

GloKi™: Global Digital Voter Identity

Ouri Poupko, Eston McKeague, David Gallup, Gery Colombo, Lars Lünenburger

Abstract

The Global Democracy Initiative (GDI) aims to build a participatory global democracy, where world citizens can decide and develop solutions for global problems through voting. To achieve this vision, GDI proposes the creation of a global digital voter identity called GloKi, that is easy to obtain, secure, and available for every world citizen. [GloKi aims to provide a sense of belonging, a secure global voting identity, and the empowerment of world citizenship.](#) The requirements for GloKi include having one identity per person, being fraud-resilient, data-protected, secured, and privacy-preserving, and not depending on government-controlled identities or centralized biometric data storage.



About the Global Democracy Initiative

Global Democracy Initiative (GDI) is a coalition of civil society organizations that are working together on conceptualizing and implementing a democratic system to find global solutions for today's global challenges. [We envision a democratic system that allows world citizens to weigh in on how global problems will be solved.](#) We strive to create a global democracy platform that provides tools for world citizens to:

1. Decide about what are global problems that need transnational solutions,
2. Develop transnational solutions for how global problems will be solved, and
3. Vote on different solutions to decide which solutions should be implemented.

Why a global digital voter identity?

The Global Democracy Initiative (GDI) consists of various working groups that examine different aspects of global democracy. The "Digital Identity" working group, in particular, is focused on a project aimed at establishing a global digital voter identity.

Currently, there is a growing number of social media platforms, petition and deliberation platforms, as well as voting tools available. These platforms enable citizens to express their opinions in multiple ways. However, a crucial element missing from all of this is a (digital) identity that can uniquely and reliably identify every world citizen across multiple platforms. To address this gap, we introduce [GloKi – a digital identity that is easily obtainable for all world citizens](#), while still ensuring security and protection against identity theft.

Our human identity is fragile, and our digital identity is even more vulnerable. When the internet became accessible to the public in the mid-1990s, many believed it would propel humanity into an era of collaboration and progress. However, we now understand that this vision did not materialize. Digital technology was influenced by various factors that existed when the internet emerged, such as nationalism and hate. We are well aware of how [online identities can be abused to spread hate or dehumanize](#) certain groups of people. Additionally, it has become increasingly common to manage multiple digital identities or personas across different platforms.

The concept of national identity represents the latest iteration of an everlasting quest for belonging. As humanity becomes more interconnected through digital technologies, the need for [an identity that transcends nationality](#) becomes increasingly evident. This identity should not be confined by the limitations imposed by nation-states. Instead, it should be linked to voting systems and debate forums forming the foundation for an effective system of global governance. It should affirm the right to vote and participate in global decision-making.

The abundance of digital identities and login systems reflects the saturation of national identities. However, the pressing global issues that affect humanity do not hold a central position within the current Single Sign-On (SSO) framework. Instead, large multinational technology companies focus on expanding their market share and generating revenue. Nevertheless, an alternative approach that empowers individuals and their rights is possible.

[By fostering a sense of belonging, providing a secure global voting platform, and empowering world citizenship, we can advance the vision and mission of the Global Democracy Initiative.](#)



The GloKi Mission

GloKi aims to enable every living human being to participate in the global democratic system through a digital identification system. [Our goal is to make one ID accessible and affordable for all people, ensuring equality and preventing fraud.](#) We prioritize security, data protection, and privacy. However, achieving this without a central authority poses challenges. We can achieve stewardship of GloKi through a central elected body, a coalition of central bodies, or individual decentralized stewardship. The voting platform determines parameters like age for voting rights, while GloKi provides the identification. Our system is applicable to all levels of governance, from local to global, and doesn't rely on national IDs to promote inclusivity and avoid conflicts. We address concerns about biometric data storage by exploring alternatives like individual control or parallel secured systems.

Creating a self-sovereign, decentralized digital identification system involves addressing substantive and procedural considerations. Substantive aspects include [prioritizing security, interoperability, privacy, transparency, and resilience.](#) Procedural considerations include compliance with relevant laws, establishing governance, adhering to standards and protocols, conducting testing and certification, ensuring user adoption, and designing user-friendly interfaces.

Regarding the technical requirements, we need to decide on the type of identification system (decentralized, centralized, hybrid), collaborate with other entities, determine the need for a physical counterpart, establish verification methods, consider self-identification, balance the power between central authority and self-identification, ensure equity, inclusiveness, and scalability, choose a suitable digital, blockchain, or crypto platform, protect global data, handle blocked persons and criminals, decide on openness of voting, assess available resources, and define the ultimate goal of our identification system. We also need to evaluate if existing platforms meet our needs or if a new platform needs to be developed.

Implementing and marketing the ID pose practical concerns such as resource allocation, stakeholder coordination, addressing political opposition, complying with laws, assessing economic feasibility and sustainability, understanding social implications, building trust, driving widespread adoption, ensuring effective communication, fostering partnerships, and securing long-term support and investment.

The GloKi solution revolves around the "3 D-s": decentralized code that is open source and subject to scrutiny, a decentralized community governing the development, and decentralized records using blockchains. [We implement decentralized authentication through peer-to-peer authentication and a web-of-trust.](#)

How does GloKi work?

In this section we present a decentralized mechanism to authenticate the validity and singularity of GloKi, the global digital voter identity.

A trustless web-of-trust

The concept of a web-of-trust goes back to 1991 to the development of Pretty Good Privacy (PGP), a text encryption program that used private and public keys to encrypt messages. The concept of a web-of-trust appears in the PGP manual as a decentralized method to authenticate users' public keys.

When trusting people it is more common to trust people that we know. A friendship network, as in Facebook or Twitter, is a good example of such trust networks. Such networks show the community structure of society, as people tend to trust other people in the same community more than they trust strangers. The problem is that fake identities can easily mimic the same trust structure, especially a group of fake identities operated by the same operator.



To address this issue we propose the notion of a trustless web-of-trust. In a trustless web-of-trust people authenticate strangers. Such a network does not show a communal structure and their structure is more chaotic. [Such a network makes it harder for fake identities to get verified, as it requires random people to authenticate the fake.](#) Authenticating a stranger is slightly harder for two valid identities, and is much harder for a fake identity to get authenticated by an honest identity.

To authenticate strangers, we require the use of digital identifiers. Each GloKi profile will include a valid piece of digital information that uniquely identifies the holder of this identity. We advocate for the use of profile images as probably the simplest form of identification. Though, admittedly, facial images are not very unique. Many people resemble each other close enough such that their picture will look like the same person, we still prefer facial images for their simplicity. In the future, an extension to GloKi might be desired, that includes a stronger identifier, like fingerprints, for more sensitive voting processes.

A well connected trust-graph

It isn't too hard for a corrupt individual to find enough corrupt friends to certify their collection of fake identities. [This is where mathematics comes into play](#). Presenting individuals as nodes in a graph, where an edge between two nodes signifies that these two individuals authenticated each other (and digitally signed each other's digital profile), we get a graph that we can use to measure the connectivity of a community. Social networks, for example, present a well connected graph of friendships, where the diameter of the graph is surprisingly small (This is known in the literature as the six degree of separation principle). However, in other measures of connectivity, such graphs are poorly connected, in the sense that they contain narrow bottlenecks between communities.

By randomly selecting who authenticates whom, the resulting graph will exhibit no such bottlenecks. Is it in such communities that fake identities will have the hardest effort to infiltrate, as it is easy for a corrupt individual to authenticate their own fake identities, but it will be hardest for their to find a random set of individuals who will agree to authenticate the fake.

Our proposed algorithm is therefore as follows - given a well connected trust-graph, of a group of people that form a community (a community may start with a small kernel of individuals, where everyone authenticated everyone else), when a newcomer wishes to join, the computer picks at random a given number of individuals within the community. [The newcomer and the selected committee then authenticate each other and digitally sign each other's digital profile](#). After verifying that the resulting graph of authentications is highly connected (no bottlenecks), the computer adds the newcomer to the community.

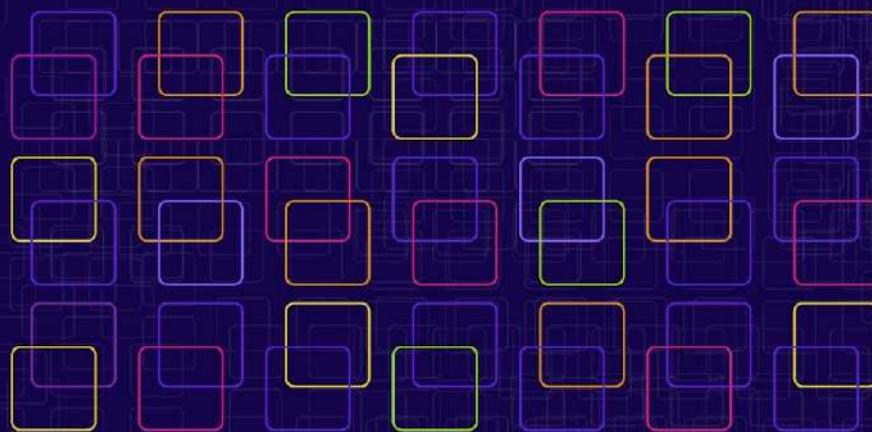
The caveat of authenticating strangers, is that there is no way for an individual to check whether another individual is using only one identity, or many. However, this is not very feasible even in networks based on trust. It is practically impossible to prove that one does not hide something, somewhere in the world. Therefore, while this caveat seems harder when authenticating strangers, it is actually hard in any system without any central authority. [We therefore split the authentication process into two steps](#). Humans authenticate that a given identifier (a profile picture for example) indeed identifies an individual, while AI authenticates that the given identifier is unique within the system.



A public reservoir of identifiers

It is a common knowledge in detective stories and films that the best way to achieve privacy is to blend in the crowd. To guarantee the uniqueness of GloKi without relying on central authorities for identification, we advocate for the use of a public reservoir of profile pictures. Measures can be taken to guarantee that such profile picture will retain anonymity, in the sense that although it is very simple to locate an image in such a database of someone you know, [it will be practically impossible to locate the real individual from their profile picture](#), assuming the reservoir is big enough to exclude exhaustive search. The database will hold only images, without any other identifying information.

Using such a public database, it should be easy for an individual to access their own image, and also to prove that their digital profile contains a valid pointer to such an image. Once such a database exists, it should be possible for a computer to find possible duplicates within the database, using software similar for example to the one used by the google photos application. [Given a profile signed by enough members of a community, embedded in a highly connected trust-graph, with a profile image verified as unique within a public database of images, these are the keys for authenticating GloKi.](#)



Limitations of GloKi

The GloKi concept has garnered support as a potential solution to enhance the integrity and inclusiveness of global democratic processes. However, there are legitimate concerns and opposing viewpoints that need to be addressed to ensure its viability. These concerns include the lack of consensus on global standards, the potential for abuse, the cost of development and implementation, privacy concerns, and technological challenges.

Inclusivity

One of the primary concerns is the lack of consensus on global standards for voter identification and authentication. Each country has its own unique systems and requirements, making it challenging to establish a universally acceptable standard. To mitigate this challenge, [GloKi will be designed to be flexible and adaptable, considering the diverse cultural and social differences worldwide](#). By incorporating input from various stakeholders and accommodating regional variations, a consensus can be reached without compromising the system's integrity.

Privacy

Another concern is the potential for abuse, as GloKi could be exploited for surveillance or tracking purposes. Moreover, privacy concerns could arise due to the collection and storage of large amounts of personal data in the GloKi system. To address the potential for abuse, [GloKi will prioritize privacy and security protections](#). Measures such as encryption, data minimization, and decentralization can be implemented to prevent unauthorized access to user data, ensuring that the system is secure and resistant to abuse. To address concerns with personal data storage, [GloKi will strictly limit the collection and storage of personal data](#) to only what is necessary for authentication and verification purposes. GloKi will also implement an opt-in for users to share anonymized information and profile pictures. By adhering to strict, legally-binding data protection protocols and ensuring transparent data management practices, the system can instill confidence in users regarding their privacy and security.

Resource Constraints

The cost of developing and implementing a global identification system is another significant challenge. However, the potential benefits of increased democratic participation and improved electoral integrity may justify the cost. Exploring funding options from various sources, including governments, international organizations, and private entities, can help alleviate the financial burden associated with the project.

Implementing a global identification system also poses technological challenges, particularly in terms of biometric authentication and data storage. However, advances in technology have made it more feasible than ever before. Leveraging these technological advancements and collaborating with experts in the field can help overcome these challenges. Additionally, ensuring system resilience against technical failures and malicious attacks through thorough testing and certification is crucial to maintain the system's integrity.

In marketing GloKi, additional challenges must be considered. Building trust among potential users and stakeholders is paramount, especially when concerns about privacy, security, or political bias exist. [Effective communication strategies will be employed to highlight the benefits of the system and ensure that users understand its proper utilization](#). Collaborations with governments, international organizations, and technology providers are essential to secure

widespread adoption and usage, particularly in regions with low technological infrastructure or literacy rates. Lastly, securing ongoing investment and support is vital for the long-term sustainability of the global identification system.

By acknowledging and addressing these limitations and challenges the public can gain a comprehensive understanding of the complexities associated with implementing and marketing GloKi. Through thoughtful planning, collaboration, and the implementation of appropriate safeguards, a global identification system has the potential to improve the integrity and inclusiveness of democratic processes on a global scale.

Conclusion

The Global Democracy Initiative (GDI) aims to establish a global digital voter identity known as GloKi. This initiative recognizes the need for a unique and secure digital identity for every world citizen, linked to voting systems and debate forums, to enable effective global governance. [GloKi's decentralized identification system involves addressing security, privacy, and central authority challenges through the use of decentralized code, a decentralized community, and decentralized records using blockchains.](#) Measures like peer-to-peer authentication and a digital coin tied to GloKi could combat attacks and promote verified participation in global democratic systems.



GloKi utilizes a decentralized mechanism called a trustless web-of-trust for authentication, making it difficult for fake identities to be verified. By randomly selecting individuals for authentication and utilizing public profile images, authenticity can be ensured without relying on central authorities. Challenges related to global standards, abuse potential, cost, privacy, and technology must be carefully addressed and mitigated. Flexibility, privacy protections, collaboration, and user trust are essential for successful implementation. Experts are encouraged to contribute and support the development of GloKi for a more inclusive and robust global democracy.

Copyright Information

The information contained within this document, including but not limited to the text, images, diagrams, and concepts, is the intellectual property of Global Democracy Initiative ("GDI"), an unincorporated civil society organization comprised of various civil society organizations from the United States, Switzerland, the United Kingdom, and Israel. GDI asserts its copyright ownership over this material and all associated rights, unless otherwise stated.

This document is provided for informational purposes only and may not be reproduced, distributed, or transmitted in any form or by any means, electronic or mechanical, without the prior written permission of GDI. Any unauthorized use, reproduction, or distribution of this document, in whole or in part, may constitute a violation of copyright laws and other applicable intellectual property rights.

GDI reserves the right to take legal action to protect its intellectual property, including seeking damages and injunctive relief, in the event of any unauthorized use or infringement. The views and opinions expressed in this document are those of GDI and do not necessarily reflect the views of individual civil society organizations or their respective members.

By accessing or using this document, you acknowledge and agree to respect GDI's intellectual property rights and to abide by the terms and conditions outlined in this copyright disclaimer.

For inquiries or requests regarding the use of this document or its contents, please contact the Global Democracy Initiative:

Dr. Gery Colombo,	GloCo,	ger@glco.ch
Dr. Lars Lünenburger,	GloCo,	lars@glco.ch
David Gallup, JD	World Citizen Government,	david@worldcitizengov.org
Eston McKeague, MSc	Young World Federalists,	contact@ywf.world
Dr. Ouri Poupko,	Ben-Gurion University,	ouri.poupko@gmail.com

Thank you for your cooperation and understanding in respecting the intellectual property rights of the Global Democracy Initiative.