upala Documentation

Release 0.1

Peter Porobov

Oct 18, 2022

Contents

Upala is a price-of-forgery digital identity system.

CHAPTER 1

Pale Blue Paper

1.1 What is Upala

Greetings human!

1.1.1 Upala at a glance

Upala is an anti-Sybil system for DApps and a decentralized digital identity.

- Provides a digital identity uniqueness score in dollars (Price of forgery).
- 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.

Check out this 4 min video on how Upala works if you prefer.

Docs moved here

View Upala on Github

1.1.2 Price of forgery

Upala provides a **digital identity uniqueness score**. The score is valued in dollars and represents the explosion price - an amount of money that an identity holder can get at any time for deleting their ID. The higher the explosion price the higher the owner values the ID and the safer it is for DApps to interact with.

The building block of Upala social graph is a group. The explosions payouts are provided by groups pools. Thus groups tend to consist of people who believe that other members value their IDs equally.

Groups may earn by providing user scores to dapps and/or from user deposits and are incentivized to gather as many users as possible. Users are incentivized to choose groups giving the highest scores. At the same time the higher the explosion price (the score), the higher is the incentive to forge an identity. The market drives these prices to the equilibrium for every user (much in the same way as insurance rates balance).

1.1.3 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 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.

1.1.4 Design philosophy

- Protect bots rights
- Right incentives first
- Everything which is not forbidden is allowed
- Crypto-economic constrains instead of code constrains

Join us:

- Telegram
- Discord
- Twitter
- Medium Blog
- GitHub
- Reddit
- Edit this documentation

Support:

- **Please introduce Upala to a fund! We are looking for funding!**
- Donate Ethereum
- Donate Bitcoin
- Fund Panvala (Upala is made possible with Panvala)
- Fund our Gitcoin grant
- Buy ads (help Upala and charity)

https://discord.gg/fa3q8rq

1.2 Anti-Sybil academy

WARNING!

This document is under construction. Upala insights are on the way…

1.2.1 Basics of digital identity

Main challenges

Sybil attack. How to prevent a malicious actor from creating multiple accounts?

Account recovery. Relying on password is not enough. Managing private keys or mnemonics is too complex. Hardware tokens are rare. We need to build a secure system for the unskilled, the absent-minded and the naive.

Incentives. Until widely adopted one cannot call it an identity system. We need a lot of businesses and a lot of users. But why would anybody participate?

It does matter who you are, where you are and who you friends with. We will often use this as a metaphor to shape our thinking when solving these problems.

Sybil attack protection

The sibyl attack problem

Imagine two situations:

1: Alice and Bob are twins. They live in the same flat. Alice is out in the morning and home in the afternoon. Bob is out in the afternoon and home in the morning. They meet different people when they are out but never the same ones. They never invite guests.

2: Isabel is diagnosed with dissociative identity disorder. She has two phones. One has an account registered with her real name. And the other is registered with her alter ego—Sibylla. Isabel is out in the morning and home in the afternoon. There she changes her pale pink standard waitress uniform for a stunning evening gown and goes to a luxurious cocktail party. She gracefully grabs the phone registered for Sibylla. Isabel and "Sibylla" meet different people and never invite anybody to "their" home.

Here Isabel is performing a sibyl attack. We need to "punish" Isabel and "reward" Alice and Bob.

1.2.2 Projects and papers

Links for digital identity enthusiasts. I use this document as personal archive and read-later list. I thought it isworth publishing. It is good source of quality info on digital identity and related topics.

Identity projects

Uniqeness, trust

- Upala - reputation that you own, no social graph analysis.
- BrightID - sybils are detected by analyzing, recovery by friends
- IDENA - sybil protection by meaningful story captcha
- TrustLines - decentralized immutable accounting system for netted IOU balances between trusted parties

- Pseudonym Pairs does it in zero degrees of separation.
- Encointer personhood through pseudonim pairs. People meet physically simultaneuosly. Incentives through UBI. Own blockchain.
- Web Of Trust
- Friend to friend
- https://tse.bitnation.co/
- https://duniter.org/en/
- https://www.humanitydao.org/ - voting for a new member
- https://www.objectivemoney.org/ - voting for a new member
- POAP - The Proof of Attendance Protocol. Allows humans to collect badges in the form of non fungible tokens every time they participate in an activity, in person or remotely.
- UBIC - Universal Basic Income Currency. Sybil-resistance is based on modern E-Passports. Users join by scanning E-Passport via NFC.
- Replica by DemocracyEarth - Quadratic voting.

Storage and access

Mainly concerned with granting access to parts of identity inforamtion.

- iden3 - zknarks, griff nentions. a claim-based model. exmp. A university claims, that a useres has a degree. No social graph. No sybil protection.
- Evernym - a hyperledger blockchain project
- uPort - ERC-725
- BlockStack todo
- http://selfkey.org
- https://www.velix.id/ - uses stellar consensus protocol.
- https://www.civic.com/

I categorize project below as ICO-boomers (sorry I may be very wrong):

- https://lynked.world/
- https://trigid.org/
- https://xenchain.io/
- https://www.peermountain.com/
- https://trustcommunity.io/

Recovery

- keybase
- gnosis safe - wallet
- Argent - wallet

- ZeroPass - recovery based on key splitting. is building a decentralized solution. ZeroPass is building a decentralized password manager.
- You - You are the password. Decentralized password manager. Uses Phone to login.
- https://securekey.com/ - funded by world bank
- https://pillarproject.io/project - “The Wallet is Everything”. Building a wallet with identity strage functionality. No details about recovery except they are planing to use hardware wallets and friends.
- https://rivetz.com/ - recovery. DUAL ROOTS OF TRUST - software wolutions for splitting keys (expl. SIM card + smartphone secure enclave)
- EIP2429 - Secret Multisig Recovery. Social recovery using address book merkle proofs.

Zero Knowledge, privacy

- AZTEC protocol- “Being able to prove that you’re part of a group, without revealing who in the group you are”.
- https://enigma.co/ - secure computation protocol, where “secret nodes” perform computations over encrypted data.
- https://status.im/ - secret messaging check it out

Blockchain social networks

- Akasha - todo
- - ethereum. todo

Other

- LNTrustChain - Experiment of trust. People passed an ammount of satoshis to those who they trust.
- https://www.takethetorch.online/Torch
- http://fermat.org/downloads/book-of-fermat.pdf - Person-to-person apps
- BAT - if they pay for ads, how can they tell people apart from bots
- namecoin
- @bloomtoken

KYC-services

- Jumio- AI-Powered Identity Verification Services

UBI and decentralized landing

- https://puddle.com - Credit powered by people
- Circles - A decentralised Universal Basic Income platform based on personal currencies
- https://www.wetrust.io/

Articles

Sybil attack protection in social networks

- SybilAttacks in Social Networks - Survey #1
- Sybil Defense Techniques in Online SocialNetworks - Survey #2
- SybilRank- Aiding the Detection of Fake Accounts in Large Scale Social Online Services
- Sybil attack on lowest id clustering algorithm in the mobile ad hoc network
- Visualization assisted detection of sybil attacks in wireless networks
- The Sybil attack in sensor networks: analysis & defenses by J. Newsome, E. Shi, D. Song, A. Perrig

Sybil tolerance

- Canal

Reputation-based

- Reputation systems - open questions on reputation systems among the list of improtant Problems of Ethereum.
- Sybilproof Reputation Mechanisms - "…there is no symmetric sybilproof reputation function. conditions for sybilproofness for nonsymmetric functions. (we can easily break symmetry by comput-ing reputation values with respect to some fixed node inthe graph. This may be useful when we can identify sometrusted user, or when each user computes separately thereputations of other users with respect to themselves."
- Propagation of Trust and Distrust - todo
- Ostra: Leveraging trust to thwart unwanted communication

Universal basic income and credit networks UBI

- Aleeza Howitt
- Bottom-Up Money

Game theory

- Deception, identity, and security- the game theory of sybil attacks
- Robust incentive techniques for peer-to-peer networks - Uses graphs. Simplifies sybil detection. Flow-based reputation.
- M. Richardson, R. Agrawal, and P. Domingos. Trustmanagement for the semantic web. Flow-based reputation.

Zero-knowledge

- Tutorial: Proving knowledge of a hash preimage - a good practical example by Zokrates team of zkSNARKS for a quick introduction.

- Getting Started with zkSnarks on ZoKrates - great write up by Gnosis team. Step by step guide to implement zero knowledge.
- Building Identity-linked zkSNARKs with ZoKrates - an example how a sender's identity could be proven using sender's private key inside snark.
- Zero-Knowledge Proof-of-Identity - Sybil-Resistant, Anonymous Authentication on Permissionless Blockchains and Incentive Compatible, Strictly Dominant Cryptocurrencies. TODO study

Password storage, Decentralized file access control

- Fruitfull Google search
- Blockchain-Based, Decentralized Access Control for IPFS
- Blockchain Based Access Control

Decentralized unique identity

- Pseudonym_Parties
- Verifying Identity as a Social Intersection
- UniqueID Decentralized Proof-of-Unique-Human - survey of decentralized identity systems

Face-recognition

- Secure Face Matching Using Fully Homomorphic Encryption
- Privacy-Preserving Face Recognition

Problems of ID in the world

400k people in Europe without IDs - https://apatride.eu Aadhar India - Aadhaar is a verifiable 12-digit identification number issued by UIDAI to the resident of India for free of cost.

Bonding Curves todo - https://docs.google.com/document/d/1VNkBjjGhcZUV9CyC0ccWYbqeOoVKT2maqX0rK3yXB20/edit - by Simon - Bonding Curves https://yos.io/2018/11/10/bonding-curves/ - Bonding Curves https://medium.com/thoughtchains/on-single-bonding-curves-for-continuous-token-models-a167f5ffef89

Join us:

- Telegram
- Discord
- Twitter
- Medium Blog
- GitHub
- Reddit
- Edit this documentation

Support:

- **Please introduce Upala to a fund! We are looking for funding!**

- Donate Ethereum
- Donate Bitcoin
- Fund Panvala (Upala is made possible with Panvala)
- Fund our Gitcoin grant
- Buy ads (help Upala and charity)

https://discord.gg/fa3q8rq

Other (study) https://identity.foundation/ion/ https://www.w3.org/TR/vc-data-model/

1.3 Roadmap and team

1.3.1 Roadmap

Roadmap moved here - https://www.notion.so/Development-Roadmap-0a2613fe99c741f3a3c3e2421460d40f

1.3.2 Team

Peter Porobov - Research, Smart Contracts

Entrepreneur, programmer. Founded and co-founded startups in 3d-printing, art and drones. Created a charity project on Ethereum, now building Upala Digital Identity.

Links: https://github.com/porobov, https://twitter.com/porobov_p

Andrei Bolkisev - Advisor (architecture).

Andrei Bolkisev is an information systems engineer and programmer with 13 years of experience and Ph.D. in computational physics. As information systems engineer he was leading projects ranged from state-scaled information systems to microcontrollers programming. In computation physics, he worked on developing novel methods applied to combustion of solids modeling. As for now, he is most interested in investigating social and economic dynamics.

Links: https://vk.com/blksv, https://www.researchgate.net/profile/Andrei_Bolkisev

1.3.3 Tasks

Moved here - https://www.notion.so/Tasks-848e6b9a047b4b6da610f1d5ad3f6edd

Next, human, have a look at the Upala Universe (all the things you can build with Upala).

Join us:

- Telegram
- Discord
- Twitter
- Medium Blog
- GitHub
- Reddit
- Edit this documentation

Support:

- **Please introduce Upala to a fund! We are looking for funding!**
- Donate Ethereum
- Donate Bitcoin
- Fund Panvala (Upala is made possible with Panvala)
- Fund our Gitcoin grant
- Buy ads (help Upala and charity)

https://discord.gg/fa3q8rq

Join us:

- Telegram
- Discord
- Twitter
- Medium Blog
- GitHub
- Reddit
- Edit this documentation

Support:

- **Please introduce Upala to a fund! We are looking for funding!**
- Donate Ethereum
- Donate Bitcoin
- Fund Panvala (Upala is made possible with Panvala)
- Fund our Gitcoin grant
- Buy ads (help Upala and charity)

https://discord.gg/fa3q8rq