Information Systems and
Machine Learning Lab.
Stiftung Universität Hildesheim
Marienburger Platz 22
31141 Hildesheim
Prof. Thomas Mandll
Supervisor

Ethical Issues of Cryptocurrency

Ragini Pant
304573, pant@uni-hildesheim.de

Contents

1. Introduction

A song from the 1966 hit musical "Cabaret" says, "Money makes the world go 'round. (Thought.Co. ,2020). It is one of the essential commodities for survival in the 21st century. With the advancement of technology, new forms of money are being developed that do not confine to the traditional aspects of a centralized authority. One such example is called Bitcoin, developed in 2009 by an anonymous programmer named Satoshi Nakamoto.[Brito, J. and Castillo A. (2013)] This new form of money is called Cryptocurrency or digital currency, powered by an earlier developed technology called the blockchain. Cryptocurrency is an evolution of the payment system. It is similar to institutions like 'PayPal'. The only difference is that Cryptocurrency like bitcoin is the currency being used to transact money between several entities, unlike dollars used in 'Paypal'.

1.1 Blockchain Technology

Blockchain is a public - distributed ledger, which works on the property that, once some data has been recorded inside the blockchain, it becomes very challenging to change it. A block in the blockchain consists of three components: data, a hash of the block and hash of the previous block.

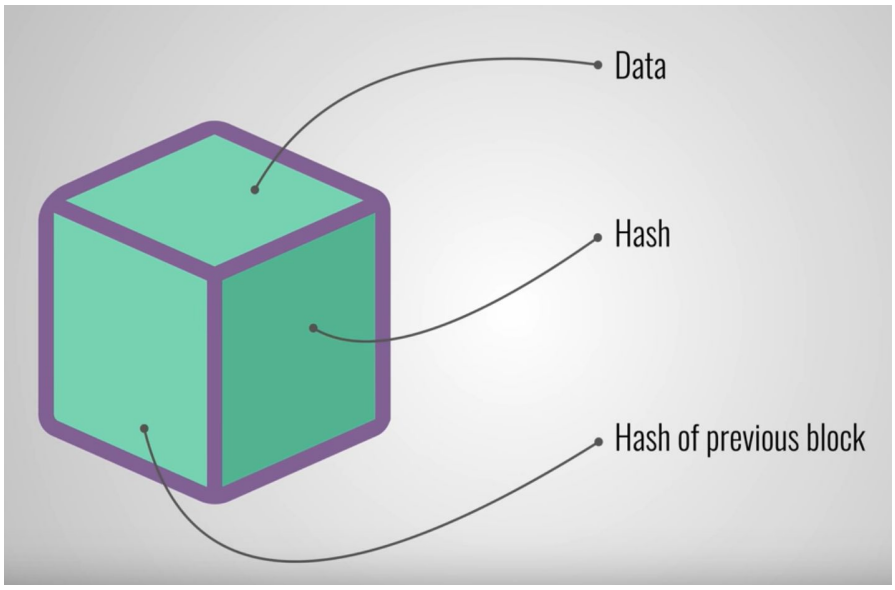

Figure 1: Contents of a block
Source: (Simply Explained -Savjee ,2020)

In the Cryptocurrency blockchain, the data that is stored inside the block includes details of the transaction such as the sender, receiver and the number of coins. The hash of the block is always unique, like a fingerprint. If someone tries to change the contents of the block, then the hash of the block also changes. All the blocks are linked to each other with the hash of the previous block, thus forming a blockchain. (Simply Explained -Savjee ,2020)

1.2 Security of Cryptocurrency

Cryptocurrency is a currency and also a payment mechanism. It has some significant security features that make it a widely popular and reliable technology. Cryptocurrency has three key security characteristics. These are :

- **Hashing**: If someone tries to tamper with a block, the hash of that block changes. This leads to all the following blocks being invalid, as they do not contain a valid hash of the previous block. However, in today's time computers can generate thousands of hash per second. So if someone tampers with a block, he can quickly recalculate the hashes of the other blocks making the blockchain valid again.

- **Proof-of-Work**: To mitigate the issue of hashing, a mechanism called 'Proof of Work' is used. This slows down the addition of a new block into the blockchain by 10 minutes. If someone tampers with the block, he will have to re-calculate the proof of work for all the following blocks.The calculation of proof-of-work is done by miners, who calculate a complex computational problem to generate the hash of the block.

- **Peer-to-Peer Network**: Another reason for cryptocurrency to be secure, is it’s distributed nature. Instead of using a central entity for managing the network, a Peer-to-Peer Network allows everyone to join. The people on the network or miners verify the transaction and add the transaction data to the global ledger; this process is called mining. If a consensus is not achieved by the miners, about the authenticity of the transaction, then the transaction is termed as fraudulent.

To successfully tamper with a blockchain, one has to tamper with all the blocks on the chain, re-do the proof-of-work for each block and take control of more than 50% of the Peer-to-Peer network to change the vote of the transaction. This is very difficult to do, hence making the blockchain hard to tamper.(Simply Explained -Savjee ,2020)

2. Life Cycle of a Cryptocurrency Transaction

Cash is stored in a physical wallet, but cryptocurrencies like bitcoin do not use it's digital wallet to store the currency. Instead, the wallet is used to safely store the public key and private key of the user. Each transaction is created by the sender's wallet, signed by his private key containing the public bitcoin address of the receiver. This transaction is then broadcasted to the network. The nodes of the network or the miners, start mining the transaction using a consensus algorithm where they verify if the transaction was indeed signed by the private key, and then rebroadcast the transaction. If the operation is valid, the miners will include it in the network. The chain validates the new block describing the transfer of ownership of the currency, along with a timestamp. Every node in the network will receive the updated blockchain with the new block added. The processing time that each transaction takes is up to 10 - 20 minutes. After this, the receiver is able to see the transaction amount in their wallet. [Ankalkoti, P. and Santhosh SG, 2017] and [Brito, J. and Castillo, A. (2013)]

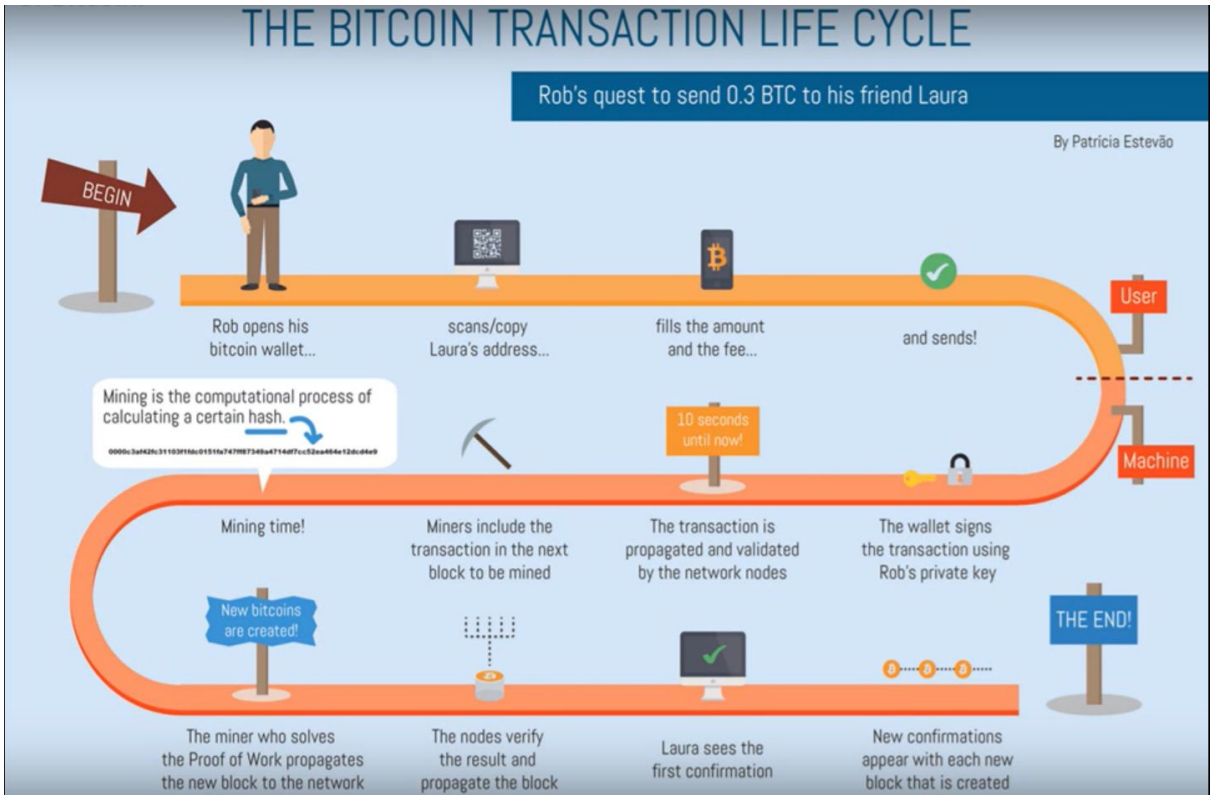

Figure 2: The Bitcoin Transaction Life Cycle
Source: Ankalkoti, P. and Santhosh SG (2017)

Since the first cryptocurrency, bitcoin, developed in 2009, more than 1600 new cryptocurrencies have been created. Though, Bitcoin still rules the market followed by Ethereum, which was developed by a 19-year-old programmer.(BitcoinMagazine, 2020) Another famous and recently popular cryptocurrency is Monero because of its privacy features.[Seele, P.(2019)] Some other famous cryptocurrencies are Ripple, Litecoin , Bitcoin Cash.

3. Ethical Issues of Cryptocurrency

3.1 Decentralization

3.1.1 Ethical Issues with inverting the power-of-chain

Unlike the banking system we currently use, where bureaucrats meet behind closed doors and determine the supply of new currency, mathematics and cryptography are used to regulate the use of cryptocurrency. That means unlike fiat currency which depends on the policies, causing price fluctuations, people can take it in their own hands to regulate cryptocurrency, hence acquiring a sense of freedom. This does invert the power of command, taking away the power from higher authorities and giving it to an individual.Thus, providing a sense of empowerment to the users.

An essential feature of Cryptocurrency is the Peer-to-Peer network. The miners can improve and propose changes in the software, but they cannot enforce those changes on every one since each person is free to choose, which software and version they want to use. However, in order to communicate with each other while mining, they need to use similar software complying with the same rules hence, if a change in the rule does not benefit a majority of the people in the network, then that change is mathematically impossible[Brito, J. and Castillo, A. (2013)]. This feature is not available in the fiat currencies, the government makes the rule and every citizen has to follow it. One such example was the implementation of Indian currency demonetisation overnight in 2016. The citizens of the country spent hours or days in a queue in front of the banks to acquire the new currency notes, or change the old ones.(Guardian ,2020). Cryptocurrencies are censorship resistance since they are not handled by a centralized entity; no one can shut it down and neither can be confiscated by the government.

Reading through the future of cryptocurrency presented by (Swardley, 2020), it can be inferred that the role of government can be felt unnecessary since in cryptocurrency, a transfer of power occurs between the government and individuals.The individuals render the government

powerless, therefore it is true that cryptocurrencies can undermine the power of the government.
The fear of inflation can also be eradicated by the use of cryptocurrencies. The circulation of the fiat currency must always be optimal; else it can cause inflation. On the other hand, cryptocurrencies like bitcoin are mined by powerful computers that help to generate new bitcoins and will continue to do so until the limit of 21 million bitcoins is reached. Thus the value of bitcoin, will not be inflated by generating further currency, once the limit is reached. (Seamus Vaughan Lucey,2020). “Bitcoin was to mimic the extraction of gold or other precious metals from the earth—only a limited, known number of bitcoins can ever be mined. The arbitrary number chosen to be the cap is 21 million bitcoins.” [Brito, J. and Castillo, A. ,p7 (2013)]

3.1.2 How can we trust Cryptocurrency, when no one is held accountable for mishaps?

The need for a central authority may arise when things go wrong; then there should be someone to hold accountable. However, cryptocurrency works on blockchain technology which is essentially a network of users and does not need a central node to prevent illicit activities like double-spending, where the same digital token can be spent more than once; or to ensure the reliability of the transactions made. [Kostakis V. and Giotitsas C. (2014)]. The miners present on the network ensure that the same bitcoins have not been previously spent and also determine if the transaction is fraudulent or not. Only if a consensus of the legal transaction is acquired, then the block is added to the chain. Also, to add a layer of trust between the parties, mechanisms like ‘Smart Contracts’ are being used. Smart Contracts are computer protocols that, when utilized along with blockchain technology, overcomes the problem of lack of trust by digitally facilitating and verifying terms of an agreement between untrusted parties. These transactions are trackable and irreversible. It is an emerging technology that is used in Ethereum currency. It can support contracts for withdrawal limits, loops,gambling markets as well as financial contracts. [Alharby, M. and Moorsel , AV (2017)]

3.2 Anonymity in Cryptocurrency

It is a common misconception that cryptocurrency provides total anonymity to the users, hence providing the ease of performing illegal and extrajudicial activities like money-laundering, dealings in drugs from anywhere in the world. Powered by the technology of blockchain, in cryptocurrency all the transactions of users are public. Though the user remains invisible to most of the legal authorities, it is not impossible to identify the users, since the transactions are identifiable by the Cryptocurrency-address of the user. Linking can be done in various ways, including the tracing of IP addresses and analysis of data made available via the blockchain. Furthermore, if the user wants to convert the currency, or buy new currency, then the user will

use a currency exchange service which requires a bank account, leading to personal identification of the user. Though not completely anonymous, it is a painstakingly long and arduous process. (Seamus Vaughan Lucey,2020) and [Seele, P.(2016)]

There were many claims regarding a new Cryptocurrency named Monero, saying it provides full anonymity to its users and can be thus used for any illegal transactions of money. Though, [Seele P. pg. 139,(2018)] discusses that it is not entirely private.

Cases like Wannacry, where cryptocurrency was used as a medium of payment to demand ransom in exchange for the encrypted files obtained using malware, tells that cryptocurrency is still a prevalent choice of payment because of its partial anonymity.(NextWeb, 2020). Andy Greenberg wrote a Forbes article about the use of cryptocurrency for crowdfunding assassinations of political leaders over a website. The website was active for four months, during which it received murder targets like former- US President Barack Obama for 40 bitcoins and 124.4 bitcoins for the murder of Ben Bernanke, chairman of the Federal Reserve and public enemy number one for many of Bitcoin's anti-banking-system users. With the rapidly growing rate of bitcoin, the assassin would receive approximately 250,000$ for murdering Barack Obama and 760,000$ for killing Ben Bernake by the current bitcoin exchange rate. (Andy Greenberg, 2020).

Nonetheless, prosecutions of those using cryptocurrency in an unethical manner have occurred, one such significant case was of Silk Road, an online marketplace founded by Ross Ulbricht. It involved dealing with drugs and various other illegal products, like forged identity documents. Later other Deep Web black markets, such as Black Market Reloaded and Sheep Marketplace went offline.[Brito, J. and Castillo, A. (2013)] .Below is a graph depicting the use of Bitcoin in Darknet, despite persistent busts in the United States Of America.

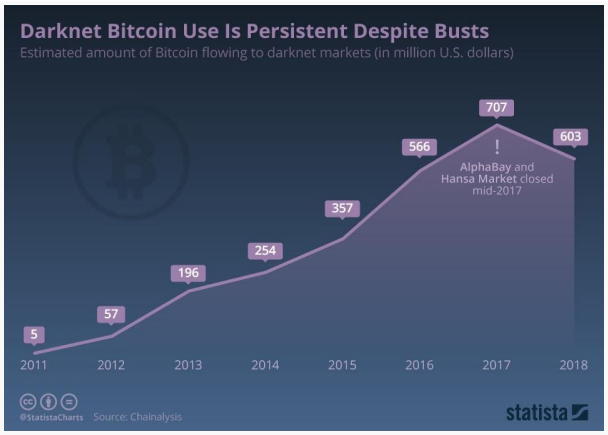

Figure 3: Use of Bitcoin in Darknet despite persistent busts.
Source: Statista (2020)

Frequent use of cryptocurrency has also been observed in purchasing child pornography. Though, various steps are being taken to prevent the illegal use of such behaviour, where bitcoin exchange is working closely with Internet Watch Foundation, a charity with a mission to reduce the presence of child pornography on the internet, to find ways to stop bitcoin being used for such ends. (Seamus Vaughan Lucey,2020).

It must be noted that utilizing the money for illegal activities is not just done by cryptocurrencies. Cash is also majorly used for such transactions. All payment mechanisms can be evil, and cryptocurrency is just another medium, being exploited for illegal and wrongful purposes. Regulations that alleviate the illicit activities of money laundering and illegal purchases, without destroying the benefits of cryptocurrency must be developed.[Brito, J. and Castillo, A. (2013)]

3.3 Potential to Combat Poverty and Oppression

According to Cifuentes and Andres F. (2019), bitcoin is emerging as a substitute for fiat currencies in Venezuela and Argentina. These countries have a spiralling economy, strict currency regulation, high inflation rate and a bureaucratic structure. People of these countries have started putting their money in bitcoins since it is an alternative outside the regime of the government.

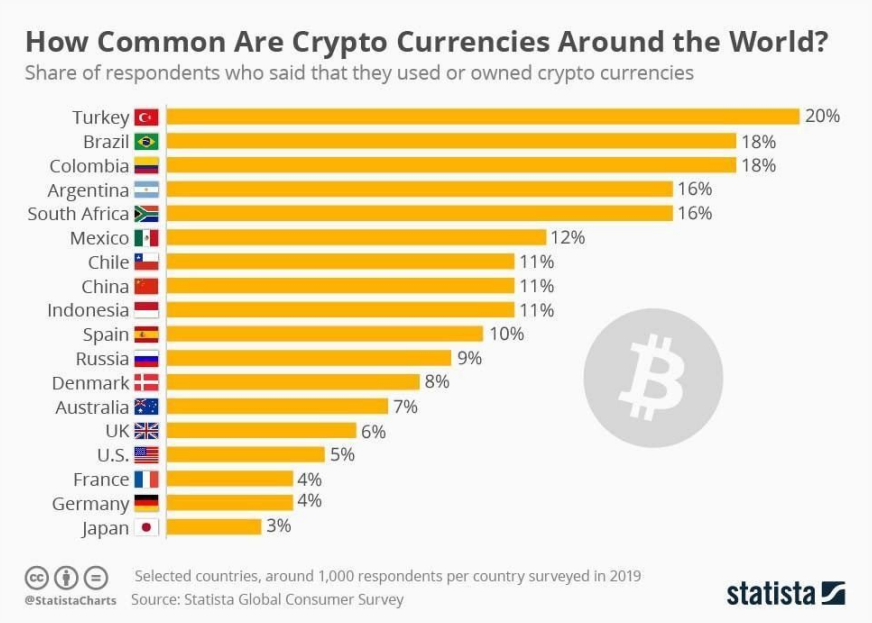

Figure 4: How Common are Cryptocurrencies in the World?
Source: Statista Global Consumer Survey (2020)

Looking at the chart above, we can see the popularity of cryptocurrencies in Argentina, and Colombia, which shares a border with Venezuela. Over the last few years, more than a million refugees from Venezuela have entered Columbia, leaving a massive amount of citizens unbanked and motivating them to shift to cryptocurrency in Colombia.

In developing countries, creating traditional bank branches has many roadblocks. In Kenya, a mobile banking service called M-Pesa is widely popular, as it allows online transactions through mobile phones. To use the service, the users have to first register at an authorised M-Pesa retail outlet. However, physically travelling to a place is a challenge in developing countries, because of the lack of transport or money. Cryptocurrency can solve this issue, since it only requires downloading a digital wallet application, like Bitcoin wallet without any prior registration.[Clegg, A. G. (2014)]

3.4 Wealth Distribution between the rich and poor

With cryptocurrencies getting very popular, people have developed a misconception that it will help them get rich. However, the wealth distribution of Cryptocurrency like Bitcoin is skewed. Research published by (HowMuch,2020) shows that 4.11% of the world's population owns 96.53% bitcoins.

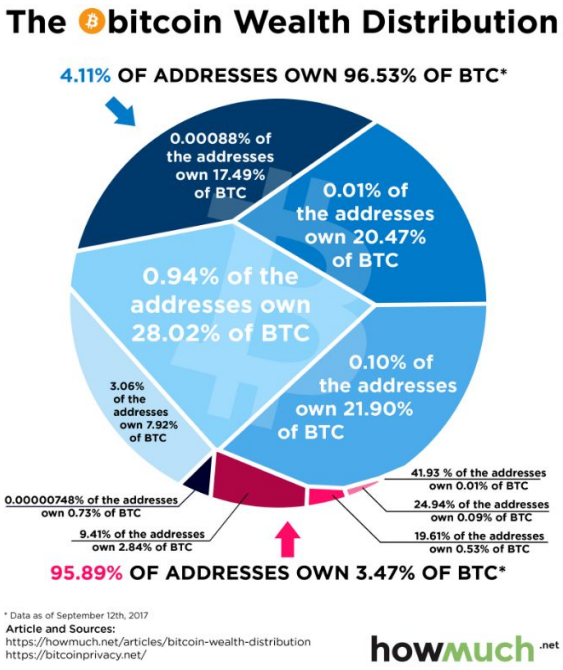

Figure 5: The Bitcoin Wealth Distribution
Source: HowMuch (2020)

People who invested in Bitcoins earlier have a significant advantage over the rest of the users. Cryptocurrency is perceived as the change for the current credit system, but an unbalanced wealth distribution which makes the rich more prosperous and the poor poorer has been happening since ages. [Kostakis V. and Giotitsas C. (2014)]

Another important aspect one must consider before using cryptocurrency is it's volatile nature. The price of cryptocurrencies, like Bitcoin, fluctuates significantly. Hence it does not make sense to manage business finances or keep savings in bitcoins if the market price swings wildly and unpredictably. [Brito, J. and Castillo, A. (2013)] Below is a graph depicting the fluctuating value of Bitcoins from 2014 to 2019.

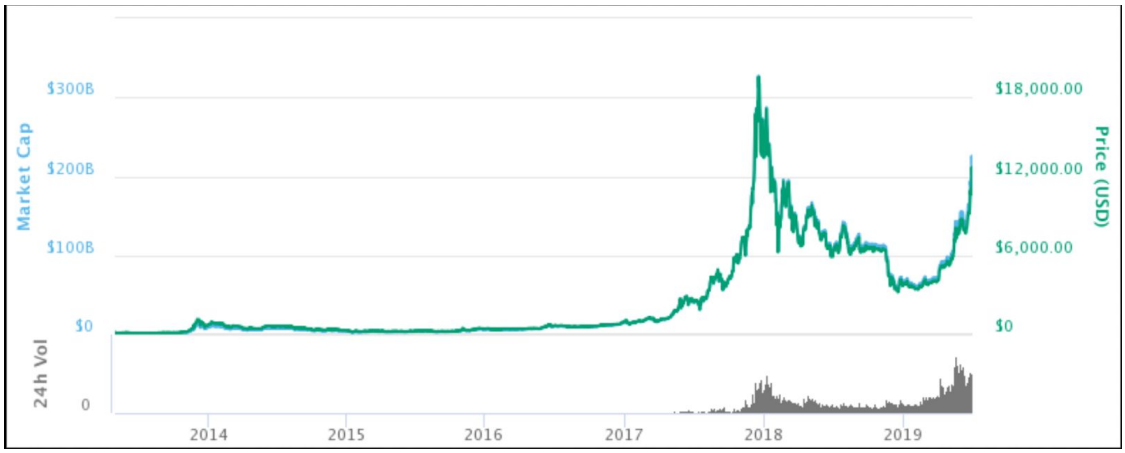

Figure 6: Changes in the price of Bitcoin (BTC) from 2014 to 2019
Source: BitCoinWiki (2020)

3.5 Sustainability

A very popular argument against cryptocurrency is, It may make a few people rich, but will kill us all. Cryptocurrency works on a peer to peer network, which depends on the miners providing their computer's computing power to do the logging of transactions. Each miner contributes his computer's processing power towards maintaining the infrastructure that supports and authenticates the Cryptocurrency Network. As Cryptocurrency gets popular, the difficulty of the computational problem increases to ensure that the currency is mined at a predictable rate.
The popularity of Cryptocurrency starts a vicious cycle where, with the increase in popularity leads to more transactions being verified by the miners, increasing the difficulty of the computational problems to be solved, further increasing the processing power of the computers, that finally causes an increase in the consumption of energy.[Brito, J. and Castillo, A. (2013)]

Below is a chart that shows that Bitcoin has a larger carbon footprint than Switzerland.

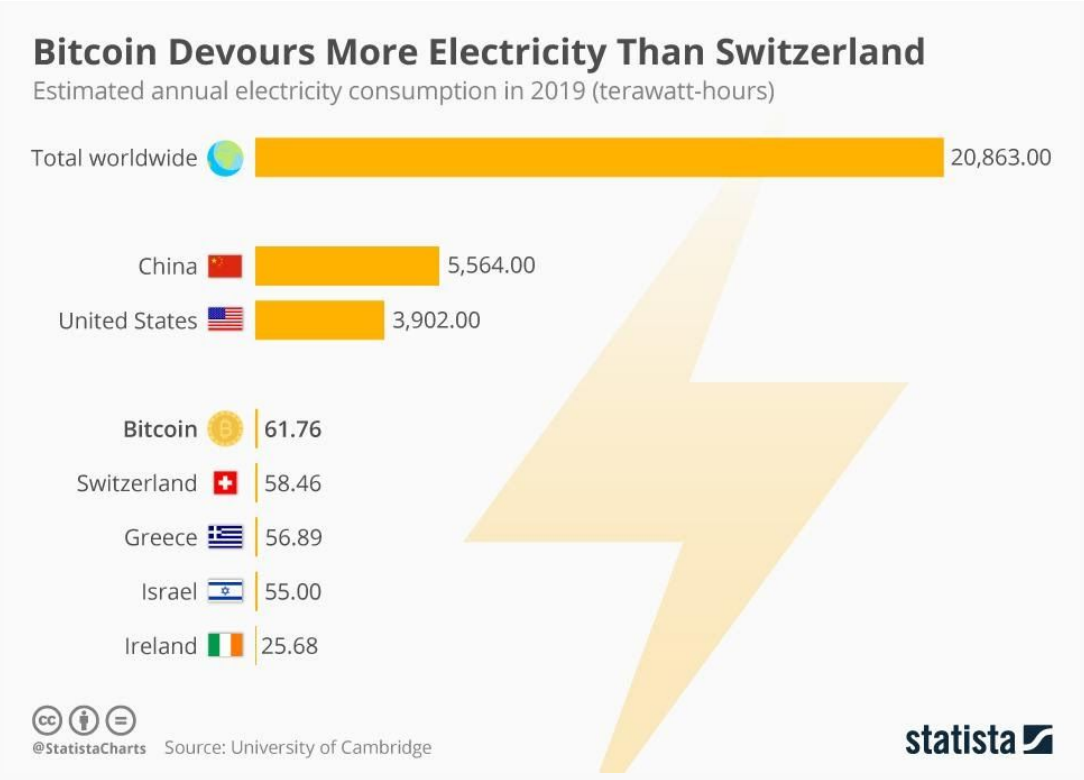

Figure 7: Bitcoin Devours More Electricity than Switzerland
Source: Statista (2020)

New advancements in the field of cryptocurrency are being made, one such instance is the development of a new Cryptocurrency called Solar Coin, which uses Solar energy for the process of mining. [Dierksmeier C. and Seele, P.(2016)]. Analysing the [Ren21 Global Status Report, 2019], we can conclude that there is an increasing trend towards the adaptation of renewable power sources by various countries. With the shift towards renewable energy, the impact of mining the cryptocurrency can be reduced.

4. Conclusion

Cryptocurrency, especially Bitcoin, is very popular with a significant user base and wealthy network. It is powered by blockchain technology and uses a peer to peer network, for making monetary transactions. Being a relatively new technology, there are still some issues like partial anonymity, large carbon foot-print, and undermining the government power. Nevertheless, these issues can be resolved by developing new regulations and policies that do a strict check on the users and the transactions occurring over the network, along with a shift towards renewable sources of energy. Other issues like skewed wealth distribution of the currency can be resolved by educating people about the benefits of the new technology.

Despite some flaws, cryptocurrency is still an up-and-coming alternative from paper currencies; being decentralized in nature allows people to break the shackles of capitalist opportunism. It also helps 3rd world countries that live in an oppressed regime. All the modes of payment can be used in an illegal manner but disregarding the benefits of a new technology that can be further reformed and used in a more ethical manner is incorrect.

5. References

Thought.Co. (2020) *Famous Quotes about Money* [online] Available from : https://www.thoughtco.com/quotes-about-money-2831124 [Accessed 29 March 2020]

Brito, J. and Castillo A. (2013) *Bitcoin: A Primer for Policymakers*. Mercatus Center : George Mason University

Simply Explained -Savjee (2020) *How does a blockchain work - Simply Explained* [online] Available from: https://www.youtube.com/watch?v=SSo_EIwHSd4&list=PLOx2Mbuzg5f-NaOcgv2oFDN82LBWzPo2l&index=3&t=2s [Accessed 29 March 2020]

Ankalkoti, P. and Santhosh, S G. (2017) *A Relative Study on Bitcoin Mining*. India: Imperial Journal of Interdisciplinary Research

BitcoinMagazine (2020) *Who Created Ethereum?* [online] Available from : https://bitcoinmagazine.com/guides/who-created-ethereum [Accessed 29 March 2020]

Seele, P.(2018) *Let Us Not Forget Crypto Means Secret. Cryptocurrencies as Enabler of Unethical and Illegal Business and the Question of Regulation*. Italy: Springer International Publishing AG.

Guardian (2020) *Cash for queues: people paid to stand in line amid India's bank note crisis* [online]. Available from : https://www.theguardian.com/world/2016/nov/28/india-bank-lines-controversy-cash-for-queuing [Accessed 29 March 2020]

Swardley (2020) Bits or pieces? [online] Available from : https://blog.gardeviance.org/2013/11/a-spoiler-for-future-bitcoin.html [Accessed 29 March 2020]

Seamus Vaughan Lucey (2020) *More on ethics of Bitcoin* [online] Available from : https://sevenpillarsinstitute.org/more-on-the-ethics-of-bitcoin/ [Accessed 29 March 2020]

Kostakis, V. and Giotitsas C. (2014) *The (A)Political Economy of Bitcoin*. Estonia: Journal for Global Sustainable Information Society

Alharby, M. and Moorsel , AV (2017) *Blockchain - based Smart Contracts : A Systematic Mapping Study.* Fourth International Conference on Computer Science and Information Technology (CSIT-2017)

NextWeb (2020) *Here's how to fight back against Bitcoin-ransoming malware* [online]. Available from : https://thenextweb.com/hardfork/2019/09/26/heres-how-to-fight-back-against-bitcoin-ransoming-malware-ransomware/ [Accessed 29 March 2020]

Andy Greenberg (2020) *Meet The 'Assassination Market' Creator Who's Crowdfunding Murder With Bitcoins* [online] Available from : https://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/#7359b25d3d9b [Accessed 29 March 2020]

Statista (2020) *Darknet Bitcoin Use Is Persistent Despite Busts* [online]. Available from : https://www.statista.com/chart/17128/darknet-use-of-bitcoin/ [Accessed 29 March 2020]

Cifuentes, Andres F. (2019) *Bitcoin in Troubled Economies: The Potential of Cryptocurrencies in Argentina and Venezuela*. Latin American Law Review

Statista (2020) *How Common is Crypto?* [online] Available from : https://www.statista.com/chart/18345/crypto-currency-adoption/ [Accessed 29 March 2020]

Clegg, A. G. (2014). *Could Bitcoin be a financial solution for developing economies?* University of Birmingham.

HowMuch (2020) *This Chart Reveals the Centralization of Bitcoin Wealth* [online]. Available from: https://howmuch.net/articles/bitcoin-wealth-distribution [Accessed 29 March 2020]

BitCoinWiki (2020) *Bitcoin history* [online] Available from : https://en.bitcoinwiki.org/wiki/Bitcoin_history [Accessed 29 March 2020]

Statista (2020) *Bitcoin Devours More Electricity Than Switzerland* [online]. Available from :https://www.statista.com/chart/18632/estimated-annual-electricity-consumption-of-bitcoin/ [Accessed 29 March 2020]

Dierksmeier C. and Seele, P. (2016) *Cryptocurrencies and Business Ethics.* Dordrecht: Springer Science

Ren21 (2019) *Renewables 2019: Global Status Report* [online]. Available from: https://www.ren21.net/wp-content/uploads/2019/05/gsr_2019_full_report_en.pdf [Accessed on 29 March 2020]