brightID

Universal Proof of Uniqueness

Whitepaper. Last Printed: January 20, 2022

Link to Living Draft with Comments

Overview

BrightID is a social identity network that allows people to prove to applications that they aren't using multiple accounts. It solves the unique identity problem through the creation and analysis of a social graph.

BrightID is a public good that exists for the benefit of humanity. It is a nonintrusive, decentralized, open-source technology seeking to reform identity verification--and thus lay the groundwork for a free and democratic society.

Principles

Nonintrusive

Data should be shared with peers, not a central organization. BrightID does not want your data. Names and photos are only shared between people making connections.

Decentralized

The solution should not be controlled by a single centralized organization; such an organization could commit hidden fraud.

Open

The solution should be open and auditable.

Reusable

The solution should be easy to build on and reuse.

As more applications integrate with BrightID, it becomes more likely that their users will already be verified, reducing the friction for adoption.

Creating and storing the social graph

The social graph contains cryptographically signed connections between people. Each user manages their own signing keys, so the ability to create connections is independent from any particular service or application. This results in a form of **self-sovereign identity**[1], since each user has ownership of their own digital identifier. The social graph itself can be used as a reference for many different services, but none of these services are in charge of the graph, nor be able to control the behavior of individual users. This architecture allows connection data within the graph to be portable and to exist on a decentralized network.

Decentralized network

Portability of connection data is essential for creating a decentralized network of computer nodes in which each has a complete copy of the graph. Decentralization allows for a wide variety of coexisting analysis methods. It is crucial for multiple independent parties to be able to use their own analysis methods on the same connection data, both to ensure that authority over verified identities does not fall under the control of any single entity, but also to allow the regular auditing of analysis methods by independent parties. This also fosters open innovation and improvements to existing analysis methods.

Each copy of the graph is kept in sync by relaying change operations through an Ethereum-based proof-of-authority blockchain called IDChain.

[1] This may be correctly termed a “social identity” since a person’s most trusted connections have the ability to recover a compromised identifier.

Analysis

In order to make a determination about someone's uniqueness, the graph is analyzed. There are many possible methods; different methods can be compared or aggregated. Nodes in the network are free to employ whatever analysis methods they wish.

Metadata

In the methods we tried[2], we found it useful to consider additional data in the form of *seeds* and *groups*. Seeds are preselected points in the graph from which trust flows. Groups--in the sense we use them--are small, combined efforts by connected users to help someone become verified. Groups provide richer possibilities for interconnectivity than single connections and we analyzed the graph of interconnected groups.

Thresholds

SybilRank, an algorithm on which part of our trial software was based, was tested with the Spanish social network Tuenti. The algorithm was used to rank vertices (users) in the graph according to their likelihood of representing duplicate users (sybils). The ordered list was given to workers who manually checked and removed suspicious accounts. Having such an ordered list resulted in workers finding many more duplicates than through user reporting[3].

A manual check like the one used in the Tuenti example may not be practical, so a verification method needs to find a threshold above which users are considered unique and automatically mark them as verified. A higher threshold may result in more false negatives (unique people being mislabeled), while a lower threshold may result in more false positives (sybils being mislabeled). Different apps can decide where on this spectrum they would like to operate.

[2] BrightID's open-source sybil attack modeling software.
[3] SybilRank

Injecting simulated attacks

One way to automatically find a threshold is to simulate different kinds of sybil attacks and inject them into the graph at various locations before running the ranking analysis. After analysis, the rankings of the simulated sybils can be compared to the new rankings of previously verified users. The threshold is set to an acceptable level of false positives and false negatives.

Combining results

Applications are free to choose the most appropriate algorithms, parameters, and thresholds. Verification methods may sample results from several other verification methods (potentially running on several nodes) and combine them however they like.

Verification persistence

A user typically doesn't lose a verification for falling below a threshold unless an important local change has also occurred--for example, being removed from a primary group or the loss of a nearby seed group.

Auditing

An application can check verification responses from multiple nodes as a way to audit nodes.

Using BrightID with applications

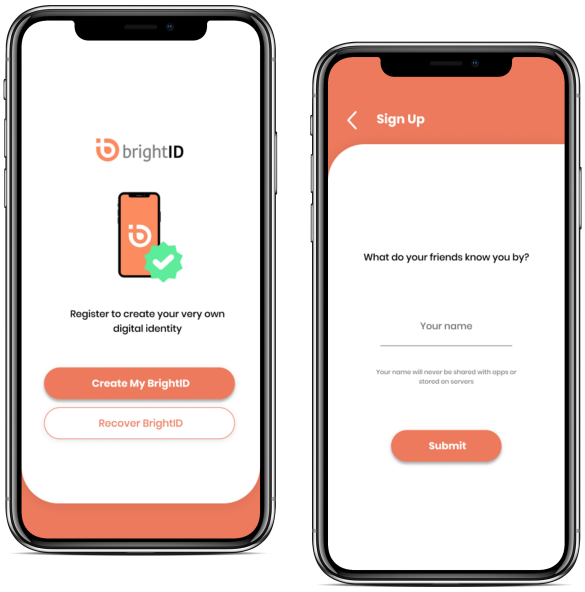
Using applications with BrightID is covered in the developer documentation.

Statistics

Statistics for BrightID-enabled apps.

Mobile reference app

The first mobile app to allow users to interact with the BrightID network was created through a grant from Aragon. It allows users to connect to each other, form groups, receive verifications and send them to applications. It also allows users to recover the signing keys associated with their BrightID.

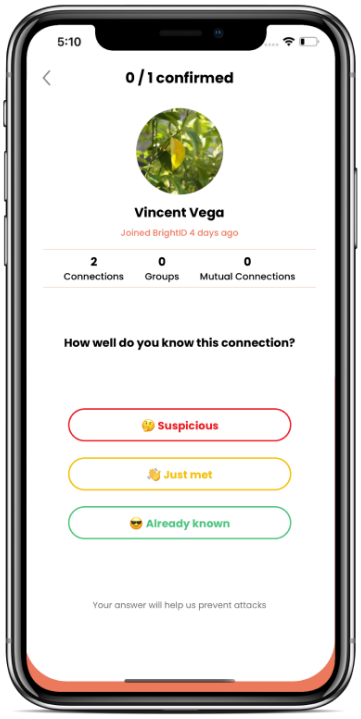


Signing up

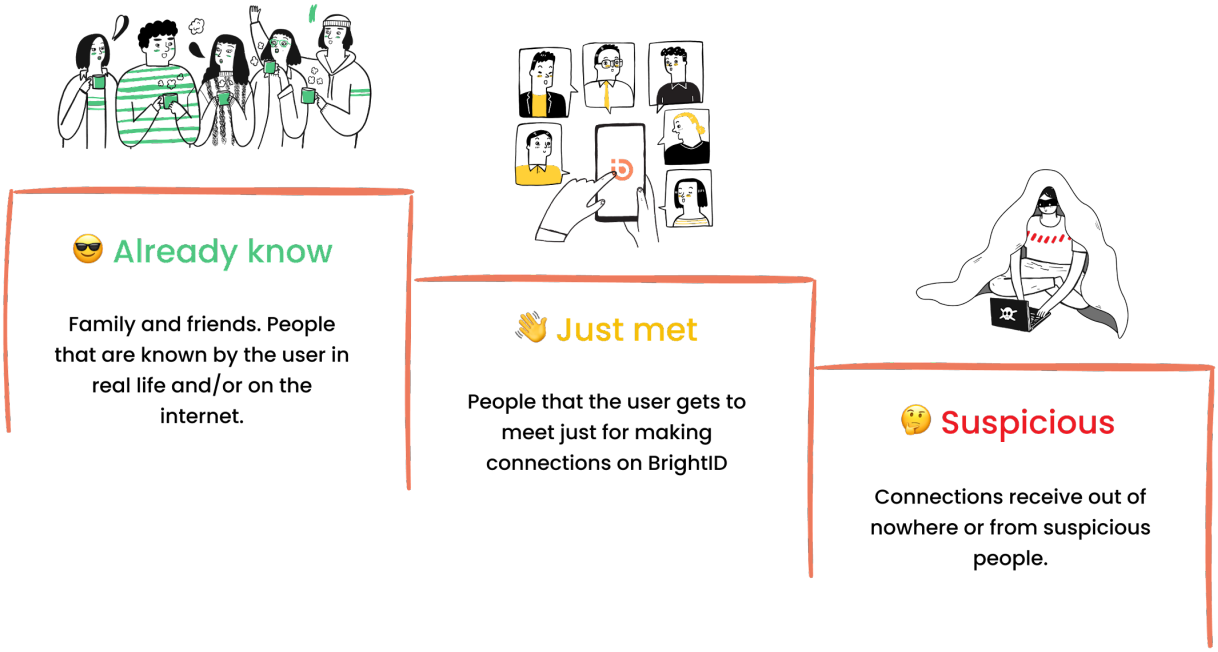
A new user is asked to add a photo and enter a name for themselves. This is used by other users to help them manage their connections. The user's name and photo are privately shared with their own connections, but never stored on servers or sent to apps.

Making a connection

Each user opens BrightID and taps “connect” on the home screen. One user creates an on-screen code that the other user scans. They each confirm the connection. The other user’s join date, number of connections, number of mutual connections, and verification status are shown. If something looks wrong, a user can cancel the connection or mark it as suspicious.



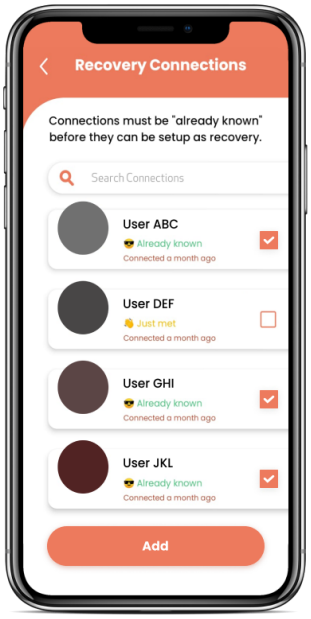
Connection levels



People have the opportunity to assess how well they know the user to whom they are connecting. This makes it harder for an attacker to make connections from their sybil region to the honest part of the graph. Detecting regions where there are only sparse connections to the honest part of the graph is a feature of many anti-sybil analysis methods.

Guide to connection levels.

Recovery



Each BrightID has a signing key pair associated with it. If a user loses access to the signing private key, or the key is compromised (e.g. a device is lost or stolen, or the data is erased), it can be easily replaced by reconnecting to two members of a set of trusted contacts. Having an easy recovery method makes bribery less effective: a user could simply accept a bribe and then replace their signing key, rendering the previous one useless.

Guide to social recovery.

Primary groups[4]

Primary groups are an important part of being verified. A person can only be verified as a unique human if their primary group has been ranked high enough by anti-sybil algorithms.

Each person chooses one primary group. Other members are notified when this happens. Over 50% of the members of the group must authorize a person's choice of primary group. In addition, any member may mark a group as unusable as a primary group and any member may veto another member's use of a group as a primary group.

A primary group represents the closest personal contacts (e.g. immediate family members) for a particular person. BrightID users should mark groups and veto other users accordingly.

[4] Primary groups aren't enabled in the default analysis created by the BrightID core team until the graph grows large enough to support them.

Seeds

Some social graph analysis systems have a notion of *seeds*[5], which are people who serve as centers of trust. Seeds are used by the system to differentiate between honest regions of the graph and sybil regions created by attackers to resemble honest regions.

Selecting seeds is especially important during the rapid growth phase of the network when subgraphs of users may arise that are not well-connected to the main graph.

BrightID Main DAO will promote the research of different seed selection methods and also the creation of tools that make seed selection scalable. Some principles to consider when creating a seed selection process are outlined below.

Seed Groups

When analysis is done on a graph of groups (as is the case in several of our initial systems[6]), it makes sense for a seed to be a group of people. This allows a seed to have a continuous lifespan.

Discoverability

A seed group must be discoverable for two important reasons.

First, a BrightID user must have reliable steps they can take to become verified as a unique person. In the stage of rapid network growth, this will often include finding and making connections with members of a seed group.

Second, DAOs given the task to assign and revoke seed status to groups need a way to find a group and ensure that it is operating well.

[5] SybilRank
[6] We created open-source sybil attack modeling software..

Grants

Important seed groups may receive grants from BrightID Main DAO to ensure their continued operation.

Seed DAOs

Seed DAOs have the authority to designate seed groups and remove that designation.

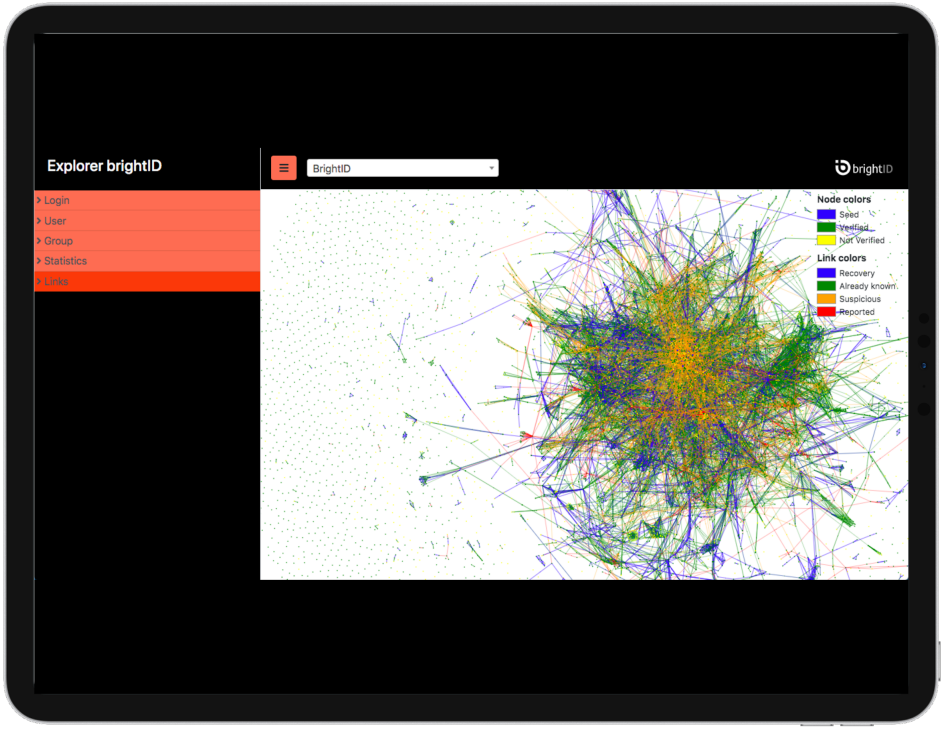
Algorithms that make use of trusted seeds can use lists of seed users published by seed DAOs. Multiple seed lists may be combined. It's up to seed DAOs to prove the trustworthiness of their selection process. Seed DAOs may be eligible to receive grants from BrightID Main DAO.

Governance

A seed DAO may choose its membership and operate however it wishes. A seed DAO's membership may include members of seed groups that it has selected. Some members of the BrightID core team created an Aragon seed DAO (called SeedDAO) on IDChain where each member has one vote on decisions to add and remove seed groups or DAO members.

Use of the graph explorer

BrightID released a tool for exploring the BrightID graph. Users can see the position of their own connections and groups in the graph.



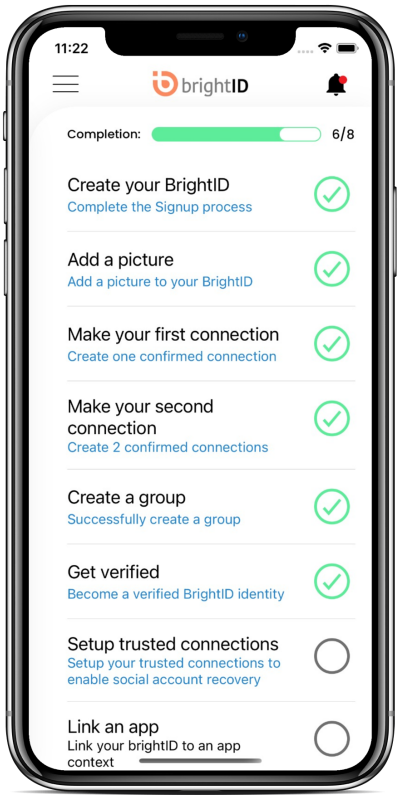
This tool can also be used to mark regions and export the boundaries to share with other seed dao members. This helps with sharing the location of seed groups and the regions they affect. A seed dao member can define a region by adding people who have been observed to connect to seed group members. This creates an area of known humans around a seed group. Those peoples' ranks can be measured over time to help gauge the effectiveness of the seed group.

Checking seed groups

A seed dao should periodically send a member to visit each seed group it has designated to make sure it's still accessible and helping the nearby regions.

Reinforcing beneficial behavior

Interfaces to BrightID (such as the mobile app) should give feedback to users that lets them know when their actions help real people or when they put the system at risk of falsely verifying sybils.



Achievements

Actions a user takes in BrightID are recorded in an action log viewable in the mobile app. Actions can have achievements attached to them.

The following is a list of Achievements:

- First connection
- Link with an app
- Get sponsored
- Two connections
- Three connections
- Set backup password
- Setup social recovery
- Connection party
- Connection party with friends or family

Long-term funding

Sponsorships

As a method for funding BrightID, each user must be *sponsored* once in their lifetime. The cost is $1 DAI[7] and can be paid by the first application that requests a user's BrightID verification.

This article explains why BrightID uses *sponsorships* as a sustainable funding method.

Added utility from choosing to buy sponsorships

For an application to want to buy sponsorships, it needs to receive benefits it wouldn't otherwise receive.

Ranking in app lists

In applications and web pages created by BrightID Main DAO, applications are ranked by the number of sponsorships purchased for their users[8]. This helps new users find an application to sponsor them, and helps applications that purchase sponsorships acquire new users. Once a user is sponsored, they may see a different default sort order for applications.

Participation in BrightID Main DAO

Applications may apply to add managers from their own communities to the DAO to represent them. Applications should have representation in the DAO proportional to the number of users they sponsor (within the constraint from the constitution that no outside group affiliation should comprise nearly half of the managers or more).

[7] The choice of token and purchase price are set by BrightID Main DAO. Scalability and price stability are the most important considerations

[8] The value used for ranking is the number of sponsorships an application has available times the number of sponsorships it has already used ($Sp_{unused} \cdot [Sp_{used} + 1]$). This rewards both new purchases of sponsorships and successful sponsorships of users.

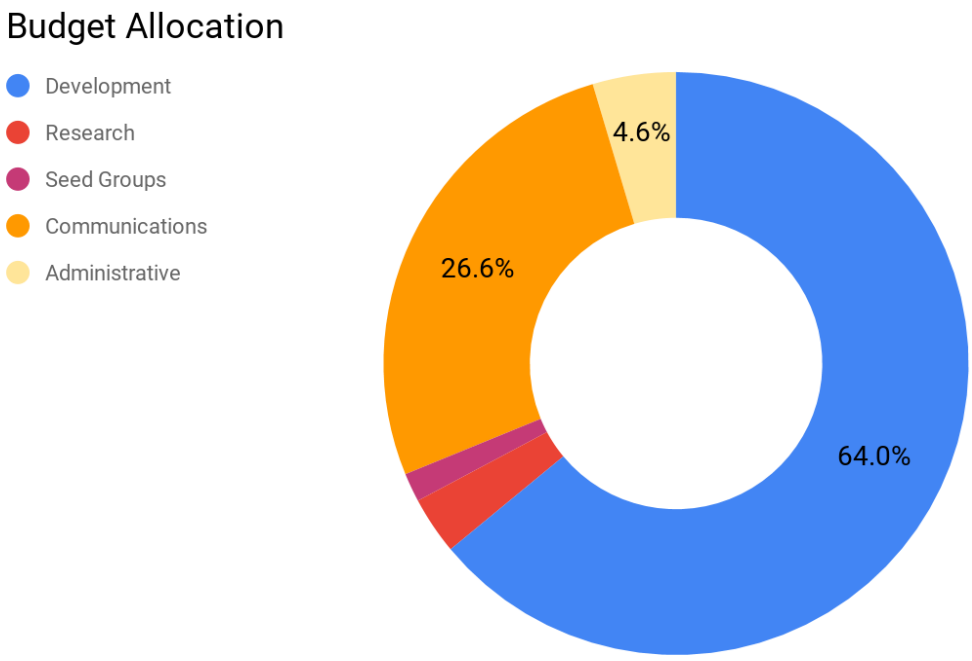
The principle at work is that BrightID is a public good, its utility is encapsulated in the utility people find in the apps that integrate with it, and sponsorships are a measure of how much utility people find in a particular app. Apps that sponsor users are therefore in the best position to judge how current revenue should be applied to create future value for BrightID users.

Refunding excess revenue

As expressed in the constitution, revenue beyond what is needed to fulfill the mission of BrightID Main DAO will be refunded to all verified unique people.

BrightID Main DAO

A decentralized autonomous organization (BrightID Main DAO) is used to represent the interests of humanity and the applications they use on the BrightID network[9,10]. BrightID Main DAO supports BrightID-related open-source software, nodes, seeds, research, and communication.



BrightID Main DAO Budget Categories

Development

Fund the development of

- Applications that allow users to make connections, manage cryptographic keys and authorize other applications.
- The peer-to-peer protocol used by BrightID nodes
- Other open-source, general purpose utilities for BrightID

[9] BrightID Main DAO on Aragon.
[10] The Constitution of BrightID Main DAO.

Research

Fund the research of new techniques for analyzing the social graph and users who wish to run nodes to incorporate these techniques. Award bounties for various general and security activities.

Seed Group Development

Bring remote communities into the BrightID network and fund research on seed selection processes.

Communications

Communicate with businesses, offer support, create public-facing documents including user and integration guides, host and attend events, engage in community building.

BrightID Team

Adam Stallard

Project Lead

Adam has worked in distributed systems since 2010 and client-server architecture since 2002. BrightID is his passion.

LinkedIn, Twitter, Github

David Wisner

Mobile Lead

David is a Javascript developer with 6 years of experience building web apps. He graduated from the University of Washington with a degree in psychology.

LinkedIn, Twitter, Github

Alireza Paslar

Research, Communications

Paslar does community management, research, and content creation for BrightID.

LinkedIn, Twitter, Github

Mahdi Heydari

Research, Mobile, Smart Contracts, Web Apps

Mahdi has over ten years of experience in programming. He also has years of research experience in economics and social criticism on banking and monetary systems.

LinkedIn, Twitter, Github

Mohsen Khan-mohammad-zadeh

Research, Smart Contracts, Web Apps

Mohsen has years of experience as a programmer. He has been researching blockchain and smart contracts for some time and is a trusted and fluent programmer in the blockchain ecosystem.

LinkedIn, Twitter, Github

Michael Bauer

Mobile, Smart Contract, Web Apps

Michael studied Computer Science in Germany and has +20 years of experience as a developer and project manager. He is passionate about blockchain and smart contract technology.

LinkedIn, Twitter, Github

Dama Vara

UI Design

Dama has years of experience as a visual designer specializing in marketing and communication content. She designs BrightID mobile apps, websites, and other communication content.

LinkedIn, Instagram

Carlos Mesa

Research, Communications

Carlos has been working towards cryptocurrencies adoption since 2013. He does community management, research, and content creation for BrightID.

LinkedIn, Twitter, Github

Mohammad Hossein Ghaznavi

Community Management

Ehsan does community management, content creation and marketing for BrightID.

LinkedIn, Twitter, Github

Bitsikka

Integration, Mobile/Web Apps, Community Facilitator

Bitsikka has been studying Web3 since 2016, has 8+ years of mobile/web frontend development, and has been participating in various Web3 communities actively for years. He helps with App/Community integration, documentation, and community management at BrightID.

Twitter, Gitcoin

Mohammad Reza Yazdani

Community Growth, Content Creation

Yazdani helps the community to grow through creating content and making advertising strategies. He has over four years of experience in business development, economics, and finance.

Twitter

Brandon Venetta

Network Development

Just an ordinary guy trying his best to do good in this world, Father and Husband.

Twitter

Sergej Müller

Community Manager, Coordinator, Integrator

He joined crypto at the end of 2017 and researched various topics in blockchain technology. He joined BrightID around Sept 2020 as a community manager. Now he is helping in coordination, integration and community management. Focusing mainly (but not exclusively) on EVM-based blockchains.

Twitter

Advisory Team

Philip Silva

Strategy, Mission

Philips helped create ZeroPoverty and the non-profit HedgeForHumanity to advance the ideas of universal sharing, crypto-UBI, and paying social dividends for all of humanity.

LinkedIn, Twitter, Github

Griff Green

DAO, Commons

Community manager for TheDAO, co-founder of the White Hat Group, Giveth, and the Commons Stack, as well as advising many other core Ethereum community projects.

LinkedIn, Twitter, Github

Luke Duncan

DAO, Commons

Luke Duncan is an advocate for open source technologies and decentralized platforms. He co-founded 1Hive and is working to advance DAO usability and adoption on the Aragon One team.

LinkedIn, Twitter, Github

Auryn Macmillan

DAO, Commons

Auryn is a community builder and user researcher with a passion for open technologies. Founder of DAOhub, BD;SM at Colony, former pro basketball player, MSc Psych & Research Methods.

LinkedIn, Twitter, Github

Ross Campbell

Legal, DAO, LAO

Ross is a Brooklyn-based attorney and programmer at OpenLaw with substantial experience developing code-based contracts and companies on Ethereum.

Twitter, Github

Further Reading and Links

BrightID Links

- Applications and Usage Statistics
- Website
- Medium
- BrightID Main DAO and Subdaos

Socials

- Discord
- Github
- Twitter
- Telegram
- Keybase
- Riot

Research

1. Anti-Sybil Systems

Podcast Episodes

BrightID Introduction on Bankless
Understanding Unique Identity with the BrightID Team

Videos

- BrightID in 2 minutes (intro video)
- Aracon 2019 Demo / Presentation
- Social Coding - 07/09/2019 - "Show and Tell"
- OpenUBI talk

- TEDx talk: “How much poverty should exist in the world”

Articles

- BrightID: A Personal Stamp of Uniqueness by Bowen Sanders of Giveth
- Decentralized Unique Identity via Graph-based Sybil Detection on a Peer-to-Peer Credit Network by Aleeza Howitt
- BrightID: Becoming a World Citizen by Alireza Paslar
- BrightID: Proof of Digital Uniqueness by Philip Silva, Adam Stallard, Rachel Gordon for MIT Solve

Thanks

Daniel Jeffries for laying fertile ground with Cicada and Why Everyone Missed the Most Mind-Blowing Feature of Cryptocurrency and creating the virtual center of the decentralized universe. Everyone who followed us on decstack, especially Alex Howlett for the endless feedback sessions. Arthur Lunn, Yalor Arnold for intros to Giveth and Aragon. Everyone at Giveth and Aragon. Yalda Mousavinia for making BrightID real. All volunteers and team members past and present. Everyone we met at Aracon, DGOV Council, and OpenUBI in Jan 2019. Robert Gilman and Bright Future Now. Grace Rachmany for writing the book on DAOs. Han Hegeman for web hosting and design. Anyone willing to talk unique identity, including Joe462, Austin Fatheree, Michael Ten and others in /r/CryptoUBI, Andrew Whitham, Santhan Naidoo, Hadar Rottenberg, Kenneth Thomas, Jose Gonçalves, Chris Gregorio, Carsten Munk, Matt Czarnek, Anna Blume, Jeff Emmett, Dani Bellavita, Pol Lanski, Vojtěch Šimetka, Lorelei Loie, Nick Emmons, Peter Grassberger, Jordi Baylina, Maria Gomez, John Light, Bingen Eguzkitza, Brett Sun, Jorge Izquierdo, Luis Cuende, Jouni Helminen, Gorka Ludlow, Ed, Drummond Reed, Alex Zimmermann, Jan Berchtold, Aaron Foster, Alfred Guo, Yoni Assia, Gilad Barner, Darrell Duane, Doug Kent, Johannes Zerbst, Philippe Honigman, Craig S. Page, Aiden Pearce, James Waugh, Dmitry Christie, Christopher Seifert, Titusz Pan, Ramona Phelps, Ben Kaufman, Christian Hildebrand, Thomas Zeinzinger, Martin Batiste, Eric Maublanc, Hugo Trentesaux, Olivier Jansens, Martin Köppelmann, David Terry, Josh Fairhead, Luuk Weber, Slava Balasanov, Johan Nygren, Tina Roh, Daniel Schmidt, Lawrence Lanoff, Alejandro Machado, Raphaël Mazet, Ilya Kachalin, Didi, Raph Carrier, Itamar Caspi, Hendrik Richter, Rick Stefanowski, Jordan Mack, Jerry Michalski, Rouven Heck, Lucas Geiger, Matt Prewitt, Glen Weyl, Abishek Punia, Tim Draper, Tomer Kagan, Jeff Dance, Craig Hansen, Trevyn Meyer, Justin Tuttle, Santi Siri, Kyle Graden, Rich McAteer, Niran Babalola, Petr Porobov, Seth Goldfarb, Vipin Bharathan, Bertrand Juglas, Nave Rachman, Clement Lesaege, Paul Cowgill, Tommy Cox, Vitalik Buterin, Barry Whitehat, Wayne Chang, James Young et. al. Everyone who tested BrightID. Seed group members: Kay Gertler, Bowen Sanders, Kris Decoodt, Josie, Pete-ster, Rachel Gordon, Jen Hansen, Heather Stallard, Chuck Peters, et. al. Hedge for Humanity (Brandon, Eric, Jon, Ken) and Code the Change Stanford (Drew, et. al).