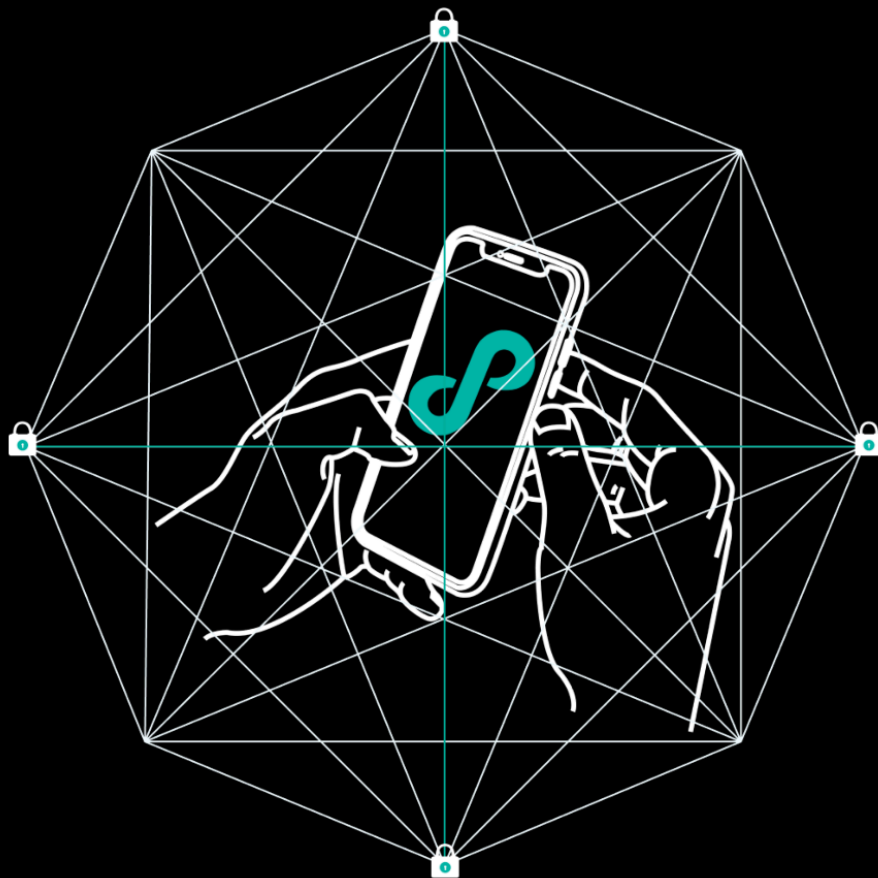


PRIVACY-FIRST ARCHIVING

Implementing Secure,
Decentralized Storage to
Protect Mobile Media



OpenArchive & **HYPHA**



With support from Filecoin
Foundation for the
Decentralized Web (FFDW)

Table of Contents

| | |
|---|-----------|
| Executive Summary | 2 |
| I. Introduction | 4 |
| II. Ecosystem Mapping | 6 |
| OpenArchive's Human Rights-Centered Approach | 6 |
| Conducting Co-Research | 7 |
| Creating User Personas | 8 |
| Pervasive UX <> Privacy Trade-offs | 8 |
| Assessing DWeb Technologies for DACs | 9 |
| Decentralized (DWeb) Storage Opportunities | 9 |
| Enhanced Security and Resilience | 10 |
| Immutability and Data Integrity | 10 |
| Independence from Centralized Platforms | 10 |
| Federated vs. Peer-to-Peer Systems | 11 |
| Decentralized (DWeb) Storage Challenges | 11 |
| Security Risks from Open Participation | 12 |
| Barriers to Accessibility and Adoption | 12 |
| Legal and Ethical Concerns Around Stored Content | 12 |
| Shared Risks with Centralized Platforms | 12 |
| Potential Downstream Risks of DWeb Storage | 13 |
| DWeb Storage: Potential Risks & Mitigation Tactics | 13 |
| III. Research → Practice, Assessing DWeb Storage for DACs | 15 |
| DWeb Storage Requirements for Decentralized Archivist Communities | 15 |
| P2P Protocol Comparison | 17 |
| Comparing P2P Protocols | 17 |
| Exploring the Chosen Protocols: Iroh and Veilid | 18 |
| DWeb Storage Considerations | 19 |
| IV. Implementing Mobile-First DWeb Storage, A Novel Approach | 22 |
| Technical App Overview | 22 |
| DWeb Storage: Future Directions | 23 |
| V. Conclusion | 25 |
| Bibliography | 26 |
| Appendix | 28 |
| DWeb Backend Privacy Overview | 28 |
| P2P Protocol Review | 28 |
| Glossary | 28 |
| DWeb Resources | 28 |
| Acknowledgements | 29 |

Executive Summary

Decentralized technologies are unlocking new and revolutionary ways to mitigate threats to expression, privacy, provenance and preservation when sharing and archiving media online. They reduce dependence on ever-growing centralized platforms by offering collaborative alternatives that inherently circumvent threats like censorship, control, media manipulation, and surveillance, which are now endemic to these platforms. In this paper, the authors — [OpenArchive](#) and [Hypha Worker Co-operative](#) — test these assumptions by researching, developing, and implementing novel DWeb storage technologies in the mobile media archiving ecosystem.

Given the ubiquity of computers and internet access, one may think that it would be easy to preserve most media shared online. However, in this *age of information centralization*, new threats to digital media are ever evolving. For example, information disappears due to linkrot and censorship, and disinformation proliferates due to AI-fueled deepfakes that manipulate media. While people are creating and sharing more media than ever before, it is increasingly at risk as it resides on proprietary platforms that prioritize profit over preservation, provenance, privacy, or rights. Despite posing increased threats to the historical record, these platforms (such as Facebook, YouTube, Instagram, TikTok, and others) are still the primary destination for most mobile media and those consuming it. In order to ensure that media is authenticated, preserved, and accessible in the future, a more intentional approach is urgently needed to protect pertinent information like citizen journalism, breaking news, and personal archives more generally.

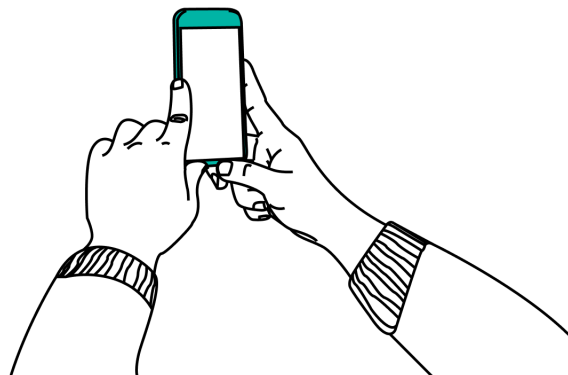
OpenArchive is a research and development organization that builds harm reduction tools and resources to improve the digital archiving ecosystem for those who are disproportionately impacted by the aforementioned challenges — documenters, archivists, journalists, historians, legal advocates, and teachers. As a pioneer of applying a human rights-centered approach to co-creating responsive and ethical tools and resources, OpenArchive is well-positioned to test assumptions about challenges and opportunities that arise when using *decentralized* storage and peer-to-peer protocols through a community-focused lens. This paper maps the research and development processes of these novel decentralized mobile archiving technologies that aim to better protect, preserve, and verify digital media.

Along with the Hypha Worker Co-operative, OpenArchive tested whether and how decentralization could mitigate digital archiving challenges to security, provenance, and autonomy. To do so, they created a proof of concept called ‘*DWeb Storage*’ — now in beta production — that integrates decentralized storage into OpenArchive’s free open source secure archiving mobile application [Save](#) that helps people securely archive, verify, and encrypt their mobile media. This approach seeks to determine if this novel mobile-first *DWeb Storage* is a viable way to foster privacy, accessibility, verifiability, and sustainability when preserving mobile media while also mitigating emergent threats.

These research and development outputs are guided by the Human Rights Centered Design Methodology (HRCDD), a responsive, intentional design framework co-authored by OpenArchive's Executive Director. In practice, HRCDD uses a collaborative and iterative approach throughout the research, threat modeling, design, and technical development phases to ensure that OpenArchive's tools and educational resources meet the needs of its beneficiaries. Top priorities include: privacy, security, and accessibility, which are centered throughout the development and integration of *DWeb Storage* into **Save**.

Through this process, the authors chose to implement two DWeb protocols — Veilid and Iroh — as the foundation of *DWeb Storage* because they best suit the needs of “Decentralized Archivist Communities” (DACs) — a term that refers to a group that collects, preserves, and maintains media archives. The authors chose these protocols because they best meet the DAC's needs by enabling peer-to-peer sharing, encryption, and redundancy while prioritizing usability. This *DWeb Storage* implementation puts theory into practice to provide a novel and ethical way to securely archive mobile media for future generations. In addition to centralization, the greatest threat to this critical harm-reductive work and the historical record is a lack of sustainable support.

September 2025



I. Introduction

“Our task is to make trouble, to stir up potent response[s] to devastating events, as well as to settle troubled waters and rebuild quiet places.”

— Donna J. Haraway, *technology and cultural theorist*¹

In the beginning, the internet was founded on open protocols, and things were good (if somewhat chaotic)². But with the rise of Web 2.0 and social media, we find ourselves in the era of the corporate network,³ which, unlike the open source ethos of the early internet, is centralized around an omnipotent, profit-first company.⁴ Entrusting our data to corporate networks endangers its longevity as businesses change hands, close, or pivot, and this is especially true for data meant to be archived — that is, stored for long or indefinite lengths of time. Working against this tide of centralization is a movement and suite of technical tools known as Decentralized (DWeb) technologies. The DWeb movement centers on people, not profits, and aims to build an Internet that is “private, reliable, secure and open.”⁵

Due to a lack of support for rights-focused secure open source technologies, most privacy-first Decentralized Web (DWeb) tools are not yet easy to use and therefore not as widely adopted as mainstream proprietary centralized platforms. Notwithstanding, the outsized need for these types of tools across nearly all sectors is twofold: they provide foundational infrastructure — like the ability to verify and preserve media — necessary for democratic discourse and practice online, and they help protect people from maligned actors.

Since 2015, OpenArchive has championed rights-centered co-research, risk and threat assessments, and co-development of a mobile tool and resources that serve a diverse community of stakeholders. Through this people-first approach utilizing human rights-centred design, OpenArchive positioned itself as a leader in creating responsive tools that reconcile the tradeoffs between secure archiving and usability.

In this paper, OpenArchive will present outcomes from its collaboration with the Hypha Worker Co-operative on integrating decentralized storage or ‘DWeb Storage’ into OpenArchive’s flagship mobile application, **Save**. OpenArchive designed the app to help people securely archive, verify, and encrypt their mobile media to protect themselves and their media for the long-term. This integration marks one of the first implementations of noncommercial, free, open-source DWeb storage for mobile

¹ Haraway, Donna J. “[Staying with the Trouble: Making Kin in the Chthulucene](#)”. Duke University Press, 2016.

² Jacobs, Ian. “[Architecture of the World Wide Web 1.0. Editor's Draft 28.](#)” W3C, November 28, 2003.

³ Dixon, Chris. “Read Write Own: Building the Next Era of the Internet”. Random House, 2024.

⁴ Ibid

⁵ [DWeb](#) (website). Accessed September 12, 2025.

media. The novel *DWeb Storage* backend combines two open-source protocols—Veilid and Iroh—that complement their respective strengths and weaknesses to provide privacy-first peer-to-peer decentralized storage for mobile media. To distinguish the novel *DWeb Storage* backend integration into **Save** from the more broad term ‘DWeb storage’, it is capitalized and italicized throughout the paper.

Section II details OpenArchive’s participatory research methodology, highlighting the team’s practice of centering human rights by collaborating with key stakeholders throughout the entire research, design, and iterative development processes. Through this extensive qualitative co-research deployment, OpenArchive works with partner communities to integrate decentralized storage technologies into their workflows. During this collaboration, emergent benefits, threats, and pain points throughout the process surface, which help determine the suitability of this technology for communities and downstream risks that could present after integration.

Section III, “Research → Practice, Assessing *DWeb Storage* for DACs”, builds upon this thread as OpenArchive and Hypha present their list of criteria for DWeb storage protocols that meet the DAC’s needs, with the goal of improving the user experience, privacy, and efficacy of DWeb storage. After mapping out the features of the various available DWeb protocols, the authors reviewed the tradeoffs between privacy and usability, created potential mitigation strategies, and chose to use Veilid and Iroh as they best met the DAC’s requirements.

In Section IV, ‘Implementing Mobile-First *DWeb Storage*, A Novel Approach’, OpenArchive presents an overview of the technical architecture of the *DWeb Storage* integration into **Save** and closes with some opportunities for future improvement.

As the internet becomes increasingly centralized, it monetizes our attention, impacts our behaviors, and creates new societal challenges while revealing new vulnerabilities. It is imperative that organizations making harm reductive, people-first tools are sustainable into the future. This can only happen with significant investment from funders who want to ensure that technologies serve humanity first and not the other way around. Without urgent and significant support, the safety of the historical record and indeed our collective humanity are at risk.



II. Ecosystem Mapping

OpenArchive's Human Rights-Centered Approach

Given that OpenArchive has focused on the ethical preservation of mobile documentation for over a decade, the team is uniquely positioned to explore emergent technologies, like DWeb technologies, that could better protect documenters and their media. When co-creating with and for [Decentralized Archivist Communities](#) (DACs),⁶ OpenArchive uses an in-depth participatory research and design process called the [Human Rights Centered Design \(HRCD\) Methodology](#).⁷ Co-created by OpenArchive's Executive Director along with design, security, and human rights experts, this methodology is the backbone of OpenArchive's research and development processes.

Through this co-research, OpenArchive is able to identify the key pain points these communities face by creating personas to map out the use cases and ecosystem they're working in. The research process includes three key components: threat modeling, conducting needs assessments, and creating user personas. This research is then incorporated into an iterative co-design process to build responsive, usable tools that help mitigate technological and material challenges DACs face.

Threat Modeling

Threat modeling is a structured process with these objectives: identify security requirements, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerability criticality, and prioritize remediation methods⁸. Threat modeling not only helps OpenArchive assess DACs' vulnerabilities and provide protective measures around DAC's practices, but also informs OpenArchive's tool development to ensure they meet the DACs' needs. Threat modeling is iterative as it must be performed throughout the research and development processes. At the beginning of the research phase, the HRCD process requires researchers to evaluate whether the collaboration and tools could unintentionally cause more harm than good to vulnerable communities.

For example, before embarking on co-research, OpenArchive assesses potential threats to the DACs that may arise throughout the research process. These could include surveillance of sites that host surveys or communications, which can be

⁶ A DAC, or Decentralized Archivist Community, is a group that collects, preserves, and maintains media archives.

⁷ C., Natalie, and Sinderson, Caroline. "[Human Rights Centered Design Methodology](#)." 2022.

⁸ BlackDuck. "[What is threat modeling?](#)" Accessed September 12, 2025.

mitigated by using self-hosted surveys and end-to-end encrypted communications platforms, respectively.

Conducting Co-Research

Once co-research begins, OpenArchive will do a needs assessment analysis in the form of a survey or focused interviews with DAC community members. This helps OpenArchive map out the DAC's needs and unique threat model. In this phase, threat modeling seeks to understand who might be interested in the DAC's data, how they could access it, and what they might seek to gain by doing so. This practice helps to protect against these threats and explore potential practices and tools DACs could use to mitigate them.

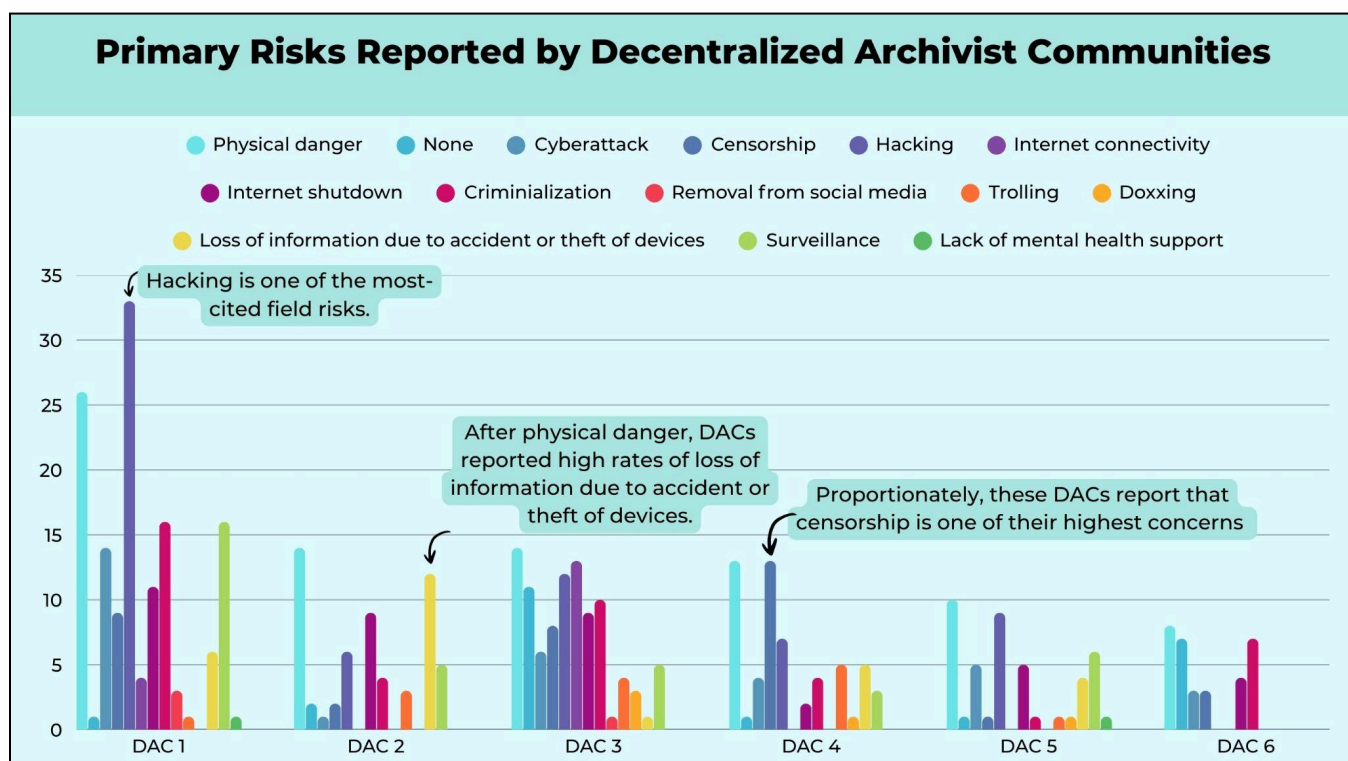


Figure 1: DAC research outcomes

The above figure illustrates many risks identified through the needs assessment research phase with six key communities. These communities are based in the Latin America and MENA regions and often work in at-risk environments facing both digital and physical risks. The surveys, or interviews when appropriate, are crucial for identifying the risks in order to mitigate them. The needs assessment includes questions on how they carry out their work, what sorts of technical tools they use and how comfortable they are using technology, what their internet access is like, and what makes them nervous or unsafe while doing their work.


Threat modeling provides a dual benefit — it is valuable for DACs as they adapt mitigation strategies, and is also invaluable to OpenArchive as a tool developer, as it helps to ensure that the tools address privacy, security, and usability concerns. Once

OpenArchive and the DAC jointly review the responses to the needs assessment survey or interviews, the OpenArchive team moves on to create user personas.

Creating User Personas

According to Patrick Faller, “user personas are [anonymized] archetypical users whose goals and characteristics represent the needs of a larger group of users.”⁹ Informed by the DAC’s responses to needs assessment surveys, the user personas became an integral part of our process to identify and better understand their roles, tasks, needs, and threat models — more specifically, their physical and digital threats. This guides the research and development processes that OpenArchive uses to develop effective strategies and tools for mitigating these risks.

Oleksandra



| | |
|----------------------|---|
| Age | 33 |
| Gender | Female |
| Role | Documenter and database manager for a Ukrainian NGO |
| Skills | Plays a dual role. Oleksandra captures evidence first-hand, then collects her, and others', evidence to organize and analyze an evidence archive. |
| Base Location | Kharkiv |

“Building and managing a secure database with limited resources is difficult, especially under the circumstances. Secure, co-developed, and user-adapted tools and trainings help keep our evidence organized and protected.”

Figure 2: A user persona based on feedback from a Ukrainian DAC

For example, the Ukrainian DAC records impact statements and testimonies from eyewitnesses. Their efforts hope to inform peacebuilding and rebuilding in the country post-war. The DAC partner in Ecuador documents environmental issues caused by extractive mining. Given the very different contexts these two DACs operate in, the needs assessment surveys identified different pain points and possible solutions.

Pervasive UX <> Privacy Trade-offs

Another key takeaway from surveying hundreds of DACs is that usability is paramount and will almost always be prioritized over safety. This likely is due to how frictionless most everyday technologies are. Due to a lack of significant investment, most digital security projects are lagging behind in usability. Given the ubiquity of easy-to-use technologies, many users are not willing to make the persistent but necessary trade-offs between privacy and usability to stay safe. Creating personas from real-world decentralized archivist communities is one way to decrease the

⁹ Faller, Patrick. “[Putting Personas to Work in UX Design: What They Are and Why They’re Important](#).” Adobe Creative Cloud, December 17, 2019.

privacy and usability trade-offs as OpenArchive learns more about both their risk tolerances and technological capabilities. This helps prevent a recurring problem within the tech world of building the tech for the developer-class and expecting non-technical users to be willing to learn how to adopt it without measuring the likelihood that they actually will.

Assessing DWeb Technologies for DACs

After gaining a better understanding of DACs' needs and risks, OpenArchive examined the emergent DWeb ecosystem to determine if and how it might serve them. First, OpenArchive conducted an [initial assessment of the decentralized storage ecosystem](#) to see what is currently available.¹⁰ The preliminary research included a review of twelve available DWeb protocols, assessed by their ability to meet the needs of the DACs, needs that included affordability, security and privacy. This research demonstrated that DWeb storage held promise to solve for some of the challenges DACs face like a need for redundant, verifiable storage that they control. Decentralized storage technologies meet these needs because they distribute data across multiple nodes, each managed by independent entities. This approach creates a resilient, secure, and collaborative method for data hosting, access, and archiving. Since novel technologies come with novel risks, it's essential to carefully consider them alongside the benefits.

From there, OpenArchive began conceptualizing how a DWeb backend would function as an additional storage destination for **Save**. Discussed in a forthcoming section, the primary aim of this [implementation of the DWeb Storage prototype](#)¹¹ is to reconcile usability with DACs' security needs. Read on to review the opportunities and challenges of DWeb storage solutions for DACs.

Decentralized (DWeb) Storage Opportunities

Decentralized Web technologies — especially those based on peer-to-peer (P2P) networking and blockchain — offer a number of benefits, including enhanced security, resilience, and data integrity. It effectively circumvents censorship and surveillance, while also providing provenance and authentication, which exposes media manipulation such as deepfakes¹². DWeb Storage technologies have the potential to challenge dominant, proprietary Big Tech companies, many of which rely on extractive data processes to meet their revenue requirements. Decentralized and open source tools play a key role in creating a more ethical, diverse, protective, and vibrant tech ecology.

¹⁰ OpenArchive. "[Mapping the Decentralized Storage Ecosystem](#)." February 13, 2024.

¹¹ OpenArchive. "[Creating the First Decentralized Web Storage Backend for Mobile Media](#)." November 21, 2024.

¹² Villasenor, John. "[Artificial intelligence, deepfakes, and the uncertain future of truth](#)." *Brookings*, February 14, 2019.

Enhanced Security and Resilience

One of the main advantages of decentralized storage is its improved security. The cryptographic foundations of well-designed DWeb systems ensure strong commitments to privacy while reducing the risks associated with centralized control. Because there's no single authority responsible for managing the data, these systems are less vulnerable to a single point of failure (SPOF)—a critical weakness in traditional centralized models.

This resilience is particularly important in regions where internet access is censored or under threat. As the Public Good App House points out: “If one node in the [P2P] network breaks down or gets hacked, the network will be able to maintain functionality. Also, P2P networks are not subject to the bottlenecks that can happen in the client-server model when an individual server experiences slow, limited service or even a complete crash.”¹³

A real-world example of this resilience can be seen in the efforts of LikeCoin's founder. When [Radio Television Hong Kong](#) announced plans to delete archival content, most notably material from the 2019 Hong Kong protests, LikeCoin used decentralized publishing to help preserve those records¹⁴. This effort was designed to protect against SPOFs such as hacking, tampering, or deletion by external actors.

Immutability and Data Integrity

Another critical advantage of DWeb technologies is immutability. In blockchain-based systems, data entries are verified through a consensus mechanism, making them functionally unalterable once recorded. This is especially valuable in combating misinformation and guarding against the manipulation of records.

For instance, SaveMyIdentity¹⁵ is a blockchain-based project developed to support marginalized populations, specifically Venezuelan refugees. By offering a decentralized identity verification system, SaveMyIdentity allows displaced people to have a form of identification that is verifiable and tamper-proof, thanks to the immutability of the blockchain ledger.

Independence from Centralized Platforms

Decentralized storage also reduces dependence on large, privately owned platforms, which often prioritize commercial interests over human rights or data integrity. Sam Gregory of WITNESS notes: “A couple of years ago, the Syrian human rights group Mnemonic saw hundreds of thousands of videos of the Syrian conflict disappear overnight, because of a change in YouTube’s moderational algorithm. Now, you have

¹³ TechSoup, “[DWeb Use Cases for Civil Society](#),” November 27, 2023.

¹⁴ Hui, Mary. “[Hong Kongers Use Blockchain to Fight Government Censorship](#).” *Quartz*, May 26, 2021.

¹⁵ [SaveMyIdentity](#) (website). Accessed September 12, 2025.

a real dependence on commercial platforms, for which human rights issues are not a primary business concern. Their moderation decisions affect the ability of [DACs] to leverage and control the footage they shoot.”¹⁶

This illustrates the risks of relying on centralized commercial platforms to store sensitive or mission-critical data. Decentralized systems offer a more secure and autonomous alternative. They also help users avoid vendor lock-in, a situation where switching platforms becomes impractical or cost-prohibitive.¹⁷ Decentralization removes reliance on a single proprietary provider and opens up access. Some researchers suggest this open model is “key to combating misinformation around conflicts,” especially when content moderation decisions affect visibility and availability of crucial information.¹⁸

Federated vs. Peer-to-Peer Systems

It's important to note that not all decentralized systems are built the same. For example, the popular social platform Mastodon is decentralized but not truly peer-to-peer or blockchain-based. Mastodon operates using a federated architecture where, similar to email, independently run servers manage user data.¹⁹

Unlike a true P2P network (like [Save's DWeb Storage](#) backend), Mastodon depends on an established, stable server infrastructure to some extent. This makes it easier to manage but also limits its resilience and independence compared to blockchain or P2P-based solutions.²⁰

Decentralized (DWeb) Storage Challenges

While decentralized storage offers many benefits, it also presents distinct challenges, particularly around security, privacy, accessibility, and legality, particularly for DACs.

Security Risks from Open Participation

Open access in decentralized networks can allow malicious actors to join the system. These individuals might attempt to deanonymize users or flood the network with harmful or disruptive content, undermining both the network's functionality as well as its promise of privacy.

¹⁶ Gregory, Sam in Thompson, Caitlin. “[Can the decentralized web help to protect human rights?](#)” *CodaStory*, November 17, 2021.

¹⁷ Ushahidi, “[The Transformative Power of Open-Source Technologies and Decentralized Web Storage.](#)” July 25, 2024.

¹⁸ Hellstern, R., D. C. Park, V. Lemieux, et al. “[Leveraging Blockchain-Based Archival Solutions for Sensitive Documentation: a Xinjiang Case Study.](#)” *DISO 1* (4), July 18, 2022.

¹⁹ Silberling, Amanda. “[A beginner's guide to Mastodon, the open source Twitter alternative.](#)” *TechCrunch*, July 24, 2023.

²⁰ Mastodon. “[Mastodon Documentation.](#)” Accessed September 12, 2025.

Barriers to Accessibility and Adoption

For many users, especially those unfamiliar with DWeb technologies, the decentralized storage model can be intimidating or confusing. Boosting technological literacy is essential so that DACs can make informed choices about their storage needs and the associated risks.

Improving this literacy can also enhance trust in new onboarding methods, like QR code access, which may be unfamiliar to non-technical users of tools like [Save](#).

Legal and Ethical Concerns Around Stored Content

Individual privacy-conscious participants may be reluctant to store unknown data from others on the network. Concerns range from legal liability—such as unintentionally storing fragments of illegal content (e.g., child sexual abuse material, or CSAM)—to ethical dilemmas, like unintentionally aiding political opponents. These fears can deter participation, even if their knowing involvement is difficult to prove.

Shared Risks with Centralized Platforms

Interestingly, many of these risks also exist in centralized systems. Social media users, for instance, regularly face threats to their privacy or safety, and supporters of archiving projects can become exposed simply by interacting with or sharing content.

The key difference is that users have grown accustomed to the privacy and legal boundaries of mainstream corporate platforms, even when they are far from perfect.

Nonetheless, the legal environment in decentralized scenarios remains less defined than in the litigated and increasingly regulated centralized spaces of cloud-based storage, and users of decentralized networks cannot easily assess the risks they may face or the accuracy of those seeking to limit the use of these networks. Additionally, compliance with data protection laws, as well as the new and emergent issues generated by this unique form of storage, is of pressing concern for DACs and developers in the decentralized space.²¹ Such legal and privacy ambiguities may damage user trust in DWeb storage.

The next section examines various DWeb protocols for the specific opportunities and challenges each provides. It also more deeply reviews the two protocols, Veilid and Iroh, that Hypha Worker Cooperative and OpenArchive selected for integration into [Save's](#) new *DWeb Storage* backend.

²¹ Ushahidi, "[The Transformative Power of Open-Source Technologies and Decentralized Web Storage](#)." July 25, 2024.

Potential Downstream Risks of *DWeb Storage*

By assessing the opportunities and challenges presented by DWeb storage writ large, some key risks surfaced, and the authors worked to mitigate them when implementing *DWeb Storage* into **Save**. Figure 3 highlights these key risks and mitigation strategies below.

DWeb Storage: Potential Risks & Mitigation Tactics

| Risks | Who is affected? | Save's Mitigation Strategies |
|--|--|--|
| Climate Impacts | | |
| <ul style="list-style-type: none"> Blockchain and decentralized storage use significant energy. Even low-power protocols impact climate. | In the long-term, everyone; in the short-term, those living in climate-vulnerable areas without adapted infrastructure. | Save uses low-resource protocols (Veilid and Iroh) that do not require mining, which is an energy-intensive process. |
| Privacy and Anonymity | | |
| <ul style="list-style-type: none"> Difficulty removing personal data due to immutability ("right to be forgotten"). Potential for unintended public exposure of sensitive content. | Everyone, but particularly those with higher privacy and/or anonymity needs. Some may want to later revoke identifying details from mobile media. | <ul style="list-style-type: none"> Strict onboarding policies and encrypted sharing (secret URLs, QR codes, disappearing messages). Good overall OPSEC. |
| Legal Ecosystem | | |
| <ul style="list-style-type: none"> Lack of legal clarity and jurisdictional acceptance for blockchain/DWeb evidence. Possibility of accidentally hosting illegal or unwanted content in a network in which a user is participating. Immutable records may not guarantee admissibility in court. | Users interested in verifying metadata, particularly those seeking accountability through legal mechanisms such as international or domestic courts. | <ul style="list-style-type: none"> This depends on the legal jurisdiction. Internationally, the ICC, ICJ, and ECHR, accepted some digital evidence, at others, the requirements to determine its veracity vary. At this stage, Save users should be advised that DWeb records do not ensure legal admissibility. When a URL could not be found (link rot), the ICC rejected digital evidence. Save offers provenance, rich metadata, and preservation, vs. proprietary platforms that disappear or remove content. Vetting actors in your network helps mitigate the possibility of future legal issues. |
| Long-Term Storage | | |

| | | |
|---|--|---|
| <ul style="list-style-type: none"> Risk of losing access to data if hosting peers or organizations disappear. | <p>Everyone, especially those interested in the long-term preservation of cultural heritage.</p> | <ul style="list-style-type: none"> Backup daemon node adds redundancy. Create a plan for secure data transfer if/when these risks occur. |
| Malicious Actors | | |
| <ul style="list-style-type: none"> Decentralized networks may be infiltrated by malicious actors who cannot easily be removed. Risk of attacks or deanonymization efforts. | <p>Users in high-surveillance environments whose networks may be penetrated by malicious actors.</p> | <ul style="list-style-type: none"> Two-person sign-off policy for onboarding new users. Strict vetting of network participants, good OPSEC policies. Secret URLs and QR codes reduce exposure risk. |
| Surveillance and Traffic Visibility | | |
| <ul style="list-style-type: none"> Veilid traffic from the Save DWeb backend is encrypted but recognizable as unusual by ISPs or government surveillance. Risk of flagging users in authoritarian regimes. | <p>Those in high-risk environments where network traffic is surveilled.</p> | <ul style="list-style-type: none"> Future plans for QUIC protocol integration. Possible addition of mesh networking for stealthier local sharing. Increasing the banal usage of Veilid will generate more overall network traffic, making at-risk users less vulnerable. |
| UX and Accessibility Concerns | | |
| <ul style="list-style-type: none"> DWeb protocols can be technically complex and confusing to casual users. May deter adoption by non-technical or at-risk users. | <p>Those without technical expertise or in very at-risk environments.</p> | <ul style="list-style-type: none"> Save simplifies onboarding with QR codes and an intuitive UI. UX research is ongoing to make decentralized storage user-friendly. Open-source development encourages community feedback and improvements. |

Figure 3: Potential Downstream Risks of DWeb Storage and Mitigation Strategies



III. Research → Practice, Assessing DWeb Storage for DACs

DWeb Storage Requirements for Decentralized Archivist Communities

Recognizing the potential of decentralized storage technologies for archivists, such as maintaining a chain of custody, ensuring verification, providing redundancy, and supporting long-term preservation, must also involve the recognition that this storage may be overly complex, nascent, glitchy, and/or have unintended malicious consequences. Shift Collective describes: “As technologies continue to evolve, community-based archives must engage with and inform the development of these ecosystems. If these organizations do not have input in the early stages of implementation and adoption, they may end up dependent on technological systems that at best are insufficient for, or worse, antagonistic to, their needs.”²²

OpenArchive identified the following conditions as requirements for a DWeb storage system that could be used by OpenArchive’s partner DACs:

- 1) No Single Point of Failure:** Avoiding reliance on a central server located on a single computer helps reduce potential threats and costs.
- 2) Direct Mobile Sharing:** Since most DACs use primarily (and sometimes only) mobile phones, it was important to allow for seamless file sharing between individuals—one user would be able to add a file, and another could upload it without needing a server in the cloud for online data storage. This also prevents the leakage of other users’ IP addresses.
- 3) Privacy and Encryption:** Privacy should be prioritized by avoiding the exposure of users’ IP addresses, which is common in many peer-to-peer (P2P) networks, risking exposure of the users’ relative location. Additionally, content in transit needed to be encrypted to protect against eavesdropping.
- 4) Good UX Design:** DWeb storage must make it easy for users with only basic technical knowledge to log in, search, and manage media. Projects that are difficult to interact with can deter potential users. One example, Civil Media Company, sought to use blockchain to reinvigorate trust in journalism, as well as to create a model for financial stability.²³ It was much maligned for its

²² Shift Collective. “[Modeling Sustainable Futures Proposing a Risk Assessment and Harm Reduction Model for Community-Based Archives Using Decentralized Digital Storage.](#)” December 2023.

²³ Bronwich, Jonah Engel. “[Alas, the Blockchain Won’t Save Journalism After All.](#)” *The New York Times*, November 1, 2018.

complexity and usability, both to understand its business model and to purchase the tokens themselves and ultimately was shut down in June 2020.²⁴

5) Secure, private storage: Because many DACs are at risk of censorship, malware, internet shutdowns, and other risks, DWeb storage must provide a high degree of security.

6) Open source: Aligning with the principles of the HRCD, the *DWeb Storage* should be open source, allowing for public accountability and access. As described in the HRCD, “This is because open source projects are transparent: their processes for how their technology is built are accessible to anyone interested, allowing for community input, and creating a kind of public audit which helps build trust.”²⁵

7) Authentication/authorization procedures: Decentralized tech is sometimes referred to as a ‘trustless technology’ because it eliminates the need to trust centralized authorities like proprietary platforms or other actors in the network. Instead, systems are secured and verified by cryptographic proofs, which provide integrity and protect against interference by malicious actors.

Additionally, Hypha Worker Cooperative and OpenArchive created a list of attributes that, while not strictly necessary, would be desirable for DWeb storage:

1) Media must be deletable: Ideally, DWeb storage users would be able to delete media from the storage. This would align with the GDPR’s Right to Forget.²⁶ Users have the right to some power over their data.

2) One-and-done connection to the backend: Ideally, only having to go through the connection process once would increase the usability of the app and decrease user frustration.

3) Verification of media authenticity: Finally, DWeb storage could allow for a secure ledger and chain of custody tracking that is encrypted. Chain of custody may also be beneficial in the legal admission of media. Users would, of course, need to research and be aware of requirements in their legal jurisdiction.

P2P Protocol Comparison

In order to meet OpenArchive’s list of essential criteria that surfaced through their co-research so that it can serve communities using **Save**, Hypha Worker Co-operative conducted a [comparative analysis of different DWeb Protocols](#). Criteria

²⁴ De, Nikhilesh. “[Media Startup Civil Shuts Down, Team Absorbed Into Decentralized ID Efforts at Consensys](#).” June 2, 2020.

²⁵ C., Natalie, and Caroline Sinders. “[Chapter 2. Working with a community](#).” In *Human Rights Centered Design*, 2022.

²⁶ GDPR. “[Article 17: Right to erasure \('right to be forgotten'\)](#).” Accessed September 12, 2025.

include usability, security, privacy, authentication, media authenticity, encryption and mobile compatibility. Deleting media and maintaining a persistent connection are considerable advantages. Usability is addressed through the sections on reliability and similar case studies, although these protocols generally emphasize technical affordances other than ease of use.

The protocols under consideration were [Arweave](#), [BitTorrent](#), [Filecoin](#), [Freenet](#), [Hyper/Pear](#), [I2P](#), [IPFS](#), [Iroh](#), [Peergos](#), [SocketSupply](#), [Source.Network](#), and [Veilid](#). With the above priorities established through community research, OpenArchive and Hypha chose two open source technologies, Veilid and Iroh, which, in combination, offer a powerful solution for a decentralized, peer-to-peer application.

By distilling the aforementioned criteria, the authors were able to examine current DWeb protocols that could integrate with mobile in order to determine which would best suit OpenArchive's stakeholders. The next section presents outcomes from a comparison of protocols based on their ability to provide: verification, privacy, anonymity, encryption, security, mutability, efficiency, flexibility, mobile compatibility, up-time, and peer-to-peer implementation.

Comparing P2P Protocols

| Protocol / Criteria | Arweave | BitTorrent | Filecoin | Freenet | Hyper / Pear | I2p | IPFS | Iroh | Peergos | Socket Supply | Source. Network | Veilid |
|---------------------------------|--------------------|------------|---------------|---------|--------------|-----------|----------------------------|-----------------------------|------------|-----------------------|-----------------|---------------|
| Open Source | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| User Authentication | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Media Verification Authenticity | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| Provenance/ History | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ |
| Encryption (at rest) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ |
| IP Address Privacy | ✗ (server) | ✗ | ✗ (server) | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ (server) | ✗ | ✗ (server) | ✓ |
| Free to Use (Cost) | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ |
| Mobile Compatibility | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Ability to Delete Media | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ? | ? | ✓ |
| Persistent Connection | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ? | ✓ | ✓ |
| Implementation Languages | Erlang, Javascript | C++ | Rust, Go, C++ | Rust | Javascript | C++, java | Go, Rust, Java, Javascript | Rust, Python, Swift, Kotlin | Java | Python, Rust, Node.js | Go | Rust, Flutter |
| P2P | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ |

Figure 4: P2P Protocol Comparison: A chart including available p2p protocols

Exploring the Chosen Protocols: Iroh and Veilid

With Veilid's focus on anonymity and encryption and Iroh's strength in managing content-addressed datasets, the [Save](#) backend can hopefully create efficient, secure,

and flexible systems tailored to mobile and multi-platform environments. Both these protocols are relatively new and thus have few existing implementations.²⁷ OpenArchive found no examples of projects similar to **Save** using Veilid/Iroh.

Veilid provides encrypted, anonymous peer-to-peer connections, where the only visible identifier is a 256-bit public key.²⁸ Even IP addresses remain concealed by routing connections between peers through several hops between random peers, making it one of the more secure protocols examined. Launched around January 2023, Veilid is still under active development and improvement, making it a dependable option for projects that require an open source, peer-to-peer, mobile-first framework for networked apps. OpenArchive did not use IPFS because it has limited IP privacy and is not designed for mobile. Additionally, IPFS may not be appropriate for applications that demand robust user authentication, privacy protections, or data deletion capabilities.²⁹

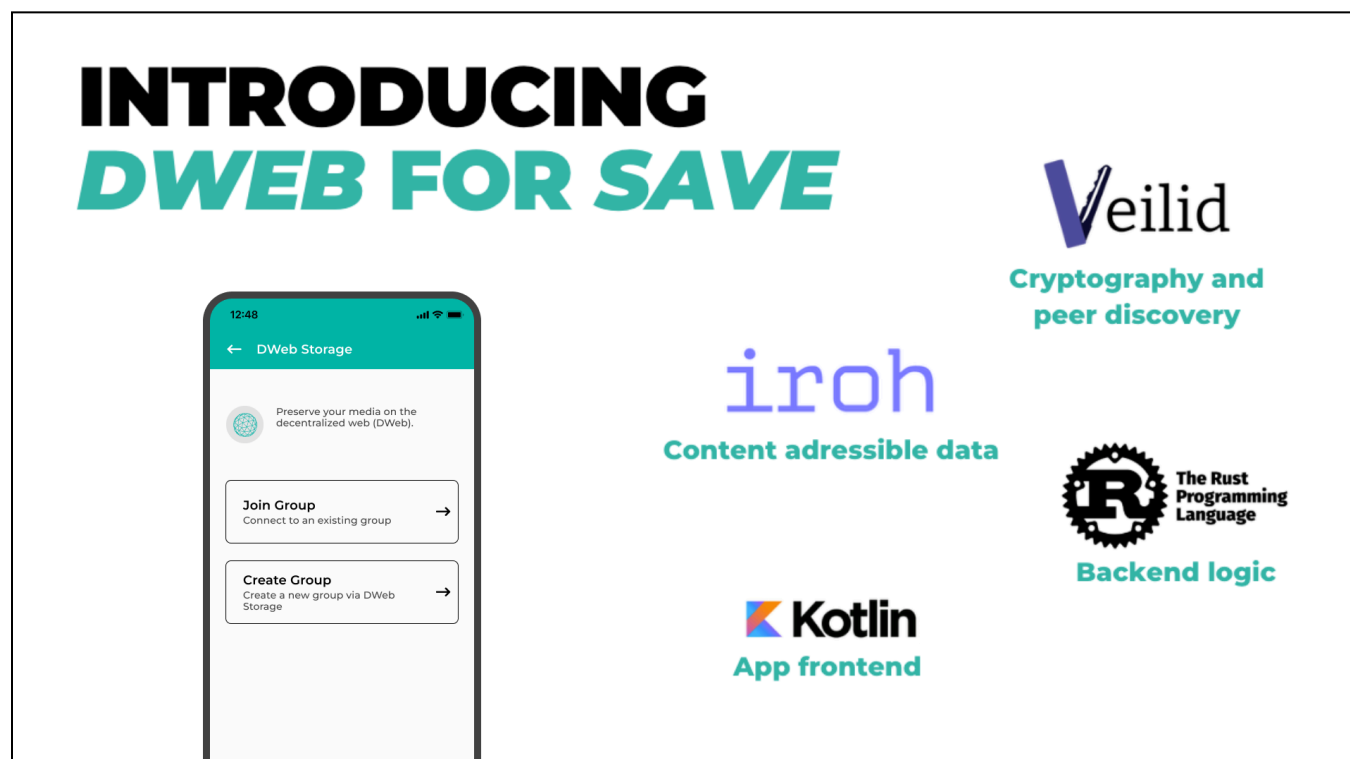


Figure 5: Introducing DWeb for **Save**, a schematic of the different layers in the app

Iroh specializes in managing large datasets that evolve. Unfortunately, it does not offer IP privacy. Still, it provides robust data storage features, making it a valuable tool for handling dynamic data collections. Iroh is actively maintained to prioritize reliability and performance. Rust-based projects can integrate Iroh crates (libraries) directly, reducing development time. Other programming languages can also access

²⁷ [VeilidChat](#), a chat application, is currently in active development. Iroh is being integrated in [Jumpy by Fish Folk](#).

²⁸ 256-bit public key encryption is a computational security system that uses two connected keys: one public key that anyone can see, and one private key that you keep secret. The keys are 256 bits long and work together — what gets locked with one key can only be unlocked with the other key.

²⁹ For more information, see the P2P Protocol Comparison document in the Appendix.

Rust code via a C-API, ensuring a streamlined development process. Rust can be easily implemented, making it especially relevant for **Save**, which needs to function across both iOS and Android.

DWeb Storage in **Save** is most useful for DACs who would like to join a trusted network but remain anonymous to one another. It is also useful for groups that do not want to use centralized cloud servers, which may expose their data to vulnerabilities like security failures and unavailability due to server takedowns, among other potential issues. This would require an institutional or organizational framework where new users can be vetted, and content can be managed in line with organizational aims (e.g., advocacy campaigns). An advantage of *DWeb Storage* for these organizations is that it can keep long-term storage costs down. With broad adoption, testing, and more funding, *DWeb Storage* has real promise to meet users where they are.

***DWeb Storage* Considerations**

While the authors chose to use Iroh and Veilid because they most closely meet DAC's needs, given that both are nascent technologies, it is critical to identify potential privacy and usability issues that could put users at risk in order to continue to refine and adapt future iterations of *DWeb Storage*.

***DWeb Storage* Privacy Considerations**

- **May not be inconspicuous:** Veilid traffic looks very unique to an internet service provider (ISP). ISPs may expose network traffic to government actors for surveillance purposes.³⁰ *DWeb Storage* makes use of custom DHTs (distributed hash tables) and TCP (Transmission Control Protocol)-encrypted data transmission, offering a certain kind of privacy; however, for an ISP undertaking packet analysis, Veilid traffic will be immediately detectable as something unusual, even if its actual interception may not be possible by these actors.
 - While *DWeb Storage* can't mitigate this problem, having more people use Veilid (and thus Veilid traffic), e.g., if it were incorporated into gaming platform messengers or similar messengers, would result in more 'mundane' traffic. In this situation, Veilid would be more ubiquitous and less noticeable to those conducting packet analysis.
- **Vulnerable to potential infiltration:** Malicious actors can remain shielded by the very security protocols designed to protect at-risk users, potentially gaining access. As such, secret group URLs should only be shared through encrypted messenger channels that are set to expire. A clear and strict process for adding new members is necessary to protect the integrity of the group.
 - How *DWeb Storage* addresses this: To access the *DWeb Storage*, a user creates a new group, which is stored only on their device and shared via

³⁰ Privacy International. "[The Global Surveillance Industry](#)." July 2016.

Veilid's DHT. This group has a unique URL, which contains secrets for how to find other members' data, such as their routes and latest file hash, and decrypt content. It is possible to share the URL with a disappearing message. Alternatively, you can allow someone to scan a QR code from your device, which will link directly to where they can set up an account and join. After joining, [they will be able to download other members' files or upload their own](#)³¹.

- In addition to technical security built into *DWeb Storage*, opsec is necessary to mitigate privacy vulnerabilities. Phones should be locked using a password instead of biometric authentication, protecting confiscated phones from being unlocked without the owner's consent. Users should exercise care when connecting to the internet to ensure secure access.

DWeb Storage Usability Considerations

- **Complexities of joining groups:** How to join a group posed a major usability challenge in the development of *DWeb Storage*. This is because of the decentralized, peer-to-peer nature of the app—to identify and verify a user account, a long, complicated URL must be entered, which could pose a difficulty for casual mobile users.
 - How *DWeb Storage* addresses this: To mitigate the complicated URL issue, Information can instead be shared via QR code, as was implemented in *DWeb Storage*.
- **Barriers to Accessibility and Adoption:** For many users, especially those unfamiliar with DWeb technologies, this *DWeb Storage* solution could be intimidating or confusing.
 - How *DWeb Storage* addresses this: Creating documentation and training materials along with the technology can help boost technological literacy so that DACs can make informed choices about their storage needs and the associated risks. Improving this literacy can also enhance trust in new onboarding methods, like QR code access, which may be unfamiliar to non-technical users.

While *DWeb Storage* presents some unique privacy and usability challenges, with the appropriate investment, it has the potential to help realize the initial vision of an internet by and for the people.

The next section provides a technical overview of the *DWeb Storage* implementation in **Save**, with a particular focus on the specific attributes of Veilid and Iroh. It also includes some opportunities and recommendations for enhancement, which could be accomplished with additional resources.

³¹ OpenArchive. "[Creating the First Decentralized Web Storage Backend for Mobile Media](#)." November 21, 2024.

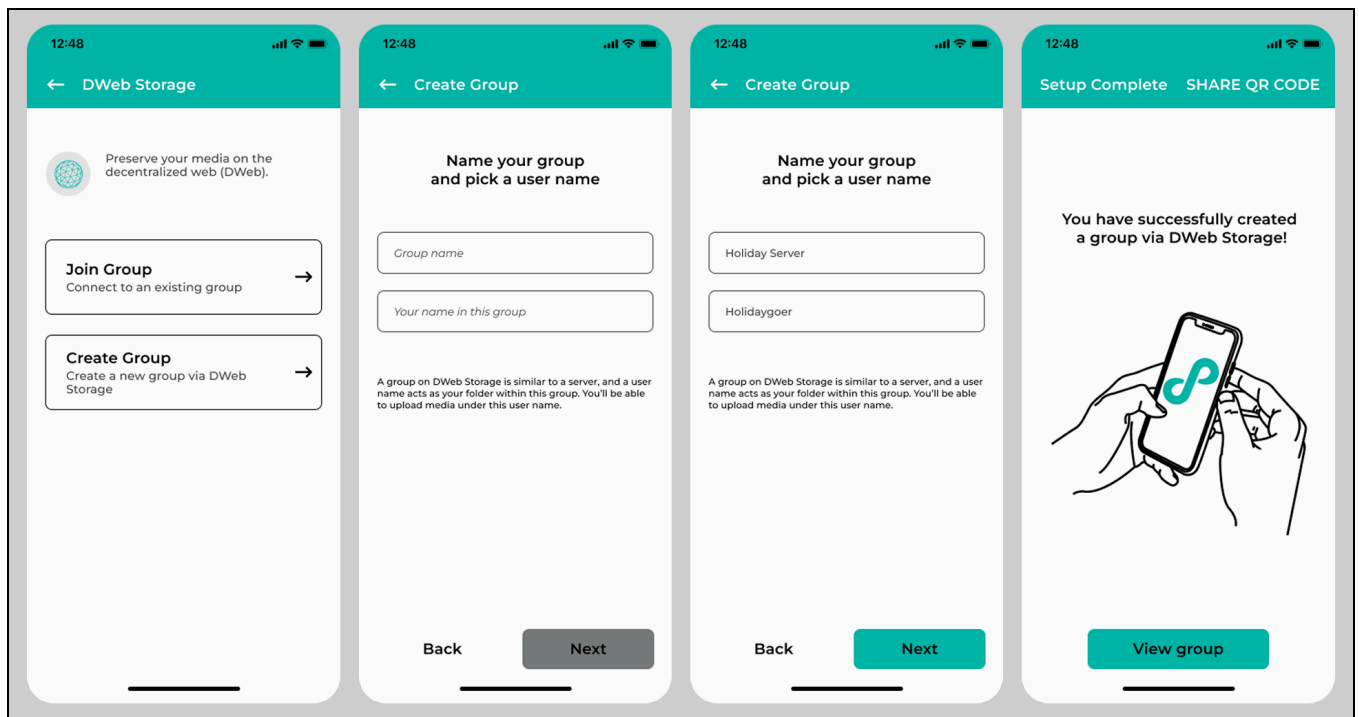


Figure 6: How to create a new group in the DWeb Storage Backend

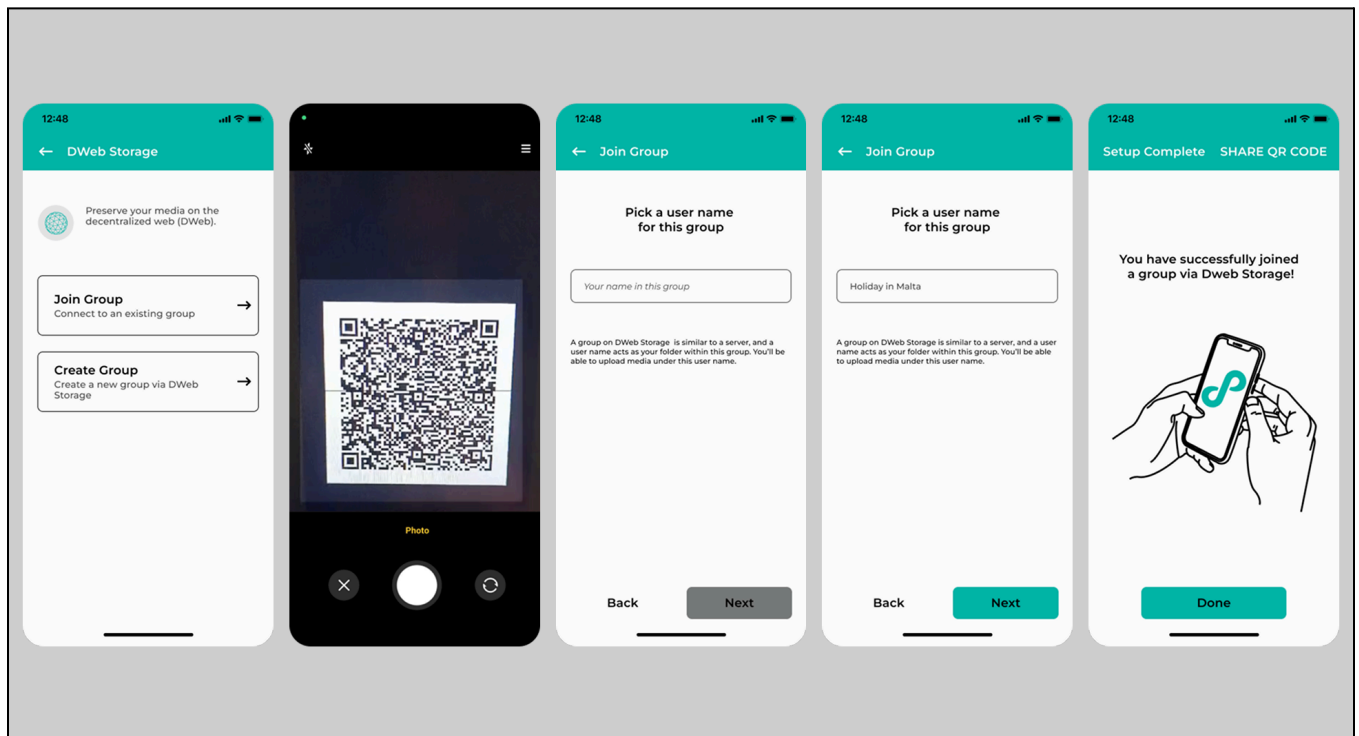


Figure 7: How to join an existing group via QR code

IV. Implementing Mobile-First *DWeb Storage*, A Novel Approach

Technical App Overview

Veilid serves as the cryptography and peer discovery component of the novel *DWeb Storage* backend. It enables private routing between peers and the discovery of small bits of data through its distributed hash table (DHT). However, Veilid lacked a mechanism for handling large data files, which is where Iroh came into play. Iroh is responsible for storing and validating files, while Veilid facilitates peer discovery and communication.

In combining Veilid and Iroh, the strengths of both protocols are harnessed, complementing each other's weaknesses. Since both are implemented in Rust, integrating them into a single process was possible and offered an efficient solution for decentralized applications. This approach encapsulates the peer-to-peer code into its own process, which can then communicate through an interface to any other code or language via Inter-Process Communication (IPC). This simplifies the deployment and makes integration with various languages, such as Swift and Kotlin, more straightforward.

All of this was encapsulated within a Rust-based backend API, which exposed its capabilities to Kotlin, acting as the app's frontend. The frontend manages user interaction and renders screens. Groups and data repositories are encrypted and stored on Veilid's DHT. Peers discover one another, exchange private messages, and validate data using Iroh. Once a peer acquires a copy of some data, they can make it available to other group members.

This interaction is hidden from the group through high-level APIs like `joinGroupFromURL` and `findFileFromGroup`, so it is seamless for *DWeb Storage*. This core backend can be used outside of the app as well. Additionally, a backup node or daemon was developed, which users can run as an always-online peer. This node can join groups and automatically downloads data as soon as it becomes available, ensuring group members can access the data even if no one else is online.

This interaction is hidden from the group through high-level APIs like `joinGroupFromURL` and `findFileFromGroup`, so it is seamless for *DWeb Storage*. This core backend can be used outside of the app as well. Additionally, a backup node or daemon was developed, which users can run as an always-online peer. This node can join groups and automatically downloads data as soon as it becomes available, ensuring group members can access the data even if no one else is online.

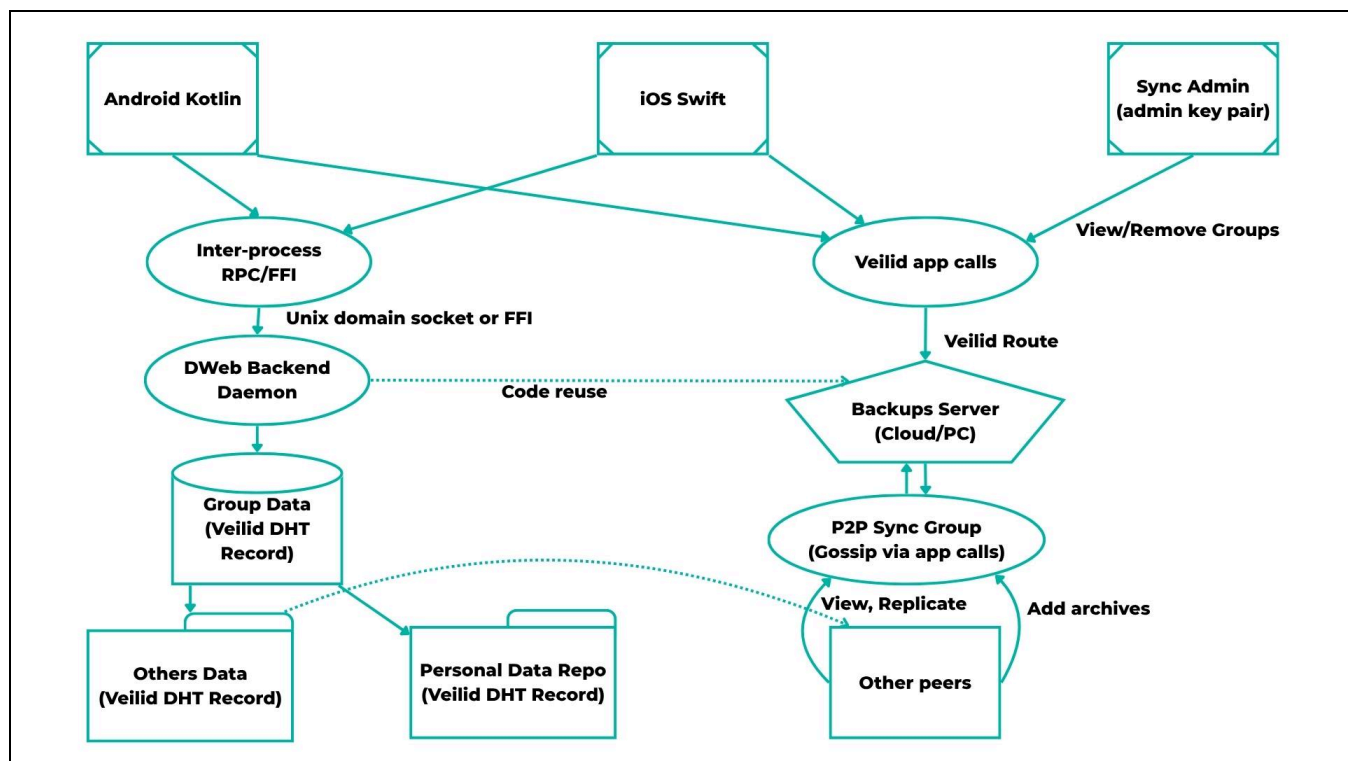


Figure 8: DWeb Storage Backend technical diagram — by the Hypha Worker Co-operative

DWeb Storage: Future Directions

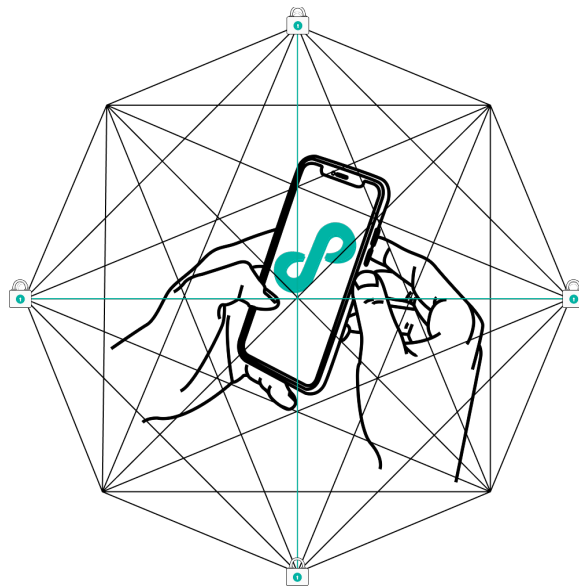
As mentioned above, there are many opportunities and challenges of the *DWeb Storage* solution OpenArchive has implemented. One challenge is that the DWeb backend in *Save* still depends on internet connectivity and doesn't work during shutdowns or splintering. As such, a pathway for further development for this type of resiliency might be integrating the ability to set up ad hoc mesh networks and to perform peer discovery and file transfers. This could result in both a new function within *Save* and a series of open source libraries for setting up hotspots on Android with little user interaction, reliable peer discovery over those interfaces, and P2P file transfer using Iroh over these local connections. This would make it easier to share data in small trusted groups and simplify building applications with similar capabilities. If successful, the code might also be repurposed for desktop, browser, and other environments.

In addition, a few protocol improvements could help to make local file sharing and mesh networking even better. Utilizing QUIC, a network transport protocol, might make Veilid traffic harder to identify, adding a layer of privacy during transfers. Also, instead of downloading a file from just one peer, the system could grab different chunks from multiple peers simultaneously. This would speed up downloads and make the process more resilient if some peers drop out. Together, these ideas would make P2P sharing in *Save*'s DWeb Backend faster, more private, and more robust in unreliable environments.

Meanwhile, the real-world demand and growing interest for resilient distributed storage systems without external controls or single points of failure grows faster than the usability and maturity of tooling of these networks.

As an intermediate measure, OpenArchive is currently exploring onboarding services that coordinate routing of content from mobile tools to a decentralized network — for instance, Storacha, a hot storage service³² that uses Filecoin to distribute content uploaded to its servers.

Long term, a solution for DACs should be a completely decentralized network, controlled and managed by its own users. Our research has shown that while this dream is not yet a reality, the desires of our archiving communities, and the emerging work in the DWeb show that, with a focus on usability, responsiveness to community needs, and the requisite funding, that possibility is tantalizingly near.



³² [Storacha Network](#) (website). Accessed September 12, 2025.

V. Conclusion

The paper outlines the urgent need for more secure ways to verify and preserve mobile media. It maps the research, design, and development methods that OpenArchive and Hypha Worker Cooperative used to create the novel *DWeb Backend* with privacy-first, p2p open-source technologies. This process surfaced the DAC's needs and tested assumptions about opportunities and challenges that the *DWeb Backend* poses. The ultimate goal of this work is to meet communities where they are and ensure the co-designed tools and resources are adapted to amplify benefits by harnessing opportunities while mitigating challenges and harm.

It included a technical overview and a comparison of usability and privacy tradeoffs between available DWeb protocols for mobile integration. From this comparison, the authors determined which *DWeb Storage* technologies best meet the DAC's criteria. It then did a deeper review of how and why the chosen protocols — Iroh and Veilid — were integrated into **Save**'s *DWeb Storage* and looked to the future of this approach.

OpenArchive and Hypha Worker Co-operative developed *DWeb Storage* to address key needs voiced by media archivists and documenters using mobile devices in certain contexts, where censorship, interception, media manipulation, and surveillance threaten mobile media archiving efforts. Though *DWeb Storage* may provide some benefits to these DACs, it is not yet suited to all use cases and should only be employed alongside intensive threat modeling and security analyses.

More broadly, decentralized technologies remain somewhat nascent, requiring more robust legal framework, usability research and improvements, as well as educational training initiatives before they should be widely adopted. As described by Walid Al-Saqaf & Nicolas Seidler, who write on blockchain, though some parallels remain:

Often portrayed as a 'trustless' technology, blockchains actually shifts [sic] the trust from intermediaries to code and coders. The technology is also not immune to governments stepping in to regulate its use, or to big companies turning the technology into centralized commercial services, potentially raising risks for expression and privacy. Some of the most radical and creative applications of blockchain technology, such as those related to eliminating a large set of intermediaries, would require a change of mindset that goes beyond a simple technological shift and requires long-term commitments to equip future generations with the knowledge and skills needed to remain relevant in what will be an increasingly automated future.³³

This paper highlights both the potential and limitations of implementing *DWeb Storage* with DACs. Advancing this work will require ongoing research, testing, and community engagement along with sustained funding to ensure these tools strengthen resilience, privacy, and autonomy in practice.

³³ Al-Saqaf, Walid, and Nicolas Seidler. "[Blockchain technology for social impact: opportunities and challenges ahead](#)." *Journal of Cyber Policy* 2 (3), November 11, 2017.

Bibliography

- Al-Saqaf, Walid, and Nicolas Seidler. "[Blockchain technology for social impact: opportunities and challenges ahead.](#)" *Journal of Cyber Policy* 2 (3), 2017.
- BlackDuck. "[What is threat modeling?](#)" Accessed September 12, 2025.
- Bronwich, Jonah Engel. "[Alas, the Blockchain Won't Save Journalism After All.](#)" *The New York Times*, November 1, 2018.
- C., Natalie, and Caroline Sinders. "[Chapter 2. Working with a community.](#)" *In Human Rights Centered Design*, 2022.
- C., Natalie, and Sinders, Caroline. "[Human Rights Centered Design Methodology.](#)" 2022.
- Creative Switch. "[Donna Stays with the Trouble.](#)" *Republic of Creative Uncertainty*. Accessed May 6, 2025.
- De, Nikhilesh. "[Media Startup Civil Shuts Down, Team Absorbed Into Decentralized ID Efforts at Consensys.](#)" June 2, 2020.
- Dixon, Chris. "Read Write Own: Building the Next Era of the Internet". *Random House*, 2024.
- [DWeb](#) (website). Accessed September 2025.
- Faller, Patrick. "[Putting Personas to Work in UX Design: What They Are and Why They're Important.](#)" *Adobe Creative Cloud*, December 17, 2019.
- GDPR. "[Article 17: Right to erasure \('right to be forgotten'\).](#)" Accessed September 12, 2025.
- Gibbs, Samuel. "[Child Abuse Imagery Found within Bitcoin's Blockchain.](#)" *The Guardian*, March 20, 2018.
- Gillett, Matthew, and Wallace Fan. "[Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom.](#)" *Journal of International Criminal Justice* 21 (4), September 2023.
- Gregory, Sam in Thompson, Caitlin. "[Can the decentralized web help to protect human rights?](#)" *CodaStory*, November 17, 2021.
- Haraway, Donna J. "[Staying with the Trouble: Making Kin in the Chthulucene.](#)" *Duke University Press*, 2016.
- Hellstern, R., D. C. Park, V. Lemieux, et al. "[Leveraging Blockchain-Based Archival Solutions for Sensitive Documentation: a Xinjiang Case Study.](#)" *DISO* 1 (4), July 18, 2022.

Hui, Mary. "[Hong Kongers Use Blockchain to Fight Government Censorship.](#)" *Quartz*, May 26, 2021.

Jacobs, Ian. "[Architecture of the World Wide Web 1.0. Editor's Draft 28.](#)" W3C, November 2003.

Keefe, John. "[How to Buy into Journalism's Blockchain Future in Only 44 Steps.](#)" Nieman Lab, September 19, 2018.

Mastodon. "[Mastodon Documentation.](#)" Accessed September 12, 2025.

OpenArchive. "[Creating the First Decentralized Web Storage Backend for Mobile Media.](#)" November 21, 2024.

OpenArchive. "[Mapping the Decentralized Storage Ecosystem.](#)" February 13, 2024.

Privacy International. "[The Global Surveillance Industry.](#)" July 2016.

[SaveMyIdentity](#) (website). Accessed September 12, 2025.

Shift Collective. "[Modeling Sustainable Futures Proposing a Risk Assessment and Harm Reduction Model for Community-Based Archives Using Decentralized Digital Storage.](#)" December 2023.

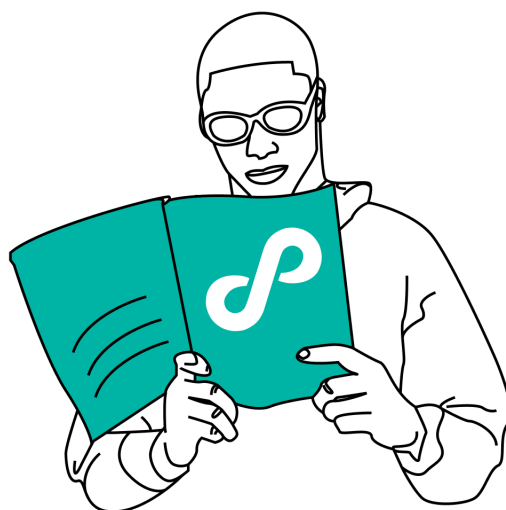
Silberling, Amanda. "[A beginner's guide to Mastodon, the open source Twitter alternative.](#)" *TechCrunch*, Jul 24, 2023.

Storacha Network. <https://storacha.network>. Accessed September 12, 2025.

TechSoup, "[DWeb Use Cases for Civil Society.](#)" November 27, 2023.

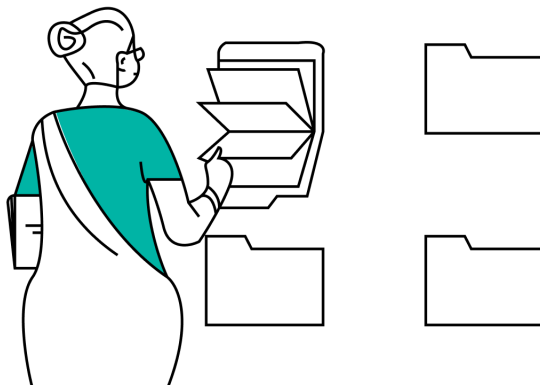
Ushahidi, "[The Transformative Power of Open-Source Technologies and Decentralized Web Storage.](#)" July 25, 2024.

Villasenor, John. "[Artificial intelligence, deepfakes, and the uncertain future of truth.](#)" *Brookings*, February 14, 2019.



Appendix

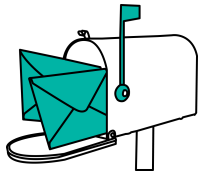
- [DWeb Backend Privacy Overview](#)
- [P2P Protocol Review](#)
- [Glossary](#)
- [DWeb Resources](#)



Acknowledgements

OpenArchive is grateful for the contributions from the Hypha Worker Co-operative and support from the Filecoin Foundation for the Decentralized Web (FFDW).

This paper would not have come to fruition without the many engaged collaborators across the DWeb and archival spaces, including interlocutors at Splintercon 2024, the Association of Moving Image Archivists (AMIA) Conference, and Global Gathering 2024. The OpenArchive team is also grateful to the [Rohingya Project](#), [SaveMyIdentity](#), and [Coalición por Venezuela](#) for their ongoing dialogues in the DWeb space.



Contact us:

OpenArchive: community@open-archive.org

Hypha Worker Co-operative: hello@hypha.coop

