We didn’t cover NFTs a lot in class, so I’m here to tell you that they’re just as whack as the rest of it.

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

The way NFTs work is that someone takes some sort of content—a physical object, a game artifact, a photo, or a video—and ‘mints’ it to put it on the blockchain. This actually requires some of the currency of whatever blockchain you’re using—the first one to implement NFTs was Ethereum, but the Bitcoin Cash blockchain and a few others promote their sale now.

Actually, though, you don’t buy the piece of art or the video or whatever NFT you’re 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 (or like, a receipt) and you get a link to the thing if it’s a digital file. There are a couple of problems with this.

One pretty hilarious problem is that, since the link on your receipt is the only thing proving your ownership, if the website hosting the file goes down or takes your file down, your NFT is functionally useless, because now you have a receipt for something that no longer exists. We’ll get to the other problem in a second.

A lot of artists have turned to NFTs to try and make more money off their work since they took a hit to their sales in the pandemic. Kings of Leon is actually selling their latest album as an NFT. Great for artists, right? Look at that ugly pixel monstrosity, whoever made that is probably really proud of themselves for selling for $7.6 million dollars, right?

Well, no, because the CryptoPunk series is generative (as are a lot of the NFT series), meaning they’re a bunch of mix-and-match auto-generated images. This one was only worth so much because it was a rare version in a batch of 10,000. It was one of nine blue ones. Obviously highly desirable.

SLIDE

But also it turns out that the mode price for NFTs in what should have been a particularly profitable moment, right after a piece sold for $69 million and made headlines, was actually $100 or less, and more than half were under $200, so the average prices are hiked up by a few wildly expensive outliers.

What’s even worse is that it’s not even necessarily the artists selling their own work! Because the minted token is what’s sold as proof of ownership, anyone with the coins to mint something can do it and then sell it. For example, my friend could post some art on twitter, and then someone could tag a bot account that automatically mints that content and puts it up for sale. I could buy that token, assuming my friend put it up themselves. Now, without their knowledge, a link to their tweet would be up on a blockchain, and they would have gotten none of the benefits of that sale.

Buying that NFT wouldn’t give me ownership over their actual artwork, but I would own the TOKEN of the URL to the TWEET where they first posted it. If that sounds like it makes no sense and nobody would do it, you’ve got the concept.

This brings us to the other problem with buying NFTs: they work exactly like any other digital file, and you can right-click save-as any image or video even if you don’t own it on the blockchain.

So if you don’t know for sure the original artist is the one selling, or there’s no point to buying one, there’s no exclusivity in it, the whole point is paying exorbitant amounts of money just to show that you can, and that you hate the environment, I assume.

ETHICAL USE OF THE BLOCKCHAIN

So it turns out that it’s really hard to come up with a cryptocurrency without all the ethical issues. Since a lot of the current system is really a proof of resources scheme in a couple of different iterations—work (hardware), stake (ability to buy out everyone else) or time (the ability to take time off from other tasks) and proof of capacity is LITERALLY just how much space you have—we tried to find a way to reverse that, and instead prioritize users with fewer resources. It ended up looking more like proof of burn, but instead of throwing it into the void we put it somewhere else!

The way we thought up to do that 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 lack of central power, to an extent.

The gist of it is that each person gets one account and a small starting number of coins. Then, they can donate those coins to a random pre-approved charity, and each donation counts as an entry in a lottery for more coins. The list of approved charities will be compiled by us, the creators, but each day a random subsection of the list will be posted, and the donations will go to a random organization on that list. This will remove some of the possibility of bias in donation, though users can still see the possibilities that their donations could go to on any given day and decide whether to opt in or not. The donations are worth 100 times as much when donated versus cashed out.

The hash for the blockchain is arbitrarily easy, and there’s no proof of work, so it should demotivate the resource hoarding and overuse of 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’s hard to know how to enforce that, though: with social security number checks, or requiring a fingerprint to sign up, somebody would have to keep that information and then securing that would become a whole other problem. We could just ask them very nicely in the Terms of Service not to make multiple accounts. In this model, however, the amount of money someone can make isn’t physically limited by their resources, so there has to be some way of enforcing a limit.

SLIDE

So! What do you think?