Proof of Humanity

Contribute

Feel free to write suggestions and comments directly on the document.
You can also discuss the project on this telegram channel.

Introduction

A common problem on the internet is the lack of sybil-resistant identity systems. Users can generally create multiple accounts using different pseudonyms (or address in the case of crypto-networks) to receive rewards multiple times, bias votes, write multiple fake reviews, etc.
We introduce Proof of Humanity, a system combining social verification with video submission in order to create a Sybil proof list of humans.

Registration Process

Submitting

Parties who wish to be included in the registry submits information about themselves serving for verification (see Evidence Required section). They can also include the deposit in part or in full.

User Vouching

Users already in the registry can vouch for people registering. By vouching for someone, a user guarantees that the person he vouches for exists and is not a duplicate of another entry in the registry. Users should only vouch for people they physically encountered. When vouching for someone, a user may also put part of the deposit for this registration.

People may remove their vouching to people they have vouched for.
The number of vouching required is decided through governance.
It is possible to vouch for people who are already registered (which can be useful for them when they need to confirm their registration).

Once a sufficient deposit and number of vouchings for a submission is reached, it goes to a « pending » state.
A user vouching can only be used for one submission at a time.
Vouchings can be used on a “first come, first served” basis. For example assume, users A, B and C are registered. A and B vouches for user D. Then B and C vouches for user E. D goes to the pending state, but since the vouching of B is already in use, E will only go to the pending state once D is registered.

Challenging submissions

Users can challenge pending submissions that they think don’t comply with the requirements for acceptance. The challenge period is determined by governance. In order to challenge a submission, they need to submit a deposit. Vouching deposits will serve as a bounty, available for users able to correctly identify false positives in the registry (duplicates, bots, deceased, etc.) as well as the dispute resolution system.

The challenges types are the following:

- **Incorrect submission**: The elements required for the submission are incorrect. This kind of challenge does not claim that the submitter is trying an attack, but just that the submission does not comply with the submission rules. It is also used for users trying to submit while having an outstanding fine or during a ban period.
- **Deceased**: The submitter has existed but does not exist anymore. The challenger can provide evidence that the submitter is dead such as death certificate, obituary, public records. The submitter can provide a video of himself reading a recent blockhash. Submitters not able to give recent proof of life are to be considered deceased.
- **Duplicate**: The submitter is already registered. The challenger has to point to the identity already registered or to a duplicate submission. If someone tries to register multiple times simultaneously, all submissions are to be rejected.
- **Does not exist**: The submitter does not exist. For example, this can be used for videos showing computer generated persons.

When a submission is challenged, the decision goes to dispute resolution in an ERC792 compliant dispute resolution system. It will originally start with Kleros, the governance is able to change it.

When a challenge is won, the submission is not directly added but goes back in pending mode. This allows challengers to challenge it again for other reasons (but the same reason can only be used once).

For the duplicate challenge, it is possible to make parallel challenges (If someone challenges a submission for being a duplicate of Alice, someone else can challenge the same submission for being a duplicate of Bob). If multiple parallel challenges are successful, the challenge pointing toward the duplicate which was first submitted will get the bounty (it is possible for a submission to be a duplicate of multiple submissions at the same time due to pending submissions, when it happens, challengers have to challenge the submission pointing at the first submitted duplicate).

If a submission is rejected for « Duplicate » or « Does not exist », all people who had vouched for it get removed from the registry. The governance may state a fine paid to the challenger and/or a ban period before which people rejected from the registry can reapply.

Once the challenge period of a pending submission has passed, the submission is accepted and the individual is registered.

Removing Incorrect Submissions

Periodic Confirmations

Users will have to periodically reapply to the registry.
This is done in order to remove people who die and malicious submissions which would still have made it into the list.
Conditions to reapply are similar as the original application.
It is possible to reapply before the current registration ends in order to avoid spending some time unregistered.
People reapplying (such that they have the required vouching and deposit) before their registration ends are considered registered for the entire period of their new application.

Removal Request

A request to remove someone from the list can be made at anytime by submitting a deposit. Anyone can put a deposit claiming the registration to be correct. If no one does, the individual is removed from the list. If one does, a dispute is created.
Note that in case of a successful removal request, people vouching for the user are not removed from the list.

Evidence

Evidence required.

Each party registering to the registry would have to provide evidence. The required evidence is to be decided through governance and can be updated to take into account technological evolutions and evolution of attacks.

Initial required elements

1. The following information.
    a. Name under which the submitter is known (any UTF8 characters)
    b. First Name (basic latin)
    c. Last Name (basic latin)

    For a., the submitter can choose any name he is usually referred by.
    This can be an official name (Federico Ast), a use name (Marc Zeller), a religious/monarch name (Benedict XVI), a name with the original non-latin characters (小明), a name with anglicized characters (Xiao Ming), a name with an initialized middle name (George P. Burdell), a stage name (Bob Dylan), a political name (Nicolas Sarkozy).
    Fields b. and c. may be void if the submitter does not have it. Note that middle names are not required.
    Names in fields b. and c. using characters other than basic latin must be transcribed to basic latin.
2. A picture taken from front.
    a. Face should not be covered under heavy make-up or large piercings. Head cover not covering the internal region of the face is acceptable (ex: a hijab is acceptable but a niqab is not).
    b. It can include items worn daily (ex: headscarf, turban, wig, light makeup, etc) provided they do not violate the previous point. It cannot include items worn only on special occasions.
3. A short bio (ex: Cypherpunk, smart contract developer). This may be void.
4. A video of the submitter showing a sign with his address.
    a. The sign should contain the Ethereum address of the submitter.
    b. The submitter must show the sign in the right orientation to be read on the video.
    c. The submitter must then say « I certify that I am a real human and that I am not already registered in this registry ».
    d. Submitters should speak in their normal voice and should not attempt mimicking someone else’s voice. Speaking before or after the required sentence is acceptable.
    e. The video quality should be at least 360p, at most 2 minutes long and in the AVI format. Lightning conditions and recording device quality should be high enough to give visual quality to the video similar to 360p.

f. The quality of the audio should be high enough such that the speaker can be understood clearly. Small background noises are acceptable as long as they don't prevent the clear understanding of the speaker. Bad English accents are acceptable.

None of the provided information should be purposely offensive (ex: a painted Hindu swastika is acceptable for picture 2., even if it can be offensive to some people unfamiliar with its meaning, but a « I hate Jews » bio is not).

Additional Evidence

Challengers can use additional information to challenge the validity of a submission. This can for example include social graph analysis (analysis of people vouching for each other's).

Potential New Evidence

The initial evidence requirements can be changed through governance to cope with an increased interest from attackers as the system becomes more used and with new technologies. Potential new evidence which may be used in the future are the following:

- Social graph scoring. Only users which score above a certain threshold in social graph analysis algorithms may be able to register (see this article for social graph analysis algorithms).
- Additional biometrics. People registering may be required to have their ears uncovered and turn their head left and right. This would allow finding duplicate registrations through « ear matching » (see this article).
- Use of new technologies such as holoportation (see this article).
- Requesting application to use a pseudonym party ticket to register (see this article).
- Requiring to connect a social network profile.

Initial Seeding Event

Since we require user vouching for new members, we must start with a preset set of users. A seeding event will be organized (for example during one of the following conferences: Devcon, ETHCC or Edcon) where all people present will verify the other people present. Users registered through the seeding event will still have to periodically confirm their registration like regular users.

Challenger Ecosystem

The challenge process starts with users manually verifying the submissions. Overtime as the volume of registered users grows higher, we expect challengers to professionalise. They will be able to use machine learning (face recognition and speaker analysis) and social graph analysis to detect likely duplicates. Submissions detected through those methods would then be reviewed manually by potential challengers. Research shows that some

people are particularly good at matching faces, so we can expect some of those to specialize in this task.

System Security

The system has to balance between the ease of use and its resistance against fake submissions. No system can guarantee 0% of fake identities (even systems run by states requiring physical presence for identification and using more biometrics still have people managing to register multiple times, for example fake identity documents would account from 4 to 6% of identity documents in France, fingerprints of German minister of interior stolen via a HD camera shot from distance), the goal is to make it sufficiently hard and risky to create fake identities that the proportion of fake identities becomes negligible.

Video Evidence

Creating convincing fake video evidence is hard. Challengers are incentivized to seek and challenge fake submissions.

Failure Cost

Users trying to register fake identities will lose their submission deposit, making attack attempts costly.

Identity Removal

Submissions rejected for the “Duplicate” and “Does not exist” motives lead to people having vouched for fake identities to be rejected from the registry. An attacker trying to register a high amount of fake identities would need to be able to on average win more fake identities than the ones he loses.

This means that is fake submission success rate should be greater than $\frac{vouchings}{1+vouchings}$(where $vouchings$ is the number of vouchings required) for an attacker to be able to create a high amount of fake identities.

Public Identities

Submitting requires vouching from people within the system who have their real identity verified. Trying to attack the system requires revealing one’s real identity. This could lead to out-of-system sanctions to attackers ranging from social ostracism to state law enforcement actions.

Limited Submission Rate

By requiring vouchings to be only used in one submission at a time, we limit the rate of submissions. This gives time to the governance mechanism to adapt the required evidence

to potential new forms of attacks on the system. In case of severe attacks, the governance could decide to temporarily halt submissions (note that it does not need to be enforced at the code level, we just need set up submission rules such that all submissions are to be rejected).

Usecases

Anonymous Sybil Resistant Identities

Identities on POH are not anonymous. It is however possible to create Sybil resistant identities from them.
We can do so using Traceable Ring Signature. This is done by batch.

- Users can generate a keypair using the **Gen** function and submit their public key on chain.
- Once the threshold of required keys is reached (for example 100 keys). Users can sign the address of their anonymous account using the **Sig** function. They publish it from that said anonymous account. The smart contract verifies that the signature comes from one of the addresses in the batch using the **Ver** function.
- This is followed by a verification where everyone can verify that the signature does not come from a user who already signed an anonymous account. This is done offchain by applying the **Trace** on the signature and all the other signatures of the batch. If a duplicate signing is detected, anyone can submit a transaction pointing to the duplicate signatures invalidating them and return the public key of the double signer. The smart contract verifies the result of the **Trace** function (but only for couples of signatures which are pointed as duplicate in order to save for gas).
- If a signature has not been invalidated after some time, it can be used in applications allowing anonymous users.

Details about the **Gen**, **Ver**, **Sig** and **Trace** functions can be found in the Traceable Ring Signature paper.
Note that observers can link anonymous accounts to the batch where the anonymous account was created, but not to the specific user in this batch who created the account. Users requiring a particularly high level of anonymity will be able to repeat the process, each time invalidating their previous account and registering a new one.
Moreover each user in a batch can create at most one anonymous account, this ensures the Sybil proofness of such accounts.

Systems allowing anonymous participants can also allow identified participants by allowing anonymous identities and identified identities who haven't created an anonymous identity yet.

Anonymous identities can be application specific. A user may be able to create an anonymous identity to be used in application A and another anonymous identity to be used

in application B. But he should be able to create 2 anonymous identities in the same application.

Universal Basic Income

Universal Basic Income (UBI) is a payment delivered to individuals which is delivered on an individual basis without requiring work or means test.
A UBI coin will be minted and distributed periodically to each individual in the registry. This would be the fairest form of coin distribution as anyone could receive an equal share of the mint.

Potential Partners

- Democracy Earth
- GoodDollar
- Universal Income Project
- OpenUBI projects

Human DAO

The registry would lead to a DAO with a 1 person = 1 vote system. Initially, this would just be used for governance of the system, but could expand to expressing opinions on global world challenges and even manage projects or assets.

Potential Partners

- Democracy Earth
- DAOstack
- Aragon

Quadratic Funding

Quadratic funding (also known as Liberal Radicalism) is “a design for philanthropic or publicly-funded seeding to allow (near) optimal provision of a decentralized, self-organizing ecosystem of public goods. The concept extends ideas from Quadratic Voting to a funding mechanism for endogenous community formation. Citizens make public goods contributions to projects of value to them. The amount received by the project is (proportional to) the square of the sum of the square roots of contributions received.”.
This mechanism requires accounts to be sybil-resistant as splitting one’s funding across multiple accounts increases the amount given to the target project.

Potential Partners

- RadicalxChange
- Gitcoin Grants

- Effective Giving
- Giveth

Universal Identifier

Accounts created on POH will be usable as a universal login method. Dapps will be able to recognize users automatically without the need of a registration.

Potential Partners

- Universal Login

Certifications

Various certifications could be added to persons registered. Registered individuals would select the certifications they want to be made public. They can be confirmed by central entities or through a curated registry. They would be displayed as a badge on the individual profile.
Certifications can include:

- Country of citizenship
- Degrees and professional certifications
- Skills (for example a “experienced solidity developer” badge which could be asses by looking at open source code published by the individual)

Certifications could be used in the context of privacy preserving KYC, for example, it could be possible to give a zero-knowledge proof showing that you are a citizen of a specific country or above a specific age without revealing who you are.

Address and Public Key Database

Proof Of Humanity would create a database Identity -> Address and Identity -> Public Key. This can for example be used to write encrypted messages that only this user can read or to be able to select an identity directly when making a payment. This would remove the risk and the need to acquire the address or public key of a user through other channels which could be vulnerable to scammers.

Social Key Recovery

Users will be able to create a proxy account which could do all the actions external (classic private key controlled) account can.

If the owner of the account loses its access (for example because he forgot his password or because his doge ate his hardware wallet), he can request a recovery from another address. During the recovery period, he can sign a transaction to cancel the recovery from the address he supposedly lost (which means that the owner can prevent malicious recoveries

even if the trusted individuals were to be malicious). Trusted individuals would vote for or against the recovery. If the majority votes for, the new address would get control of the proxy account.

Trusted individuals can be people he vouched for or a user-defined list.

In case of death of the account holder (such that he is removed from the registry), a similar mechanism allows trusted individuals to give control of the account to the designated will executor.

Self-Sovereign Identities

Self-sovereign identities are identities which are controlled by the user. Systems and entities can make claims (for example a university can claim that a user has been awarded a degree). Users of self-sovereign identity systems can then selectively reveal those claims to other parties. Proof Of Humanity would make the claim that « This user is a unique human ». Note that using the anonymous Sybil resistant identity scheme, a user could prove this claim without revealing who he is.

Potential Partners

- Iden3
- uPort
- LocalCryptos3box

Pension Plan and Related Contracts

During the economically active part of their lives, participants make contributions in the pension fund. Once they reach retirement age, the fund provides them with a pension for the remainder of their lives. The amount of contributions and payments are based on actuarial math which can take into consideration the age, the sex and place of residence of contributors.
Compared to simply saving the money, these schemes protect participants from the risk of outliving their savings.
To avoid relatives of participants to claim the pension of their deceased family member (which happens quite often in current systems), it is important to know if someone is still alive.

Other financial contracts such as longevity insurance (sum paid every year after someone exceeds a specific age), tontine (pool of money/assets which are given to the last participant alive) or viager / life estate (assets held by a tenant for life, but which are to be attributed to another party after the tenant death) can use POH in a similar manner.

Potential Partners

- Transit Fund
- MelonPort

Credit Scoring

Lending services need to evaluate the creditworthiness of a client before offering a loan. The registry can be used to store authentic credit history of an individual for lenders to calculate the credit score from, allowing a global, borderless credit service.

For a credit history to be valuable, it must contain the full loan history of a user. One scheme would be to have a “loan” registry for each POH user. Any time a loan agreement is made between a POH user and a lender, a hash of the loan must be posted in the registry. After the loan is successfully repaid, the lender would sign a “reimbursement certificate” and add it to the user’s loan registry; same thing applies when the loan defaults.

If a credit analyst wants to evaluate the credit score of a user, they can request the user to reveal the content of hashes stored in the loan registry. The analyst could then verify them while being confident that all entries are valid and none are hidden (at least within this system).

Some privacy issues with this approach would be that the amount of loan entries are publicly known, and potential sensitive information recorded within the loan details. For the former, there might be ways to take advantage of cryptographic techniques to obscure the amount of entries. One naive solution would be by posting empty hashes at a semi random interval time. As for the latter, it could be made so that the “reimbursement certificate” only contains the credit-relevant details (whether the loan is successfully repaid, duration of the loan, rates, loan size, etc), and only these certificates would be revealed upon request.

Potential Partners

- Bloom
- Ripio Credit Network

Airdrops

A popular way to distribute a fraction of some tokens is to airdrop them. However, even when requiring different forms of identification (telegram accounts, passports), those airdrop where sybil attacked. This lead to a switch toward airdrops proportional to user balance of a specific coin and lockdrops (where users need to lock some coins and receive tokens proportionally to signalling). Those techniques, despite being Sybil resistant, privilege users already having a high amount of crypto-holdings.

Proof Of Humanity will allow Sybil resistant airdrop where participants will each be given the same amount of coins.

New User Freebies

Some systems give freebies to new users. This can be items in a MMO (Massively Multiplayer Online game), a first month free subscription on a video platform or a welcome NFT (Non Fongible Token). Without Sybil resistance, users can abuse those freebies (ex: never pay a subscription, get an unlimited amount of welcome NFT) by creating new accounts.
Systems can use POH to ensure that freebies are only given to users once.

Antispam Tool

Systems often use captchas (small exercises testing user capacity to analyse an image or a sound which are hard to complete for AIs) before allowing a user action in order to prevent spam. These are wasting user time and do not prevent spam from a determined user which would solve those (or subcontract them).

People in the POH registry could be allowed a number of captcha-free interactions (potentially high enough such that they never have to fill a captcha).

Users spamming the system could get temporarily or permanently banned. Those would not be able to just recreate a new account to evade the ban.

POH side chain

The registry could be used to create a side chain secured by Proof Of Identity with a “1 person = 1 vote” principle. This would assume honest majority of humans in this registry and would work in a way similar to Proof Of Authority sidechains.

Discussion

Concerns

Perma-Challenge grief

One griefing attack I wholly suspect to see once there are benefits to being included on POH is the 'Perma-Challenge grief' in which a user consistently challenges another entity for no other reason than griefing or personal dislike.

For example, I see person X has applied to list. I don't see eye to eye with person X and the cost to challenge is low enough that I will make malicious challenges which stall the registration of this person indefinitely.

When services such as UBI/ Self Sovereign identities / Social recovery become part of the POH, the value to being listed becomes much higher than the value of a malicious challenge.

The solution may be a lieu period post challenge or, an increasing challenge cost within a certain period (say, 7 days of the first) .

First challenge = xETH
Second Challenge =xETH*2
Third Challenge =xETH*4

Answers

Idea to process challenges (at least partially) in parallel. Particularly, if there is a fixed window to submit challenges of the form "this entry is a duplicate of person A already on the list", then the entry should be a duplicate of at most one person already present on the list, so at most one challenger can be right. Hence a single deposit from the submitter + the deposits from the various challengers would cover required arbitration fees and all of these cases can be handled at the same time. (Note there may be edge cases where two different Kleros juries give inconsistent rulings - one jury says that the entry is a duplicate of person A while the other says that the entry is a duplicate of person B in which case there would not be enough funds to reward both challengers - may be rare enough situation to be acceptable or could create a dispute between challengers in this case.)

Proof of Humanity or Proof of Agency

I’m not 100% sure on whether the registry should be based on a proof of humanity.

In some not too distant future, we will probably have (non-malicious) bots who may want to have an entry into the registry. Should they be excluded from the registry? Why should they be discriminated against?

Maybe a more generic approach to the registry is have it open to every being capable of having agency. Then the “humanity feature” can be given through a badge into the registry.

Entities proving they are human will earn the “human” badge. Entities which are not human will earn a “non human” badge. This “non human” badge could potentially be split into other badges (e.g., “bot”, “vulcan”, “martian”.) This basic feature of “human”, “bot”, “vulcan” would equate to what we understand now by “country of citizenship”.

Answers

- The problem is mainly about the Sybil attack, even if we end up with bots more intellectually advanced than humans, it may still be easier for them to temporarily self-replicate to Sybil attack the system.
- Even if in the future we may encounter other life forms with level of agency greater or equal to humans (whether them being from other planets or new species emerging from human colonization of other planets), it is not something to be worried in the short term.
- If we were to decide to allow non human entities to have similar rights, nothing would prevent the registry to evolve into it.

Religious headcover

Some people wear head cover covering the internal part of the face (ex: Burqa) for religious reasons (ex: Muslim women in Saudi Arabia) and may not be comfortable removing them.

Answers

- Most forms of head cover are accepted. Religious interpretation preventing people to show the internal region of the face are rare.
- Removing this requirement would significantly impact the security of the registry.
- Removing religious items for serious reasons can be acceptable (for example this should fall into the testimony exception in some interpretations of Islam).

Religious head cover reduces the amount of features available for identification.

Answers

- Internal features of the face are the most important to recognize faces (see this article). Hair can easily be changed (change of hairstyle, dying), this provides poor protection against Sybil attackers.

Mute people

Some people with disabilities may not be able to speak.

Answers

- Removing the requirement to pronounce the sentence would decrease the security of the system (speech analysis can be used to detect multiple registrations).
- In the future we can have certified medical professionals having the ability to grant a limited number of license exempting mute people to have to pronounce the certification phrase.

Using passport or ID documents

Why not ask people to submit passport or other ID documents?

Answers

- Passports/ID info should not be made public because of privacy and identity theft risks, we would have to design specific schemes to judge on them without giving the information to jurors and challengers.
- ID cards are not standardized and most people (even in highly developed countries like the US) do not possess passports.
- A significant part of the world population (approximately 20%) do not have any ID documents. They are likely to be the ones profiting the most from a POH registration.
- Convincing fake ID are quite cheap to get (even if passports are not).

Privacy

Linking Ethereum addresses to your identity could cause privacy concerns.

Answers

- Applications can allow the creation of a unique private identity for each public identity. This can allow dapps to verify the uniqueness of people without knowing their true identity.

Twins

Twins may be challenged as duplicate.

Answers

- Humans may have a hard time distinguishing twins. However, twins are not exactly identical and can be distinguished by skilled individuals. Moreover, facial recognition algorithms tends to do a better job than human distinguishing between twins.

Deep fakes

As AI produces better deepfakes will algorithms keep up in order to offer tools to defend against this?

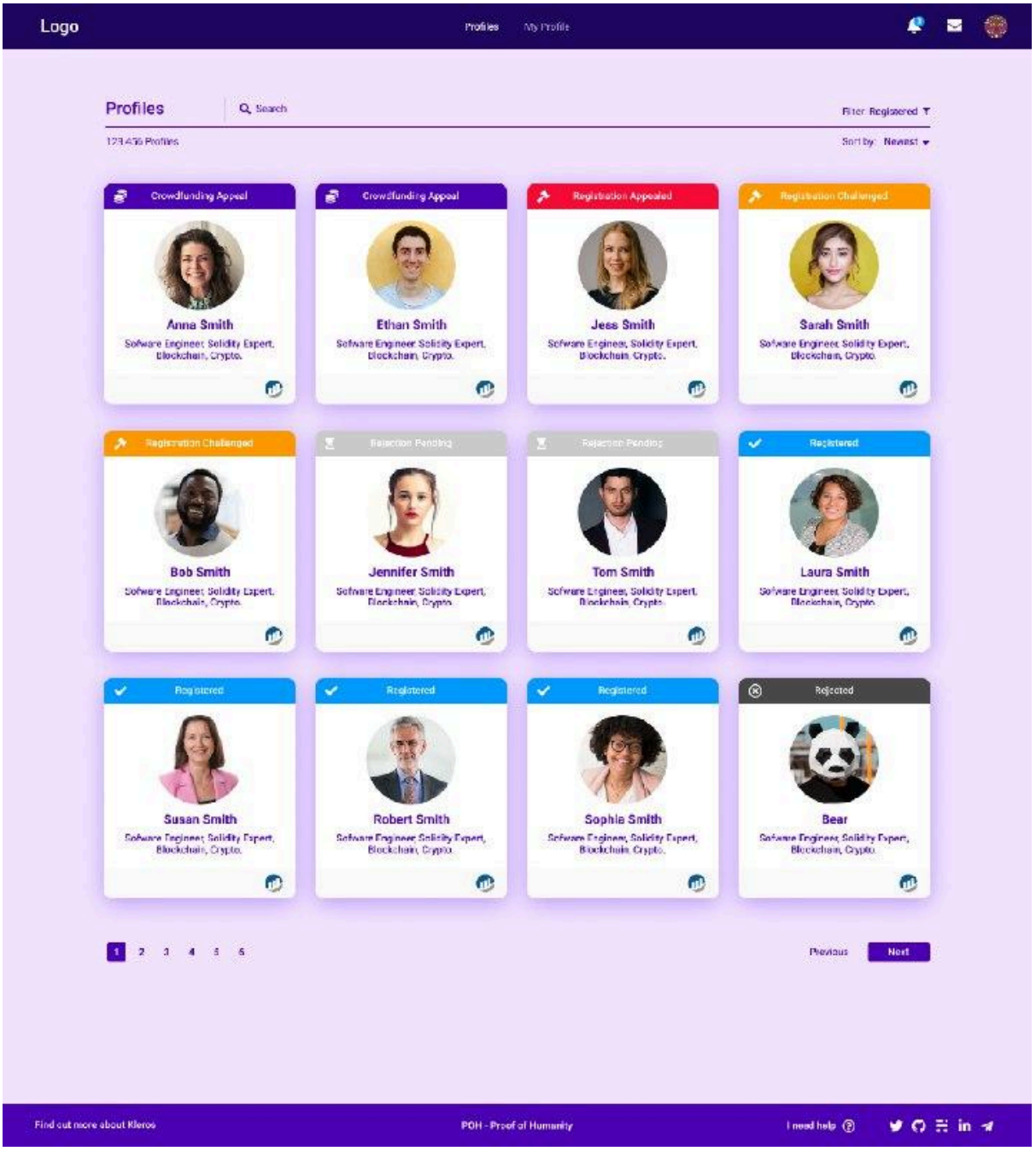
Answers

- Improvements in machine learning are likely to affect the effectiveness of both deepfake creation and deepfake detection algorithms.
- If algorithms manage to produce deepfakes not detectable by other algorithms, other evidence would need to be used (see the Additional Evidence section).

Ideas

This could be an early idea of what the interface would look like.

People make a submission with a deposit. Then it stays there for others to challenge. If it goes unchallenged, it's accepted into the list. If there's a challenge, it goes to dispute resolution.



This is an early sketch of how the interfaces could work : https://www.figma.com/file/LCKgQFI97FdWFUvFR9XX8s/POH?node-id=0%3A1

Participants

Interested

-

Confirmed

- Kleros team (contact@kleros.io)
    - Challenge system
- Democracy Earth
    - Interfaces
    - To be used for the HOUR tokens (UBI generated token).

Tasks

(Put your name and contact on a task you want to take)

- Make some presentation slides for the project.
- Reach out to projects which would benefit from it.
- Make a project website.
- Contribute to core specifications

Proof of Humanity Meetup Osaka

Points brought up in the talk.

Prove multiple DID's owned by one person.
This was discussed by Andres who has been working on a similar problem at uPort. Some users may not want to have only one online 'identity' preferring multiple linked to the root POH account.

Hand written attestations
Can we use hand written attestations to verify users?

I don't think so. It would be quite easy to have different handwriting and register multiple times.

Refugees / no identity documents.
How do we include users who have no physical documentation through war, refugee status or otherwise. How do we prove they are who they say they are? For the record, I have a friend in Scotland who has no passport, bank account or identification. This may not be an issue linked solely to underdeveloped areas.

Proof of humanity does not rely on government ID. So refugees and people without physical documentation do not face any specific challenge to register to proof of humanity.

Social graph weak links. Does one weak link break the chain?
We discussed the use of social verification via P2P/IRL vouching.

No, people in the social graph know their position in the social graph (they trust themselves and people they know). Those trusted nodes can be used in social graph analysis algorithm which can detect trivial (1 weak link) malicious subgraphs.
More weak links could be more problematic.

Twins / doppelgangers
Niche but useful to consider.

Different religious / political views which may lead to real life persecution.
Is video identification acceptable?

With anonymous identities, an external observer just knows that someone is registered. Not his activities. A state could effectively punish people registering, but at this point, there is no evidence that a state would try to prevent people being registered in POH.

Is there a 'Perfect solution' or, will just better than we currently have suffice?

Signing parties / PGP. Next Devcon, we kick off the POH physically with 3000 devs. '6 degrees of separation theory'

Perma challenge grief.
I don't like someone and consistently challenge just to keep them off the list. Crowd sourced smart contracts setup by democrats to stop a certain (or various) Republican(s) off the list.

Idea to process challenges (at least partially) in parallel. Particularly, if there is a fixed window to submit challenges of the form "this entry is a duplicate of person A already on the list", then the entry should be a duplicate of at most one person already present on the list, so at most one challenger can be right. Hence a single deposit from the submitter + the deposits from the various challengers would cover required arbitration fees and all of these cases can be handled at the same time. (Note there may be edge cases where two different Kleros juries give inconsistent

rulings - one jury says that the entry is a duplicate of person A while the other says that the entry is a duplicate of person B in which case there would not be enough funds to reward both challengers - may be rare enough situation to be acceptable or could create a dispute between challengers in this case.)

More than one
James Bond, Jason Bourne (multiple passports, multiple identities)?
You cannot have more than 1 public identity on POH.

Having multiple valid legal names - one for China (their alphabet), one for Russia (cyrylic) one for English-speaking countries

Having multiple valid identities - one for a corporate job with strict compliance rules, one for activism in countries that do not respect human rights

In this case you can create an anonymous identity, but can't use the public and the anonymous one in the same dapp.