Yoonicoin: A Proof Of Personal Identity Cryptocurrency

Author: Stephen H
Date: 30th October 2021
Version: 1.1

Quotes

"*I am speaking on behalf of the 3,500,000,000 in this world who live on less than $4 a day and others in this country and world who are underappreciated, undervalued and taken advantage of by the upper class – so excuse me if I get a bit emotional.*" – from the paper: Extreme Capitalism And The Race To The Bottom – by Ronnie Moas – Philanthropist, Philosopher, Founder of Standpoint Capital and Cryptocurrency Commentator.

"*The free market is destroying itself. It's a massive failure on a scale which is very difficult to comprehend to many who are believers of it*" – Lucy Hogarth - Astrophysics PhD student and Extinction Rebellion member – interviewed in Tipping Points Podcast – March 2021.

"Another, more truthful, more frightening, conclusion we could reach then is that we should have a society where the resources enjoyed by the fruit-gobbling elite are shared around, and the privileges, including the fruit and veg, enjoyed by everybody" – Russel Brand talking about the UK's 5 A Day health campaign which encourages the population to eat 5 fruit and veg every day – from P.18 of his book Revolution.

"Every cryptocurrency is a new form of waste—and the only way to stop that is to stop cryptocurrencies" – David Gerard in article: Chia Is a New Way to Waste Resources for Cryptocurrency MAY 23, 2021 - (I'm hoping Yoonicoin will invalidate this statement).

"*If we're going to reinvent money, we might as well help fix the climate and reduce inequality while we're at it…*" – Steve H (me), while writing this paper

Still To Do

Next:-
- Start contacting blockchain/crypto proposal groups who may be interested in working on https://yoonicoin.org/
- Start sharing https://yoonicoin.org/ with Chia people + other people in list to share with (at the end of this doc)

Later:-
- Organise this doc into clear sections:-
  - Cryptocurrency working description – just how it will work (no background sections)
  - Additional Details document – technical details.
- Possibly create a new plan of implementation which is split into staged development, with simplest version first (possibly using Ethereum first?).
- Create diagram showing elements of system (at simple stage and then at later, more complex stage).

Foreword

This paper is still in DRAFT, but is being publicised before being completed in order to achieve the following:-
- Get quick feedback in order to "fail fast". If there is something fundamentally wrong with the ideas described then I want to find out early and abandon ship, rather than wasting weeks/months gold-plating the idea and then finding out.
- Get feedback to help improve or add to these existing ideas, or to completely re-work the whole concept. This would make the creation of this paper a group activity rather than the idea being entirely mine, followed by an implementation that is (necessarily) a group activity.
- Allow a community to start working on the project.

The system described and the ideas relating to it are still at a high level of uncertainty, with some of the ideas bound to be incorrect/invalid.

I believe though that this project, if undertaken, could be as fascinating and challenging as previous important scientific/mathematical/computing projects such as [The Bletchely Park Codebreakers] and [The Manhatten Project], but hopefully less sinister than the latter.

To reiterate: This document hasn't been written with the intention of convincing you this is a foolproof and practical idea. It has been written in order to give you enough information to allow you to show me why the system **will not work**. That is why the document still has inconsistencies and incomplete ideas. There is no point in spending months or years polishing something, when you can get it confirmed as unworkable after just 2 months and then get on with something more useful ☺

Reading time of this document: Approx ??? minutes.

The Author

This paper was written by me (Steve H) in March 2021. I'm a 47 year old software engineer based in Hertford, UK – married with 2 young children. I have a Maths degree and a Computing Science Master degree. I have worked on climate related projects in my spare time since 2009, including founding Climate Change Coders and the London Quantum Computing Meetup. In the last year I've become more interested in psychology, philosophy and societal change through groups called Rebel Wisdom and a movement called Game B and have been working on ways of using these things to catalyse radical change. A video that summarises these elements is this one of Daniel Schmachtenburger called A Phase Shift For Humanity. In the last few months I've been working on the ideas in this paper that relates to crypto, inequality and climate change.

My Personal Reasons For Working On This Project

…are:-

- I've been working in my spare time for 11 years on tech climate projects + other ways of tackling the climate crisis. This cryptocurrency system looks like it may have some potential (where a lot of the other projects didn't seem to).
- I enjoy the challenging aspects of the mathematical/computing parts of this project + the imagination involved in trying to create a system that may work.
- I especially like the aspect of the project where you have to consider "bad actors" trying to scam the system and defend against those aspects. It's a lot like being involved in a virtual battle, like working in computer virus defence, IT security etc.

Glossary

This document introduces a number of new names for things in the Yoonicoin cryptocurrency system. This Glossary section contains a quick summary of what each of these names mean, so you can refer back to it as you read. If you are reading this document for the first time, you may want to skip this section.

- Yoonicoin – the name of the currency system, and the individual coin (of which there are two types, see below).
- Minting – the process of generating coins within the currency system.
- Mining – also used as a term for "Minting" – still just means generating coins.
- IP Yoonicoin – a coin that is generated for a particular IP address (or IP address block).
- Personal Yoonicoin – a coin that is linked uniquely to a single adult human.
- Yoonicoin Mint – a part of the currency system which generates IP Yoonicoins and Personal Yoonicoins for a particular person.

- Climate Orgs – the organisations that are working on helping solve the climate crisis. These include charities, NGOs, companies and government organisations.
- Fixed Mint Generator Token – a token which is obtained by donating Personal Yoonicoins generated by your Personal Mint to a Climate Org. Starts generating additional Personal Yoonicoins in your Mint after a 5 year wait.
- Wildcard Generator Token – a token which is obtained by donating cash (fiat currency) via the currency system to a Climate Org. Starts generating additional Personal Yoonicoins in **any** Mint in the system after a 5 year wait.
- Trusted Validation Authority (TVA) – a company/organisation that can verify the identity of a Mint Owner and uniqueness of the link between that Owner and a Yoonicoin Mint that produces a particular Personal Yoonicoin.

Similar Ideas Already Being Implemented

Worldcoin

https://worldcoin.org/

https://worldcoin.org/how-it-works talks about proof of personhood using iris scanner

https://www.cnbc.com/2021/10/21/sam-altmans-worldcoin-wants-to-scan-your-eyes-in-exchange-for-crypto.html

Good article about it here https://www.wired.co.uk/article/worldcoin-cryptocurrency-sam-altman

About privacy issues with new WorldCoin using iris scanners:
https://www.nasdaq.com/articles/why-everyone-is-mad-at-sam-altmans-worldcoin-2021-10-25

I'm really impressed with Globalcoin's idea and ambition and it is similar to the Yoonicoin idea, especially the concept of using Proof of Personhood, which correlates with the Proof Of Personal Identity described in this paper.

Differs from Yoonicoin in that you only get access to Worldcoin by having your iris scanned. My belief is that a lot of people will be reticent (initially) to have their iris scanned - especially in the richer countries, because:-

- They will be concerned about the physical risks of an eye scanner from a company they don't know.
- They will concerned about privacy/identity issues.
- The gain (in monetary value) may not be enough (initially) to counteract the above issues.

The aim with Yoonicoin is for the currency to grow through the uniqueness of IP address or some other method (disk use via Chia.net, or mobile phone number using something like https://celo.org/), and then become tradeable as Personal Yoonicoins through trusted partners and finally to become fully tradable with anyone by being verified by trusted parties. These parties could be people similar to Worldcoin, who track uniqueness of each human using Iris Scanners, or any other organisation, company or government who wants to do the job. This allows people to get in early without having to provide any identity information, and trade early (using IP, disk or mobile number as proof) or trade with/through their trusted friends and then, only when they feel comfortable, provide some proof of identity to the organisation of their choice, at the time of their choice.

Yoonicoin also has a core aim of providing a means of collecting funds for climate change projects, with the possibility of long term rewards for early donors to these projects.

May be an option to work with Worldcoin? Maybe not.

Summary Of The Yoonicoin Cryptocurrency System

This paper contains ideas relating to a proposed new cryptocurrency called Yoonicoin.

Yoonicoin is a currency system in which each adult human on the planet can have a digital coin produced and linked uniquely to them. This coin is created (Minted) by them, or by someone else on their behalf. The rate of production of these coins is limited and controlled by the whole cryptocurrency system.

Trust in the validity of any particular coin is determined by the validity of the identity of the associated human adult, and especially the uniqueness of the link between them and that one particular coin.

This paper discusses ideas and possible methods for implementing and running this currency system. The aim is to create a system which will evolve to the point where the currency is accepted as a global currency.

The currency system is designed to help solve the following problems:-

- Create a transferable store of value that is limited in supply and so can be relied on more than traditional, national currencies. This is the main problem the coin will provide a solution to, as confidence in national currencies is currently being eroded by high levels of borrowing, quantitative easing and national debt (NOTE: This is the same, main problem that pretty much all cryptocurrencies exist to solve).
- Provide a means of cheaply and easily making micropayments (By being similar to, or based on a highly scalable and cheap to run crypto system like Algorand)
- Provide a cheap and easy means of storing and transferring value to the world's 1.7 billion currently "unbanked" people. (By being similar to, or based on a highly scalable and cheap to run crypto system like Algorand)
- The climate crisis – by incentivising people to donate money to the climate crisis now in a way that is recorded publicly, with the possibility of being financially and socially rewarded for it in the future. Also to create a way for everyone to fairly and equally contribute to help solve the problem.
- Inequality - since the currency is Minted by (or on behalf of) each adult person on the planet, it could help solve the problem of extreme global inequality, where 690 million people don't have enough to eat.

Evolution Of The Idea

The Bitcoin cryptocurrency system uses a huge amount of electricity which is exacerbating the problem of climate change by increasing CO_2 production. As the coin price continues to increase that problem is only going to get much worse.

This is because the system is based on a concept called Proof Of Work which requires all the computers in the system to compete in trying to work out the answer to a difficult maths problem. The first computer to discover the answer, which is purely based on chance, gets to produce the next coin. Usually that computer is part of a "pool" of computers that have agreed to share the winnings between each computer in the pool (a bit like a workplace lottery pool).

A couple of years ago I investigated alternative ways of selecting a winning computer without Proof Of Work. An obvious technique would be for all the computers in the system to work together in some way to produce a shared random number that none of them individually could have predicted and, importantly, none of them could have influenced. Ideally you would want to create a system where even if a dishonest party was controlling one third of the computers and trying to cheat, they wouldn't be able to do it.

I gave up on developing this idea because I couldn't find a way of doing this shared random number generation.

In early 2021, as the price of Bitcoin rose steeply, I looked again at the problem and found a paper called No-Dealer: Byzantine Fault-Tolerant Random Number Generator that had been published just 6 months earlier in the publication IEEE Conference on Computer Communications Workshops. IEEE is the world's largest technical professional organization for the advancement of technology.

The authors of the paper seemed to have come up with a solution to the problem. The solution involved using tricks from Number Theory and some well-established methods in cryptography.

Once I had this possible method of replacing Proof Of Work I had to think more about how to limit in some way the number of coins that could be Minted/Mined. In Proof Of Work this is limited by how much it costs to run the thousands of computers that are dedicated to mining Bitcoin – the cost of running the whole system is generally going to be less than the value of all the bitcoins produced. I needed to think of other things that could be limited in supply within a cryptocurrency system.

I came up with 2 things: IP Addresses and Humans, and then worked on ways that a system could evolve that relied on the shared random number generation algorithm and used these 2 things as the limiting factors.

The IP Address limitation led to the concept of Proof Of IP Address and the Human limitation led to the concept of Proof Of Personal Identity.

Ideas about how the currency system could be developed are included in this paper.

A natural result of each human having their own, continuously produced currency should be an improvement in financial equality. This seems to be built into the system.

Having worked for a long period in my spare time on projects relating the climate crisis I wanted to include in the system ways to solve that problem as well. A cryptocurrency system can be written with whatever rules you want. It’s a game that you make the rules for and then invite people to play. If no-one plays, that’s fine. But if they do play then the rules of the system have to be adhered to. This system can be written in a way that gets round the main problem of climate change: the “tragedy of the commons”.

The tragedy of the commons can be summarised by how someone might think in the modern world about climate change: “Me, or my country, or my company, would love to do something about climate change – but if we do then we’ll be helping everyone else’s future and they all get a free ride at my expense – which isn’t fair – so I’m not going to do it.” In the case of a country it can be looked on as a problem where if my country does a lot for climate change, we’ll be less competitive and lose out in comparison to other countries. In the case of a company it could be that if it is extremely climate friendly its costs may go so high that it becomes uncompetitive and goes out of business. In the case of an individual: “why should I go vegan and stop flying/driving when everyone else is ignoring it?”

In a cryptocurrency system you can change the rules of the game so that we can all vote on what we think is a fair amount to pay and then everyone (without exception) who takes part in the system has to bear that cost equally. It’s just hard coded into the system.

You can also write the system so that those who put resources / time / money into tackling climate change now – and who will be benefiting people in many decades time, can in some way be rewarded by those people in the future. This could be social rewards or financial rewards, and those rewards could be inherited by the children of the people who are investing now. This just seems fairer than the current system where I give £10k to Friends Of The Earth to work on climate change and no-one thanks me and I have no chance of any reward in the future.

Evolution Of The System

This currency system cannot be created and function from day one in the way it is intended to eventually operate. This is because from day one the trusted organisations required to validate the coins will not exist and the levels of trust and understanding in the currency will be low.

For this reason it will be designed to go through multiple stages of evolution.

At each stage there is a requirement to use different methods to limit the supply of the currency and combat attacks on the system. Attacks can come in many forms, including Denial Of Service, illegitimate coin production etc.

The possible methods of limiting the supply of the currency include:-
- By IP address or IP block.
- By Proof Of Personal Identity - validated by a Trusted Validation Authority

A Bit Of Background On Bitcoin

The Bitcoin blockchain uses a method called Proof Of Work to decide which of the thousands of nodes that are running it gets to "mine" the next coin and write the next block of the blockchain. This involves all the "miner" nodes working to solve a CPU intensive maths puzzle in which the chances of getting the answers are the same for any two equally powerful mining machines. The difficulty of the puzzle is set in order to make the time to solve it across all the nodes approximately 10 minutes. This means a new coin is produced every 10 minutes and the winner is the one who writes the next block.

The algorithm has been written so that coin production gets harder as the number of coins grow and there is a hard limit of 21 million coins.

There are currently (March 2021) approximately 1m miners mining bitcoin. The system is written so that to affect or attack the currency system you would have to control 51% or more of the mining nodes. This is called a 51% attack, and would be very difficult/costly.

A Bit Of Background On Existing Alternatives To Bitcoin's Proof Of Work Method

To avoid using up lots of electricity people have created an alternative to Proof Of Work called Proof Of Stake.

Instead of a node on the network proving it has done work, it proves that it has a "stake" in the system – in the form of coins owned or time that it has been on the network. To avoid nodes with all the coins getting all the power, the system can do things like reset the date associated with coins once a node has produced a coin (described at https://en.wikipedia.org/wiki/Proof_of_stake#Coin_age-based_selection)

This article describes how it works: https://www.coindesk.com/proof-of-stake

https://en.wikipedia.org/wiki/Proof_of_stake - seems to be quite inconclusive about whether Proof Of Stake is something that is reliable and can work going forward.

Here's a paper talking about why Proof Of Stake is "fundamentally unable to produce a distributed consensus within Bitcoin's trust model.": https://download.wpsoftware.net/bitcoin/pos.pdf Having read this paper in full, I'm not entirely convinced by the arguments, but think there are definitely some valid points.

In the first half of 2021 a new cryptocurrency has taken off in popularity called Chia, with its mainnet release only just happening in 3rd May 2021. Instead of being based on the limited supply of computing power, it's based on the limited supply of storage space: "Proofs of Space and Time replace energy intensive "proofs of work.""

Here are some links about the system and the inventor:-
Chia Consensus – Google Doc about the algorithm
https://en.wikipedia.org/wiki/Bram_Cohen#Chia
https://en.wikipedia.org/wiki/Proof_of_space#Proof_of_storage

The Algorand "Pure" Proof Of Stake Blockchain

One of the Proof Of Stake blockchains is Algorand. Algorand is of particular interest with respect to this paper because it uses pure randomness and similar techniques to the ones described in this paper for choosing who gets to create the next coin/block.

See "Appendix 1 – Notes And References On The Algorand Currency System" for links to understand more about the Algorand system.

Algorand was founded in 2017 by Silvio Micali who was one of the original people at MIT who developed Verifiable Random Functions back in 1999, which are explored in the next section.

Background On Verifiably Random Numbers And Verifiable Random Functions

Verifiable Random Functions (VRFs) provide a method for groups of computer nodes to produce random numbers that are verifiably random, given a Seed that is known to be random. It is the main algorithm used in the Algorand blockchain.

The scheme works in the following way. If I am interacting with a remote party (e.g. a node on a blockchain) and I have no trust in whether they want to manipulate the system, then I can force them to generate a random number using a random number I generate and, using this technique, I can prove that the number they generate is as random as the number I generated.

The steps are:-

- The remote node generates a Verification Key VK which it shares with me, and a corresponding Secret Key SK, which it keeps secret. This key pair can be used to generate as many random numbers as we want (i.e. forever). It's a bit like a standard private/public key pair.
- I generate my own random number X which I know is random (I trust myself!!!)
- I send this random number X to the node.
- It runs an algorithm called the Evaluation algorithm using my random number X and its Secret Key SK. This produces an output Y and a proof ρ which the node sends to me.
- I run an algorithm called Verify(VK, X, Y, ρ) → 0/1. This is an algorithm which uses the Verification Key VK, my random number X, the output Y and proof ρ and gets an output of either 0 or 1. If I get a 1 as the output I can know that they have correctly followed the algorithm which used a combination of their Secret Key, which I know is definitely linked to the Verification Key they sent me, and they definitely used my random number to produce the output Y. This allows me to know that the random number Y that they produced is as random as my random number X.

Aside: To make this even stronger (???) it may be possible or necessary to use a method like:-
RSA Key Generation with Verifiable Randomness
which can be used to prove that the Verification Key VK generated is verifiably random, so that the node cannot try to manipulate things by creating a non-random VK at the start of the whole process.

Algorand uses this VRF method for randomly electing committees who then process the next block of their blockchain.

It's not clear yet whether we would need both this method and the "No Dealer" algorithm described in the next section, or possibly just one of them.

See also: Appendix 2 – Notes And References On Verifiable Random Functions.

The "No Dealer" Algorithm

This section give more details on the paper [No-Dealer: Byzantine Fault-Tolerant Random Number Generator – IEEE – July 2020] and the algorithm described in it which is called "No Dealer".

Discovering this algorithm was the catalyst for working on this paper, since it provided a means of running a cryptocurrency blockchain using pure randomness that is generated by all the members of the blockchain working together.

The method I developed involved each of the nodes on the blockchain registering a private/public key pair and then 1,000 or so randomly selected members of the chain working together to choose the next set of random numbers. These random numbers then determine the next coin producer and the next 1,000 randomly selected member, and so on.

As I have researched further into this area I have discovered that the Algorand blockchain already achieves these things. It also improves on my initial idea by designing the system to make the selection of the 1,000 nodes completely secret. This means that only each of the 1,000 chosen nodes can know that it is one of the chosen "committee". Each one then sends out its "vote" for the next block together with the proof that it is one of the committee. These 1,000 votes are designed to propagate very fast in a viral fashion through the network, which makes it very hard for an adversary to try to block them. A very nice article on LinkedIn by the founder of Algorand explains in a very easy to understand way how all this works [here].

The "No Dealer" algorithm provides a way for a group of nodes to work together to produce a provably random number. So long as more than 50% of the nodes are honest and stay online/available the final random number can be shown to be random.

As the open source Algorand blockchain achieves the same end goal it seems likely that there will be no need to use the "No Dealer" algorithm, but it's worth keeping it in mind as a possibly useful tool.

The Algorand blockchain is entirely open source, already invented and running, developed by an MIT Professor and running the ALGO cryptocurrency network which is currently worth $5bn. There's no benefit in re-inventing the wheel and so it's likely that if the Yoonicoin project went ahead it could do so using the Algorand blockchain, or a separate blockchain using the same algorithm, as its base.

In case you're interested in the details of the "No Dealer" algorithm you can find a more detailed description of the paper and the algorithm in "Appendix C – How The No Dealer Algorithm Works"

High Level Explanation Of How The System Would Work

In this section I give a quick summary of the main concepts of the system and how it would work (before going into more details below).

The system starts with people downloading and running the Yoonicoin Mint application that generates coins for them. They can run this on their phone, PC, laptop or a remote server. The Mint generates two types of coins:-

- IP Yoonicoins – coins that are linked to the unique address on the internet of the computer. These are verifiable as having come from that IP and so can be traded immediately. The system may generate something like 1 of these coins every 10 days, per IP.
- Personal Yoonicoins – coins that are linked uniquely to the person running the Mint. These are only likely to become tradable after a few years, once trusted authorities have come into existence that can reliably verify the identity of the Mint Owners. The system may generate something like 1 of these coins every day, per Mint.

Each day a small number of people win a large number of IP Yoonicoins in a lottery. This is just an additional incentive for running the system.

Downloading and running the software is made extremely simple and easy. Trading IP Yoonicoins is also set up to be simple and easy, without the need to provide any ID in order to join an exchange, like Coinbase.

Each person running a Mint can vote on the percentage of all coins Minted by the whole currency system that should be donated to Climate Orgs.

Each person running a Mint can also choose to have a certain percentage of their coins donated to Climate Orgs. For the coins they donate they will receive in return something called a Generator Token. This Generator Token will start to generate coins in their Mint after a period of delay, e.g. 5 years. This is a way of allowing someone to invest in Climate Orgs now and receive possible profit from that investment in the future. These Generator Tokens are called Fixed Mint Generator Tokens, as they are limited to **only** ever producing coins in the Mint from which the coins were donated. This limitation prevents someone trying to scam the system by making lots of fake Mints and then donating coins from them.

People who have spare money, and who want to donate real cash the Climate Orgs can do so through the currency system. They also receive Generator Tokens in return. As above, these Generator Tokens will start to generate coins in a Mint after a period of delay, e.g. 5 years. The difference is that these Generator Tokens are called Wildcard Generator Tokens and can be applied to generate coins in any Mint in the Yoonicoin system. These Wildcard Generator Tokens are much more powerful, and therefore much more valuable, than Fixed Mint Generator Tokens - because they were paid for using cash that went direct to Climate Orgs when they were created.

The currency system records all donations to the climate crisis. This can be also used to reward people with social recognition over the years (not just financial reward).

After some years, if the system becomes popular, then people will be able to start trading Personal Yoonicoins as Trusted Validation Authorities (TVAs) come into existence in order to verify Mint Owner's identity.

The system is designed to provide a small continuous income to everyone in the world, to improve equality. It's also designed to create funding for work on the climate crisis. By creating a new cryptocurrency with a supply that is absolutely limited – by IP addresses and human beings, it also creates a store of value – similar to Bitcoin. If it ends up being very cheap to transfer small amounts of the currency, it also could help solve the problem of "The Unbanked" – people who have no access to bank accounts.

The system could be implemented on top of the Algorand blockchain, or possibly the Ethereum blockchain (TODO: Add section about how this initial Ethereum implementation could be done). The Algorand blockchain system uses collective random number generation to control the storage and consensus needed to record all the data on the blockchain. This random number generation could also be used to generate the lottery winners.

Use Of A Distributed Random Number Generator

The blockchain described in this paper is similar to Algorand, and uses the VRF that Algorand uses. It adds some other randomisation elements and also uses additional techniques for limiting coin production. Algorand uses stake to limit the power of a node, whereas Yoonicoin uses IP Address and Personal Identity. The Yoonicoin system could also be written to include stake as one of the factors that determines how much power a node has.

All the nodes work together to create provably random numbers. These are then used to decide who gets to write the next block and who gets the next coin.

Maintenance Of The Blockchain

Once you have a method for generating random numbers you have a means of achieving consensus among all your nodes about the next block being written to the blockchain and of choosing the next node to create a coin.

Your problem then becomes how to limit the number of nodes that can join the system, since if it is unlimited then each computer can run many hundreds of miners and then you are just implementing an inferior copy of Bitcoin.

The Algorand blockchain solves this problem by using Proof Of Stake, so that the power you have on the blockchain is related to how many coins you own on the blockchain. So there is no point joining that blockchain with 1,000 nodes that have 1 Algo each because the effect is the same as joining with 1 node with 1,000 Algos stored on it.

Using IPs To Limit Mining Nodes

Limiting the number of miners to one per IPv4 address would set a hard limit of approximately 4 billion (see https://en.wikipedia.org/wiki/IPv4_address_exhaustion and https://www.itproportal.com/features/the-turning-point-for-ipv4/)

Issues With Using IPs To Limit IP Addresses

There are some problems with the idea of using IPs to limit miners which are discussed here.

IPs Being Used Up At Hosting Providers

Once it becomes profitable to run a mining node on an IP, companies that provide hosting services and provide IPs may find that their IPs are getting used up (and running low) due to customers using them for mining. Worse, the hosting companies may get to the point where it is more profitable to mine on an IP than to provide it for customer use.

A possible way round this could be to only accept a limited number of miners per 256 IP address block e.g. only accept 25 mining IPs from any IP starting e.g. 123.123.123.xxx. Any beyond that are ignored, or rotated according to the month, which would leave them free for non-mining operations.

Energy Use

To avoid people running laptop/computers/servers/phones for long periods in order to do mining, it should be possible to introduce some kind of registration system where just registering from an IP address on a weekly basis gives you the same mining effect as a week's worth of mining on that address.

Multiple Miners Running On One IP Address

If you limit to one miner per IP then there is the question of what happens when two miners attempt to mine using the same IP address.

If I live in a house and have a dedicated IP address that is unique to me, I should be able to run a single miner on my phone/laptop at that address and gain all the coins produced by that miner. If I run multiple mining devices within that household, then I gain no extra money as the coin production is shared among all miners on an IP address, and so I would only run a single device (possibly two or three to provide redundancy) and only need to make sure one of them registers at least once a week.

Some houses may share an IP address with multiple other houses. This could be due to the ISP using Carrier Grade Network Address Translation (CGNAT) which is described here:
https://en.wikipedia.org/wiki/Carrier-grade_NAT

Here are a couple of articles related to mobile phones and CGNAT:-
https://networkengineering.stackexchange.com/questions/57559/how-do-i-find-out-if-a-lan-is-behind-a-multi-level-nat
https://serverfault.com/questions/637963/do-mobile-devices-have-unique-ip-addresses

With CGNAT multiple houses or mobile phones will appear as all coming from one IP address.

In this situation if two people in two separate houses, or on separate mobile phones, run miners that end up sharing an IP address it should be possible to make it so that all coin mining is shared between those two miners. In this situation one of the households may decide to run more miners in order to gain a bigger share of the coins mined. This would obviously be unfair and so one possible way of managing this situation is described here:-

Each miner subscribes to a Shared IP Arbitration Service. This allows each miner on a shared IP to communicate messages (from a limited set of pre-prepared messages) with the other miners on that IP. If a miner on this shared IP suspects that there are too many miners running on the IP (e.g. 1000 when usually the ISP shares an IP among max 50 houses) then they can send a message to the other miners saying they suspect over-mining and ask them to limit to one per household or one per mobile pls. If the situation continues then they later send a warning message saying mining will be blocked if the numbers stay high. The rule is that any one miner on an IP can completely block all mining on that IP. If the warnings are ignored, all mining becomes blocked on that IP. Once the miner sees that the other household/mobile has reduced their number of miners they may re-enable mining. Obviously, if this becomes big business in the longer term, then ISPs or other third party services could provide a service which allows them to manage who is allowed to mine from a particular IP address.

Initial Stage – Limited By IP

Once the system is in place to limit mining by IP address/block the system will run in a way where:-

- There is only one miner at any point in time per IP address (or IP address block), or the miners sharing that IP address share the mining.

The whole blockchain system starts on Day Zero with one node seeded with a large number of provably random numbers which are mathematically proven random e.g. from a quantum random number generator machine and kept in a RandomNumberPool on the blockchain.

Each node has a unique NodeId, starting with 1 and incrementing.

Each node has a NodePublicKey which is published when it registers on the blockchain and the associated NodePrivateKey that it never shares with anyone.

Each node is assigned a NodeRandomNumber which is obtained from the pool of provably random numbers. This RandomNumberPool is kept topped up by new random numbers on each round of coin production.

Alternatively this NodeRandomNumber could be generated in a more efficient way by doing the following:-

- Node registers NodePublicKey
- Next block is completed.
- Next block is processed and creates an associated CoinGenerationRandomNumber (see below for details)
- An algorithm is applied that combines the NodePublicKey with the newly generated CoinGenerationRandomNumber to create the NodeRandomNumber. This could be the VRF algorithm described previously or something like RSA Key Generation with Verifiable Randomness (KEGVER).

Coins are minted on the system using the following process:-

- The nodes in the system play the No Dealer random number generation game to create a CoinGenerationRandomNumber. For efficiency reasons it may be that the game is performed in a way that produces 1,000 random numbers in one game, which are used to top up the RandomNumberPool.
- The random number chosen determines which node gets to produce the next coin – which will be the node with its NodeRandomNumber closest to the CoinGenerationRandomNumber.

The way in which the system reaches consensus on the next block has two possible routes:-

- The coin generating node writes the next block (like BitCoin)
- The CoinGenerationRandomNumber and possibly numbers in the RandomNumberPool are used to organise consensus among all the nodes in the system. This can possibly be done using Byzantine consensus using randomization - see details of Shared Coin algorithms in chapter 1.2.6 of From Byzantine Consensus to Blockchain Consensus

It's possible that most of this could be done instead by using the fully open sourced Algorand blockchain, in which case the above methods will not be required.

Random Number Generation Game Details

Scaling The System

To run a 1bn node system it would be impossible for each node to play a No Dealer game with all the other nodes. To get round this we want to use a method similar to the Committee method used in the Algorand system.

We want e.g. 1,000 nodes chosen (provably randomly) from the 1bn nodes, using (maybe) the following:-

- The last random number chosen by the last block is processed by all nodes through a VRF.
- The top 1,000 nodes that are closest to the random number get to be on the committee (or some other method – maybe using division of their provably random number and the last block coin random number?).
- Those 1,000 go through a game of No Dealer to find the next (or set of next) random numbers.

An attacker who controls 33% of the nodes would need to own > 500 of those final randomly chosen nodes in order to influence the outcome of the No Dealer game (their only possible influence is to prevent publication, so that another random number is chosen). If they do prevent publication then it would be very clear that this has been done on purpose and also the chances of the attacker getting lucky and getting 500 of the 1000 randomly chosen nodes is very small. The chances of getting 500 nodes out of 1000 when you control 33% of the network can be calculated using the maths at https://www.omnicalculator.com/statistics/dice and is:-
1 in 1.25 X 10^25

If you analyse this 1 in 1.25 X 10^25 value you find that if this process was repeated 1,000 times a second for a million years then the chances of this happening **once** during all that time are 1 in a billion. (EDITOR'S NOTE: see section 2 of first set of Blockchain paper notes with MATHS on top corner of paper for calculations)

If you control 33% of the network, it may also be that you can influence it in other ways anyway (if a requirement of Byzantine Fault Tolerance is that less than one third is controlled by a single attacking party?)

Possible Methods Of Attack On The System

To be filled in once working with someone else (I have given it some thought, but not writing up here yet).

Concept Of IP Yoonicoin

There will be a stage in the system's evolution where most Personal Yoonicoins will not yet have been validated by a Trusted Validation Authority (TVA). This will be in the stage when TVAs don't exist yet, or are not yet run by well known, highly trusted organisations.

During this period it will be difficult to know whether any particular Mint is minting coins that are genuinely related uniquely to a single person, **but** it will be understood by a particular person that if the system develops fully then at some point in the future the coins minted by **their own Mint** may have some value. If that particular person is only running one Mint then they will know that the coins from that Mint will eventually be verifiably linked to just one unique person (them).

They won't yet be able to sell their own Minted coins, since they won't be able to reliably prove to other people that they are genuine.

So, we introduce the concept of an IP Yoonicoin, which can be won/generated by proving IP address uniqueness and can be converted at any future point in time into a Personal Yoonicoin (one that is uniquely linked to a particular verified person).

These coins will be freely tradable at an early stage of the system development. They would be earned in small amounts per unit time that someone is registered on an IP Address (or IP block).

Lottery

NOTE: This is really an "optional extra" and not a fundamental part of the system.

In order to help the cryptocurrency become popular more quickly, it may be a good idea to introduce a random lottery system. At the early stages of the system the IP Yoonicoins being earnt will be likely to be worth very little (a few pence/cents a day?) and so the possibility of winning a $500 prize (with odds of 1 in 10,000) each day may make it more attractive?

The idea of a lottery makes the system a little bit similar to Bitcoin, which randomly creates a coin for one of the miners roughly every 10 minutes in a completely random way.

It's not clear though whether this may not be a necessary, or good, thing to include – since it complicates the system, devalues the coins being produced and partly goes against the aim of the helping with inequality.

Mining Is Currently Very Difficult / Murky Process

For most existing cryptocurrencies, running your own Miner appears to be a pretty difficult or murky process.

Mining Ada

https://www.reddit.com/r/cardano/comments/7j9lj6/how_does_the_cardano_mining_work_i_know_there_are/ says Ada is all "premined" but you can maybe mine something to do with Cardano, but the way to do it is hidden in some forums/Reddit posts… e.g.
https://www.reddit.com/r/cardano/comments/7j4cqo/questions_about_pos_ouroboros/
https://www.bitdegree.org/crypto/tutorials/cardano-mining
A quote from the above:-
"What does this mean? Well, you simply keep your Cardano **wallet** (the main one to use is called Daedalus) online, and in turn receive a certain percentage of your already owned ADA coins as payment. This method is used by the "Proof of Stake" system, which confirms transactions via already existing ADA coins, rather than by using hardware (that would be the case with mining Cardano)."

Mining Bitcoin

Very complex and involves lots of software/hardware that is difficult to set up – see
https://www.masterdc.com/blog/how-to-mine-bitcoin-beginners-guide-to-mining/
No easy to follow How To guide on the bitcoin.com website.

Mining Seeds

https://www.joinseeds.com/get-started - You have to install a Passport App and create a SEEDS account. I have found the process to be error prone and I don't like having to install an App on my phone that may not be trustworthy.

Mining Algos

Algos aren't mined. Anyone owning an Algo automatically gets approx. 7% increase in the number of Algos they have per year. You can run two types of Nodes on the Algorand blockchain – relay nodes and participation nodes.

https://algorand.foundation/faq#running-nodes- says you can't run a Relay node as they are run by VCs and universities
https://algorand.foundation/faq#participation-nodes- - you can run a participation node, but you don't get any additional reward for it (above the 7% you get for just owning the Algos).

I can't really see much of an incentive to run an Algorand node. This would be a concern to me because if there aren't many nodes then it seems that the system wouldn't seem that open.

See "Appendix 1 – Notes And References On The Algorand Currency System" for additional details.

Making Mining / Minting A Very Low Risk / Easy Thing

To get the currency to take off, it should be very easy and low risk + transparent process to mine the coins.

Someone who hears or reads about the currency should be able to mine it by doing something very easy and something that doesn't involve having to trust an App which could hijack their phone, or trust a dodgy website they've not heard of before, or install something on their computer from an unknown organisation that could introduce viruses.

An example of this could be some kind of simple shell script that any slightly technical person can read and understand, that just runs *curl* command line calls to download a long list of URLs, which validates that you are running a mining script from that IP address. It could use SSL https calls to verify the calls are signed by the person. Could even make it so that people can create their own public keys on the command line in order to register onto the currency system. This way all I have to do is understand/trust that the commands I am running are safe (or some trusted forum / developer says they are) and run them and then I'm mining.

Also, people who do have a certain level of technical knowledge could install the mining application as an extension to a Wordpress site or as a server application.

The Yoonicoin developers could set up cheap to run preconfigured AWS AMI server images which can be booted by anyone and run at very low cost and will run a webserver that can be added to this list of "IP verifying" servers and provide simple instructions for booting one up. These servers could also run mining.

There could be a graded system of mining where the amount you mine increases as you go from:-

- IP verification by running a script
- IP verification by running AWS server instance.

Climate Crisis Fund Raising

The system will incorporate 3 mechanisms for raising funds for working on the climate crisis:-

1. Universal Donation – a % of all Minted coins are diverted to the climate crisis. The % is voted on by all Mint owners.
2. Generator Tokens – these tokens generate coins within the system, and activate after an initial delay of e.g. 5 years. They generate coins based on a timetable and at a rate that I shall discuss in more detail in the following sections. They can only be obtained by donating either coins or real money to Climate Orgs. They delay in activation is designed to make these tokens a form of investment, which gives you returns in the future, thereby causing funds to flow to Climate Orgs now, which are rewarded in the future. There are two different types of Generator Tokens that are obtained in two different ways:-
    a. Fixed Mint Generator Tokens - obtained by donating newly Minted coins from a particular Mint to the climate crisis. These Generator Tokens will only ever generate coins for that particular Mint. This limitation discourages people from creating fake Mints and trying to make money out of these fake Generator Tokens.
    b. Wildcard Generator Tokens - obtained by donating real money, via the currency system, to the Climate Orgs that are working on the climate crisis. These Wildcard Generator Tokens generate coins for any Mint they are applied to within the system, and so are much more useful/valuable than Fixed Mint Generator Tokens.

I'll go into more details about each of these in the following sections.

Climate Crisis - Universal Donation

As discussed previously the system requires that each person doing Minting votes every 3 months on a number of things. If they don't vote then their Mint stops producing coins (IDEA: maybe produces 50% of coins, so that people without access to voting don't get excluded?). One of the things they are required to vote on is the top 3 organisations that they would trust to deal with climate change. They would have approximately 100 orgs to choose from, and the top 10 voted then receive funds with the top one getting the most funds.

Another thing they have to vote on is the % of **all** Minted coins generated by the whole system that should go to the climate crisis. This is called a Universal Donation. They receive no personal reward for this, but they understand that the cost is shared proportionally by all people who own Mints and so they should feel this is a fair way of donating funds to the climate crisis.

The voting system for the % value of the Universal Donation may need to be made more sophisticated than just obtaining a % value from each person and then calculating an average. This is because people who want to push the average up may vote for a 100% Universal Donation and people who want it to be lower may vote for a 0% donation. We also may not want some political persuasion of the voters to suddenly send it to nearly zero in the space of just one year.

For these reasons, instead it may be preferable to start with a value of 5% and tell people what the current % is and they get to either:-

- Vote to increase it to 6%
- Vote to keep it the same i.e. 5% (default)
- Vote to decrease it to 4%

The final % value would be calculated as:-
((votes for 6%)*6 + (votes for 5%)*5 + (votes for 4%)*4)/(number of votes)
which means everyone's votes just pull the final vote towards their preferred value.

The understanding is that the final value determines the % that goes to the climate crisis organisations.

The fact that this is a joint contribution should help avoid the problem of the tragedy of the commons where people act in their own self-interest. They may feel that if this is a problem that is going to be contributed to equally by millions of other Minters, then they are happy for the contribution to be reasonably significant (e.g. 5% of Minted coins).

Generator Tokens

This element of the system involves a new type of token called a Generator Token. Generator Tokens generate Yoonicoins for a particular Mint. The timetable and rate will be discussed in detail.

There are two types of Generator Token – a "Fixed Mint" version which will only ever generate coins for a specific Personal Mint and a "Wildcard" version which can be set to generate coins for any Mint in the currency system (but only one Mint at any point in time).

Obviously a Wildcard Generator Token would be more desirable and saleable than a Fixed Mint Generator Token, since it can be used to generate coins in any Mint rather than just one.

Fixed Mint Generator Tokens are obtained by donating a % of your Personal Minted coins as they are Minted by the system. These get donated to the same set of Climate Orgs that are voted on by all users of the system for the Universal Donation. The details will be in the next section.

Wildcard Generator Tokens are obtained by making donation of "real" money to a Climate Org via the currency system. These are basically proof that you donated money to a Climate Org at a particular point in time, and are saleable.

Fixed Mint Generator Tokens

If someone wants to donate to the Climate Orgs and be rewarded for it later, but they don't have cash, then they can do this by choosing to have a certain % of their Minted coins automatically donated to Climate Orgs. The donated Personal Yoonicoins become owned by the Climate Orgs, who can sell them once they are worth something (i.e. once they are validated).

As a reward for doing this they get a type of token called a Fixed Mint Generator Token. They get a single one of these coins for every Personal Yoonicoin that gets donated to the Climate Orgs.

These Fixed Mint Generator Tokens will generate Personal Yoonicoins over a pre-determined schedule and at a pre-determined rates. See below for details.

The Personal Yoonicoins that the Fixed Mint Generator Tokens generate will only ever be for the same, fixed Mint of the person who made the donation. This is to prevent someone creating thousands of fake Personal Mints, donating the fake coins to Climate Orgs and then being rewarded for it. The Fixed Mint Generator Tokens will only ever generate coins for their fake Personal Mint and so won't be useful to anyone.

So if you buy one of these tokens from someone else on the system you are only buying the ownership of the extra coins that will be generated over time in **that person's Mint**. Each Fixed Mint Generator Token will have a year that they were minted in and (for ever) will be linked to that particular Personal Mint, and the person who buys them will automatically gain the coin generation ability of the coin on that Personal Mint. This means that if I donate 40% of my Personal Yoonicoins coins to get Fixed Mint Generator Tokens in 2022 (year 1 of the system) and by 2025 (year 4 of the system) it is clear that the generation ability of these coins is going to be very valuable once they start generating in 2027 (year 6 of the system) then I may be able to sell them for a lot more than the 40% of coins I gave up in 2022.

I *think* the above idea can also be applied to IP Yoonicoin generation, except of course these can be sold by the Climate Orgs at a much earlier stage as they don't have to wait for the Personal Coins to be validated.

The Climate Orgs that will receive these donated coins will be the ones voted for as part of the Universal Donation detailed above.

Generator Token Generation Levels

Generator Tokens will generate Personal Yoonicoins at a rate that depends on three things:-
- The year
- The age of the Generator Token (they only start generating after 5 years).
- The number of other Generator Tokens in the system.

The total average production of Personal Yoonicoins for each Mint across the whole system will go down over the years (with a few initial years to allow lots of people to get on board – including poorer people without access to computers).

As time goes forward Generator Tokens will get an increasing % of the total coin generation ability of the whole system, so that people without any Generator Tokens will see their Minting ability diminish faster than those with Generator Tokens.

An example of how the numbers could work could be:-

Year (absolute)	Year (relative)	Average Coin Production Per Personal Mint (including generation by Generator Tokens)	% of the total coins produced that year that will be generated by Generator Tokens
2022	1	365	0

2023	2	365	0
2024	3	365	0
2025	4	330	0
2026	5	300	0
2027	6	290	5
2028	7	280	8
2029	8	270	12
2030	9	260	16
2031	10	250	30
2041	20	150	40
2051	30	75	50
2061	40	50	58
2101	80	30	60
2141	120	20	64
2321	200	10	65
2421	300	8	66
2521	500	5	66

So, the total average will go down over time, but if you haven't donated anything to climate causes your Minting rate will go down a lot faster than if you have.

The Generator Tokens only start to generate coins **after 5 years** by being included in a pool of all the Generator Tokens that were created more than 5 years previously. The coin generation ability is split equally among all of these tokens.

This means that if very few people contributed a % of their Personal Minted coins in year 1, then in year 6 the people who did donate could have a large amount of coin generation for themselves, which could even mean they make their money back or make a profit. If large numbers of people donated in year 1 then the coin generation ability, per Generator Token, would be less.

This 5 year lag means that if people contribute in year 1, when no-one knows whether it's going to make money, then in year 5, when it becomes clear it's a good investment, other people can't jump on the bandwagon and make lots of money, because of the 5 year time lag.

Of course, the dynamics of this seem to work in the favour of rich people – because they can afford to put e.g. 50% of their Minted coins into climate crisis because they don't need it, and then in the long run they will be the ones with the most Generator Tokens and so able to Mint more Yoonicoins. Poor people who need to sell all their coins for "real" cash may not put anything into the climate crisis and then will have no Generator Tokens and so a lower Minting rate in the future.

To make this less of an issue we have another type of Generator Token called a Wildcard Generator Token, which is paid for using a donation of "real" money, via the currency system, to a Climate Org. This makes it possible for rich people to invest (as much as they want) into donating **lots** of extra money in order to give a boost to their future minting rate. This would hopefully draw in a lot more of the rich people's money, which would make up for the fact that rich people are able to invest in this easily and gain from it in the long run.

Wildcard Generator Tokens

We want to allow "rich" people to be able to donate large amounts of "real" money directly to Climate Orgs, and these donations be provable in some way and result in the donors getting Wildcard Generator Tokens. These coins are similar to Fixed Mint Generator Tokens in that there is a 5 year time lag before they start to get a share of the Generator Token Holder Mint Generation Percentage (maybe one third – shared equally among Wildcard Generator Tokens).

Because we know a "real" donation happened to a Climate Org in order to get Wildcard Generator Tokens we allow the coin generation ability of these coins to be applied to **any** Mint in the system. Obviously most people would apply this to their own Mint as that is the one that is most trustworthy, but by being applicable to any Mint these coins are much more saleable than Fixed Mint Generator Tokens.

So if I donate £10k in 2022 then by 2026 there is a chance (depending on how many other people invested in 2022) that the Wildcard Generator Tokens may be worth even more than £10k. This makes donating money to the climate crisis seem less of a risky thing to do, because if I need money back in a few years (in case of an emergency) then there is a chance I may have Wildcard Generator Tokens that I can sell to get some money back.

Social Recognition And Other Non-Financial Rewards For Generator Tokens

People who accumulated Generator Tokens by:-

- Donating a % of their Personal Yoonicoins to Climate Orgs as they are Minted
- Donating "real" money to Climate Orgs through the currency system
- Buying existing Generator Tokens from other people (which helps keep the price high and therefore encourages people make to donations).

….may get financial gains later on, through the mechanisms mentioned above. They also may find their financial gains are minimal (or nothing if the system or the value of coins collapses), **but** the blockchain record of the system will be a permanent record that they contributed, that they helped get us out of the climate crisis.

In future years these people may be rewarded in non-financial ways. Their contribution may be socially rewarded, by invitations to events, by picking randomly people who donated and putting their story on TV or in books, newspapers, YouTube channels.

To start the ball rolling on this one, the currency system should start from year 1 with a "social reward" scheme where a random number generator picks:-

- 5 owners of Fixed Mint Generator Tokens
- 5 owners of Wildcard Generator Tokens

Every year these people are invited to:-

- Be interviewed to talk about why they did it
- Meet the orgs they are helping
- Be awarded something in an awards ceremony

And everything is filmed and put on YouTube and television.

In addition we could steal ideas from the crowd funding spaces (like Kickstarter) where people pay money towards something (like a film production) and according to the level that they contributed they get scaled access to things. In this case it could be (going from high levels of Generator Tokens ownership to low):-

- Spend a day with high profile climate activists / campaigners (Greta, XR Founders etc etc)
- Invited on a tour + dinner with the Climate Orgs
- Invited on a YouTube TV show about the Climate Orgs + the big donors
- Invited on a monthly Zoom meeting where people get to ask question about what the Climate Orgs are doing
- Sent a badge each month showing what things are being done in your name, that you or your children can wear
- Sent a Facebook posting badge and/or Instagram posting badge that proves what donation you did and shows what it is being spent on (these would be like non-fungible assets like

https://www.theguardian.com/technology/2021/mar/12/non-fungible-tokens-revolutionising-art-world-theft)
- (Look at the types of things people use in funding for things on https://www.kickstarter.com/ like https://www.kickstarter.com/projects/1194236337/the-yes-men-are-revolting and copy ideas)

How Does Money Get Paid Direct To Climate Orgs

There are lots of possible ways Climate Orgs could end up with money through this whole system. It's not clear yet which one would be the best, and it may be that a number of options are implemented and the Climate Orgs could get funded through any one of them.

There are a number of considerations/issues:-
- Climate Orgs will be happy to take donations in the conventional way, where someone donates money through their website or by transferring money. The problem here is that currently these orgs won't have a publicly visible way of confirming this donation that can be used to prove to the currency system that the donation happened and therefore result in the donor getting their Wildcard Generator Tokens.
- Climate Orgs, at least at first (and maybe for some permanently), will not be set up or want to do anything "special" related to a cryptocurrency system. For example, putting proof of donorship on their website, or selling Yoonicoins that are donated to them in order to raise cash funds.

As this would be a complex and evolving situation, we consider some possible ways of addressing these problems here.

Donations Coming Through An Intermediate Cryptofunnelling Charity

As discussed in the last section, the Climate Orgs may not be willing to do anything special in order to receive funds via the currency system. In this section we discuss a method of getting funds to those orgs via an intermediary charity that funnels the money to the Climate Org.

These intermediate charities could be set up to deal with the donations to the actual organisations. These charities would be responsible for dealing with the process of getting donor money to the real organisation and proving to the currency system that the money was donated.

For example, if I think that the Nature Conservancy "Plant A Billion Trees" fund should be one that gets funded I could set up a charity called Plant A Billion Trees Using Crypto.

If a person wants to donate £10k to the campaign and get their Wildcard Generator Tokens from the currency system, then the following process could be followed:-
- The "Plant A Billion Trees Using Crypto" charity is registered on the currency system, and gets voted into the top 100 orgs as people see that it is set up to donate to The Nature Conservancy charity, who they like.
- As part of the above registration the http://www.plantabilliontrees.org/ website is registered as the associated organisation domain name.
- The donor tells the currency system they want to make a donation of £10k to this org.
- The system tells http://www.plantabilliontrees.org/ through an API to register a domain name YooniCoinTransaction45678.org and put a certain page as the front page containing a certain transaction string.
- The http://www.plantabilliontrees.org/ admin person or system registers it and puts it up for sale for £10k.
- The currency system checks the registration and the front page.
- The currency system sends a message to the donor instructing them to purchase the YooniCoinTransaction45678.org for £10k and update it with a specific string.

- Once it is done the http://www.plantabilliontrees.org/donorDetails page is updated automatically to include details of the transaction, maybe using a Javascript plugin that gets transaction details out of all the transaction sites including YooniCoinTransaction45678.org.
- The http://www.plantabilliontrees.org/ admin person takes the £10k and donates it to The Nature Conservancy campaign.
- The currency system uses the http://www.plantabilliontrees.org/donorDetails page to confirm the transaction was completed and this causes the donors account to have the Wildcard Generator Tokens added to it, which will start generating coins in 5 years time (or they can sell them before then and the buyer update them to generate coins in their Mint).

Once The Nature Conservancy campaign has received a large number of donations (e.g. £50k) from this http://www.plantabilliontrees.org/ organisation, they are asked to do a Press Release and publish it on their website talking about the donations and pointing at http://www.plantabilliontrees.org/ and the YooniCoin system. The link to this Press Release is published on the front page of http://www.plantabilliontrees.org/ which suddenly makes it a lot more credible.

All transactions are made visible on the currency system through an API so it's easy to see all the donations that went to an organisation.

Once The Nature Conservancy have started to receive significant levels of donations via this route they may decide to cut out the middle man and increase the level of trust in the Fund by implementing the whole API and system themselves. The people who run the http://www.plantabilliontrees.org/ organisation/charity would help them in doing this and switch their registration url from http://www.plantabilliontrees.org/ to billiontrees.nature.org which people would then trust a lot more, as they would also be making the payments in the above process **direct** to The Nature Conservancy rather than to the http://www.plantabilliontrees.org/ charity middle-man.

Other Options For Funding Climate Orgs

If the above is too complicated other options which could be looked at include:-
- Special account gets set up on currency system for the charity org. People transfer IP Yoonicoins or Personal Yoonicoins or any type of coin, into those accounts and they get Generator Tokens in return. The charity then has to sell these coins, which is a bit of a problem as they may not want to be involved in selling coins.

After IP Yoonicoin Minting

IP Address based minting is a way of proving your uniqueness in terms of IPs which are a limited resource. As discussed in a previous section this allows us to limit the creation of coins, but isn't ideal for a global currency because it gives more control to people who control IP address resources (e.g. hosting providers, ISPs and large computer resource owners). For this reason it would be designed to be a stepping stone on the way to Personal Yoonicoins becoming tradable coins.

Over time the ability to mint these Personal Yoonicoins should become fairer and more widely accessible, even to people who don't have access to computing resources.

Person Validated Mints

This is the final state of Mints that run on the system, where there is something that uniquely links a single human adult on the planet to that Mint and is in some way verifiable.

The list of things that can uniquely identify a person include:-

- Passport number
- Driving licence number
- National Insurance Number
- Tax ID
- Fingerprint
- Retina scan
- Genetic code

Privacy Considerations

Using personal identity as a means of producing currency is going to introduce privacy issues.

Long term, ways round that may include physical "Banks" or governments issuing paper money which is tied in value to the value of Yoonicoin and can be used in the same anonymous way cash/money is now.

People wouldn't **have** to have their own Mint in order to participate in the economy as they could continue to work and be paid in Yoonicoins, traditional currencies or anonymous Yoonicoin-value-linked currencies. They would lose out though on the gains that other people would be making by having their own personal Mints producing money for them.

If it gets to an advanced stage it may be that governments and/or banks (who in most countries already have a lot of protected, personal information on you) could do the Minting on your behalf, with your permission? This would mean you wouldn't have to trust any new organisation with your personal identity details.

If the system takes off there are also going to be lots of new scams involving identity theft as well as theft of coins. Efforts will have to be directed at minimising the level and damage caused by these.

Chain Of Trust Trading Network

In this section I discuss a possible way of allowing people to trade Personal Yoonicoins with **some** level of confidence in their legitimacy before they are able to be fully validated by a Trusted Validation Authority (TVA).

This involves the idea of a "personal validation" chain of trust. This would work as follows and is described from "your" point of view as someone who has set up a Personal Yoonicoin Mint:-

- You run a **single** Personal Yoonicoin Mint.
- Your friends run a **single** Personal Yoonicoin Mint each.
- By only running only one Mint each you can all be sure that in the future the coins you are Minting will be valid.
- If you or any of your friends secretly run additional Mints then you will understand that the coins from these Mints will become invalid in the long term (once TVAs are established to check and confirm the validity of coins).
- You all verbally (and on the App/whatever) agree that you are **definitely only running one Mint each**, and if you are running more and trade them with your friends, you will be scamming your friends, because later they will own some of your illegitimate coins.
- You join a Chain Of Trust Trading Network, which may consist of many thousands of other people linked together in a large "mesh".
- Coins only ever move between your account and your friends' accounts, so that you only ever end up with a mix of your coins and your friends coins, but never coins Minted by anyone you don't know.

- Because your friends have other friends they are linked to that you are not, there can be long chains of trust which allow trades to happen down the full length of the chain. For example: someone 10 links down the chain can buy coins from you via a series of exchanges of coins between you and them.
- You make commission when your coins get exchanged in this network (because you are exchanging your coins that you **know** are valid and unique to you for coins that you **highly trust are valid** (because your friend told you so!!!) but you can never actually know that they are valid).
- You set the commission level you require for a trade with a particular friend based on the trust level you have in that friend. For example for someone you would trust with your life you may only set a 10% commission level for a trade, but someone who you've only known a year you may set a 30% commission level for a trade.
- You set a limit on the total number/percentage of your coins you are happy to have traded in this way, and are kept up to date with any trades that happen.
- As time goes on you only ever own coins that were Minted by your friends and vice versa, so if they were running a scam the coins you end up owning of theirs could end up being worthless. You never end up owning coins from Mints owned by people you don't know, and so your risk is minimised.
- If you want to buy lots of Yoonicoins there is a limit because you can only buy coins that have been Minted by your friends. If you're reckless enough to add people you don't know or trust and label them as "friends" that's up to. So if you have 10 friends you really trust, and you are rich and your friends aren't that rich you could be buying up all the coins that they are minting (10 X 30 a month?). If your friends aren't interested in selling for cash, but are OK to trade and gain commission, then as you buy up all their coins their account will become full of coins from their friends (and not their own) as they get sucked out of the remote "seller" accounts down the chain.
- If you want to sell your coins, then the trading system sells to the person who is giving the highest price on any one day and the coins only ever get transferred to your friends (with other people down the chain maybe being the ones who initiated the purchase).

This could end up working as an intermediate stage on the way to full Trusted Authority Validation, and create a limited marketplace for buying / selling Personal Yoonicoins.

How Above Feeds Into Move To TVAs

There may be a simple way of moving from a Chain Of Trust Trading Network to TVA trusted exchanges. A Trusted Verification Authority could just be added as another friend, with similar settings to existing friends and then you trust them at the level you feel comfortable with, and you also control the level of exchange that can happen with them. Anyone who has been validated by that TVA goes into that "pot" and so gets that level of trust that you are comfortable with. So if at first you add *Steve's TVA* and you think I look reasonably OK you may give me a score that means you get 40% commission on any exchanges of coins with people registered with my TVA. For a Verisign TVA you will trust them a lot more and so you may only charge 15% commission. This allows fairly unknown people to come in and start doing ID validation and making some money, which will allow the big players to see the money being made and then move in quickly.

You would also set your levels so that e.g. only 5% of your total coins (or 10% of any newly minted coins) could be exchanged via Steve's TVA if you weren't so sure about this new TVA and wanted to limit your exposure.

Final Validation By Trusted Validation Authorities

Eventually, Trusted Validation Authorities (TVAs) would come into existence and start to go through processes which allow someone to be validated as uniquely linked to a Personal Mint.

These authorities would also probably link up with each other to detect people who were trying to run multiple Mints under one identity (this could probably be done without sharing confidential/sensitive information, just by using encryption/hashing? - TODO: Would be good to try to work out if/how this comparing of information in a secret way could be done).

Idea Of PayPal Like Authority That Takes On Some Of Risk Of Transaction (In Earlier Days)

I like the idea of a number of PayPal-like authorities who spring up who people learn to trust because they have got too much to lose by not being trusted, and they have spread their risk across many thousands or millions of accounts. These authorities will do their own verification of the person you are buying the Yoonicoin from and then they will guarantee the coins, so that if it turns out when they are validated through a Trusted Validation Authority they are fake, the PayPal-like authority will refund you. Maybe the authority ends up losing 5% because of these scams, but they charge 15% for the service and so make a profit. They are just a way of people spreading the risk.

Another way of spreading the risk could be to have it so that the PayPal-like authority has a big list of coins that they trust, and they charge you for access to a random selection of that list, and then you can buy a SpreadCoin – a coin which means you get a tiny bit of each of a large set of coins, so that if 5% of them turn out to be invalid you only lose 5% of your money?

Personal Mint Storing ID Information Encrypted By My Public Key

This section contains some technical details that may be relevant to storing encrypted ID information on the Yoonicoin Blockchain.

NOTE: It may *not be actually necessary* to store **any** ID information on the blockchain. For details see the next section.

To set up my Personal Mint I could:-
- Take a photo of myself. Encrypt it using my MintPublicKey -> EncMintPhotoId
- Get a copy of my fingerprint (using App, or photo of 5 ink blots). Encrypt it using my MintPublicKey -> EncMintFingerPrintId
- Take my Country + Passport ID. Encrypt it using my MintPublicKey -> EncPassportID
- Take my Country + Driving Licence ID. Encrypt it using my MintPublicKey -> EncDrivingLicenceID
- Take my Country + National Insurance Number. Encrypt it using my MintPublicKey -> EncNationalInsuranceID
- Take my Country + Tax ID. Encrypt it using my MintPublicKey -> EncTaxID

(may not have to do all of the above).

No-one can get hold of these things unless I give them my private key (and I never would give anyone that).

But if I send a Trusted Validation Authority the unencrypted versions of my photo and fingerprint files then when I meet them physically to do validation I can show them some of the physical things (e.g. Passport or Driving Licence) and they can validate what I look like and my fingerprint (using a cheap fingerprint reader) and then encrypt them using my *Public Key* to confirm it matches the ones stored on the Mint. This would validate me as the owner of the Mint and the link between me, my identity and the Mint.

With all of this, I am thinking with this scheme that this means that Personal Yoonicoins don't really becomes tradeable until:-
- A Trusted Validation Authority exists
- I'm willing to share with them my very sensitive personal details, and can trust them to keep the information confidential and only allow comparison with other Trusted Validation Authorities in a way that doesn't actually share the full details.

- The TVAs are able to make enough money from doing this validation to set the whole thing up and do the physical footwork of being able to validate me and store/manage all that information.

Once this network of TVAs is set up and running and cooperating to ensure people don't run multiple accounts, then they will become the ones who define whether a particular person has a valid Mint and also whether a Mint has a valid person associated with them. Mints that are not validated by this set of TVAs won't really have any saleable coins in them.

The kind of companies that could start TVAs would be companies like DigiCert, GlobalSign and GoDaddy who already do [Extended Validation SSL certificates] where they validate that a business exists and is trustworthy etc.

Unresolved Question - Is It Actually A Requirement To Store Any Id Information On The Blockchain?

Answer: Not sure it is.

The TVAs do the complete job of storing ID information and (in a way that preserves privacy) comparing information with other TVAs to form linked up groups that serve to complete the task of making sure each Mint, under their monitoring eye, is linked to one and only one id-verified human adult.

All they need stored on the blockchain is the Personal Mint ID of the account that that person who provided the proof of identity says is their own.

It may be useful to have the encrypted information on the blockchain linked to the account, so that when the person provides the unencrypted version of the data to the TVA they can run the encryption using their Public Key and confirm that the ID provided matches the ID associated with the account, but it's not clear if that would actually be necessary.

Storing TVA Validation Details On The Blockchain With The Mint

It seems like a good idea to provide a means of the TVA storing their validation information on the Blockchain with the Minting record. It would probably require the Minter giving them permission to add/update a record by sharing some kind of key with the TVA or some other means of allowing them access.

Unresolved Question – How To Validate Using Different Forms Of ID

There is a problem that still needs to be solved related to different forms of ID being used to validate personal identity.

Let's imagine someone called John Smith who has two addresses - his main house and a holiday home. He could go to one TVA with his passport and NI number and his main house address and validate a Mint with them using that ID. He could then go to another TVA and validate a second Mint with them using his holiday home address, his driving licence and his Tax number.

There probably is a way of preventing (or limiting) this issue, but I'm going to leave that for working on with other people as it could be quite complex. It's an interesting logic puzzle though.

One solution could be to actually allow each person to have a Mint with each type of ID and the understanding is that for each of the main 8 types of ID most people will be running a Mint with each type of ID. Each Mint with a certain type of ID creates a certain type of Personal Yoonicoin e.g. a Driving Licence Personal Yoonicoin. At that point it's very easy to have a TVA verify that there is only one person they know of registered with that particular driving licence, and probably easy for them to verify with a large number of other TVAs that that driving licence is not linked to any other Driving Licence Mint.

Buying/Selling Coins Using Domain Name Transactions

With Bitcoin and other cryptocurrencies the current main method of trading coins is to sign up with an exchange like Coinbase.

Although Coinbase is now a very large US company that is worth a lot of money, it still doesn't feel ideal having to trust them with a large amount of personal identification details (pictures of Passports and Driving Licences etc) and also to hold onto assets of mine worth a large amount of money.

I thought it could be useful to have some other way of trading Yoonicoins that leverages existing, trusted systems for allowing trade to occur, so I came up with a way of doing this using domain name sales.

NOTE: This is probably trying to solve a problem that isn't really a big problem, and so may not be relevant. The method may be useful for confirming payments to Climate Orgs though.

This system:-

- Involves a payment to transfer goods (the domain name) that once completed cannot be reversed without both parties' consent.
- Makes it easy for the currency system to detect when the transfer has taken place, by making a call to website on that domain.

This could be done by coding the currency system so that the following process can happen:-

- Seller informs system they want to perform a sale of X coins from their account A to the buyer's account B.
- System sets up transaction and returns transaction id in domain name form: YoonicoinTransactionTransferDomain987.net (if the seller has a previous transaction id that has now expired they can re-use it to save on spending money on a new domain name).
- System instructs Seller to purchase domain name YoonicoinTransactionTransferDomain987.net (if they aren't using an existing domain name that has expired and they already own).
- System instructs Seller to put page at YoonicoinTransactionTransferDomain987.net saying "This page is for YoonicoinTransaction 12345 from Account A to Account B and the transaction is in stage: UNCOMMITTED. Expiry date of this transaction: 11th March 2021 12:00"
- System waits until that page is there.
- Once system has detected the page exists and contains the correct text, it send the following purchasing instructions to the Buyer:-
    - Please purchase YoonicoinTransactionTransferDomain987.net domain for £X
    - Once purchased please modify text of web page to say:-
        - This page is for YoonicoinTransaction 12345 from Account A to Account B and the transaction is in stage: DOMAIN_PURCHASE_COMPLETED. Expiry date of this transaction: 11th March 2021 12:00
    - Please send notification to currency system that domain has been purchased and the page has been updated with the above transaction details.
    - Please wait 10 minutes for system to verify domain and complete transfer of coins.
    - Please then confirm transfer has completed.
    - Please then update the text of the web page to say:-
        - This page was for YoonicoinTransaction 12345 from Account A to Account B and the transaction is in stage: COMPLETED and so this domain/page can be re-used by the Purchaser to complete another sale after the expiry date of this transaction: 11th March 2021 12:00

With GoDaddy people can also set up auctions and so this could allow a particular transaction to be set up for a sale of coins, linked to a domain and potential buyers of the coins could bid in an online auction to gain the ability to transfer those coins to their account.

With this method, the seller doesn't have to sign up for a Coinbase account in order to buy/sell coins, they only need to sign up to a well known and trusted Domain Name provider like GoDaddy and then follow the above procedure in order to perform the transaction.

Using Escrow

When buying or selling a domain name worth more than $5,000 GoDaddy doesn't provide assurance the transaction will go through but instead refers the user to escrow.com

For details see https://uk.godaddy.com/help/understanding-godaddy-auctions-payment-transactions-909

Escrow.com sets up and manages transactions for large amounts of money where:-
- Both parties agree terms of the transaction
- Buyer provides money to Escrow.com
- Seller sends goods to Buyer
- Buyer confirms receipt of goods and satisfaction with sale.
- Escrow.com releases funds to Seller.

If there is any dispute over the transaction then Escrow.com holds on to the money until both parties have resolved the dispute.

It could be possible for the currency system to use Escrow.com directly in order to transfer coins on the system, without involving the transfer of a domain name, although I'm not sure if/how this would work. For a description of Escrow.com's developer API see https://www.escrow.com/api/docs/basics

Obviously if people wanted to use their own, more highly trusted, legal services for providing escrow to confirm the transfer of the domain name, that should be fine e.g.
https://www.jpmorgan.com/solutions/treasury-payments/escrow-services or
https://jaffa-co.com/escrow-completion-services/

Quick Recap Of Entire Process Through Time From Two Points Of View As A User

This section contains a couple of run throughs of how things could progress from a user's point of view as the system evolves over a long period of time. It contains duplication of details from previous sections and may contain some inconsistencies.

Typical Scenario Run Through – Technical Person

In this section I go through a possible scenario for someone a little bit like me, fairly technical who knows about computers. These types of people would be the ones who would be most likely to be early users of the currency system…

2022 – Year 0

I hear about Yoonicoin somehow.

I Google it and get to Yoonicoin.com where I look at the instructions page for new people like me.

As I'm a developer who doesn't want to install untrusted Apps on my phone or applications on my computer, I download the Mac shell script and inspect it and read a couple of trusted analyses of it from well known coding sites.

I follow the instructions to run the script and it creates a Yoonicoin folder in my Documents folder containing the relevant files and keys etc. I store the password in my favourite password storage and write down my Secret Sentence in multiple physical places that I won't forget.

I'm asked to vote on a few climate related things as part of the sign up:-

- What 3 climate crisis organisations (from a list of 20) would I like to be supported by Yoonicoin? If I want I can suggest and vote for additional ones. I pick 3 that I've heard of and like.
- Climate Crisis - Universal Donation: What % of coins minted by **all** Mints do I think should go to climate crisis organisations? The current value is 5.5% and I get to choose whether to increase it to 6.5%, leave it at 5.5% or decrease it to 4.5%. As I think it should be more like 10% I click the button to vote for it to increase to 6.5%.
- Fixed Mint Generator Tokens: What % of coins minted by **my** Mint do I want to donate to the climate crisis orgs? I'm told that as the years go by an increasing % of Minted Yoonicoins will be generated by Generator Tokens (full details in previous section are provided). I am told that if Yoonicoins devalue, or the system stops running, this extra Minting ability will be worth little or nothing. I'm also told that, depending on the number of other people who donate, I may get a reasonable reward for my donation. I am also told I can sell my Fixed Mint Generator Tokens but, as they will only ever generate Personal Yoonicoins from **my** Mint, people won't want to buy them until my Personal Yoonicoins become saleable. My Personal Yoonicoins will be saleable to my friends only at first, and then only later once I've fully registered with a TVA, which may be some years away. As I am quite concerned about climate I choose to allow 15% of all my Minted Personal Yoonicoins to be donated to Climate Orgs and I get Fixed Mint Generator Tokens in return.

This sign up process creates a Personal Mint on the currency system with my unique PersonalMintID and which starts creating Personal Yoonicoins at a steady rate each day, e.g. 1 per day. The rate of production will decrease gradually as time goes on (see table in previous section).

The sign up process also creates a IP Yoonicoin Account on the currency system which starts to Mine small amounts of IP Yoonicoins, maybe 0.1 per day, for the specific IP address that I'm running on from home (obviously shared equally if there are other people running miners on the same IP address). I am told that IP Yoonicoins are not linked to my Mint and so can be sold/traded freely and that anyone who owns them can, at any point, convert them into Personal Yoonicoins. This is something that people are only likely to do once Personal Yoonicoins become saleable, which will be further into the future.

By registering at least once a week (month?) I'm guaranteed for all this mining to continue to happen, and so I get my Mac to run the scripts in the background at a low CPU priority level and only when I'm online.

I am also entered into the draw every 1 minute for the 1 in a 100,000 chance of getting 100,000 IP Yoonicoins (so approx one in 50 people win this every year at first – when there aren't many people on the network). This is a fun thing to be entered into, but isn't a big draw for me to be involved in.

2023 – Year 1

As I get more into it and trust the open source software, I decide to set up a cheap YoonicoinBlockchainNode on Amazon AWS using a pre-built shared AMI (or download the Docker image and run it on my computer). This runs a node on the blockchain. I understand that the number of Yoonicoins I get from running this node is designed to be very low (maybe a 5% cut of the IP Yoonicoins that I am earning via IP Yoonicoins) because the system does **not** want to incentivise large numbers of nodes running, as that will unnecessarily use up lots of electricity. I also understand that only 16 nodes are allowed to run and earn Yoonicoins per 256 IP addresses. I run the node because I make a small number of extra IP Yoonicoins, which cover the cost of the server with a small profit, and because I like the idea of running part of the whole blockchain that runs the currency system. The instructions also told me it should only take 20 minutes, and are also written in a really easy way for me to follow, and overall it does only take me 20 minutes to get it up and running.

Once things have been running for a year I have 365 Personal Yoonicoins and 36.5 IP Yoonicoins. I decide to cash in 10 of my IP Yoonicoins and so I sell them using a publicly accessible website to list my sale (no login) and follow the instructions to create a domain name auction for 10 of my IP Yoonicoins with a minimum sale prices of £100 for all of them. The sale of the domain goes through on GoDaddy (a popular domain name registrar) for £150 and I get my money via GoDaddy.

I've also been reading about Chain Of Trust Trading Networks and how I can increase the number of Personal Yoonicoins I own by allowing them to be traded with my friends' Personal Yoonicoins. I have 5 friends who are running Mints. I trust them enough to be fairly sure they would all be running just one Mint each, and that they wouldn't scam me by allowing me to be sold fake coins. So I chat to them about it and then join the network at the same time as them.

To sign up to the Chain Of Trust Trading Network I get the PersonalMintIDs of my 5 friends and enter them into the Trading Networks App together with their first names (or just get an invite through the App or email from them).

As part of the set up process for the App I set:-

- The limits for transfers to each friend – which I set at 10% of all my Personal Coins.
- The commission level for each friend. This is the percentage extra coins I will require in any trade with that person. For example if this is set to 20% then I would be happy to exchange 100 of my coins for 120 of their coins. As there is one friend that I'm not so sure about, I set my commission level for them to 50% and set the rest to 20%.
- The percentage of Personal Yoonicoins that are Minted by my Mint that I want to keep locked in my account and not be available for exchange (50%)
- My minimum sale price for coins, which I set at £5. I'm told that hitting this price would not automatically initiate a sale – the app just notifies me of any potential sales and I would then have to authorise them.

After a few weeks, someone 5 mesh links away is offering £15 per Personal Yoonicoin and this creates a sale chain through me onto someone else 2 mesh links away who is selling their coins for only £2 each. In this exchange process I would exchange 10 coins with my friend Bob at a commission rate of 20%. This means I get 12 of Bob's coins for 10 of mine – so I approve the exchange and once everyone on the chain has given their approval the transaction goes through and my account gets boosted by 2 coins (by having 10 less of my own coins and 12 more of Bob's).

Someone 8 mesh links away is offering £20 per Personal Yoonicoin and wants 30 coins – so £600 being offered in total, and this creates a sale chain ending at me where I will receive £6 per coin for 100 coins = £600 (by the time the coins work through the 8 exchanges the commission levels will reduce the number transferred to them from 100 down to 30). This matches all my requirements and I initiate the sale transaction with the buyer. As describes in the previous section I set up a domain name sale for £600 and the transaction goes through. I end up with 100 less Personal Yoonicoins (so 265 instead of 365) but I have made £600 fiat currency.

2024 – Year 2

After a couple of years I have 900 Personal Yoonicoins - 600 of which are still from my Mint and 300 of which are a mix of coins Minted by my friends. I'm ready to start selling to strangers and so register with a Trusted

Validation Authority. They are a big company like Verisign or GoDaddy (or Google?) that I trust with my personal details and they charge me a £100 fee and take personal ID information from me, which I trust them to keep safe. They visit me and get fingerprint ID + verify my passport. Then they get my Personal Mint ID and register it, linked with all that identity info. They also link up with other TVAs in a large network to compare this Personal Mint ID and identity information, in a way that doesn't involve actually sharing my personal details with any of the other TVAs (TODO: would be good to work out if/how this could be done in more detail).

Once I'm registered I add the Verisign TVA as a "friend" on my Chain Of Trust Trading Network trading app with a high level of trust, so that I only need to earn 10% commission on any trades. This opens up my ability to trade coins with all the people registered with the Verisign TVA, and through them with all the TVAs Verisign is linked to. Using this I'm now able to sell another 100 of my own Personal Coins for £1,300 in an auction. Of the 300 Personal Coins in my account that are owned by other people, 150 of them are registered with TVAs and so I also sell 50 of them for £600. This means I have made £1,900.

2026 – Year 4

I've been Minting and trading coins on the Yoonicoin currency system for 4 years now. I have come into some money through inheritance and, as I've been reading more and more about climate problems across the world, I'm wondering more about whether I can do something about it. I find out more about how Wildcard Generator Tokens work and realise that even though I get them by doing a donation, this is a way of doing something about the climate crisis where I may get at least some reward in the long run. I've also read that the Yoonicoin currency system has generated £300m of donations so far and the levels are rising rapidly. Finally, having read more about it, I realise that as the levels of donations are still quite low as a proportion of the people Minting coins, it's better if I do it now rather than in a few years because the Mint Generation rewards are always split only among those who invested 5 or more years previously (since the coins don't start generating for the first 5 years).

So, I make a donation of £10,000 via the currency system and receive 10,000 Wildcard Generator Tokens.

2030 – Year 8

For some personal reason (a medical problem) I find I need access to cash. I look into it and find that as my Wildcard Generator Tokens are 4 years old they will start generating Personal Yoonicoins in one year's time. They are also more valuable that Fixed Mint Generator Tokens because they can be set to generate coins related to any Mint in the system.

I use an online Yoonicoin Calculator which works out the generation rate I will get, based on the total number of Wildcard Generator Tokens that were bought up to 2026, when I bought mine. It calculates that I will get a 0.0000345% share of the 30% coin generation ability that will be dedicated to Generator Tokens in 2031. As TVAs have come online in recent years and more people have signed up to them, the value of TVA Personal Yoonicoins has increased to a level which means my 10,000 Wildcard Generator Tokens will generate an extra £1,038 worth of coins in just 2031, and increase gradually from there. Because of this, on the open Market each 2026 Wildcard Generator Token is worth £1.57, which means mine are worth £15,700. To pay for the operation I sell £5,000 worth of them, and keep £10,700 worth of them.

My £10,000, which I partly donated because I felt I might get something back, has been helping everyone on the planet avoid climate catastrophe for the last 4 years. Now, when I need help, I'm able to get some of that money back.

(Obviously, in this scenario the price went high enough and the initial number of donors was low enough to cause me to make a profit, but that is going to be the <u>exception rather than the rule</u> as the system moves forward, and generally the amount people get back from Generator Tokens will be <u>less than their donation</u> and so they <u>won't make a profit</u>).

2042 – Year 20

I'm included in a group of people in a local event (which is repeated across the world) where those who donated to the climate crisis, and helped solve it over the last 20 years, are publicly thanked.

The End (of Scenario)

Typical Scenario Run Through – Average UK Person

Here I give a fairly short description of a scenario for an average UK person. They are not technical, and are not particularly concerned about climate change.

2022 – Year 0

Yoonicoin is launched in 2022, but I don't hear anything about it because I'm not involved with or interested in cryptocurrency.

2023 – Year 1

I hear a little bit about Yoonicoin through someone I know and see it being mentioned once or twice in the press. It sounds like something that could be a bubble and not something worth my time investigating.

2024 – Year 2

A couple of people I know have started collecting (or "Minting") Yoonicoin and I've chatted with them about it. I've read about it more in newspapers and seen it discussed on TV and there are still conflicting views about it – some warning about it being a bubble, others saying it's going to be transformative technology. I'm still fairly sceptical, but I've been chatting with someone I know who's been doing it for the last year and they have made me feel more comfortable with the idea. They've been collecting the coins for about a year and have read up on it and explained it to me. They said I can start Minting the coins by installing a simple program that has been checked by multiple well known coding groups, and all it does is safely connect to lots of other computers. This apparently causes these coins called Yoonicoins to be created on my behalf. I don't really understand exactly what it all means but I do understand from him that I'm missing out on collecting the Yoonicoins the longer I leave it, so I start to think I should probably get round to it soon.

Next time I'm round his house I take my laptop and he helps me to go through the simple instructions to get it installed and running.

As part of the setup I have to answer questions about climate stuff and, as I'm not bothered much about that, I just pick 3 orgs that I've heard of, and vote to reduce to 4.5% the percentage of all Minted coins to go to Climate Orgs, as I think giving 5.5% of all proceeds sounds like too much. I don't want any of my Personal Minted coins to be donated to Climate Orgs, so set that to 0%. I'm thinking this whole thing could easily be a flash in the pan, and so am planning to make whatever money I can in the short term before it probably collapses.

My friend tells me to make sure I write down my unique "secret sentence" down in multiple secure hidden places, so I write it down in a couple of places in my house when I get home, and in the back of a book at my mum's house.

Over the next couple of weeks I keep an eye on the Yoonicoin web page that my friend put in my browser bookmarks and I can see that my Personal Yoonicoins are getting "Minted" at a rate of 1 a day and I seem to be getting IP Yoonicoins at a rate of one every 10 days. I've got no idea what that means, and don't really care, so long as I'm not missing out any more… ☺

2025 – Year 3

Since I started Minting Yoonicoins last year, quite a few other people I know have started doing the same – mainly due to the price of IP Yoonicoins going up by quite a lot since then. It seems like lots of people are taking it more seriously, and some people on the television are even talking about it being a threat to normal currency. Other people say that's ridiculous, so at the moment I'm not sure, but still think it's probably not going to last. One of my friends who is more worried about the climate said they sold their IP Yoonicoins and donated the resulting money to Climate Orgs through the currency system, which got them some Wildcard Generator Tokens. They seem to think they could get some of the money back, but they aren't worried about that – more about the climate. I think I'll only believe it when I see it (the climate being that bad, and them getting some of their money back!).

2026 – Year 4

Now more than half of the people I know are signed up and Minting the currency. The currency is getting lots of press attention because it's generated £300m in donations to Climate Orgs, and at the same time there's lots of news about methane releases in the Arctic spiralling out of control and causing all the wild weather that has been affecting global crop supply so badly earlier in the year. A lot of the news is about whether governments should ban the currency, as its growth is starting to be seen as a threat to the value of normal money – or embrace it as a useful way of raising money for climate spending. I'm still on the fence, but starting to become less sceptical.

2027 – Year 5

There have been a lot of changes with Yoonicoins this year. They've suddenly gone a lot more mainstream as big companies like Google and Verisign have started doing identity validation for the Personal Mints. My friend who bought Wildcard Generator Tokens 2 years ago has told me that these Generator Tokens will mean that their Personal Yoonicoin minting rates will up to 60% more than mine in 3 years' time. They will get 1.6 Yoonicoins Minted a day, while I'll still be on 1 a day. He said this means he's actually due to make a profit from the donation. I spoke to him about how much I'd be likely to gain if I donated today and he said I'd probably make less than he will because, as it has become popular, the number of people doing it has gone up a lot, and so in a few years' time the % increase in minting capacity I get will be less because it will be shared out among a lot more people.

I give it some thought and, because I don't really need to make a lot out of the coins and I'm getting more worried about the climate, I decide to sell 50% of my IP Yoonicoins, and donate the proceeds to Climate Orgs and get the Generator Tokens in exchange.

2030 – Year 8

I've got some savings that aren't making any interest, and after talking to my friend about it and doing a bit of online research I decide to invest in some 2026 Wildcard Generator Tokens. I know it's not donating money directly to the climate, but it is rewarding people do did donate money 4 years ago to helping the climate – which we now know is having a positive effects. I also understand that by buying the coins I'm supporting the whole system, which has now created £3.2bn of donations towards the climate crisis and has helped come up with quite a few ways of combating the problem.

So, I take £10,000 in savings and buy approx. 7,000 of the 2026 Wildcard Generator Tokens. I don't know if the coins will go up in value much over the next years, and I know they could go to nothing, but I don't really need the money that much. I'm hoping they will go up in the next years though.

2042 – Year 20

In the end my 7,000 Wildcard Generator Tokens generated a fair amount of Personal Yoonicoins in my Mint and I've worked out they are now worth about £17,000 and have generated about £4,000 worth of Personal Yoonicoins. So it was a pretty good investment as compared to leaving the £10k in the bank earning low interest rates.

The End (of Scenario)

Idea Of Loyalty Points Addition

If you buy an electric car – you're helping reduce CO_2.

Same if you buy only carbon free electricity, or insulate your home, or limit your flights (by taking local holidays) or limit your consumption of goods (especially from abroad) or buy local produce etc etc…

There could be some way of incorporating rewards for doing those things into this system.

Also green/carbon friendly companies may be willing to accept Generator Tokens as payment for their goods, at a preferential rate.

This means if you have invested in the climate crisis and you have e.g. £10 worth of Generator Tokens that are 5 years old, then you may be able to use that to get £15 worth of local produce from a local Eco food cooperative (up to a maximum of 10% of your shop?). This is an example of a "green" company rewarding you for your investment 5 years ago – as you are considered a "climate hero". Maybe if you invested 10 years ago they would give you £20 worth of shopping for £10 worth of coins?

This type of loyalty/points reward could then be added to the list of social + financial rewards that have already been detailed above.

Use Of The System In A Real Situation To Start With

The best way of getting this system going is not to start by thinking of it as a launch of a global currency that will help solve the issues listed.

Instead it is best to find an application that has immediate use. An example of this could be as gaming currency in which any gamer can earn coins by running their own IP Address Mint.

These coins are limited by IP Address and also understood to be convertible into Personal Yoonicoins at a later date.

This could be a good way of getting this system going.

Possible Attacks And Defences

Thought a lot about these, and will include in this paper at some point, but not in this first draft – more fun to do in a group too (if the idea doesn't 'fail fast' first).

Possible Additional Ideas

Gradual Devaluing Of IP Yoonicoins In Relation To Personal Yoonicoins

To avoid the system creating problems with IP addresses being used for mining (like Chia is creating problems for SSD/Hard drives – see article [Chia Is a New Way to Waste Resources for Cryptocurrency](#)), it could be a good idea to set up the initial currency system in a way which causes IP Yoonicoins to devalue over time in relation to Personal Yoonicoins? This would mean the incentives of people interacting with the system will move more towards getting the identity elements set up to support Personal Yoonicoins and away from trying to obtain IP addresses to do Minting on. It will also mean that Personal Yoonicoins will gradually be seen to be more and more valuable in relation to the IP Yoonicoins – which are tradable for "real" money from day one. Questions arise about how to time the gradual devaluation and whether to devalue to zero or not? Ideally devaluation would be in line with uptake of Personal Yoonicoins, so that as they come online and are sold, IP Yoonicoins devalue in relation to that uptake. This sounds like a difficult thing to do, but possible – with more thought.

Issues / Questions

- What happens when someone dies? Is it understood / acceptable that the coin dies with them? If so, is there a way of protecting people from owning too many of one person's coins. Does this mean old people's coins are going to be worth less than young people's coins – sounds like a property lease! Is there a way round this? (probably). Sounds like poor people's coins will be worth less than rich, healthy people's which sounds a bit like the opposite of the aim…! Maybe the coin can continue to be valid after death, with the identity proven by proof of the death of the person – as verified by a TVA? This would get round these problems.

Conclusions

Now you've completed the main section of this document, this section contains some summarising ideas relating to the system as a whole and the concepts involved.

What This System Changes

The human race is stuck. In 100 years people (if there are any) may look back and ask "Why didn't we change or do anything about climate change, when we knew it was happening?" The main answers, I think, relate to psychology, sociology and the way we have evolved. One answer, though, is a more practical one – which is that it requires group action across the whole planet and we currently have a set up where countries compete with each other rather than work together. This has a lot to do with economics and the fact each country runs separate currency and financial systems.

Even if we had a global, democratic government there are lots of things that would prevent that government from having the political will and ability to really work on climate change. These include [the power of corporations to trick the public that it's all in hand](#) and we're going to be OK. I believe a lot of people have a gut feeling that climate change is going to be a big problem, and it isn't being handled, but they don't want to be the ones to sacrifice anything to fix it. This feeling applies at the individual level, the company level and the national level.

This currency system helps solve that problem by allowing everyone who participates in it to collectively decide how much everyone jointly should contribute.

It also builds in the concept of people who contribute to helping climate change now being (possibly) rewarded in the future. This is something I haven't seen any concrete ideas around myself up until now. If I give up my money now, or my company gives up money now, or my country gives up money, now no one is going to come back from the future and say "Wow, you saved us – here's a reward" – but this system tries to rectify that issue by building into the whole currency/financial system a future reward for current investment in fixing the problem.

Finally, I think that as climate change gets worse it's not the climate or the lack of food that's going to cause all the destruction that will affect everyone. It is the increasing instability of countries, politics, mental health and technology, combined with reductions in the ability to live a life with enough food and shelter. As inequality increases nation will turn against nation, and groups within nations will turn against their fellow countrymen. That is the current trajectory, which can be seen already very clearly in the polarisation of politics in the USA and elsewhere. Governments like the UK's are creating harsher and more dictatorial laws to control their populations who are revolting against our civilisation's suicidal direction of travel. Extreme inequality and oppression are going to be a big factor in this destabilisation and destruction. If you imagine that by some miracle everyone could start sharing and living in harmony, then I think we could get through even the worst predictions of climate change, easily managing to share the food and look after each other. I believe, though, that it is a pipe dream to imagine that could happen, but this currency system goes some way to helping us on the road, by building into the financial system a simple idea: *that it would be good to make it so that everyone on this Earth has a the basic resources required to live – regardless of their situation*. There is a growing movement related to something called Universal Basic Income (UBI) related to this idea, and it's being piloted in some places.

A lot of people would argue against the idea of UBI, saying that it would lead to a huge number of people doing nothing and being kept at everyone else's expense. I believe that wouldn't be the case if you provided some meaningful way of making extra money that is sociable, and helped make it part of the culture to do work. At the other end of the scale there would be a rebalancing of "ease of life". If millions no longer are required to work in sweat-shop conditions to just about survive in abject poverty, then they won't. This will mean the average Westerner will no longer be able to buy 50 t-shirts from Primark with a single day's wages. But if you think about it for 2 seconds, why should they be able to if it means someone has to suffer so badly at the other end of the chain of supply?

This system will only succeed if the idea is developed in a way that "takes hold" and gets people to want to be involved. To the average person, if this system seems like it could better their life, and maybe better their chances of a stable future at the same time, then maybe they will buy into it? Out of 7 billion people, the majority probably would support the aims of this currency system.

Why This System May Not Work

Lots of possible reasons this system may not work or "take hold":-

- People may not believe in a system where everyone gets money for *just existing*.
- People may think it's unrealistic to think a cryptocurrency system could be used to generate large amounts of money to work on climate change.
- If it does take off, government or people with large amount of money/power may kill off the system before it can have any influence, as they would see it as a threat to the status quo.
- It all sounds far too complicated and hard to implement.
- It's idealistic, and therefore not rooted in reality, and so won't happen.
- It seems to be talking about things being "fair", but the world isn't fair – the world is how the world is.
- Lots of people believe climate change isn't a big problem, or still can be handled/fixed by politicians.
- Too many possible technical reasons for it not to work, and ways it can be attacked and overwhelmed by adversaries (for example - it's not as secure/strong as a Proof Of Work system like Bitcoin).
- People are increasingly averse to having their private details kept and monitored by organisations and/or government, and so will not want to take part in a system that requires strong requirements for confirming their identity and linking it to a currency. One of the main appeals of Bitcoin to many people seems to be the anonymity involved in the system.
- This system has a requirement for "Trusted" authorities in order to verify the uniqueness of the link between a single person's identity and their Mint. This could possibly to contradict what is says in the main paper about Bitcoin called Bitcoin: A Peer-to-Peer Electronic Cash System i.e. "the main benefits

(of a peer-to-peer cryptocurrency) would be lost if a trusted third party would be required to prevent double spending". The comparison is not exact, since in our system the trusted authority is there to confirm there is only one account on the system related to a unique physical human - but it's possible this is not much different to that authority being trusted with maintaining the crypto "balance" of that one individual and avoiding double spend? (this was pointed out by C.P.)
- Someone else does it first (and/or better?) - see e.g. https://worldcoin.org

Sharing This Document

Plan:-
- Get on Telegram and Discord communities and go to the Proposals/Pitches area, and post details of the idea. For example, pitch idea in few sentences and share website with white paper after:-
    - Celo blockchain - https://celo.org/ - also uses mobile phone.
    - Pi Network - launching mainnet at end of 2021, so are very new. Mobile phone. They have open proposals board, and want to grow the community.
    - Cardano - growing a lot now and doing a lot of different projects. Use Python.
    - Crypto.com - L has a contact there.
    - EIP - Ethereum I????? Proposals - place where people on Ethereum propose ideas and they get voted, and lots of votes gets more interest.
    - Ethereum - if someone gets interested in Ethereum, will def grow in fast way, as it is massive.

When contacting people:-
- Do 2 or 3 lines to pitch. Then link to website. Then ask them to contact me via website contact page if interested in getting involved.

3 line pitch:-
Hi. I'm Steve and I'm working on developing a revolutionary new cryptocurrency called Yoonicoin, in which every human has the opportunity to have their own unique coin continuously "Minted" on their behalf, for free and until they die. The system uses Proof Of Personal Identity and also incorporates mechanisms for raising funds to work on the climate crisis. If it takes off it could be a world changing technology. I'm currently looking for collaborators and investigating ways of funding the project launch. There's a 2 page summary and a White Paper at https://yoonicoin.org/ If it's something you're interested in being involved in please contact me via the website.

Contacted So Far

- *27th Oct 2021 - Posted "pitch" on Celo Discord channel - https://discord.com/channels/600834479145353243/817165752149999637 and Also posted message at https://celo.org/alliance*

Other People/Orgs To Contact

First:

https://youtu.be/Dp-z4PyJ8lk - *Ronnie Moas -- bitcoin ... cryptocurrency ... and income inequality presentation* – a talk about Bitcoin and crypto, including lots of stuff about inequality and the Food For The Poor charity that has raised $1bn. Talk is by Ronnie Moas – Philanthropist, Philosopher, Founder of Standpoint Capital and Cryptocurrency Commentator
Emailed – replied – not interested in side projects.

Then:-

https://davidgerard.co.uk/blockchain/ - Author of
https://foreignpolicy.com/2021/05/23/cryptocurrency-chia-waste-resources-bitcoin/
Chia Is a New Way to Waste Resources for Cryptocurrency
What Bitcoin does for electricity and Ethereum for video cards, Chia does for hard disks.
And of
Attack of the 50 Foot Blockchain
Emailed him 23rd May 2021 (see email title "Crypto without the waste")
No reply still on 11th Sept 2021.

My brothers - Sent
Derek - friend - Sent.

David - friend (also knows one of founders of Hedera Hashgraph blockchain – see https://en.wikipedia.org/wiki/Hashgraph based in Texas + "The company was co-founded by Leemon Baird and Mance Harmon") - Sent.

Bram Cohen – at Chia Networks – founder of BitTorrent (can email him at that address) - and creator of Chiacoin – see
https://foreignpolicy.com/2021/05/23/cryptocurrency-chia-waste-resources-bitcoin/ "Bram Cohen is famed as the creator of the hugely popular BitTorrent file distribution protocol. Cohen turned his attention to the proof-of-work problem. He explicitly wanted a "green bitcoin," so Chia, founded by Cohen, works very much like Bitcoin apart from proof of work. Chia's business white paper advocates the same conspiracy theory economics that was embraced by the Bitcoin subculture: It assumes that governments fundamentally cannot be trusted to issue money and wasting a country's worth of electricity is a better alternative." - he wanted a green bitcoin, but his invention is going to lead to huge waste in SSD/Hard Drives if it does well. Yoonicoin avoids that by making the IP address and the human the things that are limited in supply (and you can do things to avoid IP addresses getting wasted or used up, and it's unlikely that humans are going to be "farmed" or wasted as a resource in order to generate Yoonicoin). Could be better to connect with the Chia Network people by starting a chat on their Keybase channel at https://keybase.io/team/chia_network.public and post a link to the website once it is up and running. Steve H has joined their chia_network.public team, so can chat on this group at any time.

Russel Brand – Maybe even as a comment in https://www.youtube.com/watch?v=Oe4MrUhuE60 which is a lot about inequality – and mentions bit in his book where he quotes someone called Slingerland who talks about "humankind's innate expectation of fairness".

Richard D. Bartlett – who created Microsolidarity group and introduced me to SEEDS cryptocurrency + ask him to intro me to any people he knows who may be interested in this paper.

Delton Chen - Coin guy I'm in contact with on email and had Zoom session with in Australia. Talked about in this paper https://mashable.com/feature/carbon-coin-climate-change-crypto/?europe=true https://www.yayzy.com - to contact maybe when launch paper, as they have written a system to try to make people more sustainable and seem very technical. They contacted me at Climate Change Coders.

Ecosia - contact them with details of the paper, anyone who helped found it or funded it – as they did the search engine that puts money into buying trees (so obv green and v technical).

Universal Basic Income campaign groups.

Climate Change Coders meetings.

ClimateAction.tech

Later:-

Climate Emergency Fund - https://climateemergencyfund.org/
Founded by rich Silicon Valley entrepreneur who had a "wake up call" to climate change when he narrowly escaped death when his house burnt down in Californian wild-fires. Provides funds to projects related to climate change.

https://youtu.be/QalnmhzFdwE - *Can crypto solve wealth inequality? | The Future of Money | Yang Speaks* - discussion about how crypto addresses inequality – would be good maybe to add these people to the list of people to send paper to (later stages).

George Monbiot – author of The Age Of Consent which describes democratic, political globalisation. Maybe a cryptocurrency system like Yoonicoin could be a route to having global voting and global investment in important areas such as climate change. Having read the book myself, I couldn't see a route from where we are now to the global government described in the book. Maybe a global cryptocurrency like this could be a means of heading in that direction?

Tim Jackson – Author of Prosperity Without Growth

https://www.paulmason.org/bio/ - author of Postcapitalism – "economics editor at both BBC Newsnight (2001-13) and Channel 4 News (2013-16)"

Elon Musk – co-inventor of PayPal (so knows a thing or two about money) and also crypto investor, but now critical of Bitcoin due to environmental concerns. Also founded Tesla, one of most popular electric car makes (so low CO_2).

https://soundcloud.com/user-184737530/lucy-hogarth - "*Lucy explains why she is interested to learn more about why people don't want to talk about climate change, why Extinction Rebellion is seen as a left-wing group, and some difficult conversations she has had with her family*." Interesting quote at 14 minutes saying: "The free market is destroying itself. It's a massive failure on a scale which is very difficult to comprehend to many who are believers of it". Yoonicoin maybe gives us a possible way out of this as no regulation involved? Everyone joining system voluntarily.

https://soundcloud.com/user-184737530/dr-aaron-thierry - Dr aaron Thierry - really nice guy who is researching how Climate Orgs can communicate more effectively science.
https://wiserd.ac.uk/about-us/people/aaron-thierry Thierryat@cardiff.ac.uk   "My past experiences have led me to become fascinated by the question of how to accurately convey scientific warnings of

environmental risks in ways that help wake the public to action. To better understand this crucial conundrum, I have chosen to return to research and have begun a new PhD examining the interplay between reason and emotion in the communication strategies of organization's in the climate emergency movement."

People Angus could recommend?

Crypto investor people

Algorand founder + company?

https://youtu.be/QalnmhzFdwE - talks about how crypto addresses inequality – would be good maybe to add these people to the list of people to send paper too (later stages)

https://youtu.be/WDo_Jlov9R4 - *Can Bitcoin and other cryptocurrencies solve root causes of poverty? | Nir Kshetri | TEDxGreensboro* – TEDx talk about how Crypto could help with poverty.

Savva – as interested in Crypto investments.

Relevant YouTube Videos I Found

https://youtu.be/Dp-z4PyJ8lk - *Ronnie Moas -- bitcoin ... cryptocurrency ... and income inequality presentation* – Talk about Bitcoin and crypto, including lots of stuff about inequality and the Food For The Poor charity that has raised $1bn. Talk is by Ronnie Moas – Philanthropist, Philosopher, Founder of Standpoint Capital and Cryptocurrency Commentator.

https://youtu.be/QalnmhzFdwE - *Can crypto solve wealth inequality? | The Future of Money | Yang Speaks* - discussion about how crypto addresses inequality – would be good maybe to add these people to the list of people to send paper to (later stages). Mentions Andrew Yang's Universal Basic Income system - https://www.newyorker.com/news/our-local-correspondents/andrew-yangs-ideas-on-universal-basic-income-earned-him-fans-but-can-he-win-votes

https://youtu.be/WDo_Jlov9R4 - *Can Bitcoin and other cryptocurrencies solve root causes of poverty? | Nir Kshetri | TEDxGreensboro* – TEDx talk about how Crypto could help with poverty. References quite a few useful/relevant organisations and charities including:-

- https://humaniq.com/
- https://www.digitaltrends.com/cool-tech/world-food-programme-building-blocks-iris-scanning-blockchain/ and https://innovation.wfp.org/project/building-blocks

https://www.givecrypto.org/ - Charity founded by co-founder of Coinbase, Brian Armstrong, which has raised $4m (May 2021) by giving cryptocurrency to people living in poverty.

Next Steps

To be filled in.

- Send out to people in list above asking for feedback

- Especially search for and target people who understand/interested in Economics/Crypto – so they can say if/why this system would not work.
- Include people's feedback in later versions of this doc (perhaps publish online if no reason to keep secret?)
- If find people interested in idea then:-
    - Work on developing this paper and ideas further with them, and doing further research with them, including contacting further people who could be interested.
    - Possibly look into getting funding for the idea?
    - Possibly look into creating an alpha version of the system?

Getting Involved

You can get involved by contacting me via the website contact form.

Last (Joke) Word

"I believe in Yoonicoins! Do you believe in Yoonicoins?"

This Document – Still To Do

- Add few sentences about Chia Coin - https://en.wikipedia.org/wiki/Bram_Cohen#Chia and https://en.wikipedia.org/wiki/Proof_of_space#Proof_of_storage
- Possibly move No Dealer section into Appendix and refer to it as a possible use, rather than an expected use?
- Time a full reading of this doc (not inc. Appendices, and add Appendices).
- Send email with 2 pager attached to other people

Appendices

Appendix A – Notes And References On The Algorand Currency System

See https://en.wikipedia.org/wiki/Silvio_Micali for details of its founder and for details of the product.

See https://www.algorand.com/resources/white-papers for a list of white papers and https://algorandcom.cdn.prismic.io/algorandcom%2Fa26acb80-b80c-46ff-a1ab-a8121f74f3a3_p51-gilad.pdf for the white paper describing the algorithm used.

https://www.linkedin.com/pulse/algorands-core-technology-nutshell-silvio-micali/ - is written by Silvio Micali, the founder of Algorand, and describes Algorand's "Pure Proof Of Stake (PPoS)" protocol, which he compares with other Proof Of Work and Proof Of Stake protocols. It describes how a random selection process is combined with the number of coins a node has to determine whether it will be "elected" into a committee, which then decides which node produces the next block.

https://www.algorand.com/resources/blog/secure-blockchain-decentralization-via-committees - does more comparisons with existing Proof Of Stake blockchains.

https://algorand.foundation/algorand-protocol/core-blockchain-innovation - says "Algorand uses cryptographic sortition to select users to propose blocks for a given round. When a block is proposed to the blockchain, a committee of voters is selected to vote on the block proposal. If a super majority of the votes are from honest

participants, the block can be certified." More details at:
https://algorand.foundation/algorand-protocol/core-blockchain-innovation/protocol-participation

There is a "protocol overview" at:-
https://www.algorand.com/what-we-do/technology/protocol-overview which describes how committees of nodes are created to propose blocks, then a "soft vote" is performed to propose the new block, then a "certify vote" is done with a newly selected random committee of nodes to certify the vote before it is finally written. The bigger stake you have in the system, the more likely you are to get to take part in this process.

This protocol is designed to withstand attacks from a combined group of malicious users, so long as their combined stake is less than one third of the total.

https://medium.com/@jsign.uy/the-intuition-behind-algorand-cryptographic-sortition-526e76e87e97 - gives a non mathematical (i.e. intuitive) description of "cryptographic sortition" which is how users in the Algorand system are selected to be on the committee that can propose the block for the next round.

https://www.algorand.com/resources/blog/opensourceavailable is about open sourcing Algorand system.

https://medium.com/algorand/algorand-releases-first-open-source-code-of-verifiable-random-function-93c2960abd61 is about open sourcing the VRF code and includes a section on the VRF syntax and properties, a section describing its use on the Algorand blockchain.

https://github.com/algorand/libsodium/tree/draft-irtf-cfrg-vrf-03 - This is the GitHub site for the open source version of the Verifiable Random Function code.

https://forum.algorand.org/t/relay-node-rewards/724 - seems to show that in March 2021 it's fairly unclear whether you can earn money by running the Algorand blockchain, and the situation is fairly confusing.
https://algorand.foundation/faq#running-nodes- - seems to show there is confusion as to whether the Algorand blockchain is mostly run on a series of controlled VP and University nodes, but the answer explains that only the Relay Nodes are run on that set list of places and they just provide performance.
https://www.purestake.com/blog/algorand-rewards-distribution-explained/ - explains how anyone running the Algorand blockchain gets rewards in the form of a set level of interest on their Algos.
https://www.coingecko.com/en/coins/algorand - Price history showing an Algo started out at around $1.50 and then was about $0.20 for most of 2019 and 2020 and went up to $1.10 for Feb + Mar 2021
https://medium.com/algorand/introducing-sandbox-the-quick-way-to-get-started-on-algorand-8082c2d18854 - How to run Algorand using Docker in a few minutes, using code created at https://github.com/algorand/sandbox
https://www.algorand.com/about/our-history - A history of Algorand up to August 2019 (including launch of "MainNet" in June 2019).

Algorand sites:-

- https://www.algorand.com/
- https://developer.algorand.org/
- https://algorand.foundation/
- https://forum.algorand.org/
- https://community.algorand.org/

Appendix B – Notes And References On Verifiable Random Functions

A really good description of VRF including a Technical Walkthrough can be found at Chainlink VRF: On-chain Verifiable Randomness

The internet draft about Verifiable Random Functions is at:-

https://tools.ietf.org/id/draft-goldbe-vrf-01.html#:~:text=A%20Verifiable%20Random%20Function%20(VRF,of%20hash%2Dbased%20data%20structures.
Another internet draft on Verifiable Random Functions including descriptions of the constructions when using both RSA encryption and Eliptic Curves can be found at:-
https://tools.ietf.org/html/draft-irtf-cfrg-vrf-00

Wikipedia page:- https://en.wikipedia.org/wiki/Verifiable_random_function

The libsodium security library was forked by the Algorand and then the following commit added the VRF implementation:-
https://github.com/algorand/libsodium/commit/23b235c09e9c77fc64f027d59d6ea30d1a698a5c#diff-0fa10ddd90b025e289f8346708cdbacb60fc7c8dfae620f3c619346d60f973c4

The README for the above addition to the libsodium library to create the VRF code can be found at `src/libsodium/crypto_vrf/ietfdraft03/README` and contains a useful description of each of the classes supplied.

Relevant papers/urls:-
- Making NSEC5 Practical for DNSSEC – The 2017 Goldberg paper describing Verifiable Random Functions.
- The 2002 paper RSA Key Generation with Verifiable Randomness may be relevant to this.

Appendix C – How The No Dealer Algorithm Works

As mentioned previously, the algorithm for creating the random numbers could make use of a recently invented algorithm called "No Dealer" (No-Dealer: Byzantine Fault-Tolerant Random Number Generator – IEEE – July 2020).

TODO: if going to use this algorithm: check whether it's legally OK to use an algorithm like this in a system without explitely obtaining permission or paying for it it – see this relevant thread.

As mentioned in the main section, it may be the case that this algorithm is not actually required in order to implement this system, since random numbers could be generated in a provably random way using the Verifiable Random Functions (VRFs) that are used in the Algorand blockchain.

On the other hand it may be useful as a complementary method of choosing a random member of the final committee in order to reach consensus on who generates the next coin.

In this section I give some details of the algorithm described in the No Dealer paper and it's possible use in this system. If you're not that interested in the detailed implementation of this algorithm you can skip this section. It's enough to know that this is a recently invented algorithm that allows a group of computer nodes on a network to generate a provably random number through collaboration in a way that prevents anyone manipulating the outcome, unless they control half or more of the nodes. As an example if there are 100 nodes and 51 of them are honest, then 49 of them cannot calculate or manipulate the final random number produced – even by "disappearing" at any stage during the process.

The paper can be obtained and downloaded for a fee of $33 from this URL on the IEEE website.

In the introduction to the paper the authors say that the algorithm described in the paper could be used as "a building block" of a distributed ledger (blockchain). That is what I am intending to use it for (if it's required).

The paper provides some useful background on the problem being solved. This problem occurs when you want to have a group of computers on a network collaborate to produce a provably random number. In our case this would be a set of hundreds or thousands of blockchain nodes all working together to produce a provably random number that will be used to select the next coin producer.

It's easy to devise an algorithm that produces a provably random number when you can be sure that **all** players in the game can't leave the game. If, for example, you wanted to generate a random number between 1 and 1000 using 10 nodes you could use the following algorithm:-

- Get all nodes to create a provably random public/private key pair using something like the algorithm described at [RSA Key Generation with Verifiable Randomness]
- All nodes generate a random number between 1 and 1000 and encrypt it using their public key.
- They publish the public key and the encrypted random number to everyone and keep the random number and the private key secret.
- All nodes confirm all public keys generated are definitely random.
- All nodes reveal their random number, in whatever order.
- All nodes confirm that encrypting the random number using the published public key produces the encrypted random number previously published.
- Calculate final random number as the sum of all the 10 random numbers modulo 1000 (i.e. obtain the remainder after dividing the number by 1000)

If no-one leaves the game during play then the number you end up with should be a random number between 1 and 1000. In order to influence the final number you would have to have control of all 10 nodes (i.e. the entire system) because even if you controlled 9 of the 10 nodes you have no idea what Public Key the other "honest" node is going to publish, and you have no idea what random number it has chosen. Your 9 "cheating" nodes are forced to publish random public keys and once all 10 are published, you can try to manipulate the outcome by choosing different random numbers, but you won't be able to. That is because:-

- If you want a low random number (e.g. < 300) then you may get your 9 cheating nodes to all choose "1" as their random number, but then the 10th "honest" random number is going to be randomly between 1 and 1000 and so end up giving you a random number anywhere between 10 and 1000 and 1 and 10, i.e. a random number between 1 and 1000.
- Once all public keys and encrypted random numbers have been published there is no way to change the final random number (apart from disappearing) and you still don't know at this stage anything about the random number chosen by the honest node.

So, this all sounds very hopeful. But then you start to realise that nodes **can** influence the outcome by disappearing off of the network ("my broadband went down!"). If the above game is being played and you were trying to influence the random number then you could just wait until everyone else has published their random number, work out what the final random number will end up being once yours is published and if you don't like that number just "disappear" so the game gets cancelled (presumably after a certain "timeout" level) and then re-join for the next game. You could just keep doing this until a number that you like comes up (e.g. one that gives you the next coin production rights).

There are ways of limiting the ability to cheat in this way – which include getting nodes to commit a certain amount of "stake" before playing a game and then losing that stake if they disappear (as punishment). These techniques aren't entirely reliable and there are ways round them.

The "No Dealer" paper comes up with an algorithm which solves this problem. This is done by having all 100 nodes go through a series of steps and calculations where each node communicates with all the other nodes and performs calculations based on those communications.

The steps are similar to the ones described above where there are phases where nodes commit to a certain outcome by submitting encrypted versions of their calculations.

The way the algorithm is done prevents anyone being able to control, or stop publication of, the random number unless they control half or more of the nodes on the network.

In an example with 100 nodes, it's possible to have someone trying to cheat the system who controls 49 of the nodes, but still not be able to influence the final random number or prevent its publication.

This is because, in the final stage where each nodes takes it in turns to reveal their final calculation the following is true:-

- Like in the previous scenario – at publication stage it's impossible to fake your numbers - you are committed to revealing the true random number you committed to earlier in the process. Your only way to try to cheat the system is to "disappear"
- Knowing 49 of the 100 numbers is not enough to work out anything about the final random number.
- Once 51 nodes have published their final number, the final random number can be calculated by anyone in the system.

So it doesn't matter what your 49 nodes do, or which 49 nodes they are. If some of them publish their number (e.g. 10 of them) then only 41 of the honest nodes need to publish and then everyone can calculate the final random number. If 2 of the honest nodes publish, then you can straight away work out what the final number will be using those 2 numbers + the 49 you know – but if you don't like the number you can't prevent publication since "disappearing" your 49 nodes will have no effect. The remaining 49 honest nodes will publish their numbers and then the final number will be able to be calculated.

The maths used in the paper isn't too advanced – probably about degree level. The code for running the algorithm has been written in Python and has been made available for viewing and download, although it has no licence associated with it and so isn't open sourced. The URL provided in the paper for this code no longer works, but it seems likely the code has just been moved from that URL to another publicly available one at https://gitlab.com/gregorymel/bft_rng_hashgraph with a different name.

One of the main potential problems with the algorithm is that it requires all nodes to communicate with all other nodes. For a 10,000 node system that would take a lot of time and computing resources. So I can imagine that this algorithm may be useful for 10 -> 300 nodes if you want to run the algorithm within a few seconds?

The algorithm also relies on a reliable shared storage for publishing the results as it proceeds (like a blockchain). Not sure if that could present problems? Hopefully not, if you can use the blockchain that you are running using the algorithm (is that a circular argument?)

Finally, the algorithm assumes a synchronous network – i.e. one in which messages between nodes are delivered within a set amount of time T. How this could work on the internet in a blockchain system, I'm not sure, but I don't think it would have to be a blocker. If a message isn't received within time T from a node, then probably you can just assume that node has gone (either accidentally or on purpose) and you re-start the whole algorithm, or if you are in the final stage of the algorithm – you just calculate the final number without it.

Appendix D – Ditched Ideas That May Still Prove Useful At Some Point

The appendix contains some ideas that didn't make the final cut, but may end up being useful in some form later?

Ditched Idea - Physical Address Limited Minting

(Ditched because it may overcomplicate the plan, and now think that IP Yoonicoins that are convertible later into Personal Yoonicoins is enough to kickstart the whole process, and Personal Yoonicoins will start being minted early, then will be validated later by TVAs without the need to introduce intermediate physical address and phone stages).

A possible way of limiting minting could be through physical address verification. This is possibly a good way of doing things, since addresses are already public (names obviously are not), although of course then there is a link between the blockchain account and a physical address, which may not be ideal if you own a very large number of coins – as it may make you a target.

Probably this isn't a great way of doing things and introduces complications, but I'm leaving it in here for the moment – and may remove it later.

Ditched Idea - Phone Number Limited Minting

(Ditched because it may overcomplicate the plan, and now think that IP Yoonicoins that are convertible later into Personal Yoonicoins is enough to kickstart the whole process, and Personal Yoonicoins will start being minted early, then will be validated later by TVAs without the need to introduce intermediate physical address and phone stages).

There are 4.88 billion cellphone owners in the world today, 62% of the population. As approx. 30% of the world population are under 18 this means there are 5.46 billion adults and 2.3 billion children. So maybe 80% of adults own a mobile phone?

Most people who know other people have them linked to only one phone number, and historically most people only have one mobile phone number.

It could be possible then to create Mobile Phone Mints that can be trusted as being linked to a person by all the people who have known that person to own that phone number for a while. This doesn't stop any person going and getting 10 other phone numbers, but people who know them would be unlikely to trust the Mints they create that are linked to those phone numbers.

All this would be done on the understanding that Mobile Phone Mint is a step on the way to getting a Person Validated Mint where some Trusted Verification Authority can use whatever method to make me trust that the Mint I am buying coins from is uniquely linked to the adult human that it is meant to be linked to.

It's also not clear whether this Phone Number Mint stage adds any value, or whether it may overcomplicate things. It could be a valuable and useful stepping stone to Person Validated Mints.

A possible benefit of this stage of minting is that it allows people who don't own computers, but do own mobile phones to validate themselves and participate in using currency, even if this is only by validating transactions by sending secret string over text messages.

A problem with this is the idea of making public a mobile phone number on the blockchain. There may be ways round this where the Mint is uniquely linkable to a mobile phone number if you know the mobile phone number, but you can't get the mobile phone number just by knowing about the Mint? If this is done simply using a public encryption technique then unfortunately it can be brute force attacked easily where you go through every phone number in the world, follow the algorithm to get to the Mint and then record the ID and repeat until you have the full list – at which point you can just look it up in the list to find which phone number is linked to a particular Mint. Ways of preventing this attack could include:-

- You only get to find the Mint ID when you are doing a paid transaction, which would make it too expensive to do a brute force attack?
- There is no link provided with the Mint ID when you do a transaction on a phone number. It happens in a non-traceable way but you do get a transaction receipt which verifies that you own that amount of coin, but the details of which Mint it is in are hidden from you (but traceable through the system via a number of replicated nodes – so that the **system** can do the transaction without you knowing who's Mint it came from – a bit like the Dark Web and the Onion browser which allows you to connect to an end point with

content but for you to have no way of knowing what IP address that endpoint is running on without hacking into or controlling every computer that is on the chain between you and the endpoint). The system also records the details in a way that means it is permanently verifiable but untraceable to the Mint without you having access to or controlling a large number of nodes that link you to the source where the Mint details are stored. (NOTE: Not sure if this idea is useful, or possibly completely invalidates the whole idea of having a Person/MobilePhone connected Mint?)

Ditched Idea - Only One Type Of Validation Per Minted Coin Type

(Ditched because now we have three simpler stages (1) IP Yoonicoins (2) Limited exchange of Personal Coins using personal trust chains (3) Wider exchange of Personal Coins using TVAs, and adding different Personal Yoonicoin types would just complicate things. Instead the TVAs would have to link up and manage it so that one person can't have a TVA identified Mint using a Passport and a separate TVA identified Mint using a Driving Licence)

Because each Minted coin needs to be linked to a person in a one-to-one relationship it means that we have to be sure that that person is not linked to more than one Mint for that type of coin. To do this we have to strictly define and limit the **way** in which the person is identified for that particular coin type (not sure this is needed any more ????)

To show this, imagine we had a system where you could use any of the above methods to identify a person. This would mean I could cheat the system easily by running two Steve Mints:-

(1) A Mint with ID = Steve123 identified by Driving Licence ID: UK – AB123ZXY
(2) A Mint with ID = Steve567 identified by Passport Number: UK - 123456789

I could be verified (using whatever technique – even a Trusted Validation Authority) for both of these types of IDs, but I'm still running two Mints in my name without anyone being able to confirm I am not.

It seems the only way around this is to have a whole Coin Type that is defined by the method of identification that blocks me from creating two Mints for myself on that Coin Type.

So, there could be a Driving Licence Validated Personal Yoonicoin which is a type of Yoonicoin that is uniquely linked to me through by Driving Licence ID country and driving licence number. Or similarly a Passport Validated Personal Yoonicoin that does the same using my country and passport number.

It would have to be understood (and made clear) that each of these currencies are separate.

Ditched Idea - Documenting Method Of Driving Licence Validation

(This idea was ditched because it was about being able to validate someone else's identity on my own without using a TVA – don't think we need that now as have multiple stages on the way to full TVA without having to do this stuff, and providing identity validation information over the internet to strangers could create lots of issues).

Don't think I like the idea of people using ID forms of validation direct one-to-one between buyer and seller any more, since this involves exchanging some forms of personal information with people you have no understanding of trust about.

This method **could** be used in the UK by Trusted Verification Authorities to easily verify a driving licence ID, but probably isn't strong enough to do the job on its own. If we decided to use direct one-to-one trust of people you don't know (or even people you do know?) this could be one tool in the box.

In the UK you can verify someone's driving licence record using a govt service which involves getting them to issue you a Check Code.

The person with the licence goes to:-
https://www.gov.uk/view-driving-licence

and enters their:-
- Driving licence number
- National Insurance number
- Postcode

The government database confirms the details and then issues an 8 digit one time use Check Code.

They give this to the person who needs to check the licence, together with the last 8 characters of their driving licence number and that person goes to:-

https://www.gov.uk/check-driving-information

and enters the information and is then given access to the person's driving record which includes their full name.

If this was used on the blockchain then:-
- The Mint account could be stored with a combination of the FullName + Last 8 Digits Of Driving Licence – encrypted using the Public Key of the Mint to create FullNamePlusLast8DigitsDrivingLicenceEncrypted that is permanently stored on the account.
- When buyer A wants to purchase coins from seller B they could request a Check Code and the last 8 characters of their driving licence to verify their account.
- Seller B follows process above and sends code to buyer A.
- Buyer A follows process on govt website to get full name of Seller B.
- Buyer A uses the Mint public key to encrypt combination of the FullName + Last 8 Digits Of Driving Licence and compares this with FullNamePlusLast8DigitsDrivingLicenceEncrypted on the account. If it matches they continue.
- Crucially, Buyer A **only** transfers money through online banking services (or by paying into bank account at Seller B's bank) and **only** in a way that verifies Buyer A is the correctly named account holder. If the account name doesn't match, the sale transaction does not go through.

The main problem with this is that it doesn't allow an easy way of verifying that this particular seller isn't running 1,000 Mints using the same ID details, which makes it fairly useless.

Could make the combination of the FullName + Last 8 Digits Of Driving Licence public, but that becomes a massive privacy issue.
Could encrypt it using some shared public key, but then this could be brute force attacked to match up lists of know people + known driving licence numbers with accounts to reveal account information.
Even if you do the above, it doesn't get round the possibility of the person having one Driving Licence ID Mint and another Passport ID Mint and making money off one while they know the other one is the one that will end up genuine (at which point they could claim the other one was set up by a scammer, not them and the people who bought the coins from that dud account end up with worthless coins).

Ditched Idea - Concept Of Supercoin

(Ditched this idea because IP Yoonicoins are saleable from an early stage and can end up being converted into a single Personal Yoonicoin that the person knows is genuine, so this does the equivalent of a Supercoin as defined here and so makes it redundant. Also can imagine the process of accounting for a coin that is a tiny portion of every coin on the system could get very complex).

While the system is developing and maturing, it's harder to determine whether any particular coin is genuine and only being mined by one single person, **but** it is possible to know that for every person doing mining there will be a Mint which they will/should end up declaring as their Mint and can be verifiably owned by them.

So, we introduce the concept of a Supercoin – which is a coin which is recorded in having a tiny, equal stake in every single Minted Coin currently in production on the blockchain.

Anyone owning this coin would understand that once, in the future, the individual coins become verified, they will be able to conduct transactions in which the ownership of those coins is verified.

Unlike normal Minted Coins this Supercoin should be tradable from a very early point in the system, without any need to verify anyone's identity – just a belief that the system will evolve in some point in the future to a point where many of the current Minted Coins are verifiable.

Ditched Idea – Mining IP Yoonicoins By Making Calls To Well Known Website APIs

The following text related to a possible idea about creating an easy way of allowing people to mine Yoonicoins – just by visiting a web page on a system they trust (e.g. Facebook, Wordpress etc)

I removed it from the main text as just seemed to complicate things, but I've put it here as there is a chance it could be useful.

Ideally, just visiting a particular page on a large number of trusted websites could be enough to verify that person's IP to the system and therefore gain the mining rights for that week (or period of time). Obviously if other people visit from that IP block then IP Yoonicoin mining rights would be shared. Mining of Personal Yoonicoins could be done by any person on any IP, although there would probably have to be some way of limiting the number of new registrants (maybe by referral and/or by IP?)

We need to work out how this IP address could be verified and the information about it distributed across the whole system.

Example of things that *may* be able to log and publicly prove IP address:-

- Facebook Apps?
- Wikipedia and/or other WikiMedia site tools that log edits by IP address for anonymous users?
- Wordpress Comments

The mining could be done manually by the person if it's only a few web pages they have to visit and comment, or it could be done using a script running on their computer that just calls a few web page APIs. An example of this API could be the Wordpress "comments" API described at https://developer.wordpress.org/rest-api/reference/comments/ which provides the IP address of any person who sent a comment.

If people don't like downloading and running scripts another way it could be done is that the mining person goes to a webpage and then clicks on a link to e.g. a Facebook page, which contains the next link to e.g. Wordpress.com site which contains the next link to e.g. a Google website page etc etc. Maybe by following these breadcrumbs they can prove their IP address on 10 systems once a week, which would be enough to count as their mining work for the week – and may only take 5 seconds to do. They can see from the url of each website e.g. yoonicoinsite25.wordpress.com that the pages they are clicking on are all on trusted websites and so they won't feel that it's risky to go to these pages.