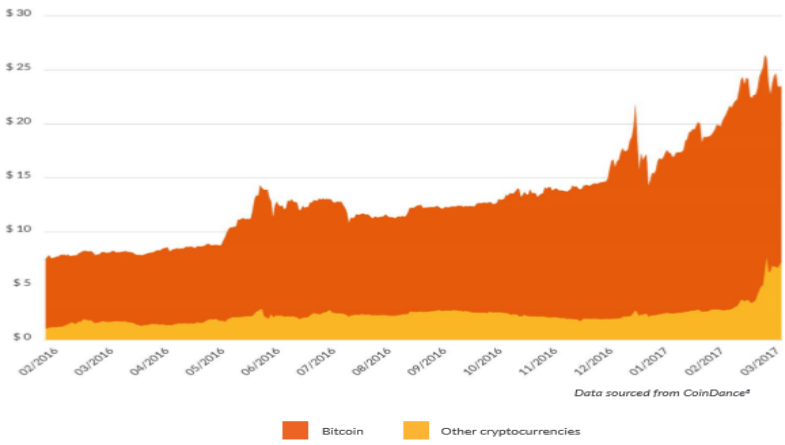
Bitcoin began operating in January 2009 and is the first decentralised cryptocurrency, with the second cryptocurrency, Namecoin, not emerging until more than two years later in April 2011. Today, there are hundreds of cryptocurrencies with market value that are being traded, and thousands of cryptocurrencies that have existed at some point. The common element of these different cryptocurrency systems is the public ledger ('blockchain') that is shared between network participants and the use of native tokens as a way to incentivise participants for running the network in the absence of a central authority. However, there are significant differences between some cryptocurrencies with regards to the level of innovation displayed (Figure 1). The majority of cryptocurrencies are largely clones of bitcoin or other cryptocurrencies and simply feature different parameter values (e.g., different block time, currency supply, and issuance scheme). These cryptocurrencies show little to no innovation and are often referred to as 'altcoins'. Examples include Dogecoin and Ethereum Classic.

Figure 1: The world of cryptocurrencies beyond Bitcoin



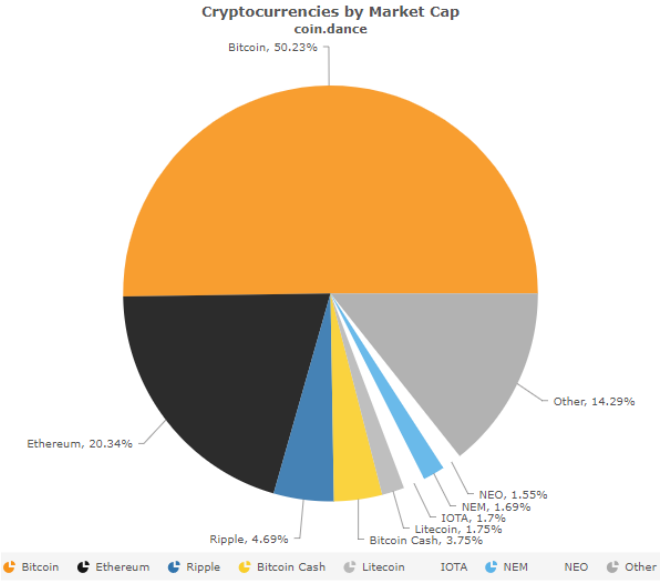
In contrast, a number of cryptocurrencies have emerged that, while borrowing some concepts from Bitcoin, provide novel and innovative features that offer substantive differences. These can include the introduction of new consensus mechanisms (e.g., proof-of-stake) as well as decentralised computing platforms with 'smart contract' capabilities that provide substantially different functionality and enable nonmonetary use cases. These 'cryptocurrency and blockchain innovations' can be grouped into two categories: new (public) blockchain systems that feature their own blockchain (e.g., Ethereum, Peercoin, Zcash), and dApps/Other that exist on additional layers built on top of existing blockchain systems (e.g., Counterparty, Augur).

Figure 2: The total cryptocurrency market capitalisation has increased more than 3x since early 2016, reaching nearly $25 billion in March 2017



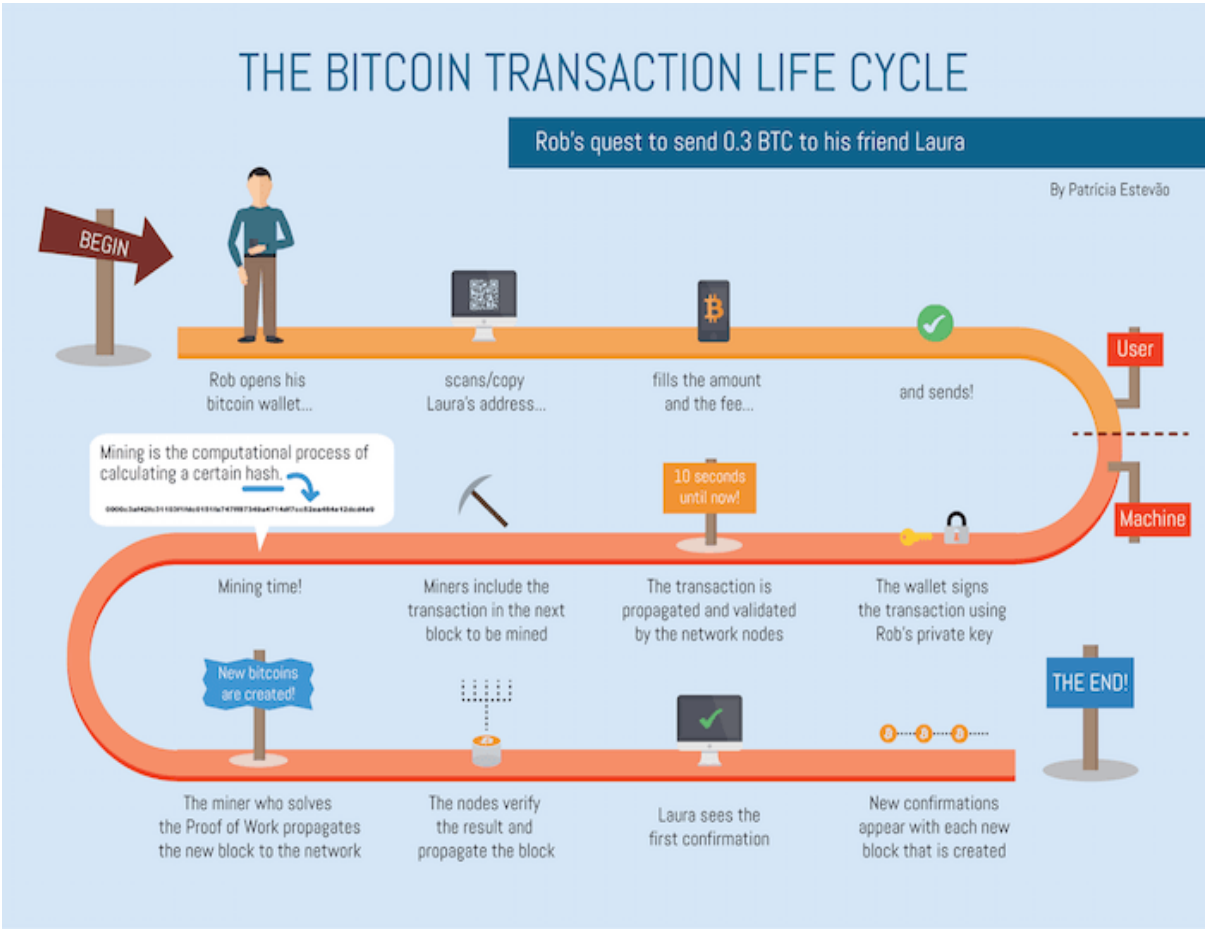
The combined market capitalisation (i.e., market price multiplied by the number of existing currency units) of all cryptocurrencies has increased more than threefold since early 2016 and has reached $27 billion in April 2017 (Figure 2). A relatively low, but not insignificant share of value is allocated to duplication (i.e., 'altcoins'), while a growing share has been apportioned to innovative cryptocurrencies ('cryptocurrency and blockchain innovations')

The following Pie Diagram as on 15th August 2017



MARKET CAPITALIZATION OF CRYPTOCURRENCIES

There are almost 455 different types of Cryptocurrency in the world the maximum market capitalization is taken by the Bitcoin which is 50.23% as it's the well-known cryptocurrency over all the cryptocurrency because it's the oldest and most transacted cryptocurrency Almost it has taken over more than 50% of total cryptocurrency. Then it's the Ethereum which as 20.34% market capitalisation followed by Ripple which is 4.69% shows the huge gap between Ethereum and Ripple, followed by Bitcoin cash, Litecoin, IOTA, NEM, NEO, Monero, Dash, Ethereum Classic, Bitshares, Bytecoin, Dogecoin, Peer coin, Mona Coin, Black Coin and many more.



EXPLAINING THE CRYPTOCURRENCIES WHICH HAS A GREATER MARKET CAPITALISATION

BITCOIN

Bitcoin is the first digital currency introduced by a group (pseudonym Satoshi Nakamoto) in the year 2009. Nowadays many people are dealing with Bitcoin since it has become a more popular form of cryptocurrency. It is a digital currency created electronically. This currency is not printed like normal currencies. However, Bitcoin is produced by People and businesses that are running computers utilizing the mathematical problem-solving software.

DASHCOIN

Dashcoin is formerly known as Darkcoin. In March of 2015, Darkcoin was rebranded as Dashcoin. Dashcoin is a cryptocurrency based on the X11 algorithm. Notable features include fast, secure, anonymous transactions from anywhere in the world. Dashcoin is mined using the X11 algorithm - CPU mining and GPU mining is possible on Windows, Linux and OSX using ccminer, sgminer and other mining software. NVIDIA and AMD video cards are used for GPU mining and Dashcoin ASICs are coming soon. Bitcoin shows all the transection to the blockchain which makes the user uncomfortable to use it. Due to blockchain on the internet, it can become the leakage of bitcoin software but Dash doesn't show such a transaction even to the blockchain. Dash uses a two-tier network to improve its efficiency. Henceforth, the Transection done by Dash is just like a cash delivery. It works in a real time all over the world.

LITECOIN

LiteCoin is a peer to peer digital currency and it operates globally. It operates through a secure, transparent, decentralized network without any central authority monitoring. However, this open source network operates with instant almost zero cost payment all across the world, where users can control their own finances. This currency is a proven solution for online transactions like trade volume, liquidity, industry support. Therefore, this digital currency works as a complementary currency of BitCoin. The introduction of Litecoin version 0.8.5.1 has come into place in November 2013; however, during 2014 the second version of this digital currency was released.

ETHEREUM CLASSIC

Ethereum classic is an independent platform where exertion of any types of project is possible. It provides a platform to the businessman, consumer, and employee to develop the product and create a market virtually. However, Ethereum classic is the type of immutable, decentralized and unstoppable. It never goes down for working. It provides the decentralized system by which you can easily operate the business, work, market form any place even from your home. This Cryptocurrency also secures you from the third-party brochure. Here you can directly meet with your client and easily communicate with them. Due to its decentralized system, you escape from corruption, nepotism, stagnation, and unaccountability.

ETHEREUM

Ethereum (ETH) is a platform to make your contract system smart. This provides your online and offline mode contract policy between you and your shareholders. It never goes down according to the network. Hence, it removes the third parties between your contract systems. Here you directly communicate with your shareholder. So there will not be any chance of fraud. This is a decentralized system. So you can in distributed manner complete your work freely and submit your work. Therefore, all the things are very sharply preserved and make your contract system transparent. It follows the rule of bootstrap. That means it suits for your any size of your project. In today's smart culture this is the best place to generate your market. Therefore, on your innovative idea or project, you can directly meet with your shareholder and increase your business.

MONERO

Monero is a type of online currency. This monero currency is private, secure and untraceable. Monero platform provide user a open source and is available to for all type of user. When you use Monero you simply think that you are your own bank. You can everything manage it only by yourself. And the fund transaction, security, privatization is only becoming your responsibility. You will able to all the things which is by your bank for you. With the help of you will get three basic and most important things. Which are: Secure - Because it is used in online mode so for batter security it uses Distributes peer to peer network. This network is completely make secure with the latest high version of cryptography. And your data is locks in several layers so that it become impossible to crack by the hacker and others. And if stolen then any type of account file not be retrieves form thieves. Untraceable - The funds you transfer or spend here and there is not traceable for the any outer person. The Ring Signature scheme is used for this purpose. It creates too much ambiguity on each transaction so that it became untraceable. Private - Due to digital signature it became private. Only you can open your account file. No one can open your file without your remission.

RIPPLE

Ripple is a networking type website. It is made for making the transaction of money in real time throughout the world. The service provided by ripple is instant, low-cost, certain international payments. Now a busy and technology growing age every consumer aspect that very fast like in real time our working can be done. In this manner to make the financial consumer reliable ripple come into existence. Ripple directly works with banks to transfer the finance from one place to another in real time. This is really a very good step in our growing economy. It really utilizes the role of internet in our fast life. In simple word ripple is a type of distributed financial technology, which enables the banks to send the payment in real-time in international standards across the existing network.

ZCASH

Zcash is a decentralized &open source cryptocurrency. Therefore, it was developed by the Zerocoin Electric Coin Company. Hence, it offers privacy and selective transparency of transactions. The coin's protocol was developing in 2014 through collaboration of Zerocoin researches at John Hopkins University and a group of cryptographers at the Massachusetts Institute of Technology. Zcash uses a zero-knowledge proof construction called Zk-SNARK. These ZK-SNARKS. Therefore, helpful in proving that nobody is cheating or stealing as the transaction metadata encrypts. The cryptocurrency is integrating arbitrage trading into web interface for coin holders in order to trade across various exchanges they integrate.

IOTA

IOTA, the first cryptocurrency without a blockchain, uses a protocol called the "Tangle," which is based on DAG technology. In a traditional blockchain, various transactions are bundled in each block before this bundle of transactions is verified by miners. In the Tangle, every single transaction forms a new block and is essentially verified by itself: In order to successfully conduct a transaction, you first have to verify two randomly chosen transactions is the network.

REVIEW OF LITERATURE

The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments
Authors: Joseph Poon and Thaddeus Dryja

The author presented their invention: The Bitcoin Lightning Network, which is an extension of two-party payment channels applied in such a way as to permit instant transactions between any number of participants.
Lightning transactions are normal bitcoin transactions, but— except for rare cases — are not actually posted to the Blockchain. Because the bulk of the transactional data is stored privately, lightning transactions are expected to be significantly less expensive than on-chain bitcoin transactions, thereby enabling affordable micropayments.

The Bitcoin Backbone Protocol
Authors: Juan A Garay, Aggelos Kiayias and Nikos Leonardos

The authors "extract and analyse the core of the Bitcoin protocol," framing their analysis in terms of two novel properties they refer to as common prefix and chain quality. The common prefix property relates to the network's ability to converge upon a single history, while the chain quality property describes the degree to which a malicious entity can gain an advantage in excess of its mining power.

Eclipse Attacks on Bitcoin's Peer-to-Peer Network
Authors: Ethan Heilman, Alison Kendler, Aviv Zohar and Sharon Goldberg

Security researchers have been eager to identify new attack vectors against the bitcoin network since the authors of the "selfish mining" paper garnered praise and publicity in 2013. Presented in August during the 24th USENIX Security Symposium in Washington, DC, authors Heilman, Kendler, Zohar and Goldberg reveal the "eclipse attack", in which the attacker "monopolizes all of the victim's incoming and outgoing connections, thus isolating the victim from the rest of its peers in the network". The attacker can then trick the victim by feeding him misinformation about the state of the ledger, or coop the victim's computing power for its own nefarious purposes.

OBJECTIVE OF STUDY

- To study different type of cryptocurrency and their process
- To know about how the distributed ledgers are created and operated
- The market capitalisation of cryptocurrency and their volume and nodes
- How the mining of cryptocurrency is done
- Cryptocurrency Blocks and Blockchain.

RESEARCH METHODOLOGY

Define a Problem

The respondents are not aware about the Cryptocurrency and those who are aware they don't know how to do transaction with the cryptocurrency and the benefits of investing in the cryptocurrency.

Research Design

The research design of the paper is to conduct a proper mixture of open ended and close ended questionnaire followed by the Data and interpretation of it in proper graphs with each graph having a proper interpretation of questionnaire.

Sources of Data

Primary Source

My Primary source of collection of data will be purely survey method where they will be given a set of questionnaires and then they have to respond without any biasedness.

Secondary Source

The secondary source for me was Literature review, Books etc.

Sampling

The sample for survey would be taken on the following basis.
Sample Frame: Name, Age, Gender, Occupation.
Sample Unit: Students and Working professionals
Sample Size: 50 respondents
Time Frame: 2 Months
Sampling Method: Simple random sampling (SRS)

Statistical Tool: IBM SPSS

DATA ANALYSIS AND INTREPERTATION WITH HYPOTHESIS

Sample Independent T test for Gender by Overall Satisfaction

Test Variable: Overall Satisfaction
Grouping Variable: 1= Female & 2= Male

T-Test

Group Statistics

	Gender	N	Mean	Std. Deviation	Std. Error Mean
OverallSatisfaction	Female	21	2,19	,873	,190
	Male	29	2,03	1,017	,189

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
OverallSatisfaction	Equal variances assumed	,013	,909	,567	48	,573	,156	,275	-,397	,709
	Equal variances not assumed			,582	46,532	,564	,156	,268	-,384	,696

Here significant value is 0.573 and 0.564 which is greater than 0.05 therefore accept Null Hypothesis, that means overall satisfaction is independent on gender.
(**Ho: $\mu_1=\mu_2$** i.e. Overall Satisfaction is same on both the gender.)

ONEWAY Anova Average Transaction by Occupation

a. Dependent Variable: Average Transaction
b. Grouping Factor: Occupation

➔ **Oneway**

Descriptives

AverageTransaction

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Student	13	2,23	1,363	,378	1,41	3,05	1	6
Service	23	2,04	1,022	,213	1,60	2,49	1	4
Business	5	2,20	,447	,200	1,64	2,76	2	3
Professional	9	2,11	,782	,261	1,51	2,71	1	3
Total	50	2,12	1,023	,145	1,83	2,41	1	6

ANOVA

AverageTransaction

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	,327	3	,109	,098	,961
Within Groups	50,953	46	1,108		
Total	51,280	49			

Here Significant value is 0.961 which is greater than 0.05 therefore accept Null Hypothesis That means Average Transaction is independent on Occupation.

(**Ho: $\mu_1=\mu_2=\mu_3=\mu_4$** i.e. Average Transaction is almost same to all the Occupation.)

<u>ONEWAY Anova Reasons for buying Cryptocurrency by Gender</u>

a. Dependent Variable: Reasons for buying Cryptocurrency
b. Grouping Factor: Gender

➔ **Oneway**

Descriptives

Reason

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Female	21	5,24	1,546	,337	4,53	5,94	1	6
Male	29	4,24	2,047	,380	3,46	5,02	1	6
Total	50	4,66	1,902	,269	4,12	5,20	1	6

ANOVA

Reason

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	12,100	1	12,100	3,517	,067
Within Groups	165,120	48	3,440		
Total	177,220	49			

Here Significant value is 0.067 which is greater than 0.05 therefore accept Null Hypothesis That means Reasons for buying Cryptocurrency is independent on Gender.

(**Ho: $\mu_1=\mu_2$** i.e. Reasons for buying Cryptocurrency is almost same to all the Gender.)

FINDINGS

- Almost half of the respondent did not know about the cryptocurrency
- Those who know about it have fear in Investing in it.
- No Regulation on Cryptocurrency in India
- No strong Internet access in India as it is a developing country
- Indian treat digital wallets as something which will cheat them. They prefer transaction in cash rather than Digital wallet.

LIMITATION

1. The study confines itself to the respondents of "Thane" only. Hence findings would not be relevant to other cities.
2. People mind set about the survey was an obstacle in acquiring complete information & positive interaction.
3. Respondents were very busy in their schedule. So, it was very time consuming for them to answer all the questions properly.
4. Some Respondents were dishonest about answering the questionnaire even they feel that the questionnaire won't affect and it is just a waste of time.

SUGGESTION

1. Awareness should be created for cryptocurrency and on how to buy them its benefits.
2. There should be a proper rules and regulation in buying the cryptocurrency and a regulatory body should take the charge.
3. Transaction in Digital wallets, Digital Money, Digital Coins should be made more easily and available for everyone.

CONCLUSION

Not every cryptocurrency can be considered 'decentralised' as this depends on multiple factors such as the proportion of independent and non-colluding nodes and miners, as well as the amount of hash power securing the blockchain, among others.

There are potential scenarios in which a transaction could get censored by miners, and/or specific units of the cryptocurrency could be 'tainted' or 'blacklisted' which would break fungibility; but these are beyond the scope of this report.

The exact speed depends on a variety of factors that include among others the average block time, the size of the mempool (i.e., the number of transactions that are waiting to get confirmed) and the number of confirmations (i.e., additional blocks mined on top of the block in which the transaction is included) one would like to wait to consider the payment to be final and irreversible.

It should be noted that there are major differences between cryptocurrencies with regards to the size of transaction fees – see the discussion of bitcoin transaction fees in the 'Mining' section. This means that micropayments via 'on-chain' cryptocurrency payments do not always make economic sense.

REFERENCES

Web Source:

- Available at https://coin.dance/volume/localbitcoins (Accessed: 20 August 2017).
- Available at https://coinmap.org/ (Accessed: 20 August 2017).
- Available at https://bitnodes.21.co/ (Accessed: 20 August 2017).

Books:

- Bitcoin Book
- Mastering Bitcoin
- Princeton Bitcoin and Cryptocurrency Technology