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

3.1 Problem Statement

3.2 Terminology

3.2.1 Human

3.2.2 Decentralized

3.2.3 Incentives

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 be the host for 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

4.8 Implementation

5 Challanges

5.1 Geographical Dispersion

5.2 Privacy

Trust Tokens

Biometric Data

Secure Logins

5.3 Hard Forks

5.4 Massive Computation and Storage

5.5 Identity Theft or Death

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 End-to-End Secure Voting

7.3 Universal Basic Income

7.4 Reputation Systems

7.5 General Framework for Operations

7.6 Social Media

7.7 Fake News

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