Before reading about the protocol I want you to tune in a bit into our thinking.

…In the long run identity is all about money (human accounting, mitigation of risks). Here is a question then: what is the price of a state ID

?

Issue price

One has to pay a commission to get a passport or to reissue it. So, there is a price to issue an ID.

Black market price

Identity could be stolen or forged. There are markets for stolen and forged identities. And there are prices for both.

Market price

There are prices that reflect how valuable your ID is to a counterparty. For example an average threshold loan amount a credit organization is willing to give without any other inquiries than a valid state ID. Or an average rate for renting a car (or maybe renting a car in a foreign country). These are risks. Due to market effectiveness, these prices incorporate many interlinked parameters (like forging price, law enforcement effectiveness, etc.) and show the market's trust to an ID issuer

.

Replicant price

And at last, there is a price that reflects how valuable your ID is to yourself. But we need to go a little forward into the future. What is the price of creating a realistic doll looking and behaving just like you and with the same credentials but controlled by someone else (or something else, phew!)? And even a trickier question. What is the price for which you will let someone control your avatar? This is yet another dimension to the state ID price.

So what is the price of a state ID? I don't have a good answer right now. If you do please share your ideas in the comments. By sharing these thoughts I wanted to prepare the ground for price-of-personhood concept and hopefully a discussion. Here are some things to bear in mind:

1. Identity can be priced.

2. There is no direct evaluation. The risks are outside of an identity system (one can rent 100 cars a day and sell them). The market gives the best possible evaluation available.

3. There is no 100% Sybil-proof even with state ID systems.

Now to the protocol. Below is the latest snapshot of Upala documentation.

Upala at a glance

- Provides a digital identity uniqueness score. In dollars (Price of Person-hood).

- Utilizes the social responsibility concept ("Invite only trusted members, or lose your money and reputation").

- Hierarchical social graph. Built with groups. Stored on-chain.

- Simple off-chain graph analysis and on-chain proofs.

- Upala is a protocol. It enables to build different identity systems united under the same scoring standard.

- The protocol can wrap over existing systems (Bright ID, Humanity DAO, Idena) and unite them.

The Protocol and the Universe

Upala is a protocol and everything built with it.

Rather than building a single system, we developed a digital identity scoring protocol. We use the protocol to build a family of unique identity systems, wrap around existing ones and provide tools for other developers to build their own unique identity solutions. The protocol unites different identity systems under the same scoring standard

.

The main idea of the protocol is the notion of bot reward. It is an amount of money that any user can run away with. The money is collected by all participants. So everybody is incentivized to allow only trusted members. The bot reward is a kind of stake

. It signals the quality of a participant.

Users join groups. Groups join larger groups (groups of groups). Larger groups join even larger groups. And so on. This creates a hierarchy with massive groups at the top and users at the bottom. DApps can request users' scores from any group.

The Upala protocol

([Explosive bots protocol](#)) is a simple incentive layer that helps build different identity systems. It also helps to unite Upala-native identity systems and existing ones (by wrapping Upala around them) under the same identity standard.

Upala Universe

is everything built on top of or wrapped with the Upala Protocol.

How Upala works

The code is [here](#).

Groups

Users join groups. Groups join larger groups (groups of groups). Larger groups join even larger groups. And so on. This creates a hierarchy with massive groups at the top and users at the bottom.

A group sets scores to its members (users or lower-standing groups). The score means an amount of trust and is expressed in percents from 0 to 100.

A user score

is calculated relative to a group and relies on all the scores down the hierarchy.

Say Alice has a 90% score in group A, group A has a 80% score in group B. Group B has a 70% score in group C.

Alice score in group B is then: 0,90 x 0,80 x 100=72%.

And Alice's score in group C is: 0,90 x 0,80 x 0,70 x 100=50,4%

Users are allowed to join multiple groups and leave a group at any time. The same applies to groups (similar to MolochDAO rage quit feature).

The process of group creation is completely decentralized. The hierarchy grows naturally in a bottom-up direction. Thus several top-level groups could emerge with millions (or even billions) of users in their subgroups.

A DApp may decide to trust any group and estimate user scores relative to that group. A DApp may choose a number of groups to trust.

[

_images/groups-1.jpg

3295×2546 425 KB

](https://ethresear.ch/uploads/default/original/2X/8/8780763e7e83b26928c34668200723560a117977.jpeg)

Explosive bots

Every group has a pool of money (DAI). Every group member has a share in the group's pool (not necessary, simplified here).

Every user has an option to attack any group. That is to steal a portion of the group's pool. The amount of theft depends on the user score in that group. The attack affects all groups along the path from the user to the attacked group.

If Alice decides to attack group C, that would also affect groups B and A.

A user performing such an attack is considered a bot. A bot is effectively stealing from other users because the value of their shares drops. Presumably, there is no way for this same user remains friends with. The act of stealing is immediately followed by self-destruction. Thus the name exploding bots.

[

_images/bots-1.jpg

3372×2606 518 KB

](https://ethresear.ch/uploads/default/original/2X/3/3cfbf2249e5575eda352dcb93bb31663e386fc2f.jpeg)

Pools and Upala Timer

Changes to the group pool, users' scores and anything that may affect bot reward are delayed. The delay prevents group owners from front-running bot attacks. The delay also allows for bot-net attacks.

The Upala Protocol (bot explosion protocol)

Users may be represented by simple Ethereum addresses or wallets. Groups are Ethereum smart contracts using Upala Protocol (experimental code is here).

The contract defines bot explosion rules

- the only rules necessary for compatibility with other contracts:

- maintain a pool of money

- provide member scores

- reward an exploding bot with a portion of a pool (and get locked for not doing so)

That's it! The rest is out of protocol.

A group may choose any behavior as long as it can pay bot rewards in DAI.

Upala Universe

What can be built with Upala.

The protocol allows groups to choose any incentives and governance model

as well as many other parameters. A group can pay to its members or to charge them. It can issue a token or it can stick with the DAI. It can decide to be a MolochDAO type or a Token Curated Registry type. Groups are free to choose everything that is not restricted by the protocol

. Other examples:

- Member entering conditions (e.g. may require payment, an on-chain fact proof, a number of votes from its current members, etc.)

- Profit distribution rules (if the group is profitable)

- Scoring rules (how exactly a group scores its members)

- Exit rules (e.g. define shares refund policy)

- Privacy policy (e.g. visibility of group members to each other and to other groups)

- Score calculation fee for DApps or/and users (e.g. based subscription, lifetime membership, per transaction, free of charge, etc.)

- Governance model

- etc…

Due to the freedom of options, it is possible to build groups with very different properties. Thus groups can bear different roles within the system. We refer to groups with similar properties as Group types

.

Group types

Score provider.

A group may or may not provide access to user scores. Some groups may decide to charge users or DApss for the information.

For-profit.

A group may decide to be profitable (or at least try to). Such a group may "tend" to earn from users (through entrance fees) or DApps (score calculation commission).

Bank with benefits.

Groups requiring an entrance fee may decide to hold their pool in a bank (like Compound). Members of such groups will receive interest on their fees. Plus the uniqueness score (benefit). A feature like this does not mitigate the risk of bot attack, however, it could speed up onboarding.

Buffer.

A philanthropist may decide to bring a group with a small pool and small bot reward into a more expensive group. This person then bears a part of bot attack risks having nothing in return. This way buffer groups can be created to help bring developing countries

into high-level expensive groups.

Groups with Fixed Hierarchy Levels.

There are no leveling constraints per se. The hierarchy is built naturally with initiatives. But one can create a group that allows only subgroups of a particular type to be included as members. A group like this could become a building block of a state ID based identity system (described a little further).

TCR Group.

A group may decide to use a Token curated registry to curate its members.

Score cache.

A group that caches user scores and saves gas on calculations.

Branches

We can go further and build whole identity systems

using Upala protocol. We call them branches

. There are two flavors of branches: Upala native branches and Wraps. The whole set of projects using Upala Protocol is called The Upala Universe

.

Upala-native branches

These branches use Upala groups as building blocks. Upala protocol is built-in. Here are a couple of example branches:

Friends based identity system (branch).

Friends join groups. Groups of friends join larger groups. And so on. Groups of groups will probably form around leaders. A betrayal (bot explosion) is seen by closest friends and naturally rumored around in the real world. A traitor will find it difficult to enter friends based system again. The same is for the group leaders. Everyone is incentivized to allow only trusted people. The hierarchy of groups will reflect the real-world reputation.

State ID based identity system (branch)

. Such a branch could rely on group types with fixed hierarchy levels. A user is allowed to join only a city-level group. City-level group joins region-level groups. Then come country-level and world-level. Every level with its own entering rules, governance and incentive models.

Radical ID

. Set a price for which you are willing to sell your identity to anyone willing to pay. Pay a "tax" relative to the price.

Reputation tracker

. Servieces (DApps) give scores to users for interactions. Services are curated via Token Curated Registries.

Wraps

The Upala protocol may be used to wrap existing identity systems and bring them into Upala Universe as well. A wrap is basically a group that invites members of another system to join. Copy is another way to think of a wrap. Members and scores are copied from an existing system into Upala group(s). Here are examples:

Humanity DAO Wrap

. Everyone in Humanity DAO is invited to join the wrap (a Upala group). The group smart contract checks if the member is really a Human (in Humanity DAO terminology) and lets them in with 100% score. It may require a fee to fill the group pool with cash. The same procedure may be used to wrap around Moloch DAO

, Metacartel

, or other DAOs.

Random Handshakes Wrap

. The Random Handshakes system was proposed earlier in the Upala blog. It relies on face recognition and the real-world intersection of people. This whole system or its parts (i.e. based on location) can be wrapped with Upala protocol.

Layer 2 Analyzers

. A wrap could use several identity systems as inputs (collect data from other branches, wraps or existing non-Upala projects) and uniquely calculate user scores. It could use some complicated off-chain graph analysis (like the one that Bright ID does).

Unions

A DApp could choose to trust several branches to get scores for its users. This is one way of combining branches. But it is not very effective because every DApp is responsible for choosing the right (reputable) branches. That is to do curation work by itself. We don't want that.

A better way is to create a group with branches as members. It will unite several identity systems (branches). Groups like this may be called Unions. A Union group may be a For Profit group and earn by charging DApps for score calculation (or confirmation).

Thank you for reading!