Bitcoin - Time Travelling Energy

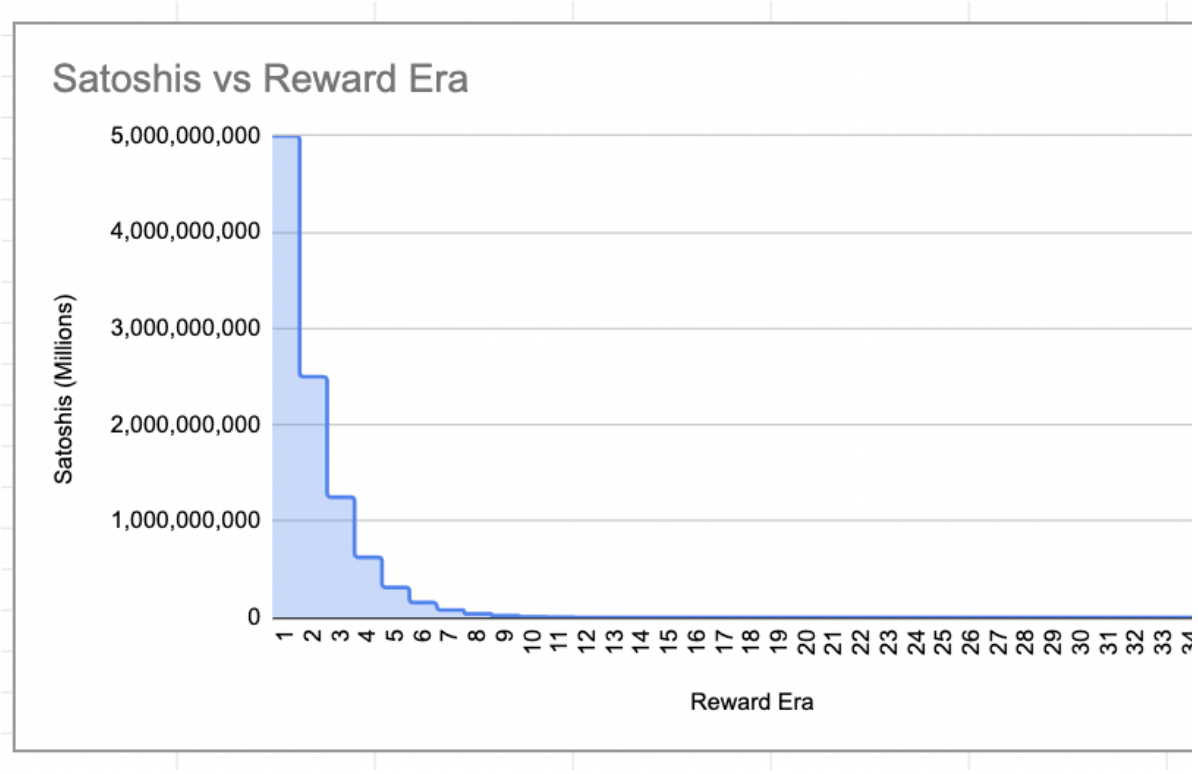
QmSkBQmja48hZ5hmJzm5Vasdg846VsMUipKLE56PcVBb1J

Our timechain is #bitcoin and our Energy Rewards are new coins introduced to the protocol. Mined by electricity. We commonly refer to this as proof of work. Because that's quite literally what it is :) No technical jargon, nothing more fancy than what it sounds like. You diet and lose 10kg's, that's proof of work. You step in a puddle, and your socks are soaked, that's proof of work. Right now, Bitcoin is the heaviest piece of work, that humanity has ever been capable of making. It's seemingly alien just how gorgeous this is architected. With the most elegant flow of behaviours and incentives, concocted into a masterpiece of work. But good things can't last forever. Or can they?

Analysing Bitcoins incentive model, it leaves some fascinating observations, and interpretations that can take humanity far beyond the realms of sound money, and into a Type 3 civilization. Lets break this down for a second and walk through the networks incentives for introducing new energy into the system. When more energy is introduced to the system (this is done by "mining") the system rewards that behaviour with a predefined amount based on the blockheight which was mined.

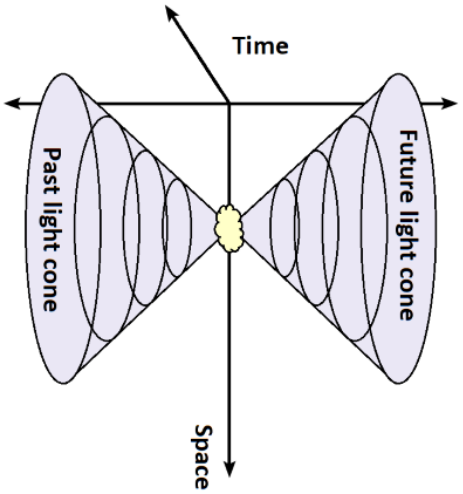
Reward Era	Satoshis	Blockheight
1	5,000,000,000	210000
2	2,500,000,000	420000
3	1,250,000,000	630000
4	625,000,000	840000
5	312,500,000	1050000
6	156,250,000	1260000
7	78,125,000	1470000
8	39,062,500	1680000
9	19,531,250	1890000
10	9,765,625	2100000
11	4,882,813	2310000
12	2,441,406	2520000
13	1,220,703	2730000
14	610,352	2940000
15	305,176	3150000
16	152,588	3360000
17	76,294	3570000
18	38,147	3780000
19	19,073	3990000
20	9,537	4200000
21	4,768	4410000
22	2,384	4620000
23	1,192	4830000
24	596	5040000
25	298	5250000
26	149	5460000
27	75	5670000
28	37	5880000
29	19	6090000
30	9	6300000
31	5	6510000
32	2	6720000
33	1	6930000
34	0	7139999

Nothing too fancy, we see that it starts with a reward of 5 Billion Satoshis (50 Bitcoin) and every 210,000 blocks it winds its way all the way to 0 Satoshis per block. Then what? There is no incentive to produce any more blocks. So the block reward era 34, ends at block 7,139,999. Block 7,140,000 would have to have half of 0 as the block reward if it were to continue the pattern.



Lets take a second to think about this. Think about how valuable a single Satoshi will be in the future when it is the sole block reward. It will represent an absolutely gargantuan amount of energy. Even if we assumed the networks energy consumption never grew, it still means that it would be beyond astronomical at that point in time because 1 satoshi would represent such an unbelievable amount of electricity. The reality is though, the network will grow exponentially, and the amount of electricity represented by a Satoshi will be almost all known usable energy known to humanity. An energy blackhole. If we consider our reward graph, more like an energy conic section, the representations are no different.

Imagine each ring on our cones to be a reward cycle. Visually, it would look like the below.



Just like we see in Einsteins special relativity with wormholes and energy, there's no difference here. Heavy sources of energy converging to single points of observation.

Thinking about the amount of energy over time, we know that future blocks will carry more energy over time, if the network is to remain unchanged as if it is valuable today for its immutability, then it will always be more valuable tomorrow if its immutability is unchanged. This is because immutability is a compounding property orientated solely around energy over time. The block size, the total number of coins, and the issuance cycle are the three properties which never change. Additional upgrades that don't amend these properties preserve immutability so should be possible.

The Last Block Of The Last Energy Cycle

7,139,999 is a special number here. Because as a number itself, it is a prime number. It's the last prime number in this finite field size (measured in number of blocks). So we are using a prime number to represent this final entropy moment within our system. Because the system conditions change after this block. Deterministically and objectively for all observers within the system (aka participants making Satoshis move around on Bitcoin).

Lets analyse the root layers of the numerical values, and the significance they hold. For those unfamiliar, wikipedia defines digital roots as follows:

The digital root (also repeated digital sum) of a natural number in a given radix is the (single digit) value obtained by an iterative process of summing digits. This is important, because in information, this is the fastest path light can take, to represent this information in the smallest possible capacity. Lets think of this essay in terms of entropy, and how much entropy it produces. It means that the number 7139999 would become entangled with that, and the number *may* have significance. Much like we hear the number 21,000,000 and it immediately sparks a thought that we are thinking of bitcoin. So now we have all the entropy of this essay encoded into that number. Like a thought in our mind, it goes from "scenes" or snapshots. You see a red car, and that then takes you back to the first time you went in a car, and it was your aunties red car growing up (random example). The entropy thats encompassed with you "seeing a red car" is much more than just the red car. Well, the prime number in this context, 7139999 is a representation of this entropy in this writing, if that's making sense? Like how web pages have backlinks, it's sort of the same thing for your train of thought.

Digital Root Layer	Number	Is Prime
0	7,139,999	YES
1	7+1+3+9+9+9+9 = 47	YES
2	4+7=11	YES
3	1+1=2	YES

We can now draw an agreed significance on this number. It is the end of the current timechain as it stands today, and it's number and digital roots are prime numbers all the way to 0. Making these points geometrically related in any environment. These are points or thoughts to reference the number, and understand its significance.

What about block 7,140,000 then what happens?

An old wives tale surrounding a shortcoming in Bitcoins design. People believe that because the reward runs out, there is no solution available for longevity. We don't want to change the number of coins, because that is breaking its rules. Well, we first need to think, where do coins go? They're not leaving the protocol, they can't just get up and walk away. To solve the incentive model, my proposal is to follow the pattern outlined in thermodynamics for this.

In thermodynamics, we see this behaviour of colliding blocks within a phase space producing a predictable result based on the conservation of momentum and energy. I highly recommend watching this video

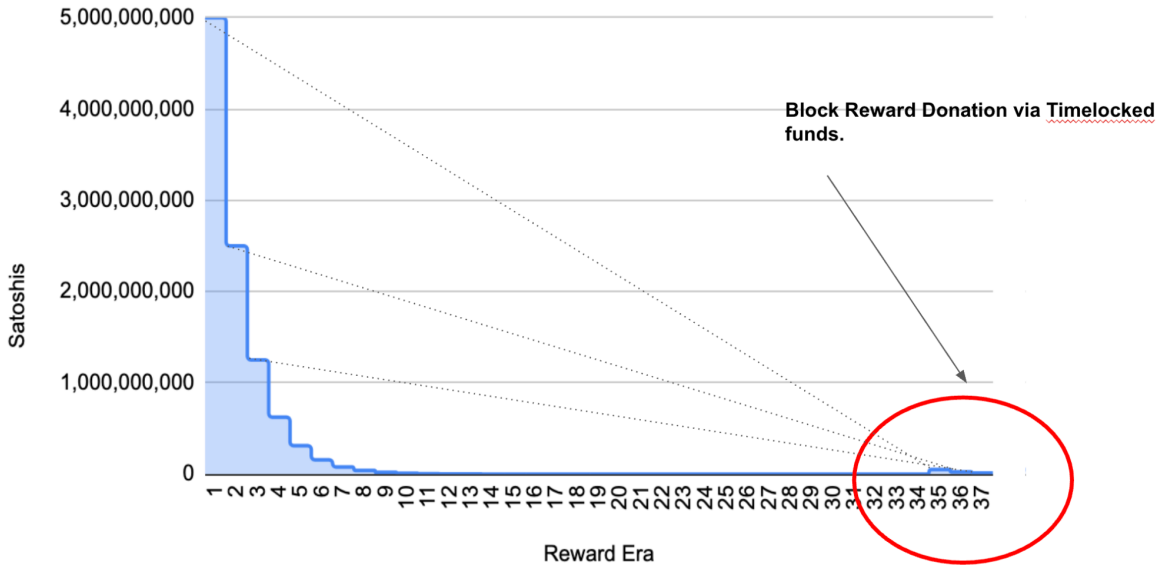
https://www.youtube.com/watch?v=jsYwFizhncE

At block 7,140,000 we follow the same count of blocks, but instead of the protocol rewarding more coins (which it can't, because it has run out by now), we plan today, the path we can take for donations to future civilizations.

Reward Era	Satoshis	Blockheight
1	5,000,000,000	210000
2	2,500,000,000	420000
3	1,250,000,000	630000
4	625,000,000	840000
5	312,500,000	1050000
6	156,250,000	1260000
7	78,125,000	1470000
8	39,062,500	1680000
9	19,531,250	1890000
10	9,765,625	2100000
11	4,882,813	2310000
12	2,441,406	2520000
13	1,220,703	2730000
14	610,352	2940000
15	305,176	3150000
16	152,588	3360000
17	76,294	3570000
18	38,147	3780000
19	19,073	3990000
20	9,537	4200000
21	4,768	4410000
22	2,384	4620000
23	1,192	4830000
24	596	5040000
25	298	5250000
26	149	5460000
27	75	5670000
28	37	5880000
29	19	6090000
30	9	6300000
31	5	6510000
32	2	6720000
33	1	6930000
34	0	7139999
35	50,000,000	7140000
36	25,000,000	7350000
37	12,500,000	7,560,000

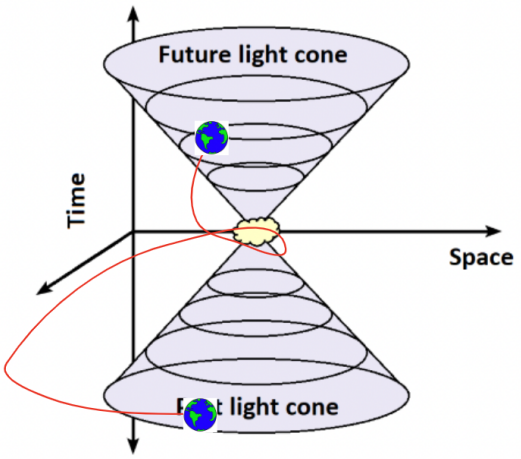
We have followed the same pattern for reward cycles, 210000 blocks, but we have reduced the reward down by 1:100

When a miner would've gotten 50 Bitcoins, they're now getting 50M Sats. Instead of 25 Bitcoin, they're getting 25M Sats, 12.5 Bitcoin becomes 12.5M Sats, and so on… But there's still a problem here. We don't have any more coins to give and we can't change it, otherwise we break the immutability. Instead, we achieve the same result in a different way.



So now our chart starts looking somewhat like this when we put the pieces together. We're sending coins into the future, from the past, in an effort to preserve the future. Kind of the opposite to fossil fuels. Because we're giving our fossil (the timelocked sats) to the future, on purpose. Like a map to an oil field that is thousands of years old, or buried treasure, this is no different.

Blockheight 7,140,000

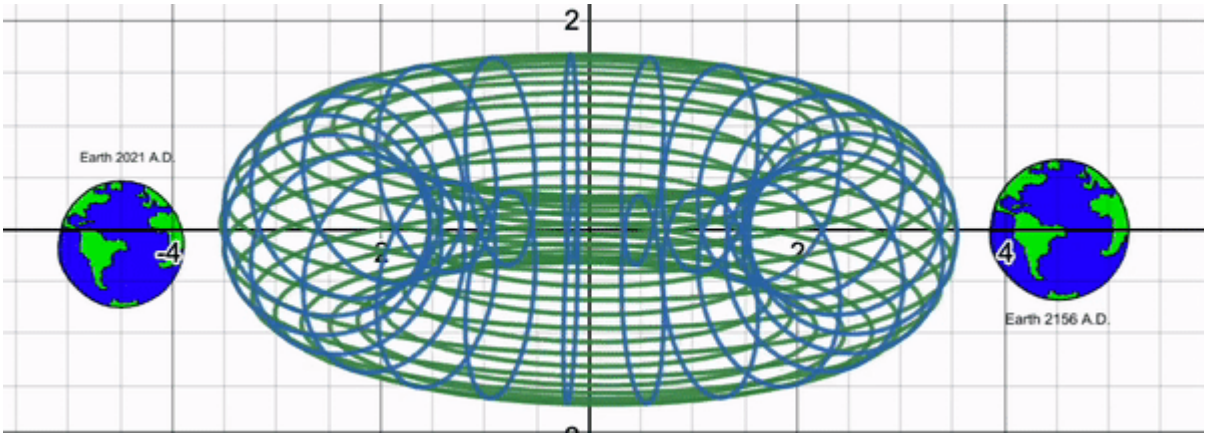


Blockheight 691,271

This is our wormhole. Pretty neat, right? Well, we're not sending a spaceship through it obviously, but theoretically we are sending something through it. What is that something? Well, it'll be a private key. Because if we know that something will exist at a point in the future, then we know it must exist the duration between now and that point in the future.

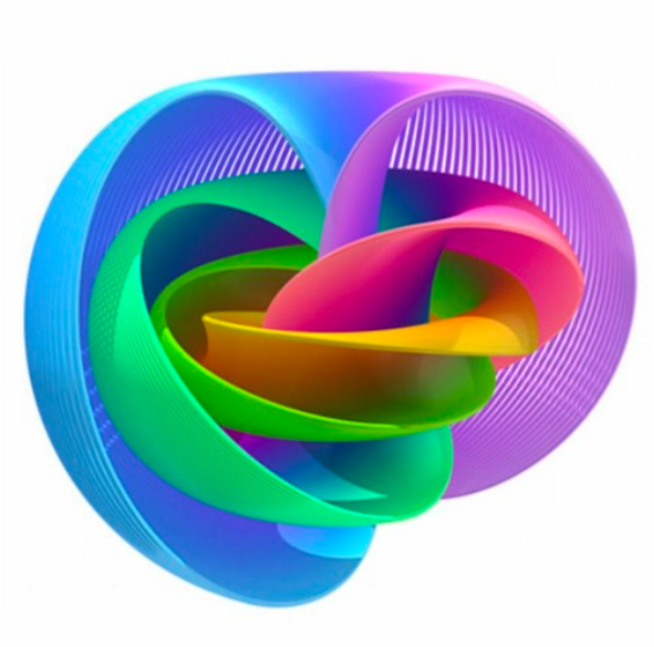
The wormhole is opened using a cryptographic key, secured by the energy of the network, and not the obscurity of the keys attributes. This way, we avoid the necessity for it to be secured through obfuscation, and behave the opposite. Meaning the more people that hold this key, the higher the probability for the network longevity it would result in. Due to the amount of energy it accesses.

Mathematically, we're trying to come out the other side to a world where it is many years into the future when this block would occur. Looking a lot like a wormhole, within a higher energy field. Basically a torus.



Source: <iframe src="https://www.desmos.com/calculator/hnbjrnopsp?embed" width="500" height="500" style="border: 1px solid #ccc" frameborder=0></iframe>

We see if this pattern repeats over time, we're left with a cyclical energy system, recycling its energy without emissions. Congrats to Eric Weinstein (made this graph), you're almost spot on!



Generate an OP_HODL address for our blockheights, and these are locked with a private key known to everyone.

Example HODL Address

https://blockstream.info/address/39QWbnkbcPFcrJFEB6yvVDc12eX5zqVt3y

This address was created using a private key, and locked the funds to be redeemable after block 7,140,000. So this is a reward for anyone around at the time that block arrives. It's only a reward if they're able to access this though. 50M Satoshis. The private key is:

"WIF": "(private key 5JMdSZpSr8TNBkqHZpq1fKPcCvyafE8uwhfeeZNF1YL8SAa9ZR9)",

"hex": "(private key 472ab2a7873f7703d94d90252a82988f766f520b002a9036fff663a0372e0003)",

"string":"(brain wallet plain text "1+1=3=Pi")"

You can see for yourself, don't need to take my word for it! Essentially this key is access to an astronomical amount of energy in the future.

Now imagine that same pattern, for every block into the future… Because it is 1:100 of the block reward, it means that it would require a total of 210,000 bitcoins to replicate the block reward in this way. Functioning like each block containing its own unique UTXO or more recently referred to as NFT's.

We lock coins following the same pattern into the next halving, which would be block 7,350,000 which using this private key, to derive the public key, and the hodl address, it would come out as the following 3ALzRjackuKZYPsDZ75KSCNzPYcSWSvjVM. So it sets the expected behaviour for that reward era.

Repeating the process, we goto the next “halving”, which would be 7,560,000 3AKSGQKTgXpHTj1qD69xX8BUkEPL4ozMSe. So we’ve got a 1:100 relationship with the previous cycles, but now we allocate a public reward to keep the network going. Overall this is investing 1% of the network, in order to keep the network going indefinitely for the rest of history. Sort of like, preparing an energy recycling plan, but for a problem 100+ years away. Whatever civilization looks like at that point in time, it’s highly likely they have solutions to very very hard problems in mathematics, and quantum systems.

Meaning, if we can donate energy into the future, then it is likely the last piece of the puzzle they need to operate large scale machines requiring infinite energy. Having an energy system that is perpetually recycling based on the observed laws of thermodynamics in block collisions, can be an energy preservation system. If something exists and his immutable, then it can be used for others as clues or pointers to our civilization. Because we’re etching this information into this prime number for the future civilization to discover. Numbers are a universal canvas that everyone possesses, the only difference is the frequency (context) they’re observing it from. This private key for example, is a number that carries a lot of entropy, so it is valuable. If observing it from a numerical context, it’s the decimal number of the key.

This is the simplest explainer I can give and I put most of this work onto https://github.com/MikeD123/Energy