Blockchain and Bitcoin

An Analysis of the Blockchain, Cryptocurrency, NFTs, and a Proposal for an Ethical Cryptocurrency

Ivy Yeoh

CS 451

Willamette University

[icyeoh@willamette.edu](mailto:icyeoh@willamette.edu)

Cami Lawson

CS 451

Willamette University

[cjlawson@willamette.edu](mailto:cjlawson@willamette.edu)

Brooks Danielson

CS 451

Willamette University [badanielson@willamette.edu](mailto:badanielson@willamette.edu)

# Abstract

In this paper, we describe how cryptocurrencies, blockchain consensus, and non fungible tokens work. We illuminate the subjects by detailing their history, implementation, controversies, and ethical implications such as environmental impacts and socioeconomic inequities. We then propose an “ethical” use of the technology of our invention, based on a similar structure to the proof of burn consensus algorithm. By the end of our project, we hope to have adequately explained the foundation and fundamental issues of the technologies, as well as suggested a convincing alternative.

# Introduction

With the rising popularity of cryptocurrencies and their increasingly common role in cyber attacks, there is a need for a larger discussion of its effects on the environment, economy and the general public. The discussion must be informed by an understanding of the technological implementation of the blockchain. This is how cryptocurrencies function.

# Background

### Blockchain

Blockchain technology is used as a type of distributed ledger, so people can have recorded transactions that are decentralized supposedly and publicly accessible at all times. The blocks are linked together by cryptography so each block is added by finding the hash of the previous block and that’s essentially what mining is. There are many different types of cryptocurrency out there right now and some of them use different hashing functions to secure the blockchain. For example, Bitcoin utilizes the SHA-256 hash function while Ethereum uses Keccak-256. Keccak is a broader term for a family of hash functions which are basically SHA-3. The blockchain contains the transaction data, the hash from the previous block which secures its place in the chain, and a timestamp. To achieve accountability and trust on a distributed ledger, the blockchain has a consensus algorithm. The current models for these consensus algorithms are proof of work, stake, burn, capacity, and elapsed time. Proof of work and proof of stake seem to be the two most popular forms of consensus algorithms, but there are a few reasons why both are lacking.

### Consensus Algorithms

The proof of work system is based on the idea that the higher your hash rate, the higher your chance of mining the next block is, so it actually encourages companies to participate in mining pools which detracts from any decentralization. With mining pools, there is a chance of the 51% attack which is when pools of miners hold the majority of hashing power and can basically control the blockchain that way. According to the Cambridge Center for Alternative Finance, in September 2019, four companies in China accounted for 75% of the hashrate power in the world.

Proof of stake is the most common alternative to proof of work. Miners are called ‘validators’ instead, they put their own coins at stake and are randomly selected, but the chances of them being selected are proportional to how many coins they put at stake. The stake is more than the reward which means if a validator consents to a fraudulent transaction, they can be punished financially and that’s how you’re supposed to trust them. This has the same dangers as the 51% attack, but that attack is slightly less practical than the proof of work system depending on the value of the crypto, it could be unfeasibly expensive. While the proof of work system allows for big companies to take advantage of the economies of scale when buying expensive mining equipment.

Proof of stake also uses less energy because it doesn’t let everyone mine for blocks, only select validators. There are some proposals for trying to remedy this rich get richer scheme like the coin age selection method in proof of stake. Two examples of current proof of stake models are in Ethereum’s “Casper” and Cardano’s “Ouroboros”.

Proof of burn is like proof of stake mixed with proof of work. Instead of putting coins at stake, validators ‘burn’ coins by sending them to an address from where they are irretrievable. From there, they are put into the same random selection process for which the validator gets to mine the next block using the proof of work system. The more coins they burn, the better are their chances of being selected to mine the next block. Depending on how proof of burn is implemented, miners may burn the native currency of the blockchain or the currency of a different chain.

### Hash Functions

Hash functions are integral to a complete understanding of computer security as a whole. Hashing is a way of mapping data to outputs of fixed size. Hash functions take inputs of arbitrary length and code them into an output which is often used to index a table. Hashes are used for a huge variety of tasks but are most often used for encryption purposes. There are many families of hash functions including SHA functions and the earlier MD5.

### Bitcoin

The first blockchain was outlined in 1991 in the paper “How to Time Stamp a Digital Document” published by Stuart Haber and W. Scott Stornetta, but it was first implemented by Satoshi Nakamoto in 2008 with the use of bitcoin and the internet.

Bitcoin has a fixed limit of 21 million coins, a hallmark of its supposed hedge against inflation, but Nakamoto also created the bitcoin as divisible by 100 million pieces called satoshis. The SHA-256 hash function that bitcoin implements is based on the hashcash design created by Adam Back in 1997 which was originally meant to limit email spam and denial of service attacks The idea here being that the time and processing power it takes to go through that proof of work system is not worth it. Of course, we will be discussing what that much power use looks like for the environment and where it is currently being sourced. When it comes to mining bitcoin, the reward is cut in half roughly every four years, as it is right now the reward for mining a block is 6.25 bitcoins. Currently, bitcoin is valued at roughly $51,000, but this could change, because of its volatility.

### NFTs

NFT stands for Non-Fungible Token. To be fungible means that something can be replaced by another equal part, like Fiat currency or bitcoin, where any coin can be used to pay a debt of that coin’s worth. Every NFT, however, is unique.

Some content—a physical object, a game artifact, a photo, or a video—is ‘minted’ to put it on the blockchain with some of the currency of whatever blockchain it is on. The first blockchain to implement NFTs was Ethereum, but some others promote their sale now. You do not actually buy the piece of art or the video or whatever is attached to the NFT you are paying for, you just buy the token. Storing the actual files on the blockchain would be too unwieldy, so you buy the token as a sort of certificate of ownership (comparable to a receipt) and a link to the file is put on the blockchain.

One issue with this system is that since the link on your receipt is the only proof of your ownership, if the website hosting the file goes down or your file atrophies, your NFT is functionally useless. Now you have a receipt documented on a blockchain as a record of buying something that essentially no longer exists.

Another problem with buying NFTs: the files themselves work exactly like any other digital file, and you can save and distribute them with the same level of ease regardless of whether you own them on the blockchain.

# Ethical Dilemmas

### NFTs and Art

Despite claims to the contrary, NFTs are not particularly profitable for artists trying to sell their work. Many NFT series are generative, meaning many unique images can be generated with little effort by mixing and matching features or characteristics, and rarity is artificially created that way. Even so, the mode price for NFTs in what should have been a particularly profitable moment was actually $100 or less, and more than half were under $200. The reported high average prices are hiked up by a few wildly expensive outliers.

Even worse, it is not even necessarily the artists selling their own work. Because the minted token is the only proof of ownership, anyone with the coins to mint something can do so and then sell it. Buying that NFT would not give the buyer ownership over any of the actual artwork, but they would own the token of the URL to, for example, the tweet where the art was first posted. Now, without the artist’s knowledge, a link to their tweet would be up on a blockchain, and they would have gotten none of the benefits of that sale.

### Environmental Impacts

With the climate crisis already upon us, the mining and transactions of cryptocurrency only speed up the process. Bitcoin’s proof-of-work system is particularly harmful on this front. An ongoing study at the University of Cambridge found that Bitcoin has used around 117 TWh per year - roughly the same as the Netherlands and Argentina. Given the relatively low amount of people that are actually partaking in the cryptocurrency, the environmental damage that it causes is disproportionately high. Virtually none of the energy used is renewable, as it would only increase the cost for an already volatile currency. The crypto climate accord is an initiative to get cryptocurrencies to switch to all renewable energy, though Bitcoin remains off of the list of signatories.

With the incredibly difficult proof of work system, hardware systems are being run through faster - especially those at “mining farms.” While an excessive amount of fossil fuels are being used to keep up with the energy demand, older hardware needs to be replaced to keep up with mining. Roughly, mining hardware needs to be replaced every year or so. This causes a higher amount of e-waste as the need to replace hardware rises with the more difficult problem solving.

### Other Ethical Dilemmas

Implementing an inherently socialist structure of currency in a capitalist dominated global economy is made possible through heavy exploitation of the system. In theory, the workers hold the means of production. The distribution, however, is heavily in favor of those who have the means to own a high amount of resources. The first system to solve the hash wins the bitcoin, and the more systems you own, the higher your chances are of winning. If the end goal of a cryptocurrency is to become a legitimate form of an exchange for goods and services, it has to be stable enough for the working class to sustain themselves with.

The ultimate goal of those who invest in cryptocurrency isn’t legitimacy of the system, but rather the prospect of an easy profit. To ask the working class to invest their money into a system that is so volatile in which they may very well lose everything is inherently unethical. But that’s exactly what crypto needs to keep thriving; The more people that buy into the system, the higher the value of the coin. The higher the value of the coin, the more difficult it is to mine.

With the anonymity of crypto, it begs the question of how much illegal activity can be overlooked in order to keep that benefit. For those in favor, it’s about as harmful as cash and other forms of physical currency. Cash transactions are anonymous, and it can even be wired to reach other areas of the world. However, cash is traceable; crypto isn’t.

# Implementation

It turns out that it is rather difficult to come up with a cryptocurrency without all the ethical issues while keeping all the reasons they have become popular.

Many of the current consensus algorithms are a test of proof of resources, in a couple of different iterations: proof of work is proof of most resources of or to obtain hardware, proof of stake is proof of resources to purchase the most cryptocurrency, proof of time is proof of the resource of time and the ability to take time off from other tasks, and proof of capacity is blatantly just how much space you have.

Considering that, we tried to find a way to reverse the proof of resources and instead prioritize users with fewer resources.

# Results

Our system ended up looking the most like proof of burn, but instead of making some proportion of coins completely unreachable by anyone, we have them going somewhere beneficial to those in need.

### CamooksyCoin/BrivamiCoin

The best way we thought up to accomplish that goal is by proof of donation or proof of charitable giving. To implement this you lose a lot of the reasons people like existing cryptocurrencies, like the anonymity, the ability to pay to win, and even the lack of central power, to an extent.

The gist of our proposed system is as follows: each individual user gets one account and a small starting number of coins. Then, they can either donate those coins to a random pre-approved charity or cash them out at any time. Each donation counts as an entry in a lottery for more coins, and the coins are worth more when donated versus cashed out, at a rate of 100:1, using cash-out fees to make that rate feasible. The list of approved charities will be compiled by us, the creators, but each day a random subsection of the master list of charities will be posted. The donations that day will go to a random organization on that smaller list. This will remove the bias of direct donation, though users can still see the possible organizations that their donations might go to on any given day and decide whether to opt-in or not.

The hash for the blockchain is arbitrarily easy to demotivate the resource hoarding implicitly encouraged in other cryptocurrencies.

The one account per person rather than per computer rule is to avoid the possibility of someone with a thousand computers making an account on each of them and immediately cashing out the starting coins. It would be hard to know how to enforce that, though: with social security number checks, or biometrics like requiring a fingerprint to sign up, that information would have to be stored somewhere and associated with an account on the blockchain. Securing that information would become a problem of similar complexity to our goal of creating a theoretically ethical cryptocurrency. Alternatively, we could just ask users very nicely in the Terms of Service not to make multiple accounts, but that would be quite easy to attack. Malicious users would theoretically be perfectly willing to break the terms of service. The lack of security on the initial incentivizing starting coins threatens the liveness of the system. In this model, as opposed to other cryptocurrency models, the amount of money someone can make isn’t physically limited by their resources, so there must be some enforcement so as not to completely devalue the currency.

The possible names for this theoretical cryptocurrency are two different combinations of the authors’ first names. Some contention has arisen as to which is the best name.

### OuroborosCoin

Another option is that rather than organizations that we the founders consider the most beneficial and worthy, we choose exclusively anti-crypto and/or anti-NFT organizations. If we were to take that direction, this product would fund its own destruction, and hopefully, take down all other cryptocurrencies with it.

The name OuroborosCoin comes from the ancient symbol Ouroboros, a snake eating its own tail.

# Conclusion

We presented on the history, methods, and implementation of blockchain technology, specifically the hashing and consensus elements, as well as bitcoin and NFTs. We introduced the ethical dilemmas of the technology and its uses, and proposed a more ethical alternative. Our alternative has several flaws, which might be improved with more collaborative thinking. Otherwise, this serves as evidence for the impossibility of an ethical use of blockchain technology.

# References

Antsstyle. “Why Nfts Are Bad: The Long Version.” Medium, Medium, 2 Nov. 2021, <https://antsstyle.medium.com/why-nfts-are-bad-the-long-version-2c16dae145e2>.

Back, Adam. Hashcash -A Denial of Service Counter-Measure. 1 Aug. 2002, <http://www.hashcash.org/papers/hashcash.pdf>.

“Blockchain.com Explorer: BTC: ETH: BCH.” Blockchain Explorer - Search the Blockchain | BTC | ETH | BCH, <https://www.blockchain.com/explorer>.

“Cambridge Bitcoin Electricity Consumption Index.” University of Cambridge Centre for Alternative Finance, 2021,

<https://ccaf.io/cbeci/faq>.

Haber, Stuart, and W. Scott Stornetta. How to Time Stamp a Digital Document. 1991, <https://link.springer.com/content/pdf/10.1007%2FBF00196791.pdf>.

Kinsella, Eileen. Think Everyone Is Getting Rich Off NFTs? Most Sales Are Actually $200 or Less, According to One Report. Artnet News, 29 Apr. 2021, <https://news.artnet.com/market/think-artists-are-getting-rich-off-nfts-think-again-1962752>.

Martin, Katie & Billy Nauman. “Bitcoin’s growing energy problem: ‘It’s a dirty currency,’” Financial Times, May 19 2021,

<https://www.ft.com/content/1aecb2db-8f61-427c-a413-3b929291c8ac>.

Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 31 Oct. 2008, <https://bitcoin.org/bitcoin.pdf>.

Purtill, James. Artists report discovering their work is being stolen and sold as NFTs. ABC Science, 15 Mar. 2021, <https://www.abc.net.au/news/science/2021-03-16/nfts-artists-report-their-work-is-being-stolen-and-sold/13249408>.

Stubbs, Sam. “Is it ethical to invest in cryptocurrency?” Stuff, 12 Oct. 2021,

<https://www.stuff.co.nz/business/opinion-analysis/126635309/is-it-ethical-to-invest-in-cryptocurrency>.

Vishal Chawla, et al. “What Are the Top Blockchain Consensus Algorithms?” Analytics India Magazine, 20 Jan. 2020, <https://analyticsindiamag.com/blockchain-consensus-algorithms/>