Identifi-NZ

Decentralised Digital Identity

Matthew Hill

Table of Contents

Scope

The initial scope of my project was to create a prototype for a decentralised digital identity system, that focuses on the uploading and storage of identity documents in a decentralised manner. Upon reviewing surrounding literature I found that a common theme between sources indicating that lack of trust and transparency were a key concern amongst identity services. In my research I also found multiple authors providing convincing arguments for alternative means of identification, particularly biometric data. Researchers claim that these means of identification support equal opportunity to services for persons without formal documentation common in the developing world or amongst asylum seekers (Beduschi, 2019).

When developing my application, I opted for utilising the decentralised hypermedia protocol IPFS (*IPFS Powers the Distributed Web*, n.d.) to store users identity information. While this reflects the values quoted in literature, a key limitation with this approach is that it relies on IPFS's content ID's acting in a similar way to an unlisted YouTube video. If a user has the content ID of a particular item, they will be able to view and access it. While this does provide some privacy a consequence is that there is no way to revoke viewing permissions.

The avenue of biometric data is one that is certainly worth exploring, however, fell outside the scope of this initial research. In a system which reads and stores biometric data the approach of privacy via obscurity from IPFS's content ID system is likely not a strong enough guarantee, and encoding the data in a truly private manner would be a requirement for such a system.

Literature Review

Introduction

As modern life becomes ever more intertwined with digital technology, there is an increasing need for the verification of digital identity (Schneider et al., 2020). Most attempts at creating digital identification are based on traditional infrastructure being ported to the digital space such as government agencies offering their services online (Sánchez-Torres & Miles, 2017).

This literature review aims to highlight some of the problems created by these structures and focuses on how digital native solutions such as decentralized digital identifiers can be used to solve the problem of digital identification. It begins by addressing the matters of authentication and authorization of users, then demonstrates the importance of privacy and censorship resilience for matters of digital identification. From there, it explores how decentralization can be utilized to address key pain points in traditional identification systems. Finally, it demonstrates how self-sovereign identity principles can be utilized to create more equitable systems for all.

The final output of this work aims to create a solution to digital identity which is not reliant on large entities like governments or certification agencies and as such is more resilient to censorship and security breaches, has a greater degree of privacy, permits the verification of data without information disclosure by utilizing zero-knowledge proofs and allows equal access to the verification of legal identity.

Definition of Key Terms

Anti-Pattern – A commonly occurring solution to a problem that is either ineffective or yields considerable downsides.

Blockchain – A list of transactions collected in blocks that are securely linked together using cryptography.

Decentralization – The process of distributing responsibilities away from a central entity.

Reverse Turing Test – A Turing test in which the objective or roles of computers and humans has been switched such as a computer verifying if the subject is a human.

Self-Sovereign Identity – An approach that gives individuals control of their identities.

Web of Trust – A method of establishing authenticity which utilizes direct and indirect trust to create a decentralized web of confidence.

Zero-Knowledge Proof – A cryptographic technique that allows one party to prove to another that a statement is true without disclosing any additional information.

Authentication and Authorization

At the heart of all identification solutions, whether physical or digital is a need to authenticate users, and provide authorization to restricted materials. These restricted materials come in many different shapes and forms with differing degrees of information disclosure associated. Many use cases are very clear such as age verification for purchasing alcohol, but the well-known anti-pattern of the password is also an example of authentication.

The prevalence of passwords as the de facto authentication system of digital technologies is a massive security risk (Bonneau et al., 2015), and attempts made at increasing security even at the expense of user experience often do more harm than good. An example of such is the forced usage of special characters resulting in users creating shorter passwords to deal with the cognitive load of adding said characters. This in turn results in a password with less entropy as the length of the password dominates the size of the pool of characters used, as seen in the password entropy formula below.

$$E = \log_2 N^L = L \log_2 N = L \frac{\log N}{\log 2} \quad (1)$$

where N is the size of the pool of unique characters which we construct passwords from and L is the length of the password.
E is the entropy of the password measured in bits.

Other attempts to remedy problems with passwords have been met with varying degrees of success, such as OAuth2 and password managers such as LastPass, Dashlane, and Keeper. Recent studies conducted by Alodhyani et al (2020) found that low levels of adoption for password managers do not seem related to user experience. Upon performing a heuristic evaluation using Nielson's (1994) method, although some problems were found such as the use of jargon and the ability to enter incorrect data, they report that usability is not a major problem. Instead, they suggest that issues surrounding trust and transparency are the primary cause of a lack of adoption (Alodhyani et al., 2020). This reinforces my views that solutions for digital identity should, be trust-less, decentralized, and transparent which indicates that decentralized ledger based solutions are a potential fit for this problem.

Whilst single sign-on is often thought of as an improvement in security, it is not without significant drawbacks. OAuth2 is one of the most widely used authorization frameworks and is used by many industry-leading platforms such as Google, Microsoft, and Facebook (Siriwardena, 2020). These models hold both risks of theft of the authentication data stored by identity providers, as well as considerable privacy concerns, as agencies that provide identity services can track user activity (Mir et al., 2022). This is particularly concerning when used in combination with Online Advertising platforms such as Google's AdSense, as large amounts of incredibly accurate data could be harvested from users of said systems without their consent (Cucchietti et al., 2022).

Centralization and Decentralization

The centralization of these systems draws parallels to traditional infrastructure, with government agencies dispensing documents such as passports, birth certificates, and driver's licenses which act as master identity documents in the physical world. We even see many government agencies simply porting that traditional infrastructure to digital means, the New Zealand government's RealMe (*RealMe*, n.d.) is an example of this.

Current identity systems are typically built around hierarchical trust, in which sets of certification authorities such as governments or other corporate entities are declared as trustworthy and hold a great deal of power in said systems. This assumption of universal trustworthiness is itself at the heart of the problem (Goodell & Aste, 2019), as even if such an entity were ethically infallible major security breaches surrounding certification authorities, have proven time and time again that a singular point of trust can easily lead to a singular point of failure.

A distributed ledger based solution can be used to eliminate the need for a trusted third-party entity and reduces the risks of singular points of failure (Ismail et al., 2019), greatly reducing the impact of security breaches or malicious actors. However, a distributed ledger requires significant privacy measures to be introduced along with it as the transparency and immutability of the data contained within proposes a major ethical problem if not addressed (Dunphy & Petitcolas, 2018).

Privacy and Censorship Resilience

In the age of free software, where user data is often harvested and resold without consent, it is no wonder that privacy is of utmost concern when it comes to matters of digital identification. This is particularly concerning to LGBT human rights. As of 2018, more than 70 countries still criminalize same-sex consensual sexual activity (Shaw, 2018). Even in New Zealand, the recent mandatory usage of My Vaccine Pass has highlighted the importance that transgender people are considered whenever matters of legal name and identity are at hand. As many people may not have updated their legal names and the act of providing identification documents could disclose people as transgender and potentially put them at risk of discrimination (Earley, 2021).

One of the consequences of digital identification is that any time information is disclosed it can be recorded which is in stark contrast to physical interactions. When providing documents in physical places there is implied privacy in the transaction, as it would be unreasonable to assume that the verifier can memorize all the information provided, as well as the information of all other users (Windley, 2021). Therefore particular care must be taken to ensure that no additional information is disclosed when verifying a user's credentials.

One particularly promising technology which can be utilized to enhance the privacy of users is zero-knowledge proofs. Researchers propose a solution that utilizes zero-knowledge proofs to verify identity claims built on top of a blockchain. This simultaneously addresses the concerns of centralization and privacy (Yang & Li, 2020).

Self-Sovereign Identity

The concept of self-sovereign identity is prevalent throughout the digital identity sphere, as the internet itself is a shining example of the benefits of decentralization, even though that very decentralization is being threatened today. The previously discussed anti-pattern of the password is also an excellent example of what it means to have self-sovereign identification in the digital space, and blockchain addresses are an even further extension of those principles.

Self-sovereignty is a particularly powerful tool for leveling the playing field and offering equal opportunity for identity verification. Ana Beduschi's (2019) work provides a strong case for systems that are not reliant on traditional documentation such as birth certificates and passports. Their work highlights that a lack of formal documentation, which is common in the developing world or amongst asylum seekers, compromises an individual's human rights to equal treatment due to the difficulties faced with access to identity verification.

Digital solutions have a unique position in that they can readily leverage developments in biometric data such as fingerprints and iris scans. By utilizing these innate methods of identification rather than constructed ones like birth certificates, an identity solution would facilitate an equal opportunity to services such as banks or education which individuals without formal documentation would not typically be allowed access to (Beduschi, 2019).

A related project, Proof of Humanity (*Proof Of Humanity*, n.d.), uses a similar approach for managing digital identities. It acts by combining webs of trust and reverse Turing tests to create a list of verified humans. However, their usage of video footage to verify identity is problematic due to Deepfakes, synthetic media which uses machine learning to replace a person's likeness. Deepfakes are typically created via the use of generative adversarial networks, a type of neural network in which two neural networks are trained simultaneously, one network is a generative model which synthesizes new content, while the other is a discriminator which deduces whether the new content is fabricated or not (Goodfellow et al., 2014). This method of training models ensures that both the creation and detection of faked materials will always be roughly equivalent, therefore creating an arms race of computing power between those trying to mediate and those trying to fake access to the system.

Conclusion

This review demonstrates the issues with typical identity verification structures and the lack of transparency of these systems. This lack of transparency also brings up considerable ethical concerns, particularly surrounding the centralization of the system, as breaches of such a system would result in drastically increased damages if the primary account is compromised.

Though some projects seek to use decentralization to help remedy these issues, none have seen wide-scale adoption. Some key areas still requiring additional research are how to construct a protocol of decentralized identity which does not rely on falsifiable data such as video footage, and is it enough to rely solely on a web of trust or is some additional manner of authentication necessary. Additionally, more research is required surrounding the social acceptability of both users, and of platforms that rely on current identity frameworks.

My research aims to create a platform that allows methods of identification, authentication, and authorization, without the reliance on centralized authorities such as governments. The nature of this work requires a dual approach, as the technical aspects of the system need to be explored in a proof of concept, followed by quantitative research to analyze the performance of the system. In particular, I would investigate how adding a decay function to the web of trust might be able to increase the level of trustworthiness, at the potential risk of disconnecting the underlying graph.

However, being so closely tied to social issues, an important part of the proposition would be to gather information via surveys to better understand user and business expectations and hesitations surrounding the decentralization of digital identification.

Prototype

The produced high-fidelity prototype is a functional mobile application developed for android devices using the Kotlin programming language. It utilises a RESTful API to communicate with an IPFS gateway which stores the identity information of users.

To accompany the mobile prototype, the Pinata service (*Pinata | Your Home for NFT Media*, n.d.) has been used to host and distribute the IPFS content, as well as to host a Gateway to the content for faster content retrieval. However, due to limitations surrounding Pinata Gateway's being read-only, the process of uploading Identity Fragments ends with access being denied. This issue can be fixed by hosting an independent gateway, however due to server costs and time constraints, this fell outside the scope of this initial prototype.

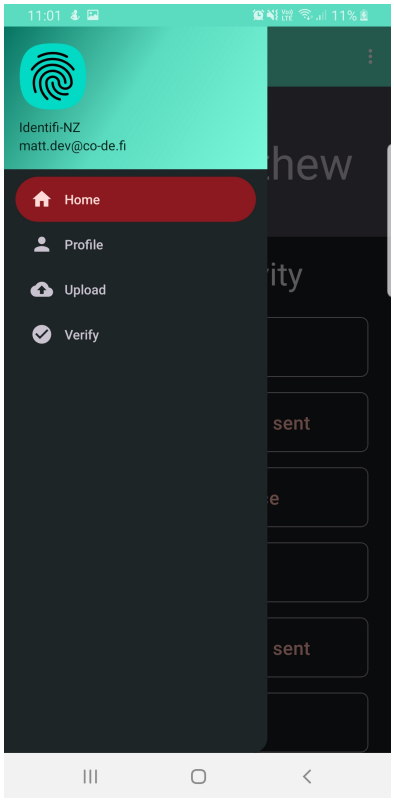

Figure 2: All screens contain a top navigation bar which opens the navigation drawer. Within the navigation drawer users can see their current location and select new screens to visit.

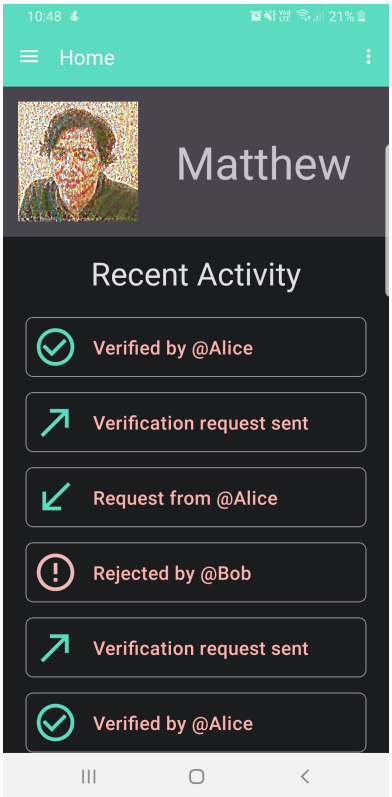

Figure 3: The home screen displays the currently logged in user, as well as querying IPFS to find all the users recent activity and populating the view.

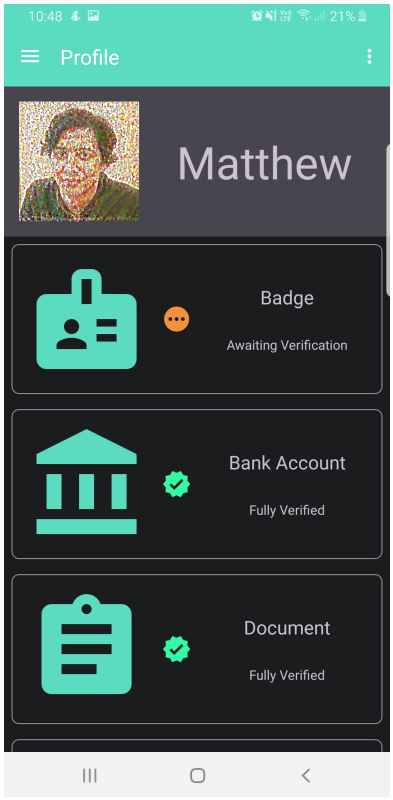

Figure 1: The profile screen also displays the currently logged in user, and queries IPFS to find and display all the users stored Identity Fragments.

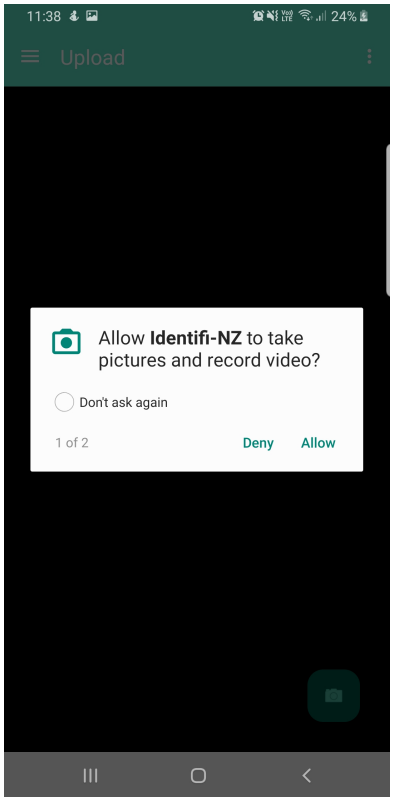

Figure 4: Upon visiting the Upload screen for the first time, the application requests permission to access the camera.

Figure 5: The upload screen consists of a viewport of the camera, and a floating button to take a picture.

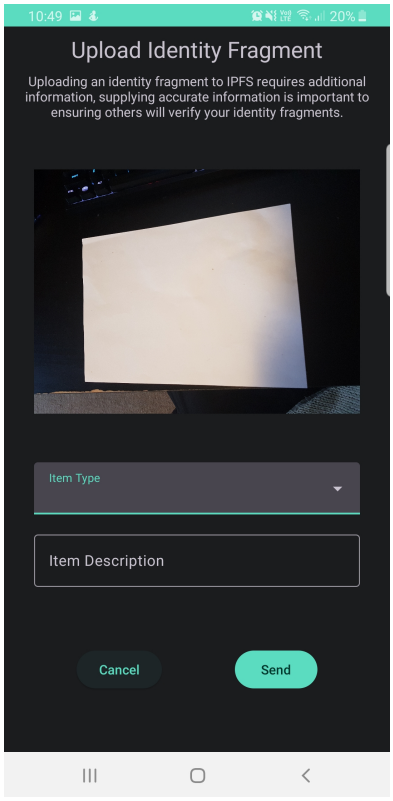

Figure 6: After taking a picture, a dialog appears which asks a user to input additional information about the new identity fragment.

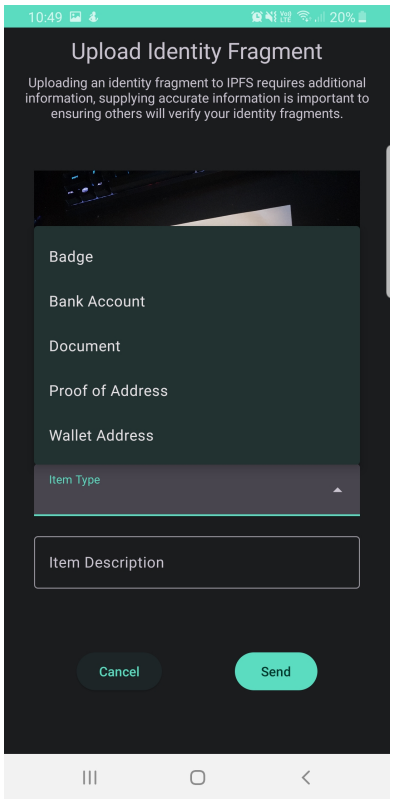

Figure 7: A user selects the type of Identity Fragment from a dropdown box.

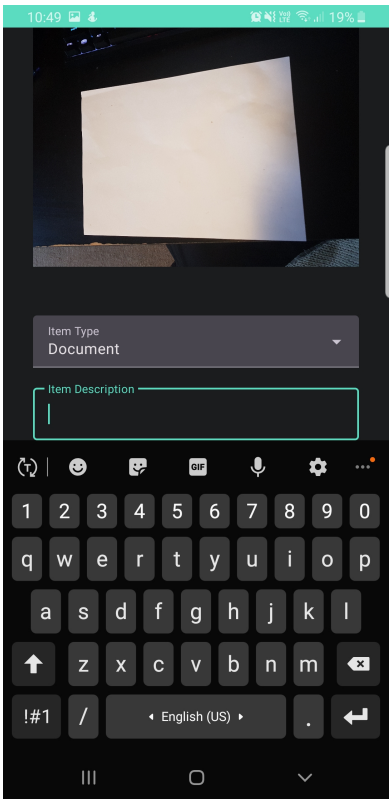

Figure 8: A user inputs a description of the Identity Fragment.

Context of Innovation

My project lies firmly in the field of decentralised digital identity, and self-sovereign identity. The major innovation which I am making is by allowing users to verify the credentials of other users which they know personally and then utilising indirect trust to create a decentralised web-of-trust. This approach is similar to that of PGP encryption (Stallings, c1995), and with enough usage will provide strong guarantees that identities produced through this manner are trustworthy, providing the number of indirect links is somewhat low.

A potential way to increase the level of trust of the overall system is to introduce a decay function, whereby each level of indirect trust reduces the certainty that an identity is legitimate by a set amount. This decay would likely increase exponentially, so that two or three levels of indirect trust has a very high certainty but five or six should not. This approach will likely cause the underlying graph to become disconnect, which draws parallels to federated systems such as in Mastodon (*Mastodon*, n.d.). Federated systems such as Mastodon have proven that, when communities are given appropriate tools they are able to self-govern effectively (Derek Caelin, 2020). This however does raises some ethical consideration, as allowing moderators and administrators access to real power within the system could result in similar defederation situations arising as in Mastodon's defederation of Gab (Mahmoudi et al., 2022). The consequences of defederation for isolated communities could severely restrict their access to identity services, constituting in a denial of their human rights. As such these concepts lie outside the scope of this research.

Prototype Decentralisation

Identifi-NZ is a platform which leverages decentralised storage to manage identity information. By using a decentralised means of storing these identity fragments it is able to guarantee that uploaded documents will remain available and will be unable to be tampered with.

A further aspect of decentralisation which is in development is the inclusion of a verification network which allows users to request others to verify identity fragments such as documents, photographs, or even biometric data. The goal of including these peer-to-peer verifications is that over time as users verify documents for each other they will accumulate trusted links between themselves and other users. This accumulation of trusted links cause the emergence of a decentralised web-of-trust, whereby it is expected that users should be able to authenticate one another through indirect trust.

As the system includes other means of identification such as biometric data it will become less reliant on artifacts created by governments or other centralised entities. In addition, through the usage of zero-knowledge proofs users will be able to authenticate their identities without any additional disclosure of information. This provides users with strong privacy and censorship resistance which would not be achievable in a traditional centralised system.

Legislative and Regulatory framework

Current New Zealand legislation (Electronic Identity Verification Act 2012) dictates that electronic identity credential systems may contain information surrounding an individuals name, sex, date of birth and place of birth. Additionally, the act supports identity photographs in the context of issuing identification documents and for comparison in the verification process. The explicit listing of what is allowed to be stored by an identity system could mean that allowing users may need to be restricted in what they can store as Identity Fragments with current law.

However, a new Digital Identity bill (Digital Identity Services Trust Framework Bill (78-2)) which is currently in it's second reading (*Digital Identity Services Trust Framework Bill - New Zealand Parliament*, n.d.) could mark significant changes to the current digital identity landscape. The bill itself is mainly focused on the creation of the board and not on the details of the regulations it means to introduce, however, it does seem to be somewhat aligned with the values presented in this project. The bill aims to "to give people more control over their information, to support people to prove who they are online, and to make it easier to access online services" with the expectation that "service providers would include government departments, existing identity service providers and private sector organisations" (Digital Identity Services Trust Framework Bill (78-2)).

In relation to biometric data, New Zealand does have precedent for using biometric data for identification (*Immigration New Zealand*, n.d.). Immigration New Zealand collects photographs and fingerprints to identify and check the identities of migrants and refugees (The Immigration Act 2009). Additionally, they claim to use DNA sampling in certain circumstances. While these methods are not seen in current identity systems, the increased access to necessary tools such as fingerprint scanners being present on many modern phones could see such methods being more commonly used in the future.

Research Proposal Poster

DECENTRALISED DIGITAL IDENTITY

Research Aims and Objectives

Investigate the cultural and political implications surrounding the decentralization of identity platforms.

Explore the technical requirements and feasability of decentralised identity solutions.

Research Topic

This study will investigate how decentralization can be used to improve digital identification solutions. We will investigate how decentralisation addresses the privacy, censorship, and equitability of digital identification platforms.

Perform critical analysis of existing solutions which is informed by supporting literature.

Identify the advantages and disadvantages that come with utilizing a decentralized model.

Investigate social acceptability of decentralized identity models and self-sovereign identity.

Design and create a prototype mobile application informed by the cultural and political environment.

Evaluate the efficacy of the prototype in relation to both technical and cultural perspectives.

Methodology

Research through Design
Critical Making

HOW CAN THE CONCEPT OF DECENTRALISATION BE APPLIED TO IDENTIFICATION SOLUTIONS TO IMPROVE PRIVACY, CENSORSHIP RESILIENCE AND EQUITABILITY?

Research Methods

Literature Review	Understand the wider environment which this research lies within.
Surveys	Gather qualitative information about social acceptability of digital identity.
Thematic Analysis	Analyse qualitative data gathered from surveys and construct themes which reflect the data.
Prototyping	Create both low and high fidelity prototypes in the forms of click through wire frames and a mobile application.
User Testing	Gather feedback from users and utilize feedback to improve the system iteratively.

Research Outputs

Research portfolio

Click-through wireframes

A proof-of-concept mobile application

MATTHEW HILL

Meakonxd (n.d). science-and-technology-high-tech-earth. Canva. https://media-public.canva.com/dxeng/MAE1OCdxeng/1/tl.png

Emiltimplaru (n.d). Finger Print Vector Illustration. Canva. https://media-public.canva.com/ze6Vo/MAEWkTze6Vo/1/tl.png

Sketchify (n.d). Glitch Background Illustration. Canva. https://media-public.canva.com/v9C9o/MAEQl3v9C9o/1/tl.png

Future Research

As the verification of other users documents would require an additional layer of integration with a blockchain with both strong privacy guarantees and smart contracts, this functionality falls outside the scope of the project. It does however highlight important areas of future development in the blockchain ecosystem, as while privacy chains have seen some degrees of interest in the past, there seems to be far fewer projects trying to enact these sorts of visions.

Two important areas of future development would be to expand the project to include biometric data, and the implementation of zero-knowledge proofs. By allowing users to upload data not granted by centralised entities the system becomes more equitable, especially for those in situations where formal documentation is difficult to obtain. The usage of zero-knowledge proofs also greatly increase the privacy guarantees of documents contained within the system.

One team which is working in a similar space is Proof of Humanity, who aim to create a Universal Basic Income token, which is handed out to all verified users on there system. While they do acknowledge that their sybil resistance methods are susceptible to deepfakes, they dismiss that they are a real threat to the system due to them being not entirely convincing. This viewpoint is obviously problematic as advances in deep learning in the recent past has been incredibly rapid, and the lack of proper response to such a problem casts doubt over an otherwise promising protocol.

References

Alodhyani, F., Theodorakopoulos, G., & Reinecke, P. (2020). Password Managers—It's All about Trust and Transparency. *Future Internet*, *12*(11), 189. https://doi.org/10.3390/fi12110189

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, *6*(2), 2053951719855091. https://doi.org/10.1177/2053951719855091

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. *Communications of the ACM*, *58*(7), 78–87. https://doi.org/10.1145/2699390

Cucchietti, F., Moll, J., Esteban, M., Reyes, P., & García Calatrava, C. (2022). *_carbolytics, an analysis of the carbon costs of online tracking.* http://carbolytics.org/report.html

Derek Caelin. (2020, September 27). *Decentralized Social Networks vs the Trolls*. https://www.youtube.com/watch?v=yZoASOyfvGQ

Digital Identity Services Trust Framework Bill—New Zealand Parliament. (n.d.). Retrieved June 3, 2022, from https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/BILL_116015/digital-identity-services-trust-framework-bill

Digital Identity Services Trust Framework Bill (78-2)

Dunphy, P., & Petitcolas, F. A. P. (2018). A First Look at Identity Management Schemes on the Blockchain. *IEEE Security & Privacy*, *16*(4), 20–29. https://doi.org/10.1109/MSP.2018.3111247

Earley, M. (2021, November 22). *Covid-19: Concerns raised over "deadnaming" on vaccine passes*. Stuff. https://www.stuff.co.nz/national/health/coronavirus/127046939/covid19-concerns-raised-over-deadnaming-on-vaccine-passes

Electronic Identity Verification Act 2012

Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. *Frontiers in Blockchain*, *2*, 17. https://doi.org/10.3389/fbloc.2019.00017

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative Adversarial Nets. *Advances in Neural Information Processing Systems*, *27*.

https://proceedings.neurips.cc/paper/2014/hash/5ca3e9b122f61f8f06494c97b1afccf3-Abstract.html

Immigration New Zealand. (n.d.). Immigration New Zealand. Retrieved June 3, 2022, from https://www.immigration.govt.nz/about-us/policy-and-law/identity-information-management/how-biometric-information-is-used

IPFS Powers the Distributed Web. (n.d.). Retrieved June 2, 2022, from https://ipfs.io/

Ismail, L., Materwala, H., & Zeadally, S. (2019). Lightweight Blockchain for Healthcare. *IEEE Access*, *7*, 149935–149951. https://doi.org/10.1109/ACCESS.2019.2947613

Mahmoudi, H., Allen, M. H., & Seaman, K. (Eds.). (2022). *Fundamental Challenges to Global Peace and Security: The Future of Humanity*. Springer International Publishing. https://doi.org/10.1007/978-3-030-79072-1

Mastodon. (n.d.). Retrieved June 2, 2022, from https://joinmastodon.org/

Mir, O., Roland, M., & Mayrhofer, R. (2022). Decentralized, Privacy-Preserving, Single Sign-On. *Security and Communication Networks*, *2022*, 1–18. https://doi.org/10.1155/2022/9983995

Pinata | Your Home for NFT Media. (n.d.). Retrieved June 2, 2022, from https://www.pinata.cloud/

Proof Of Humanity. (n.d.). Retrieved May 5, 2022, from https://www.proofofhumanity.id/

RealMe. (n.d.). Retrieved May 2, 2022, from https://www.realme.govt.nz/

Sánchez-Torres, J. M., & Miles, I. (2017). The role of future-oriented technology analysis in e-Government: A systematic review. *European Journal of Futures Research*, *5*(1), 15. https://doi.org/10.1007/s40309-017-0131-7

Schneider, D., Klumpe, J., Adam, M., & Benlian, A. (2020). Nudging users into digital service solutions. *Electronic Markets*, *30*(4), 863–881. https://doi.org/10.1007/s12525-019-00373-8

Shaw, A. (2018). From disgust to dignity: Criminalisation of same-sex conduct as a dignity taking and the human rights pathways to achieve dignity restoration. *African Human Rights Law Journal*, *18*(2). https://doi.org/10.17159/1996-2096/2018/v18n2a12

Siriwardena, P. (2020). *Advanced API Security: OAuth 2.0 and Beyond*. Apress. https://doi.org/10.1007/978-1-4842-2050-4

Stallings, W. (c1995). *Protect your privacy: The PGP user's guide*. Englewood Cliffs, N.J. : Prentice Hall PTR.

The Immigration Act 2009

Windley, P. J. (2021). Sovrin: An Identity Metasystem for Self-Sovereign Identity. *Frontiers in Blockchain*, *4*. https://www.frontiersin.org/article/10.3389/fbloc.2021.626726

Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security*, *99*, 102050. https://doi.org/10.1016/j.cose.2020.102050