UBI 4 all

Gaston Maffei

May 2021

1 Introduction

The UBI project based on the Proof of Humanity (PoH) protocol is an ambitious quest to provide each unique existing individual with a basic income, no strings attached. In part to protect the network from easy malicious attacks such as double sign ups, the registration process requires the person to deposit a non-negligible amount of money (0.157ETH or 471 USD at the time of this writing) as a guarantee while the profile is inspected. If a flaw is found, the deposit is lost. On top of that, the registration is quite expensive in terms of gas. The problem is: the people that could benefit from UBI the most are often unable to provide such funding by themselves, let alone risk losing it. While the protocol incorporates the possibility of a 3rd party funding another person's application, the problem still remains: many people who would greatly benefit from UBI don't have the resources or don't know people with the resources (both monetary **and** of technical knowledge to operate ethereum transactions) to fund their applications.

2 Objective, Caveats and Constraints

The objective, then, is to create a system which allows for people to get validated into the PoH network even when they lack the financial resources and/or personal connections to do so in the conventional way. As is the case with everything that's built, this system has some design constraints which it should meet. They are listed below.

1. **Transparency.** The management of funds should be done according to clear and transparent rules.
2. **Risk dilution.** No one individual should face the financial consequences of a failed profile registration (for example in the case of a challenge against it).
3. **Little contributions.** The system should support the decentralized donation of little amounts of money so that anyone can contribute that which they are able/willing to.

4. **Easy to use.** It should be fairly easy to contribute financial aid to the crowdfunding system.

5. **(Weak) trustless.** The continued working of the protocol should not depend on a single person or on the confidence deposited in a single person.

6. **Efficiency.** Some of the money is necessarily going to be lost on gas. The protocol should obviously spend the money as efficiently as possible.

7. **Scalability.** The protocol should easily scale to help hundreds and even thousands of people.

8. **Reach.** The protocol should cover the registration costs *after* the profile has been submitted. This means that the profile submission fees are still on the person being registered.

3 Bits and Pieces

3.1 Protocol Overview

An elevator pitch of the crowdfunding protocol would go as follows:

"On one side, people who need funding sign up on a website and only their relevant data (PoH profile, etc) is stored in a database. All applicants are ordered dynamically according to simple rules and this data can be accessed through a simple REST API. On the other side, money (of many possible sources) is deposited in a multisig wallet, the VAULT*, with n trusted owners, the* GUARDIANS*. Guardians run a bot that continuously queries the API for instructions on who gets to be funded next and proceed to sign off on the relevant transactions between the wallet and the PoH SC. Profiles are therefore continuously being registered and funded."*

Now, in more detail.

3.2 Frontend and Backend

Applicants that wish to have their submissions funded apply through a simple website in which they enter their PoH profile (which they must already have to receive a crowdfunded deposit). This, along with other relevant metadata (application date and time, registration status, etc.), is sent to a backend, which hosts two important pieces: a database where the data is stored and a REST API which can be queried to gather relevant information about the crowdfunding state (such as who gets to get funded next, etc.).

3.2.1 Stored Data

For each applicant, the following data is stored in the DB:

1. PoH profile
2. PoH profile status
3. Date and time of application to the crowdfunding protocol
4. Internal crowdfunding status
5. Number of applicants verified (explained later)
6. Duplicates found (explained later)

3.2.2 Ordering

The ordering is done according to very simple and clear rules to make the process transparent. Priority is given in the form of points to those who applied first. To incentivize actions that make the protocol self-sustainable and also help deter possible duplicate attacks, applicants are given extra points in the following scenarios:

- some extra points for verifying and certifying the validity of other profiles. Should a certified profile be found to be a duplicate or otherwise fraudulent/in breach of PoH rules, that profile **and** all the profiles which certified its validity will be permanently removed from consideration for further funding. **Important:** certifying at least two other profiles is mandatory to be considered for crowdfunding. Certifying more will grant more points. The crowdfunding protocol might assign the profiles to validate to the applicants.
- a **significant** amount of extra points for finding a PoH profile that has applied for crowdfunding and is in breach of PoH rules (and whose registration would therefore cost the entire deposit).

Much like with PoH, certified profiles will undergo a short period during which they will be shown for verification to other applicants in order to accumulate at least p positive results and reduce the chance of fraud. After that period, and conditional to them having verified at least two other profiles, they will be eligible for crowdfunding.

3.2.3 Interacting with the API

The API is meant to be able to handle:

- adding new applicants
- querying the order of the crowdfund
- assigning new profiles for the applicants to certify
- giving out specific instructions (explained later)

3.3 Guardian Bots

To manage the funds (in a way explained in the following section), n people called *Guardians* will be trusted with special keys, m of which are necessary to approve operations. Managing funds requires doing the following tasks over and over again:

1. Checking for available funds.
2. Querying the API for funding order and instructions on how to proceed. The result might be to fund X's deposit or to fund Y's start accruing.
3. Approve the corresponding transactions.
4. Wait for funds to return.

For a bunch of applicants this is doable but tedious. For tens, cumbersome. For hundreds, crazy. For thousands, impossible. Luckily, humans need not perform this repetitive tasks by themselves: they are easily automated by means of a bot, a *Guardian Bot*, that has the necessary data to operate the funds in a safe manner. Guardians are responsible for keeping their own bots both safe and up and running.

3.4 Vault

The *Vault* is the on-chain smart contract which holds all the funds. It is a multisig wallet which has n owners (each one corresponding to one address operated by a Guardian Bot), m of which are needed as a minimum to sign a transaction (to leave room for Guardian Bots which are down temporarily or permanently for whatever reason). The Vault will only be able to perform two actions:

1. interact with the PoH SC
2. swap ETH/DAI for UBI

The reason for this is to allow for only two things to happen with the funds: funding applicants registrations and eventually burning UBI in case no more funding is needed.

The money deposited into the Vault might come from many different places, such as:

- Private donations
- Earnings from providing liquidity to the UBI pools
- Earnings from a yearn vault

4 Constraints Recap

Let's see if and how the constraints are met under the proposed system.

1. **Transparency.** The management of funds is of course transparent on-chain. Off-chain, the assignment of the recipients of the deposits is done according to clear and simple rules
2. **Risk dilution.** The funds being pooled together, no one person's/institution's donation is lost in case of a faulty registration.
3. **Little contributions.** Any person can donate as much as they want to the pool.
4. **Easy to use.** Any person can contribute as simply as donating to the pool.
5. **(Weak) trustless.** The trust is deposited and distributed among n individuals.
6. **Efficiency.** The wallet only funds deposits and start accruing operations.
7. **Scalability.** Hundreds and even thousands of people can sign up and apply for crowdfunding. Validation and oversight is incentivized in applicants themselves. The whole operation runs smoothly without the need for human intervention other than improvements to the protocol.
8. **Reach.** All stages after profile submission are funded entirely.

Seems good to go.

5 Going Forward

Of course, all contributions are more than welcome. A few topics which could use some additional brain power are:

- How to make this completely decentralized without incurring in extra unnecessary costs.
- How to further protect the protocol from attacks which are now much less costly (profile submission fees vs fees + 0.157 ETH).
- How to make it so that even someone with zero money can enter PoH.

6 F.A.Q.

6.1 What happens if the Vault has a ton of money? Is that not too much power in the hands of the Guardians?

Yes. Guardians are meant to be trustworthy, but the spirit of blockchain is meant to be trustless among other things, and this protocol should aim to be that as much as it can too. One quick and easy partial solution is to have a cap on the amount of money that a single Vault can manage, creating the need for another one with extra Guardians to be created if such a threshold is met.

6.2 What happens if a certified profile is found to be fraudulent and the certifier has already been funded completely?

We will all have to burn some steam. There's nothing to be done at that point other than performing an exhaustive scrutiny of said profile to find out, to the best of our abilities, if it was an honest mistake or if there is a fraud inside the PoH protocol.

6.3 What happens if a Guardian or its Bot goes down?

To account for such a situation and avoid an eventual inevitable loss of funds, the multisig wallet containing them will only need m approvals operate out of the n owners. This way, one or multiple Guardians could, for whatever reason, fail to sign on transactions and the system would continue to work as intended.