CRYPTOCURRENCY: DAWN OR DUSK FOR THE DIGITAL CURRENCY?

SATPREET MAKHIJA

Computer Science Department
Professor Debayan Gupta
Ashoka University

May 2021

ACKNOWLEDGEMENTS

This course has been an eye-opening experience for me in many ways. The extent to which technology impacts our daily lives is something that most of us have a vague idea about but don’t truly understand. This course has helped me in bridging this gap. Many thanks to Professor Debayan Gupta, the TAs Aishwarya Praveen Das, Aastha Amul Shah, and Reuel John K. Last but not least thank you to all my peers enrolled in CS-2378. It would have been even more fun to attend this course in person but nevertheless, it has been a pleasure.

Abstract*: In the digital technology-driven world of today, an individual has the ability to create a new currency not backed by gold or by the government but built on the trust of the people without third-party interference. This paper analyses the viability of cryptocurrency as a long-term solution and replacement for the government-issued fiat currency we use today. We will look at some of the technical aspects of cryptocurrencies, with a special focus on Bitcoin and Ethereum, their advantages, disadvantages, and the challenges ahead for cryptocurrencies.*

A note for the reader

The intended audience for this paper is anyone interested in cryptocurrency. No prior knowledge is required to understand the paper. Although, I'd recommend watching *But how does bitcoin actually work* to anyone who has no knowledge of cryptocurrencies. There are some technical and economical concepts that you may encounter while reading the paper. To ensure understanding, these concepts have been explained in layman terms abstracting away the details, nevertheless, the gist of these concepts remains the same. Since some of the topics require some background knowledge, many a time, I will digress from the topic at hand, give some background knowledge for the reader's understanding and then come back to the topic being discussed. A list of glossary has also been provided for the reader wherever deemed necessary.

Table of Contents

(click on the section number to go to the respective section)

1.History of cryptocurrency: When did it all start?

“The one thing that’s missing, but that will soon be developed, it’s a reliable e-cash. A method where buying on the Internet you can transfer funds from A to B, without A knowing B or B knowing A. The way in which I can take a 20 dollar bill and hand it over to you and there’s no record of where it came from. And you may get that without knowing who I am. That kind of thing will develop on the Internet.” - Nobel Laureate Milton Friedman in 1999.

Bitcoin is the first modern cryptocurrency that we know of today. It was created in October 2008 by a pseudonym Satoshi Nakamoto who sent out the research paper describing Bitcoin to his peers in an email. [1] Today after a decade or so, bitcoin’s worth has skyrocketed to an astronomical figure ($1 in 2011 to $60,000 in 2021 per bitcoin). But, the history of cryptocurrency precedes almost forty years. In the early 1990s, three computer scientists launched a mailing list to discuss cryptography[1], philosophy, and politics. The members of the group were called cypherpunks. [2] During those times, the internet was in its infancy with hobbyists using it. But, the cypherpunks understood that the internet would become central to society and a medium of expression for the people. They foresaw the capacity Internet provides to the governments in terms of online censorship and surveillance. They believed that cryptography would play a central role in the defense for freedom of the Internet.

[1] It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

One of the members of the Cypherpunks, a cryptographer named David Chaum was working on the idea of electronic cash. He founded a company called Digicash in the year 1989. Digicash launched an electronic payment system called ecash for people to perform transactions online. Ecash promised to be more efficient than the credit card system in terms of security and fees. At the peak of it, even Bill Gates was talking to David Chaum to integrate ecash into every Windows-powered machine. [3] But, due to NSA's involvement as strong encryption was considered to be a military munition and illegal to export from the United States as well as competition from other digital payments platforms like Paypal, ecash went bankrupt. The investors pitched the company's idea of electronic cash to the banks but they were reluctant as the technology was new and the idea in itself was experimental. The banks stuck to the credit card system ignoring ecash. This is when the first wave of cryptocurrency died.

In 2003, one of the ex-employees of Digicash, Nick Szabo proposed a virtual currency called Bitgold. [4] Bitgold was based on the concept of Proof-of-Work[2] (PoW) The idea was simple. You present your Proof-of-Work for an input string, and depending on the hardness of the puzzle, you were awarded bitgolds. But, there is a major conceptual difference between Bitgold and Bitcoin. Bitgold was to not act as a token of electronic currency that represents fiat currency, but as a reserve currency which would 'back' another form of currency in the same manner physical gold once backed the fiat currency of the countries. But, Bitgold always remained a proposed cryptocurrency. It was mentioned in blogs and articles but was never implemented.

In hindsight, one must ask what is the difference between Digicash, Bitgold, and Bitcoin? Broadly speaking, ecash was still dependent on third parties such as banks for issuing tokens which meant that the power still lied in the hands of the bank. This was against the idea of decentralization. On the other hand, Bitgold was not a currency, per se. It was a reserve currency that backed the physical currency just like gold did in the past. But, Bitgold's concept was an economic system of decentralization with the help of PoW where no third party was involved. Therefore, in some sense, Bitgold was the missing link in Digicash which paved the path for Bitcoin.

[2] *Proof of Work* (PoW) is a form of cryptographic zero-knowledge *proof* in which one party (the prover) proves to others (the verifiers) that a certain amount of computational effort has been expended for some purpose.

2. Why do we need cryptocurrency in the first place?

I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something they can't stop." - Nobel Laureate Friedrich Hayek in 1984.

Throughout history, we have witnessed the phenomenon of decentralization of power from the kings and queens to the commoners, from monarchies to democracies. Decentralization has increased at a meteoric pace with the advent of the internet. With the privatization of industries and the existence of free markets, the people have a plethora of opportunities to choose what they want. But, there is one process over which the government has a monopoly, i.e., the printing of currency. What makes the $100 bill have any value? The central government issues the notes with a statement "I promise to pay the bearer the sum of hundred dollars" and everyone believes that the bill holds a value of $100. The problem here is that the value of that $100 bill depends on how many $100 bills the government prints. Imagine, if the government suddenly decided that it is going to double the number of $100 bills. Even though you have the same number of $100 bills with you as you had earlier, their value has halved. In November 2016, the Indian government took the 500 and 1000 rupee notes out of circulation which they claimed was done to close down illegal transactions with black money leading to corruption. [5] It is not about whether the scheme worked or not but the extent of power that a government has over the value of a currency that is in question here. It is this monopoly of the government over the supply and demand of currency that cryptocurrency curbs.

In his book *The denationalization of money*, Friedrich Hayek argues that the existence of a centralized government that issues currency leads to social inequality as it prevents the discovery of an efficient method of meeting the market's demands and needs. [6] The central entity is inadequate in keeping up with the information of the vast and enormous society, creating regular boom and bust cycles of demand and supply of the currency. On the other hand, people decide the value of the cryptocurrency dynamically. Everyone has a say over what its value is. Cryptocurrency is not limited to the geographical location of the user. It transcends the boundaries of countries and states. Therefore, the people are protected from a situation where the national fiat currency of a country goes downhill.

3. Issues with cryptocurrencies

3.1 Nobody wants to spend money:(Deflation

Imagine you have \$100 today. The same \$100 would not have the same worth after 10 years. But why? This has to be understood with the concept of purchasing power[3]. We will determine the power of today's \$100 as the basket of goods that can be bought with it. Imagine an economy where the only goods are apples. Let's say that each apple costs \$20 dollars, so you bought 5 apples with your today's \$100 bill. After ten years, the same apple's cost rises to \$50 dollars and now in the future, you can only buy 2 apples from your \$100 dollar bill. This means

[3] It is the value of a currency expressed in terms of the number of goods or services that one unit of money can buy.

that the purchasing power of today's $100 bill has decreased. But, why would we want that in the first place? Why is it the case that the price of goods should increase with time? Why can't they just be static? When we think in terms of economics, the decreasing value of money incentivizes people to consume more products and helps in growing the economy. To understand this, let's take a counterexample. Say, after 10 years, the price of each apple decreases to $10 each. This means that after 10 years, you can buy 10 apples. This is termed deflation as the relative price of the good has decreased. Now, therefore, it is in your incentive to not spend your $100 bill today but save it for the future as it will be worth more in the future. This will lead to the *hoarding problem.* Now, it is in the favour of the people to not spend their money but save all of it as its purchasing power will increase in the future. But, as a whole, it is bad for the economy as an economy cannot flourish without its consumers consuming the products. The very definition of consumer rests on its ability to consume. Therefore, we now know why deflation is undesirable.

But how does the hoarding problem relate to bitcoin? Well, in order to make my case, let's us look at the case of James Howells from Newport, Wales who has offered his city council $70 million to dig up his hard drive that we threw away in 2013. [7] The only way to use those bitcoins for Mr. Howells is to get his hard disk back. This can also happen when one loses one's password. This is contrary to the system we have in place when we have a centralized system such as banks. When you forget your debit/credit card pin or your password for online transactions, you go back to the bank, prove your identity and after some process, you are able to reset your password/pin. But, here in the bitcoin world, we do not have a centralized system. It is the opposite of that. We have a decentralized system where one has no means to change the password for their bitcoin account to access their bitcoins if they forget their password (private key).

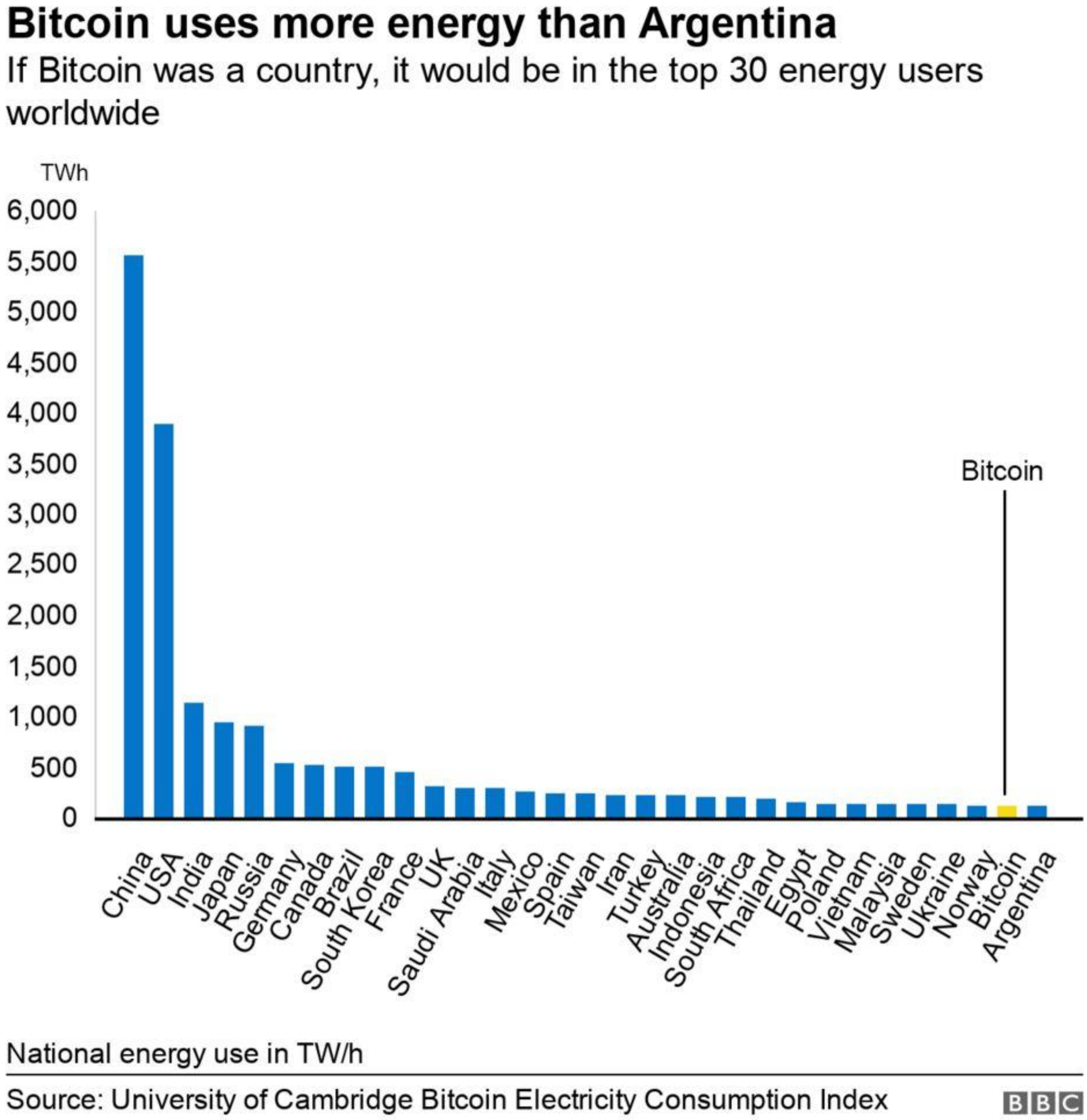
Now, when a miner validates a transaction, the miner earns a commission. Part of the commission is the transaction fees given by people who did the transactions and part of it is newly created bitcoins. This is the way new bitcoin is generated in the system. In Bitcoin, the creation of new bitcoins is algorithmically designed in such a way that the number of bitcoins generated decreased by 50% every four years. Therefore, by the end of 2040, all of the bitcoins would be mined. The total number of bitcoins that can ever exist is 21 million. [8] Satoshi Nakamoto has 1 million bitcoins in his account which hasn't moved from the starting of bitcoins.

Now, connecting the cases of one losing hard disks, flash drives, forgetting private keys, there is no way to recover those bitcoins. One can treat them as nonexistent. This means that the number of bitcoins is not increasing but actually decreasing. So, what? why does it matter if the number of bitcoins is decreasing? The reason is this. If the total number of bitcoins is actually decreasing, then each bitcoin's worth is increasing. Now, do you remember the example of apples? With each bitcoin's *purchasing power* increasing in the future as compared to the present, it is in the best interest of the consumer to save the bitcoins and not spend them as they can but more apples with the same bitcoin in the future. The value of your money increases in the future. This brings back the problem of hoarding that we discussed earlier. **Therefore, contrary to common belief, bitcoin is not inflation-free but deflation-prone.**

3.2 Switch off your lights: The electricity conundrum

Here's a question for you. Are the resources on Earth limited or infinite? The resources present on Earth indicate that it has finite resources. This leads to a logical implication that we cannot sustain an ever-growing population. But, our minds and the ideas that spur from it are also resources. Anyways, our reach of resources is dependent on the technology we have today and we will base our arguments treating that as a maxim which states: We have finite resources.

We have previously discussed Proof of Work (PoW). It is central to the consensus mechanism for Bitcoin to function. Mining is the process of going about doing so. Mining is the concept of solving a complex puzzle to prove that you solved the problem. It is used for verifying the block. But, solving this complex puzzle is computationally expensive. It requires a lot of electricity. The electricity required to produce the computation power to solve the puzzle has a great impact on the global warming front. With that being said, we need to understand how much electricity does bitcoin alone consumes?



Considering the strides made by technological leaders in accepting bitcoins, electricity consumption is only going to increase in the coming years. We are talking about building a new currency and surely one of the attributes we must question is its viability, whether we can have such a system of currency for an extended period of time (and I’m talking at least a hundred years). One must be careful while forming statements such as *Is mining a waster of energy?* The short answer is No. This is because mining is what causes the verification of the transactions and ensures solving the double-spending problem. With that being said, is the concept of mining a viable option when we consider the amount of energy it uses which causes global warming. The proponents of bitcoin argue that most of the electricity used for mining is generated from renewable sources. Coinshares, a cryptocurrency analysis firm, claims that bitcoin gets 74.1 percent of its electricity from renewable sources. [9] They also claim that many renewable power generators are so poorly located and underused that mining bitcoin has become the only viable use for that electricity. But, the problem is this. We know that for PoW one needs computation power. We will call it hash power. Now, since these mining intensive areas are only certain geographical locations where there is abundant electricity, whether generated from renewable or non-renewable resources, the mining power will always lie in the hands of a few. The issue with that is 51 % attack[4]. It is estimated that around 65% of bitcoins are mined in China with Xinjiang alone accounting for some 35.76%. [10]

3.2.1 Solution for the electricity consumption of Cryptocurrencies?

The ultimate challenge for having a cryptocurrency without third-party interference is how to reach a consensus. Another proposed method to do so is Proof of Stake (PoS).[5] Like PoW, PoS is a mechanism to achieve consensus. In a PoW based consensus-system, the miners had to solve a difficult puzzle that required heavy computational power that then required heavy electricity. But, in a Proof of Stake based consensus system, there does not exist the concept of

[4] A 51% attack is a potential attack on a blockchain network, where a single entity or organization is able to control the majority of the hash rate, potentially causing network disruption. In such a scenario, the attacker would have enough mining power to intentionally exclude or modify the ordering of transactions.

[5] It is a concept states that a person can mine or validate block transactions according to how many coins he or she holds. This means that the more coins owned by a miner, the more mining power he or she has.

miners but of validators. The validators are required to verify the transactions. But, wouldn't a malicious validator include some false transactions? Well, PoS solves this problem by using the concept of stake. So, when the validator validates a block, they put the cryptocurrency *they* own as a stake, i.e., if any of the transactions validated by the validator is false, then the validator loses their stake. So, to make things clear, in a PoW-based consensus mechanism, the miner is incentivized not to include a false transaction in the chain as they will have to spend computational resources first to mine the block and if there is a false transaction in that block, then that block will get rejected meaning loss for the miner who spends resources to mine the block in the first place. But, in a PoS, the validator is incentivized not to include a false transaction in the block because if they do, they will lose the stake that they had put to validate the block in the first place.

But, what if someone owns 51% of the cryptocurrency? Wouldn't then this validator in theory can validate any block and create a blockchain long enough that it is treated as *the* block? Accordion to game theory, it is not in the best interest of this entity to do so? This is because if this entity does violate the integrity of the transactions, then the value of the currency will itself decrease which would decrease the total worth of the entity. There's no point in retaining 51% of something which in itself is worthless. The currency is only valuable in the first place when the people agree that it holds some value. It is also difficult to hold 51% of the total cryptocurrency in the first place as that would require a lot of money. But, the concept of PoW is new and experimental.

3.3 The Scalability Problem: Transactions per second

In a blockchain, the transactions are stored in a block and these blocks are linked to each other. Now, Bitcoin uses blockchain technology to save its transactions. Each block contains a number of transactions. Let's see how many? Currently, the block size in bitcoin is set to 1 Megabyte

(1, 048, 576 bytes) and on average each transaction requires around 440 bytes. [11] This gives us the total number of transactions per block as 1 MB/440 = 2383 transactions. Every 10 minutes, one block gets mined. Therefore, TPS is 2383/600 approximately equals 4. So, on average 4 transactions get completed for every second on Bitcoin. On the other hand, Visa processes around 1700 transactions per second. [12]Therefore, Visa's TPS is around 425x than that of Bitcoin. Needless to say, if Bitcoin wants to act as a micropayment method for all the people, it needs to increase its TPS. So, how can we increase the TPS of Bitcoin? The following methods have been proposed:

- **Increase block size** :

  When Satoshi Nakamoto was the lead developer for Bitcoin, he capped the block size to 1 MB which has stayed the same since. There are two scenarios, first what happens when we decrease the block size and secondly when we increase the block size. In the first case of decreasing the block size, the drawback is that a lesser number of transactions will fill in the block and hence TPS will decrease even further as TPS is directly proportional to the number of transactions that fit in a block. In the second scenario, when we increase the size of the block, there are two problems. Let's say to increase the TPS, we increase the size of the block to 425 MB from 1 MB as Visa's TPS is 425x faster than that of Bitcoin. Now, surely, the TPS of bitcoin is equal to that of Visa. But, since the size of each block is so huge, the number of hashers who run the entire blockchain (all the blocks))stored locally will decrease drastically and the blockchain will lie only in the hands of a few who have the resources to store blocks of that size. This can be understood via an analogy. Remember, we do not have a centralized third party that checks how much money an individual has. We depend entirely on the consensus mechanism to reach a conclusion as to how much money an individual has. Let's say that there are 100 hashers in the Bitcoin system. They all keep the entire node saved in their local systems. Now, when a block needs to be validated, first a hasher will mine the block, send the signal to all the other nodes in the network that that block has been mined, the other nodes will cross-verify the block and if 51% or more agree then that block will get added to the blockchain. But, now that we have increased the block size, imagine that some of these hashers do not have the resources to store such huge blocks locally which will result in say 30 hashers dropping out and so we are left with a system with 70 hashers. As the size of the block increases, more and more hashers will drop out and the only ones left will be the ones who have the entire blockchain. This results in the centralization of the verification of blocks which is undesirable. Another problem with the increased block size is that once a block has been mined, the block needs to be broadcasted to the other nodes. But, since block size has increased, broadcasting the block will also be time-consuming further reducing the TPS.

- **Decrease hash complexity** :

  Now, we know that a new block gets mined every ten minutes. And, we also know that TPS is inversely proportional to the time taken for each block to get mined. In simple terms, we can reduce the mine time per block by making the puzzle easier. Now, to understand that we need to understand the puzzle that a miner needs to solve to mine a block in bitcoin. Bitcoin uses the SHA-256 hash function[6] A hash function essentially takes an input of arbitrary length and produces an output of a fixed length. Given an output, it is very difficult (computationally infeasible) to know the input. This is called the one-way property of hash functions. Now, in bitcoin mining, the miner is supposed to keep feeding input to the SHA-256 hash function and is expected to produce an output starting with a fixed number of zeros at the beginning of the output. The lesser the number of zeros required in the output, the lesser time it takes for the miner to find the input that will produce the desired output when passed to the SHA-256. So, one can essentially decrease the number of zeros required in bitcoin to decrease the mining time per block which in turn increases the TPS. But, the problem is that the very reason PoW works are because it makes sense for the miner to not add fraud transactions in the block as it will get rejected by the other nodes, and the resources spent by this fraudulent miner will go in vain. But, if less and less computational resources will be required then the fraudulent miner has the incentive to include fraud transactions in the block.

[6] It is a mathematical algorithm that maps data of arbitrary size (often called the "message") to a bit array of a fixed size as the puzzle for the miner to solve.

The problem with both these approaches is that they have a ceiling limit to which they work. If Bitcoin needs to reach the TPS of Visa, both of these solutions individually or combined will not solve the problem of Bitcoin scaling. Then do we have a solution? As it turns out using Proof of Stake (PoS) can be a useful mechanism to increase the scalability of Bitcoin. In a PoS consensus mechanism, the validator is chosen randomly by the code that gets to verify the transactions. Therefore, the mining time is completely removed here. Ethereum currently works on PoW but Ethereum's founder Vitalik Buterin has announced that Ethereum is working tirelessly to move from being PoW-based to PoS. [13]

3.4 An investment or currency?

An investment and currency are completely different in terms of their end goal. An investment is supposed to provide growth for you to make profits. You expect its value to grow at a steady rate. But, on the other hand, the currency is supposed to be stable. You don't want a currency that is worth $10 one day and $100 the next day. In recent years, the way cryptocurrencies are working, especially, Ethereum and bitcoin, are being treated more as investments and not currency. The problem also rises as for anything to be accepted as currency, everyone else must also be willing to expect it as payment. But, one is willing to take something as a viable payment when that person knows that the value of that currency is going to be relatively stable. But, I believe that issue will be solved once the big players in the market start accepting payments in cryptocurrencies, which many have already started.

4. So, what’s the verdict?

"The difference between a bad electronic cash system and well-developed digital cash will determine whether we will have a dictatorship or a real democracy". David Chaum, 1996.

Cryptocurrency has shown the potential that a decentralized currency with no third party involved can exist and flourish. Sure, these cryptocurrencies have a long way to go to be used as payment methods more frequently. We have seen the problems that Bitcoin and other cryptocurrencies face currently both technically and economically. But, their implementation and successful run for the last few years has shown the citizens that they do not need a government to have a currency.

5. Questions to ponder upon

There are some more questions that need further investigation.

- How much of a say does the entity who creates a cryptocurrency have over it in the long run? In the case of Bitcoin, this is interesting as one does not know who the creator is. But, in the case of Ethereum, Vitalik Buterin is the creator. Even though the source code of these currencies is open source and the community decides on further technical changes required in the future through consensus, one cannot deny the influence the creators of the currency have over these decisions.

- We have seen how the theoretical limit of the number of Bitcoins leads to the *hoarding problem* which causes deflation. So, how should we go about designing the algorithm for a cryptocurrency so that it is actually inflation-free?

- Bitcoin has faced a lot of backlash with regards to being used for illegal transactions and the infamous Silk Road which was an online black market. With anonymity comes the challenge of having accountability. How will this anonymity of transactions in cryptocurrencies impact the world?

References

[1] Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 31 October 2008.

[2] Qureshi, Haseeb. "The Cypherpunks." *Nakamoto*, 2019, https://nakamoto.com/the-cypherpunks/. Accessed 18 April 2021.

[3] Magazine, Bitcoin. "The Genesis Files: How David Chaum's eCash Spawned a Cypherpunk Dream." *Nasdaq.com*, 2018, https://www.nasdaq.com/articles/the-genesis-files%3A-how-david-chaums-ecash-spawned-a-cypherpunk-dream-2018-04-24 . Accessed 18 April 2021.

[4] Szabo, Nick. "Bit gold." *Unenumerated*, 2008, http://unenumerated.blogspot.com/2005/12/bit-gold.html. Accessed 18 April 2021.

[5] Doshi, Vidhi. "India withdraws 500 and 1,000 rupee notes in an effort to fight corruption." *The Guardian*, 8 November 2016, https://www.theguardian.com/world/2016/nov/08/india-withdraws-500-1000-rupee-notes-fight-corruption.

[6] Hayek, Friedrich A. *Denationalization of Money*. Institute of Economic Affairs, 1976.

[7] Murray, Tom. “A man who says he threw away a hard drive loaded with 7,500 bitcoin in 2013 is offering his council $70 million to dig it up from the city dump.” *Business Insider*, 16 January 2021, https://www.businessinsider.in/international/news/a-man-who-says-he-threw-away-a-hard-drive-loaded-with-7500-bitcoin-in-2013-is-offering-his-council-70-million-to-dig-it-up-from-the-city-dump/articleshow/80302306.cms.

[8] Hayes, Adam. “What Happens to Bitcoin After All 21 Million Are Mined?” *Investopedia*, 2021, https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/ . Accessed 18 April 2021.

[9] Irfan, Umair. “Bitcoin is an energy hog. Where is all that electricity coming from?” *Vox*, 18 June 2019, https://www.vox.com/2019/6/18/18642645/bitcoin-energy-price-renewable-china.

[10] Tuwiner, Jordan. “Bitcoin mining in China.” *buybitcoinworldwide*, 25 March 2021, https://www.buybitcoinworldwide.com/mining/china/.

[11] *TradeBlock*, 2021, https://tradeblock.com/bitcoin/historical/1h-f-tsize_per_avg-01101 . Accessed 22 April 2021.

[12] Sedgwick, Kai. “No, Visa Doesn’t Handle 24,000 TPS and Neither Does Your Pet Blockchain.” *Bitcoin*, 20 April 2021, https://news.bitcoin.com/no-visa-doesnt-handle-24000-tps-and-neither-does-your-pet-blockchain/.

[13] Kim, Christine, and William Foxley. “Valid Points: Ethereum’s Proof-of-Stake May Happen Sooner Than You Think.” *Coindesk*, 17 March 2021. Accessed 23 April 2021.

Bibliography

3Blue1Brown. “But How Does Bitcoin Actually Work?” 3Blue1Brown, 2017, https://www.youtube.com/watch?v=bBC-nXj3Ng4 . Web.

Agashe, Aditya, Parth Detroja, and Neel Mehta. *Blockchain Bubble or Revolution: The Present and Future of Blockchain and Cryptocurrencies*. Paravane Ventures, 2019. Print.

Tapscott, Don, and Alex Tapscott. *Blockchain Revolution: How the Technology behind Bitcoin and Other Cryptocurrencies Is Changing the World*. London, England: Portfolio Penguin, 2018. Print.

“How the Bitcoin Protocol Actually Works.” *Michaelnielsen.org*. N.p., n.d. https://michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/ Web. 28 Apr. 2021.