DoI-SMS: A Diffusion of Innovations based Subsidy Minting Schedule for Proof-of-Work Cryptocurrencies

October 2018
Version 1.1

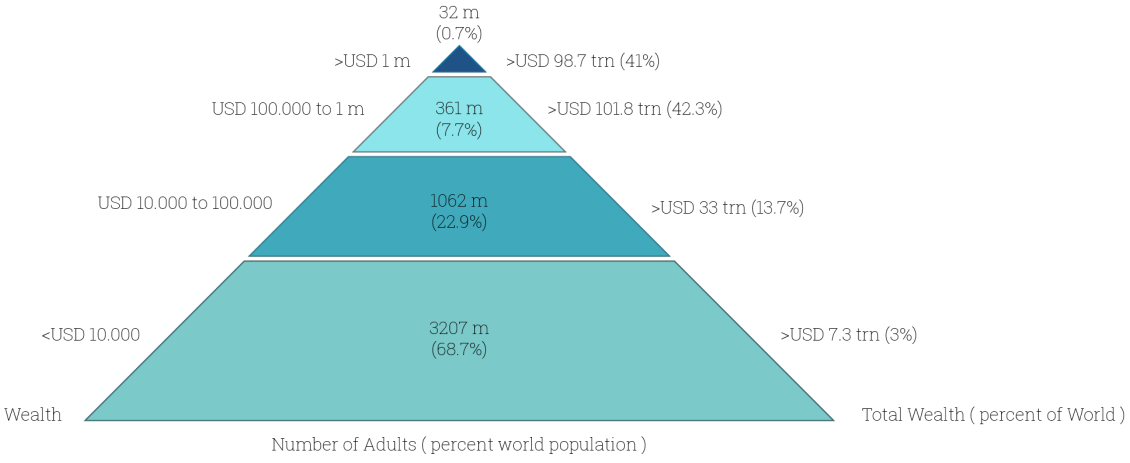
Janez TROBEVŠEK, Calem SMITH, Federico DE GONZALEZ-SOLER
Zerozed Project

www.zero-zed.com

Abstract. Fifty percent of the world's net wealth belongs to one percent of the population. The emergence of Cryptocurrency has brought about a rapid disruption across many industries but none more than Finance and Economics. Due to the inherent flaw in Bitcoin and by extension 99% of Blockchain based Distributed Ledger Technologies, "Crypto" has succumbed to the same fate as Fiat. Riddled with systemic issues and mass centralisation of supply. This is all due to the inflation model otherwise known as the "halving-mechanism", one of which no one has seemingly questioned. This paper seeks to solve these problems with an alternative model for incentive and inflation. In replacement to the standard halving-mechanism employed by the greater majority of Cryptocurrencies to-date, we demonstrate the modeling of an inflation schedule guided by the theory, Diffusion of Innovations.

1. Introduction

One of the greatest ethical and logistical challenges humanity has been forced to face is one that has not changed since the dawn of society itself. The fair and even distribution of wealth and power.



The Global Wealth Pyramid
Source Credit Suisse 2013 Global Wealth Report

We live in world where half of the world's net wealth belongs to 1% of the population. The emergence of Cryptocurrency has brought about a rapid disruption across many industries but none more than Finance and Economics. Due to the inherent flaw in Bitcoin and by extension 99% of Blockchain based Distributed Ledger Technologies, "Crypto" has succumbed to the same fate as Fiat based currencies. Riddled with systemic issues and mass centralisation. This is all due to the inflation model otherwise known as the "halving-mechanism", one of which no one has seemingly questioned.

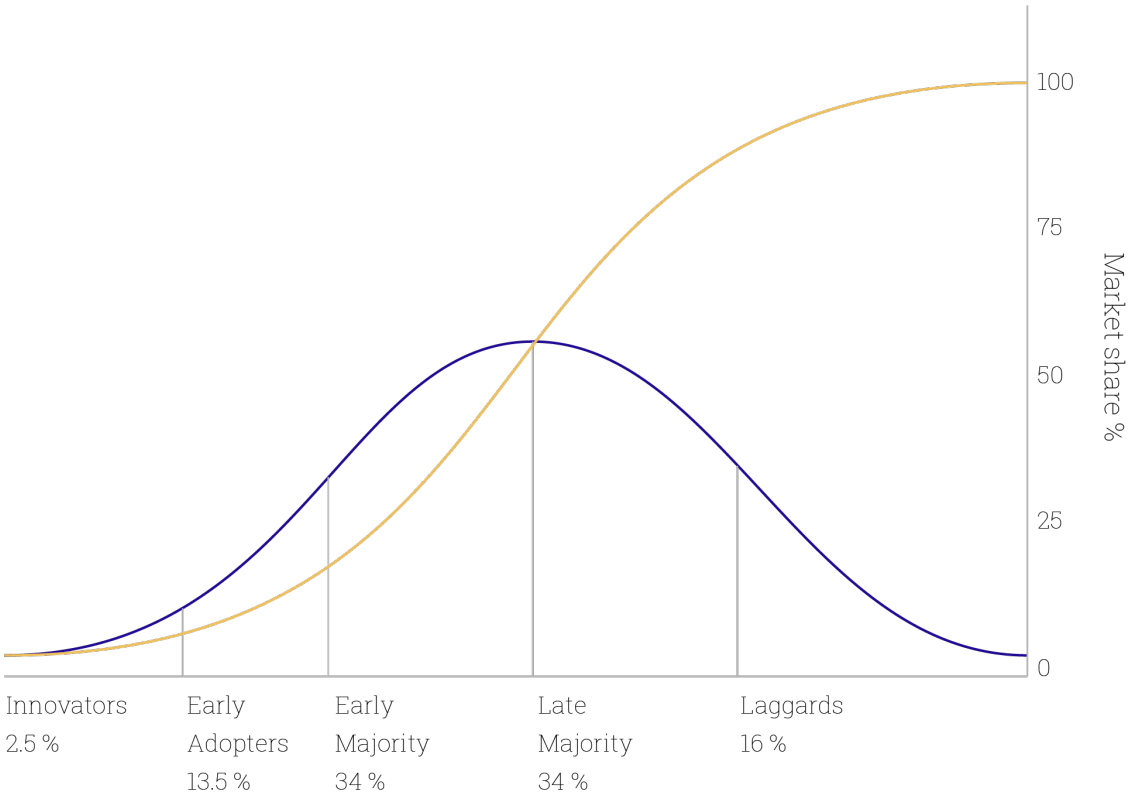
The core incentive model for current Crypto heavily relies on competition and scarcity, much like gold, giving the network and the coin itself intrinsic value which allows it to be priced based on supply and demand. This old model does not work in the new system that Satoshi was trying to achieve. Over 99% of the World’s population has yet to acquire any cryptocurrency at all. Roughly 80% of the supply has already been mined with the remaining 20% to take the next 100 years to produce, the bulk of which will be exhausted by 2033.

Bitcoin Inflation versus Time

Supply has been so tightly confined into the hands of the few, extreme price instability and supply centralisation has become the norm due to the onboarding supply bottleneck created by the mechanism itself. Bitcoin has failed to achieve diffusion but we can use this to bootstrap a radical and innovative Socioeconomic Ecosystem to organically and passively redistribute the World's wealth.

2. The Diffusion of Innovations

To quote Wikipedia, “The Diffusion of innovations is a theory that seeks to explain how, why, and at what rate new ideas and technology spread.” It describes the process in which new technologies are adopted and diffused across all markets and social groups within society. The process, rate and stages of the DoI are firmly understood and plays a major role in understanding how technology itself evolves over time [1].
There are 5 categories of adopters within the social system, each with their own traits. Innovators, Early Adopters, Early and then Late Majority finalised with the Laggards. All 5 process must occur for the technology to attain market saturation. Failed diffusion merely implies 100% adoption was never attained before succumbing to technical obsolescence [1].

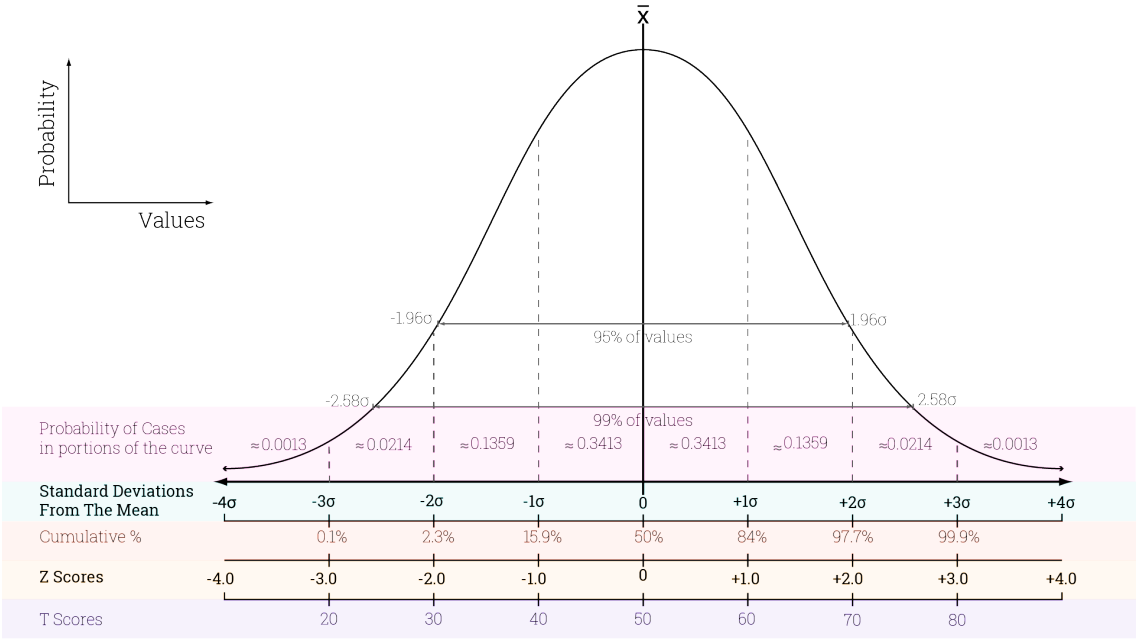


Diffusion of innovations

3. Normal Distribution

To quote Investopedia, “The normal distribution is a continuous probability distribution wherein values lie in a symmetrical fashion mostly situated around the mean [X].”

Achieving a normal distribution standard score of 0Z within a socioeconomic environment implies the middle class make up the greatest majority with the lower and upper classes of society are by far the lesser in prevalence.

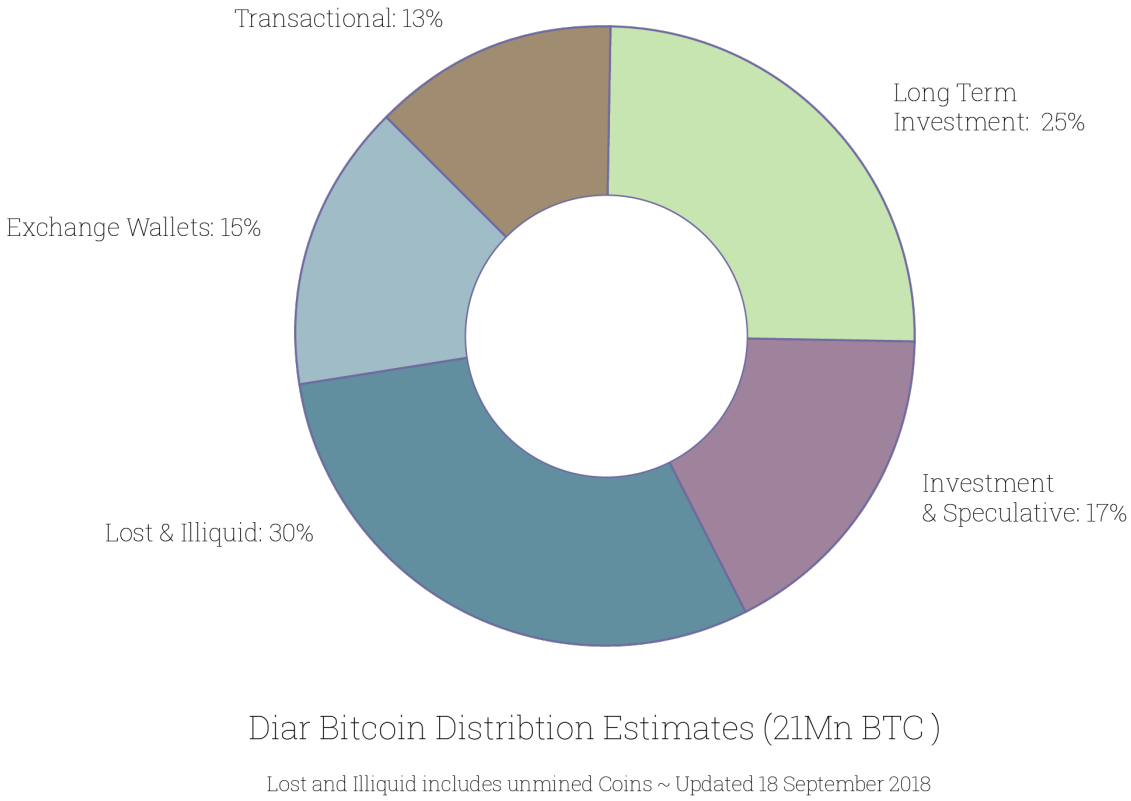


The Normal Distribution

4. Incentive

The core incentive model for current Crypto heavily relies on competition and scarcity, much like gold, giving the network and the coin itself intrinsic value which allows it to be priced based on supply and demand. This old model does not work in the new system that Satoshi was trying to achieve. Less than 1% of the World’s population has acquired any cryptocurrency at all. 80% of the supply has already been mined with the remaining 20% to take the next 100 years to produce, the bulk of which will be exhausted by 2033. Supply has been so tightly confined into the hands of the few, instability and wash trading has become the norm, leaving the world begging for Government intervention via ETFs and regulation.

Bitcoin has failed to achieve diffusion but we can use this to bootstrap a radical and innovative Socioeconomic Ecosystem to organically, passively and evenly re-distribute the global populations net wealth.



5. Altruistic Egoism

It is within the individuals best interests for the standard living of those below them be closer to the mean as this leads to slower population growth, the development of technology and the diffusion of innovations, further-spread education and the tools necessary to enable the individual. This in turn increases abundance and the broader accessibility of resources for all. Demand-side economies of scale such as Bitcoin, rely on network effect both direct and indirect whilst encouraging interoperability in order to achieve successful diffusion. Most of the elements come together but ultimately altruistic egoism falls apart under the current incentive model backing cryptocurrencies.
Due to Bitcoins competitive as opposed to collaborative incentive model we have now been presented with a sharding of the technology in what can only be described as a mad land grab for digital assets. HODL, the act of hoarding and not spending the crypto one acquires, is not only prevalent but encouraged and

completely endorsed by some of the most prominent figures in the space. Alongside FOMO, the fear of missing out, HODL is an attitude that is both a symptom and contributor to the many systemic issues heavily hindering adoption of cryptocurrency amongst the broader public of whom are yet to onboard.
Within a Diffusion of Innovations based inflation model, no one misses the boat. The earliest of adopters are still rewarded whilst maintaining fairness, collaboration and sharing in the system. When inflation grows in proportion to the amount users on a network, a close-to-optimal balance of supply and demand can be met ensuring abundance to stimulate growth whilst still factoring in the intrinsic value of scarcity.

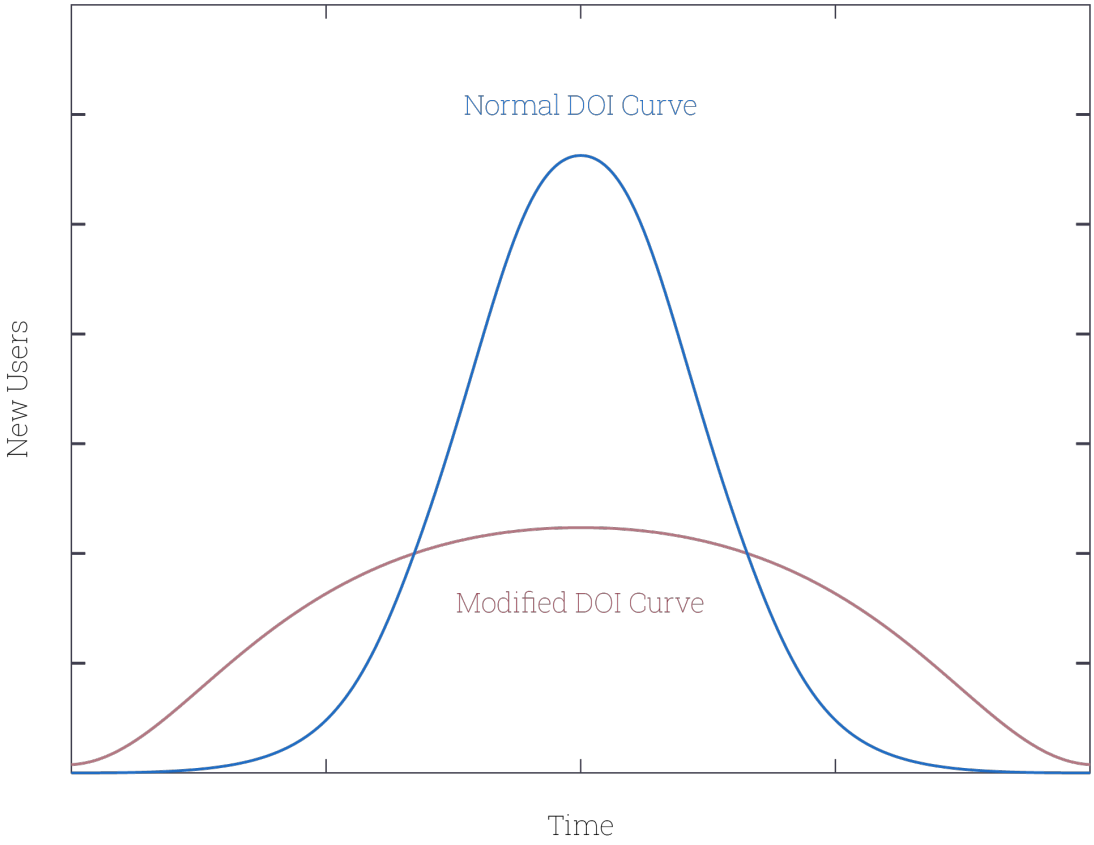
6. Process

We seeked an alternative to the standard block-halving mechanism employed by the majority of Cryptocurrencies in order to break away from the ties to not only the US Dollars inflation rate but also the supply centralising nature of Bitcoins halving schedule.
By utilising the Diffusion of Innovations to base an inflation model, along with an industry supported tried and true mining algorithm as well as cross-chain transactions via Atomic Swaps, a potential now exists to solve a long time challenge surrounding not just volatility but how to achieve successful diffusion whilst maintaining the normal distribution with a standard Z score of zero.
We theorised subsidy should be governed by findings regarding technological adoption rates and behaviors popularised in 1962 by Everett Rogers. We proposed to use what resembles a Logistic function, the Diffusion Of Innovations (DOI) sigmoid curve, as the baseline for controlling the inflation of supply. The initial failed model is pictured below.

“A number of gaussian curves are used there, to model the inflow of new people, but because the crypto field tends to expand faster and with steeper onsets and more leveled tops, we initially used a reciprocal-inverse exponentially modified gaussian curve. After a failed launch, we realized the beginning needs to be steeper, and that starting funds are mandatory to avoid initial price surge.” - Hiyatus

Taking into consideration Moore’s Law, we modified the standard DoI curve with a more “broader” middle and longer ramp-up in order to account for the initial difficulties which attribute to the lack of network effect Cryptocurrencies experience because of the competitive nature within the broader crypto economy and online social environments. Due to proof-of-work based cryptocurrencies needing as many miners as possible in order to stay secure and maintain consensus, the first leg of the modified DOI was made marginally steeper compared the final leg, in order to attract the critical number of miners required to secure the chain as viable as possible.

Based on other projects observed and worked on prior to the launch of x0z, our MVP demonstrating DoI-SMS, we made certain assumptions and extrapolated the rate of adoption that should be expected. From this we generated a set of integers and applied a recursive fitting algorithm to them. The result of our findings was a polynomial of 8th degree, which we termed 'DoI-SMS' and is the focus of this paper.



Project funding was generated as a product of securing initial supply via an 8% premine in order to prevent early hijacking as was experienced in one of a number of failed launches of x0z itself. This premine becomes heavily diluted and diffused within the first half of the initial inflation cycle of 60 months. This is a necessity because bootstrapping funding and network security via methods such as ICO breaks the incentive model due to the fact that this essentially creates additional supply outside of the inflation models control.

7. Algorithm

Converting to C code...

```
CAmount GetBlockSubsidy(int nHeight, const Consensus::Params& consensusParams)
{
        double nSubsidy = 1 * COIN;
         double nsubsidy_function = 0;
        double Xheight = 0;
         if (nHeight == 1)
        {
                nSubsidy = 2000000.0 * COIN; // Premine 2 Million
        }
        else if (nHeight > 1 && nHeight < 1274030) // Sets max block height
        {
                Xheight = nHeight * 0.0000038051750381;
                nsubsidy_function = ((3583.5719028332051*(pow(Xheight,8)))
                                        - (67959.212902381332*(pow(Xheight,7)))
                                        + (500144.30431838805*(pow(Xheight,6)))
                                        - (1806581.9194472283*(pow(Xheight,5)))
                                        + (3537339.4754780694*(pow(Xheight,4)))
                                        - (4712758.2800668897*(pow(Xheight,3)))
                                        + (4535015.6408610735*(pow(Xheight,2)))
                                        + (834937.06954081857*Xheight) + (1000845.7073113875));
                nSubsidy = ((floor((nsubsidy_function*(1.0/60000.0)*0.33757734955)*100.0))/100.0)
                * COIN; // our emission curve [no. of coins per block]
        }
        else
        {
                nSubsidy = 0 * COIN; // Coins cease production
        }

        return nSubsidy;
}
```

8. Inflation

The DoI-SMS system is being tested within the Cryptocurrency Zerozed (x0z), formerly known as "Crypt0z". Zerozed will undergo at least 2 inflation cycles. The first 60 month period will be used to gather the required information to retarget supply in order to continue a fair distribution to those still yet to onboard with cryptocurrency as a whole. As of block height 87294, the network is currently on target with a block reward of 9.23 and total supply of ~2,623,959 x0z.

Month	Coins	Height	Subsidy
1	2,126,860	21,600	6.17
2	2,268,500	43,200	6.98
3	2,430,030	64,800	8
4	2,615,390	86,400	9.18
5	2,827,630	108,000	10.49

https://umine.org/explorer/x0z?height=87294

9. Scaling

In order for a cryptocurrency operating on a DoI based inflation model to achieve successful diffusion, certain assumptions need to be made and a number of unknowns acknowledged.

Assumptions

- Less than 1% of the population has been on-boarded. Currently the safest estimate.
- Development of On-chain scaling continues to prove promising.
- Ray Kurtwhiles estimations on the Singularity remain true.
- Crypto adoption will continue to grow over the networks initial inflation cycle.

Unknowns

- The amount of time required for cryptocurrency to gain critical mass.
- Percentage of Total Market Capitalisation by the end of the initial inflation cycle.

"After the initial 5 year test, x0z will scale up with a new DOI cycle. Lasting longer and yielding a substantially higher number of coins to account for a continental adoption.
If all goes well, there will be a third DOI cycle for global x0z adoption. In this regard we can consider every new DOI cycle as a fractal of the previous - just like we can observe it in nature." – Hiyatus

10. Issues and Corrections

The presented implementation has a small potential for creating orphaned blocks. This is because the equation relies heavily on floating point operations and different systems will use varying numbers of them. In certain cases this, one per roughly every 150 blocks, may lead to two different values for that particular blocks subsidy and thus one of the two calculations will be orphaned based on Bitcoin's consensus rules.
While this does not pose a serious threat for x0z security, it does create an annoyance for the miners. To solve this in code, the function governing the x0z DOIsms and pertaining rules, should be rewritten using CBigNum instead of int64. With this, all miners with enough ram can handle the necessary number of floating points and will always obtain the same subsidy value without ever drifting. As the successor of DoI-SMS, the Zero Zed Algorithm, is in development, a substitute table is now currently in place to continue the planned supply rate without deviation.

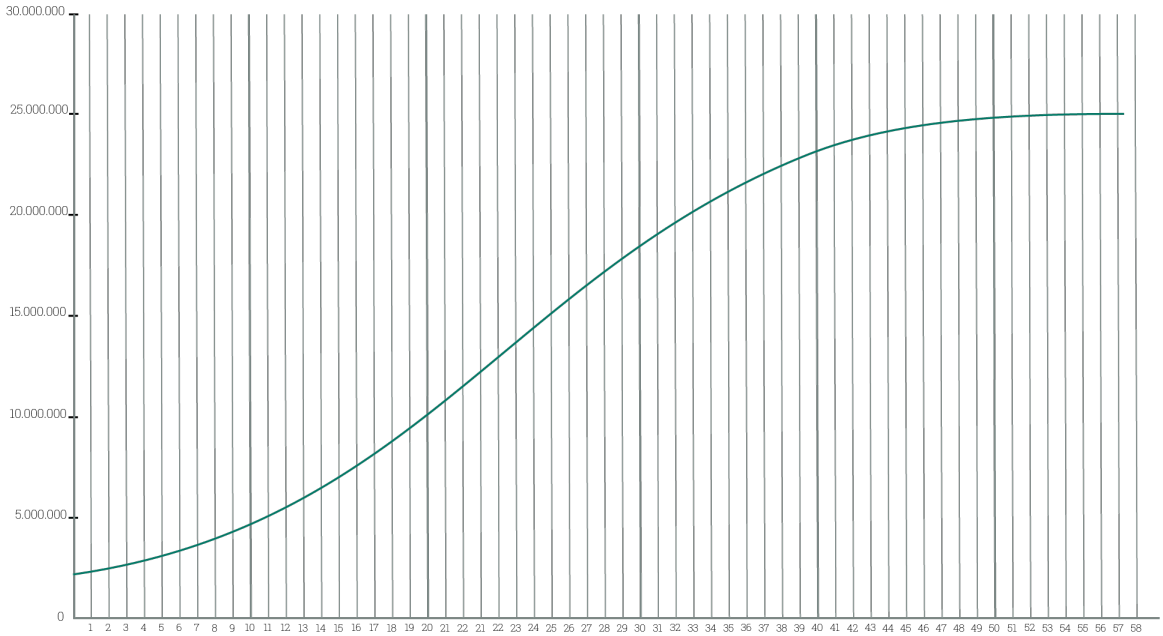
11. Trustless Financial Public Services

A potential opportunity to combine suitable technologies in order to create a Universal Basic Income for users of the network exists within a DoI-based Cryptocurrency. By utilising a fee algorithm controlled by on-chain contracts, alongside the Diffusion of Innovations as the basis for the coins release schedule, we can not only achieve a Universal Basic Income but other trustless public services like decentralised Superannuation and Universal Basic Healthcare for those utilising the system.

12. Conclusion

We have proposed an inflation model for Cryptocurrencies yet to launch, as well as coins existing today, to set or retarget subsidy schedules in order to follow a more sustainable and diffusion-viable incentive model. By utilising the Diffusion of Innovations we can establish the Normal Distribution within a socioeconomic environment and the Zerozed team have set out to prove this via bootstrapping a brave new Cryptocurrency with our MVP, x0z.
The Zerozed team will endeavour to contribute and assist with broader crypto innovations and interoperability in order to provide all the necessary conditions which provide the best chance of survival within the ever evolving space. If proven successful, the Zerozed project is expected to thrive well beyond the initial inflation cycle and is set to bring to light information that will assist the industry as a whole, in turn gaining broader acceptance and diffusion of Cryptocurrencies and Distributed Ledger Technologies throughout society.

Zerozed (x0z) Initial Inflation Schedule



Month	Coins	Height	Subsidy
1	2,126,860	21,600	6.17
2	2,268,500	43,200	6.98
3	2,430,030	64,800	8
4	2,615,390	86,400	9.18
5	2,827,630	108,000	10.49
6	3,069,110	129,600	11.89
7	3,341,650	151,200	13.36
8	3,646,630	172,800	14.89
9	3,985,060	194,400	16.45
10	4,357,640	216,000	18.05
11	4,764,740	237,600	19.65
12	5,206,440	259,200	21.25
13	5,682,520	280,800	22.83
14	6,192,420	302,400	24.38
15	6,735,240	324,000	25.87
16	7,309,740	345,600	27.31
17	7,914,300	367,200	28.66
18	8,546,940	388,800	29.9
19	9,205,290	410,400	31.03
20	9,886,640	432,000	32.03
21	10,587,900	453,600	32.88
22	11,305,700	475,200	33.56
23	12,036,400	496,800	34.06
24	12,775,900	518,400	34.38
25	13,520,300	540,000	34.51
26	14,265,300	561,600	34.43
27	15,006,400	583,200	34.16
28	15,739,500	604,800	33.68
29	16,460,200	626,400	33.01
30	17,164,300	648,000	32.16
31	17,848,000	669,600	31.12
32	18,507,500	691,200	29.92
33	19,139,600	712,800	28.58

34	19,741,200	734,400	27.11
35	20,309,900	756,000	25.53
36	20,843,500	777,600	23.87
37	21,340,600	799,200	22.15
38	21,800,100	820,800	20.4
39	22,221,700	842,400	18.63
40	22,605,200	864,000	16.89
41	22,951,400	885,600	15.18
42	23,261,300	907,200	13.52
43	23,536,200	928,800	11.95
44	23,778,200	950,400	10.47
45	23,989,400	972,000	9.1
46	24,172,100	993,600	7.84

47	24,329,000	1,015,200	6.71
48	24,462,700	1,036,800	5.69
49	24,575,700	1,058,400	4.79
50	24,670,500	1,080,000	4.01
51	24,749,500	1,101,600	3.32
52	24,814,700	1,123,200	2.73
53	24,867,900	1,144,800	2.21
54	24,910,500	1,166,400	1.75
55	24,943,700	1,188,000	1.33
56	24,968,400	1,209,600	0.96
57	24,985,400	1,231,200	0.62
58	24,995,600	1,252,800	0.33

References

Rogers, Everett (16 August 2003). Diffusion of Innovations, 5th Edition. Simon and Schuster. ISBN 978-0-7432-5823-4.

Article, The Normal Distribution
https://www.investopedia.com/terms/n/normaldistribution.asp

Image, Diar Bitcoin Distribution Estimates (21Mn BTC)
https://diar.co/volume-2-issue-37/

Block height 87294
http://18.217.129.225:3001/block/34f0eba87d8a4fb6b36416ed2f436a74b9dcd07e44a971b2172ca0840d910529