oeis and a nft standard

May 23, 2022

Abstract

There are people that have mined combinatorial objects instead of bitcoin. Not knowing that bitcoin was being mined, and assuming that btc was just another scam. This writeup goes to the hosts of the podcast "cryptocafé".

Let alice be on the park and seeing bob, she turns to carol and says : "did you know that he owns the largest prime number in the world?". As carol never liked numbers that much she wonders how that could be. So bob has some connections and in fact owns large datacenters. He used these datacenters to mine the largest prime number known to humanity at a certain point in time `t`. After that he created a little file, that has :

A `string id` of this standard.
The `sequence number` of oeis, the hash of that number, the hash of the index within that list of numbers, and an extra hash of data that *could* be necessary.

Now anyone could have this file. It could be leaked to oscar for example or bob could even make it public on the internet. In this way anyone would *own* that number. However if bob would have hashed that file and placed it on a blockchain, then he would have proved that it was him that found the number `first`. Note that anyone could claim having put that hash in that block. Therefore bob needs to also be able to sign the change address of the transaction that contains that `op_return`, at any time. Thus proving that only he owns that prime number. However bob lives in a little town and they have a cryptocurrency running there wich has a fairly low overall hashrate, compared to the energy that is spent on btc. Not only that he first placed that `op_return` on his personal blockchain that he is running on 10 computers at home, a testnet where he is trying out a new scaling mechanism. Now for alice, if bob would turn to her and show her after a dinner at his house, trying to impress her :"look you see this hash? That proves that i found this prime number at a time `t` !" Clearly alice would start to doubt bob (in other ways too, let's stay in context), because he could have gotten that prime number from somewhere else, from some `outside` source. So following this line of thought if the prime number would be on a blockchain that is used worldwide then alice would be more impressed. However if it's only some shitcoin she would turn and say :"ah come on there are only also 33 computers running on that chain! You probably co-opted also that..." However if bob puts that hash on the heaviest chain then alice would have no more arguments and would clearly fall in his arms with total adoration. For he owns the largest prime number in the world (assuming she is a gold digger). In this case it is more like :"not your keys not your nft". The standard here is important because it needs to be accepted as such. Oscar could, one week after time `t`, place a new hash of a diferent file format that proves ownership of that prime. So in that case which file format would be accepted? This needs therefore a *standard*.
Owning something means that it should also be possible to sell it. In this case that `op_return` can be sold only by that change address. A new transaction is done from that change address to the new owner of that nft. The nft itself is an `op_return`, that contains a hash. And the transaction therefore has one input and one output. Where the input is the change address from the previous owner, and the current change address belongs to the current owner. Now the amount in such a change address may become dust and therefore making the nft stuck, not being able to be sold again. This is, the change address has exactly 0 sats or not enough to pay the fees for the next transaction. Before this is the case, a second input must be included in the transaction to fund that change address. There needs to be a unidirectional chain of transactions, each of wich contain the same `op_return`, that transfers the ownership of that nft in a non ambiguos way. If the nft is on an output address that only has dust, then the nft dies. This is bad because then it can only be sold by exchange of the private keys of it's address.
There are therefore 3 requesites for a nft to have any value whatsoever :

1. A standard.
2. It must be on the heaviest chain.
3. Only the first occurrence of the nft counts. If the nft gets sold, only the last within that chain of transactions counts.

Of course there could be multiple change addresses each of wich could then own with the same property

rights that nft. That clique of people all own the largest prime number in the world. And any one of them would be able to sell it. Also if one btc transaction allows for more than one data field, then it could contain multiple `op_return`'s, one for every nft. Also it could be possible to strictly concatenate multiple such standard file hashes into one merkle root hash. In other words a script could be run, that goes through all the lists of numbers of the http://oeis.org/, gets the last number in each sequence, and makes a nft out of it. Then all of those nft's get joined in a merkle tree and only the root is placed in a transaction.

On the other hand it so happens that nowadays there are nft's that don't follow any standard. More strangely lets take a work of art, a .jpeg file for example. That jpeg gets hashed and placed on a blockchain. Now oscar comes along and changes one pixel in that work of art, hashes it and places it on a blockchain. Oscar now claims that it was him who made the work of art and that the previous first occurence of that jpeg is false, fake not the original! How can this make any sense whatsoever? The nft's that belong to these networks only have value because the free market says so, and there are people trying to trade them as collectibles. Furthermore the nft's might have some extra utility. However if a work of art is placed in a blockchain as a nft then there must be one central authority that makes a standard for such a purpose, say the *global open sotheby's*. If this is not the case, then jpegs as work of art, in blockchains are utterly useless.
The last argument in favor of such a model for nft's is that the hash for the extra data can contain works of art related to finding such numbers. The sequence itself of numbers could be plotted in a nice way, or if it is a graph it could be presented in some *fancy* way.