UniqueID

Decentralized identity system based on biometric data and trust networks

March 2018
uniqueid.network

Abstract

Salaam.

1 Introduction

1.1 Paper organization

2 Preliminaries

2.1 Bitcoin

2.2 Smart Contracts

2.3 Decentralized Systems

2.4 Cryptography

3 Problem Specification

In this section we define our problem formally.

3.1 Problem Statement

The simplest formulation of our problems is :
Create a decentralized system for assigning exactly one public key to every human, without violating users privacy.
This definition can create some debates. First, we must define words like user, human and decentralized, as we see in next section. We can see this system as creating a list of valid public keys, without trusting any centralized authority. By "system", we mean some socio-economic design, where some group of people, incouraging by economic incentives, forming a specific structure toward achieving a goal.

3.2 Terminology

3.2.1 Human

When we want to design an identity system for "humans", we must tackle with two questions :
1. What makes an entity a "human" ?
2. What makes this human presistent over time? How can we say one person is "same" over time?
The first question is crucial, to knowing "who" can enter the system. Can we name strong Artificial Intelligence a human? It seems that all of us have some consensus on a definition of a human. It's a combination of some specific body properties (shape, face ...) and intellectual abilities (memory, language ...).

Second question is harder, and a famous unsolved problem in philosophy. If we want to project the identity of a person to any of his properties, we loose something. for example, if we define a personal identity over time as person's body, It is known that all body cells are replaced after some time. But we just need some properties that are presistent over time for most persons (without any fundumental philosophical reason). We can name three of this properties:
Biometrics: Some specific human body structures proven to be presistent and unique over time. Fingerprints, DNA and iris scan are examples of these biometrics.
Memory: Brain of normal person can memorize some data and recognize it over time. presistence of memory is almost true for all persons.
Trust: This is less clear than previous properties. Trust is how other people know and recognize one person. Basically it is combined from some of mind-body properties, But here "judging" over these properties are up to others. Trust is how other people see someone presistent and unique over time. Human judgement can make some errors, But it works well in many situations.

3.2.2 Decentralized

Defining decentralization, specially in rigorous form is very hard. We can think of decentralization in political form here : there is not any specific entity - state, corporation- or person who can affect the system, creating or removing identities. One side of this decentralization is unablity of an entity in changing ledger information : account balances, biometrics etc. Blockchain already make this part possible. Another side is unablity in adding identities and influencing how people trust each other, and here is where our design should gain such decentralization.
We always see the first side as *"How much money or coordination is needed for attacking system"*, e.g. Bitcoin hashrate gives us minimum on computational power (that can be expressed in computational devices that one can buy with money) that an attacker needs for double spending attack. Also, how current hashrate distributed shows us another aspect of decentralization : number of entities that form 51 percent of system. However, we have harder times dealing with second side. One can formulize that as *"How many persons should collude, and how much money they need, in order to bring X to system?"* X can be making one fake identity, making infinite fake identities, preventing someone from entering the system (censorship) and any other unwanted incident. We analyse our system from this point of view in section 6.

3.2.3 Incentives

We can see this kind of systems as a form of cooperative games, Which people interact each other for reaching shared goal. For this reason, there must be enough incentives for parties to participate. Formally speaking, we should define amount of effort, energy and other resources every party should put, and how many tokens he get back. Analysing this market can gives us the equiblirium

and the prediction of what will happen at the end. In the case of Bitcoin,e.g., There are always incenvtives for some group of people (miners) for running full nodes and miner equipment for earning new Bitcoins, So the system will be alive as long as these coins paid to them.

3.2.4 Privacy

4 UniqueID Design

In this section we will explain how UniqueID works and solves decentralized proof-of-unique-human problem. Our system is based on some concepts and components that we will cover them in this chapter in detail. Before that we provide overal flow of the system.

4.1 Overal Flow

Uniquid aims to provide a permanent and reliable identity for everyone without violating his privacy. Users should submit their biometric data on blockchain and then prove that they have submitted valid data. This proofs are social and based on trust: It means you must get some biometric reproducing certificate from current accepted users or validators. these validator asks you to reproduce your claimed biometric and preventing fake biometrics attacks.
There are some questions arising here, such as how users assigned to verifiers, what is the incentives of verifiers for checking others claims and Where is the starting point of the system. for addressing these questions and concepts, we discuss them in depth in following subsections.

4.2 Biometrics

Biometric data is how we identify and know "humans". We need permanent, unique and well-studied biometric for our system that storing them on blockchain do not create any privacy concerns.

TABLE

4.3 Trustless Setup

In a system where current users should approve new ones, we should have a mechanism for approving very first users. One method is to begin with suffiecient number of trusted persons and include their biometrics and keys as verified users. The challenge is how to select these persons without any need for central third party? Below we explain three solutions for this issue.

Transparent Peer-to-Peer Setup

Transparency can be the key for solving trustless setup. There are a community of enthusiastic people around the project that can build healthy setup.

Providing relevant information in a public channel, the community invited for joining public party in special place and time. everyone who aims to join sending his proposal including name , biometrics and some identity document -just for transparency purposes. In the party they start to verify each other in a peer-to-peer manner. Because the party is public, everyone can join and there would no monopoly or closed individuals in starting. Also it's near impossible to fake an identity because it can detected and claimed by just one person in a party. There can be a live cast of all of the steps of party in public channel for forward transparency.

Trusted Famous People

There are some people with public profile who have no incentive for sabotaging system, e.g. University Professors, known artists and athletes or popular cafes, usually because of their high reputation among other individuals. Collecting some of these people who wants to join in early verifying, and showing all the informations and profiles can be a starting point for system.

Decentralized CAPTCHA Party

CAPTCHAs **??** are mechanisms for recognizing humans from machines. CAPTCHAs are AI-hard and it takes reasonable time for humans to solve them. Consider we construct some hard CAPTCHA that takes about 2 minutes for an average person to solve. We then organize a CAPTCHA party: in a specific time around the world, based on some common randomness(blockhash) a predefined smart contract starts assigning CAPTCHAs to everyone.

4.4 Verification Mechanism

There are number of verifiers, say 100, in the city. Location and city of every verifier recorded in blockchain. We assume that user's public key is pk.

after one user enters the system with his biometric, he should get certificates from sufficient number of these verifiers(3 is enough here). Assigning verifiers to users done via blockchain with user's location and some common randomness. This randomness can produced with another smart contract, with methods like randHound **??** or ... This randomness,R_i combined and hashed with user's public key ($SHA256(R_i||pk)$ can determine the assignment.
User then goes to verifier in person and **reproduce** his biometric in presence of verifier. Reproducing means sampling biometric data with verifier's biometric device, and then ensuring equality of this sample with previous biometrics on blockchain with some local computation. If verifier ensure that two biometrics are same, he *accepts* user and issue a certificate with his signature on blockchain. This is one of the most important components of UniqueID, because here verifier can make sure that the biometric is real and belongs to the person who claims it. This will prevent fake biometrics attacks and identity thefts from happening.

After user gaining these certificates, the system automatically accepts him as a valid and unique person. If only one of verifiers does not issue the certificate, user can ask for a reassignment. This is possible when one of the verifiers is corrupted or has made some error. at the end, if user verified ... (What is the mechanism for punishing this verifier??)
For this procees being meaningful, and no one with many attempts can not break it and assigned to his favourable verifiers we add a barrier in entering the system. There are just three ways you can enter the system :

- Via *invitation*. Every verified user have two invitations that can give to other public keys and bring them access for submitting their biometric and verification proccess. because there is limited number of verified users, there will be always limited number of verifications (and performing an attack needs large human resources).
- Via *Stake*. User can put some specified amount of money on stake. If he verified by system, this stake returned to him, if not, he loose it. The amount of stake has direct relation with all unverified stakes in that city, more unverified stake, more stake a user should put.
- Via $Verifiers$. Every verifier -subject to his reputation and trust- can bring specified number

RANDOMNESS TOKENS disributed , PoS,

4.5 Trust Delegation

Trust is a fundumental key in bringing healthy behavior in our system. Every valid person has one "trust" token and can delegate it to every one. With this non-tradable token one can give his ability of verifying to someone else, because he can not actively verify new users. Thus the verifier with large number of trusts have more verifying power, leading to slightly more tokens he give for every new user.
For more resilience to attacks, we can give verification power to those with more than x trust tokens. this parameter can set based on city populations and maturity of system. This leads to collecting trust tokens by verifiers, but how they can do this? Transparency is the key, Imagine verifier who brings live cast of his place on a youtube channel, or providing access to his office for everyone (doors are open!). By providing more transparency, more people can trust you. Also every user must have incentives for : delegating her trust, and delegate it to a correct person. Restricting some important features of system (e.g. Universal Basic Income) to those who delegated their trust is one solution. Also for a corrupted verifier (there is some mechanism for finding corrupt behavior), all his trust get suspended for some period of time.

4.6 Native Token

We introduced a native token for our platform, However, For every token system we should answer to at least 3 questions:
1) What is the nessecity of creating new token, Or why the system needs it?
2) What is the utility of this token for users, Or why it has non-zero value?
3) What is the monetary system, Or how tokens issued and distributed.
Nessecity: First, we need a token for creating incentive mechanisms. every decentralized platform needs sophisticated and well-studied incentives, for encouraging healthy behavior and punishing bad actors. One of the powerful tools for designing mechanism is money, because it is related to person's desirability and profits. In our system verifiers rewarded by tokens every time they verify a new, fresh user. Also new users get some tokens for the first time they enter the system. Also some important applications, such as UBI, needs some form of currency.
Utility: The most obvious usage of such a token is for payments and store of value. Incentives bring new users to the system, and new users bring more acceptability and wider market, projected in token price, bringing new incentives for further users. This positive network-effect, combined with mechanism for more incentivising first movers(but not make them big Whales!) can bring non-zero value for the token.(TODO : This is because of the nature of our system). Also this system can host many other applications which need unique and permanent identity, such as digital banking, property and real estate on blockchain, reputatution systems etc. These systems can provide their services on UniquID blockchain, using native token or at least paying fee's for their smart contracts.
Monetary system: Our goal is to achieve an issuance scheme which is fair and keeps value of the token. Our proposal is selling fix amount of tokens (say, $a * x$) in pre-sale (with an Initial Coin Offering or similar methods) and then issuing x tokens for every new user. This tokens distributed between verifiers of that user and herself. So after a new users, tokens in the hands of users is equal to ICO tokens. This can provide $fairness$ for the system, because initial holders are not giants anymore, and after system became popular(=more users) their influence get reduced. Also initial investors have incentives for investment, because they can buy tokens cheap early. It will be promised to them that their tokens have an influence equal to a users, and they can guess what they earn by estimating value of an identity system with a users. This issuance scheme is linear in number of users, However the utility of users(network effect) is quadratic, so we can predict slight rise in price over time. At least, It's not an super-inflationary system : More user's, more utility, more demand and more supply responing them. Choosing a parameter and schemes for incentivising early users (e.g. changning reward over time) is for further research.

Figure for comparing network effect and money supply.

4.7 Decentralized Governance

There is no idependent entity for decision-making in decentralized systems, so they face governance problems in many levels. Long discussions on Ethereum DAO fork and Bitcoin Segwit2x proposal are clear examples of this issue. In UniqueID, There is new concept that should be governed as well : human work. There should be some mechanism for detecting and punishing *corrupted* verifiers.

UniqueID is inherently one-person-one-vote, and this gives us new oppurtunities for shaping our governance model. We introduce some hierarchial representative democratic system, based on three layers of representatives.

First, small communities of $50-100$ persons choose one person from themselves. They put their trust and vote on him, and can also track his activity and ask him about that. Because they are small group of people, it is expected that they know each other well, and can make nessecary communications between themselves and choose qualified representative. these are layer-1 representatives, and they should know each other and follow system changes and discussions, and also choose layer-2 persons. Every $30-40$ of these layer-1 representatives should gather and choose one representative. And the same for layer-3 : every $20-30$ layer-2 people can choose one layer-3 representative from them. See figure X for visual ...

This system should decide for critical decisions such as choosing parameters and consensus rules. Majority consensus seems a very good method for making decisions in a system with verified identities, but also can cause some problems. Not **every** decision can be made by a majority (51 percent) of votes. Changing some critical parameter of a system (number of verifiers needed for verifying one person) is a clear example of this. So we need to group desicions based on their importance, and put some thresholds on percentage of votes needed for making decisions in every group (super-majority rules).

Because of low participation, lack of incentive for voting and lack of knowledge for making corret decisions we should give some authority to representatives. But for lowering corruption and collusion, in addition to transparency, every decision needs greater consensus among higher layers. for example, if we need 51 percent of all user votes for some parameter change, we need 68, 85, 95 percent of votes for layer 1,2,3, respectively.

In this process, people can track their trustee activities and votes, and ask for explaination and reasons. Everyone can change his trustee everytime, and delegate his trust to another one. However, represetatives should not loose their position with leaving one of their trusts, so there can be a threshold(e.g. 20 percent) that when they leave, the person becomes invalid.

preventing ads and ... in votes

4.8 Implementation

4.9 Improvements over verification

The verification system we purpose face some challanges. Bribing or coordinating some verifiers for creating fake identities is the most important one. Fake-ID prevention is the only thing we design our system for solving that.
We can see two directions for solving this attacks. First, Set some sophisticated and hard rules for entering people that guarantee hardness of attacks. Second, design some mechanisms for detecting and removing fake identities and punishing bad verifiers. In this section we explain a mechanism of second kind.
We first design a very secure registeration way that there is zero-probablity in entering with fake identity, calling it A-judge. This can be very hard process, including being verified by all verifiers in specific city. There can be gathering of verifiers every 6 months in a public place, and handling all A-judges there.
Using A-judges, we can design a system for lowering amount of coordination between verifiers for creating fake identities. We give every verifier and every layer-3 representative limited number of *Identity re-checks* per month. They can use these re-checks for calling specific identities (here, biometrics) for going through A-judge. These called identities should pass A-judge in specified time, Otherwise they loose their identity. Also they have great incentive for going through this judge, because they rewarded by tokens. This way we can find fake-identities and punishing bad verifiers.
Every verifier stake X tokens and lock them. If system determines some verifers as a bad verifier, his stake goes for anyone who called A-judge for his fake identity. So verifiers have incentive for calling A-judges over fake identities, if they know any. This make coordination very hard : even if you bribe heavily some verifiers, After that they can call A-judge over that identity. There should be also some random checks for preventing other forms of bad behaviour.

5 Challanges

5.1 Geographical Dispersion

Until now we assume that there is one city, where all verifiers and users are close to each other and interaction between them is easy. In real world, however, we have thousands of cities in different countries, villages, no-residence areas etc. This variety make some seriuos challanges for a system relying heavily in peer-to-peer verifications in same place.
First problem is how new cities and places will join the system? So far we design our system and "first verifiers" based on assumption that they are all in same place, That's not true in real world. Imagine a scenario where we start the system from Tokyo, and after a while people in Vienna want to join the system. Should they go to Tokyo and Verify their identity?
Some possible solutions we talk about them here, but sovling this problem need more thinking. First, we can have another trustless setup in the new city.

But for keeping integrity of system, another existing verifiers around the world should take place in this setup. System should choose these people and provide their expenses in a secure and decentralized way (Making a data feed for list of valid cities, and some kind of voting or random assigning between volunteer verifiers). So based on these new verifiers, users in this city can start their verification processes. Another solution is to make as many as verifiers in first setup, Bringing people from different locations around the world in one borderless place (an airport, e.g.) and then start the system with these verifiers.

Second is how residences in small cities and villages can join the system? Areas with population less than 10000 may don't have any verifiers at all. One possible solution is assigning them to nearest cities, But it make a entry barrier for them. Another solution is sending some verifiers from near cities for verification, But it can bring some attack vectors and unpredictable behaviour.

Another methods

It seems that using another methods for verification, we can solve the identity problem without facing geographical dispersion. We think that this challenge is fundumental, i.e. near every system for securely verifying identites has this problem.

First, verifying human identity always require some human work. Until now, It's impossible for an AI for answering the question of "sameness" of two human objects over time. Nature of identity, Combination of physical and mental attributes, is the root of this hardness. So people should identify people. Now, we have choices of making this verification in same physical place, or from long distance. We argue that long distance methods are prone to errors and attacks : Every long distance method consist of sending some documents and information, and making some interaction (video chat, voice chat etc.) between verifier and user. Both have limitations : every document (video proof of your biometric, voice captcha etc.) can hacked with AI methods. Even further, AI enables us to fake a face in real-time video chat.
Geographical dispersion of people around the world make some fundumental challenge for identity systems. Even in a simple(and bad!) system which you should get some certificates from your friends (and you get verified after that) we face this problem, because people you know are mostly near you.

5.2 Privacy

Trust Tokens

Biometric Data

Secure Logins

5.3 Hard Forks

5.4 Massive Computation and Storage

The current design of UniqueID requires permanent storage of all claimed biometrics and also a computational infrastructure for automatic uniqueness check of new claims comparing to previously verified ones. While It is theoretically possible to do all the storage and computation on the blockchain, say Ethereum, but practically in that case the cost of operation will become prohibitively large. In the early stages of development, UniqueID will utilize IPFS or other production-ready decentralized storage solutions to store biometric claims. TrueBit protocol offers a general purpose solution to make computation off-chain at the cost of negligible less decentralization.
While TrueBit protocol can practically mitigate the problem of prohibitive computation costs, it is important to note that the special task of checking uniqueness of new biometric claims is capable of being done in parallel. One can think of a smart-contract that offer a reward for the one who finds the closest previously verified unique biometric to the new claim, the results can be verified using a TrueBit like protocol. This design prevents waste of computational resources to a significant level.
To get most out of UniqueID network, it is reasonable to develop an independent blockchain and storage layer. It will enable the potential for Proof-of-unique-Human mining system which is explained in "Novel Mining System" section.

5.5 Identity Theft or Death

Identity needs to be secure against theft or getting lost, on the other hand, to enable some features like UBI, it is required to eliminate dead identities.
As we suggested in "Problem Specification" section, there is a close relationship between the definition of human in our design and trust, based on that point of view we propose a solution for identity theft problem. Each user has to declare a group of at-least 5 trusted ones (friends, family or lawyer) as her trust circle, which have the authority to agree on identity theft or loss and owner of that account can reclaim his identity with new private-key by participating in the validation process.
Based on how much the system can tolerate the dead identities, one can think of a extending process for identity holders, similar to new identity registration process with less redundancy.

5.6 Centralization of Validation Mechanism

5.7 Fairness

5.8 Lack of Incentive

6 Analysis

7 Applications

7.1 Novel mining system

properly designed, I think this PoH can solve PoS problems with reputation and unforgeable unique signatures...

7.2 Accountable Voting and Survey

Voting is a critical part of all democratic systems, also surveys play an important role in media and decision making processes, but there's no solution for running a public and accountable online voting without trusting any third-party to protect it against Sybil attacks or fake identities.
Recent advancements in cryptography and blockchains technology offer many powerful solutions for end-to-end secure voting and auditable decentralized voting systems. UniqueID as a decentralized identity solution will make it possible to use all those advancements for social benefits without compromising people privacy.

7.3 Universal Basic Income

Universal basic income (UBI) is a kind of welfare system that is based on giving everyone a guaranteed basic income, totally independent of any other income. The idea of national basic income dates back to 18th century but various technical and political issues such as lack of trusted computational infrastructure or a form of trusted universal identity prevented implementation of a UBI system. Though UBI idea originally was presented as a way to save the society from poverty and injustice, many AI experts claim that given the fast and tremendous success of AI technology the world is heading toward a mass unemployment and a UBI system is inevitable and certainly required.
UniqueID provides a trustable universal identity and building a UBI system on top of it is just as easy as writing a simple smart-contract on Ethereum network or any other blockchain with access to UniqueID's validated identities.

7.4 Reputation Systems

Reputation systems are tools to build trust in online communities. Many motivations including the emergence of sharing economy and online marketplaces encourage using a reputation system. Theoretical studies in game theory and

practical experiments agree that a valid and reliable reputation system must have a long lifetime and be protected against Sybil attacks.
Creating reputation systems on top of a decentralized identity system such as UniqueID will make Sybil attacks impossible or very expensive and on the other hand, can guarantee a long lifetime.

7.5 General Framework for Organization

In an abstract and conceptual level, Bitcoin's idea is to decentralize a specific computational process using redundancy of computation, Ethereum extended this idea and made it possible to decentralize any computational process.
UniqueID's idea is to decentralize operation of a specific organization which is responsible for providing universal unique identity, and we claim that by extending same governance scheme and redundancy of operation, one can think of a general framework to decentralize operation of organizations.

7.6 Social Media

7.7 Fake News

7.8 Rethinking Governance

8 Reviews

We categorize previously existing ideas in this area in two different categories, first decentralized identity management solutions which aim to provide a decentralized infrastructure to host centralized issued identities, including DID, Sovrin, and uPort. Second one is decentralized identity issuance solutions which aim to create or define a new kind of identity that is decentralized from its origin, including Democracy Earth and Bitnation, Proof-of-Personhood.
Our work can be categorized in the later one, decentralized identity issuance systems. We want to emphasize that despite previously known solutions, UniqueID can bring decentralized, permanent, unique identity into reality by utilizing biometric authentication and social smart contracts.
In the following section we briefly review some of the mentioned schemes and compare them to UniqueID in measures of political and operational decentralization, sybil attack resistance permanence of issued identities, and proper governance and incentive mechanisms.

8.1 uPort

uPort is a decentralized infrastructure for claiming identities and receiving verification from other parties in the network. One can use uPort to host and digitize her identity such as national ID card or driving license and get verified by officials or other people for being the owner of the claimed identity.
First of all, uPort is not designed for a decentralized originated identity which

is well defined. Due to lack of a general identifier in uPort network, uPort do not provide a direct solution to anti-sybil attack and enabling a universal basic income system. Though uPort provide the possibility to define decentralized originated identities but there is no intrinsic incentive or mechanism to do it.

8.2 Sovrin

Sovrin is a protocol and decentralized app based on its own blockchain, aiming to create sovereign identity and decentralized trust, it is focused on delivering a kind of identity which is secure, private, and partially provable. In current design of Sovrin system, a trusted set of operations maintain issuing new identities in a semi-decentralized manner. By utilizing its own token, issuers are economically incentivize to participate in system, though theres no governance mechanism to prevent issuing fake identities and sybil attacks. While Sovrin claim that it will become fully decentralized in future but currently theres no clear scheme for decentralizing issuing new identities in Sovrin network.

8.3 Democracy Earth

Democracy Earth is going to be a decentralized app mainly concerned with providing a infrastructure for liquid democracy and voting. Naturally it does need a unique identity scheme to prevent sybil attacks. Although currently it is proposed that each new user upload a video from herself in a concrete format to prove her uniqueness but theres no clear scheme with acceptable error that compare videos and verifier uniqueness of new users. It is also suggested that Democracy Earth utilize other platforms to identify its users.

8.4 everid

8.5 DID

8.6 ID2020