TRAVERSE:

AN AUSTRALIAN RED CROSS CASE STUDY OF THE CREATION, DESIGN, AND END OF A DIGITAL IDENTITY PLATFORM

Authors:
Emrys Schoemaker (Caribou Digital)
and Millicent Womble (Caribou Digital)

ACKNOWLEDGEMENTS

Support for the production of this report from the following organisations is gratefully acknowledged:

This report was made possible by funding from the American Red Cross.
Thanks also to the authors, Emrys Schoemaker and Millicent Womble, and all the interviewees for their contributions.

Contact us:
Requests for commercial reproduction should be directed to the IFRC Secretariat:

Address: Chemin des Crêts 17, Petit-Saconnex, 1209 Geneva, Switzerland
Postal address: P.O. Box 303, 1211 Geneva 19, Switzerland

T +41 (0)22 730 42 22 | **F** +41 (0)22 730 42 00 | **E** secretariat@ifrc.org | **W** ifrc.org

Contents

Executive Summary 2

Introduction 4

- Digital ID: A brief guide 4
- Methodology 6
- Genesis: The 'Identity Project' is born 7
- Selection and implementation of the solution 8
- The unique organisation of Traverse: A commercially viable startup 8
- A number of problems were identified for which a digital ID could be a solution 8
- Verifiable credentials and blockchain selected as the solution to the problem of volunteer management 8
- Critical elements to solving the identity problem: Traverse and the Trust Alliance 9
- Partnerships are critical to identity systems 9

Why did ARC stop Traverse? Adoption and commercialisation 11

- Trust and risk issues limited adoption 11
- Tensions between commercialisation and humanitarian goals 12

Learnings 12

Future opportunities 14

Glossary 15

Executive Summary

The following case study outlines the process and learnings from Traverse, an effort led by the Australian Red Cross (ARC) to solve the challenge of onboarding and managing volunteers and staff for rapid local and international mobilisation.

Traverse was intended to develop a verified identity platform for the humanitarian sector that would address a gap in the market for an ethical, user-centric, portable, and secure platform. This decentralised, self-sovereign approach was selected because it was seen as a way to give users ownership over their own data and control over how credentials are shared, while making it easier for participating organisations to onboard staff and volunteers.

The initial exploration led to the establishment of Traverse, a verifiable digital credentials solution, and the Trust Alliance, a forum of organisations who would work towards creating trust standards and developing an identity ecosystem in which Traverse could be used.[1] The team behind Traverse adopted the Web 3.0 technologies blockchain and verifiable credential technologies as the basis for their solution, which was intended to be a commercially sustainable digital identity product. A Web 2.0 technology stack was built at a later stage in an effort to reduce barriers to engagement.

Blockchain technology can be simply defined as a decentralised, distributed record that archives the source of a digital asset. Verifiable credentials are the result of an open standard to reliably represent the kinds of information found in physical credentials, such as passports or licences. They are a cutting-edge solution to the problem of verifying an identity or claim whilst protecting privacy. While the humanitarian sector has made little use of these technologies, the private and public sectors have started to utilise and produce them. In this context, Traverse was a pioneering initiative to use cutting-edge technologies to solve long-standing challenges in the humanitarian sector.

Despite successfully producing a web and mobile application and establishing the Trust Alliance and partnerships with internal ARC departments, in October 2021 ARC closed Traverse, largely because it couldn't get anyone to adopt the technology. The main challenge to enrolling others to adopt Traverse was the absence of a governance or legal framework for identity and claims within the humanitarian sector. ARC did not have the investment capital required to sustain Traverse until such a framework was established, though ARC supported the creation of the Trust Alliance to achieve this. Although Traverse was shut down, it provides learnings for both ARC and the wider humanitarian sector on both the specific technologies of blockchain and Web3 and the humanitarian sector's approach to developing and adopting innovative technologies.

Key learnings and insights include:

- **The selection of technologies must be assessed against technological maturity, ecosystem development, and the humanitarian sector's relatively conservative risk appetite in deploying unproven technologies—especially in crisis contexts for vulnerable populations.** At present, blockchain and the Web3 technological ecosystem are not sufficiently mature for the humanitarian sector to easily deploy at a system-wide level and, especially for identification management, lacks an authorising environment for the use of these technologies. In other words, inter-organisational trust standards, processes, and policies are required to enable the use of verifiable credentials.

- **Humanitarian actors need to be clear about the expectations of particular roles and approaches to innovative technologies.** These roles can include innovative technology startups, users of innovative technologies, and actors in the wider humanitarian sector ecosystem. ARC enrolled technology consultancy companies, private foundations, civil society organisations, and academics to the Traverse and Trust Alliance initiatives, on the assumption that different skill sets, perspectives, and capabilities across sectors and stakeholders would lead to useful, ethical, and responsible innovation. However, ARC was only able to understand the expectations and interests of critical roles, such as relying parties after selecting a technology, which revealed the importance of an enabling ecosystem and governance framework to support the use of verified credentials.

- **Humanitarian organisations need to understand the commitment required to develop innovative technologies and explore potential partnerships.** ARC mobilised over $750,000 in financial and pro bono support across corporate, humanitarian, government, and philanthropic sectors. However, this was insufficient to support the long-term runway required to build the technology and the governance framework required to successfully deploy Traverse.

- **Innovation within an ecosystem of actors happens at the pace of the slowest mover.** While Traverse's capacity for innovation was high and fast-paced, the humanitarian ecosystem has a far slower pace of development, with wider and more pressing organisational commitments, such as emergency responses and a global pandemic, prioritised over providing support and resources to Traverse

- **The humanitarian sector focuses on addressing specific problems, so humanitarian innovations should be problem-led rather than solution-led.** This requires deep understanding and definition of the problem itself as a precursor to any technological innovation or application—and may mean that the most appropriate solution, especially when dealing with vulnerable populations, might involve basic technologies (e.g., pen and paper) or process reform rather than the application or innovation of advanced, cutting-edge technologies.

Introduction

Digital identity (digital ID) is an increasingly important part of our digital state, economy, and society. The term is broad, encompassing IDs issued by government, private companies, and online for-profit companies, as well as the technologies the humanitarian sector uses to provide services to vulnerable individuals. It is also controversial, with debates around approaches such as China's 'social credit score' and ideas such as individualist 'self-sovereign identity' raising issues about power, control, and autonomy. This brief report outlines the efforts of the Australian Red Cross (ARC) to develop an innovative digital wallet approach to digital identification.

Digital ID: A brief guide

Digitisation has driven a rapid and comprehensive process of transformation in the humanitarian sector, one that has been accelerated by the COVID-19 pandemic. The need to prove who one is in this increasingly digital world means digital ID is a central pillar of this transformation. While the commercial digital identity sector is growing rapidly, the humanitarian sector has struggled with the use of technologies that are not designed for the specific use cases and contexts of humanitarian crises.

One of the evolving technologies designed to prove one's identity is verifiable credentials, a standard used to digitally represent the kind of information currently found in physical credentials, such as passports. A verifiable credential is a tamper-evident credential with authorship that can be cryptographically verified. Individuals, governments, and private and public companies have a common interest in building a trustworthy identity verification system. However, humanitarian actors argue that the functions and needs of the humanitarian context require systems and technologies designed with the sector's specific requirements in mind, especially to combat the challenge that many people are unbanked or lack formal ID. This brief guide details three topics related to digital ID: innovation, wallets, and trust frameworks.

Digital ID innovation: Wallets and trust frameworks

There are different approaches and models to digital identification systems. The traditional, established model is one in which a centralised issuer of an identity credential—a driving licence, a medical record, or supermarket loyalty card—collects information from an individual to verify that this person is who they say they are. The issuer then creates a record that the individual can use to authenticate their status or entitlement to a right or service. In this model, data is collected and stored in a centralised fashion. The positives of the traditional form of credentialing is that it's simple to use, inexpensive to run, and familiar to users who want to use the system. However, these traditional systems can also risk becoming honeypots for hackers and can be manipulated by untrustworthy owners.

Alternative models are driven by innovation in technology and approaches to the governance of identification management.

Wallets

One emerging approach is the idea of digital identity wallets. Rather than being stored in a centralised repository, an individual's data is stored in a location of the user's choosing, such as a mobile phone or laptop. This approach promises individuals more control over the use of their data. Conceptually, digital wallets hold statements about identity that can be verified and, when presented by the holder, relied upon by third parties as proof of an individual's rights or entitlements.

This is the approach adopted by the European Commission, which has realised the potential and necessity for digital ID as part of the region's wider digital transformation. It has advanced plans to create an EU Wallet, which would allow EU citizens to use an app to hold different documents or credentials that they can control and use in order to prove who they are. The European Commission will begin testing this technology in October 2022 and hopes to have it unveiled to citizens by September 2023. The president of the European Commission, Ursula von der Leyen, stated that 'the Commission will propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves and what data is used and how.' Ursula von der Leyen has highlighted digital ID as a solution to protect citizens' data and enable individuals to prove who they are in an increasingly digital European Union.

Trust Frameworks

Another approach—which can be complementary—is to establish rules and regulations that determine how identification is managed. Instead of specifying technologies, these frameworks define the rules around which the verification and authentication of individuals are managed.

Like the European Commission, the UK government recognises the importance of digital identification in an increasingly digital world. Instead of creating their own wallet, it is establishing principles, policies, procedures, and standards that will govern digital identification. This 'UK Digital Identity and Attributes Trust Framework' sets out guidelines for the sharing of information to verify citizens' identities or personal details, such as their age or address, in a consistent way, without specifying what technologies must be used to do so. The governance-

centric approach enables both public and private groups to participate in the management of identification and aims to stimulate a wider marketplace of identification management.

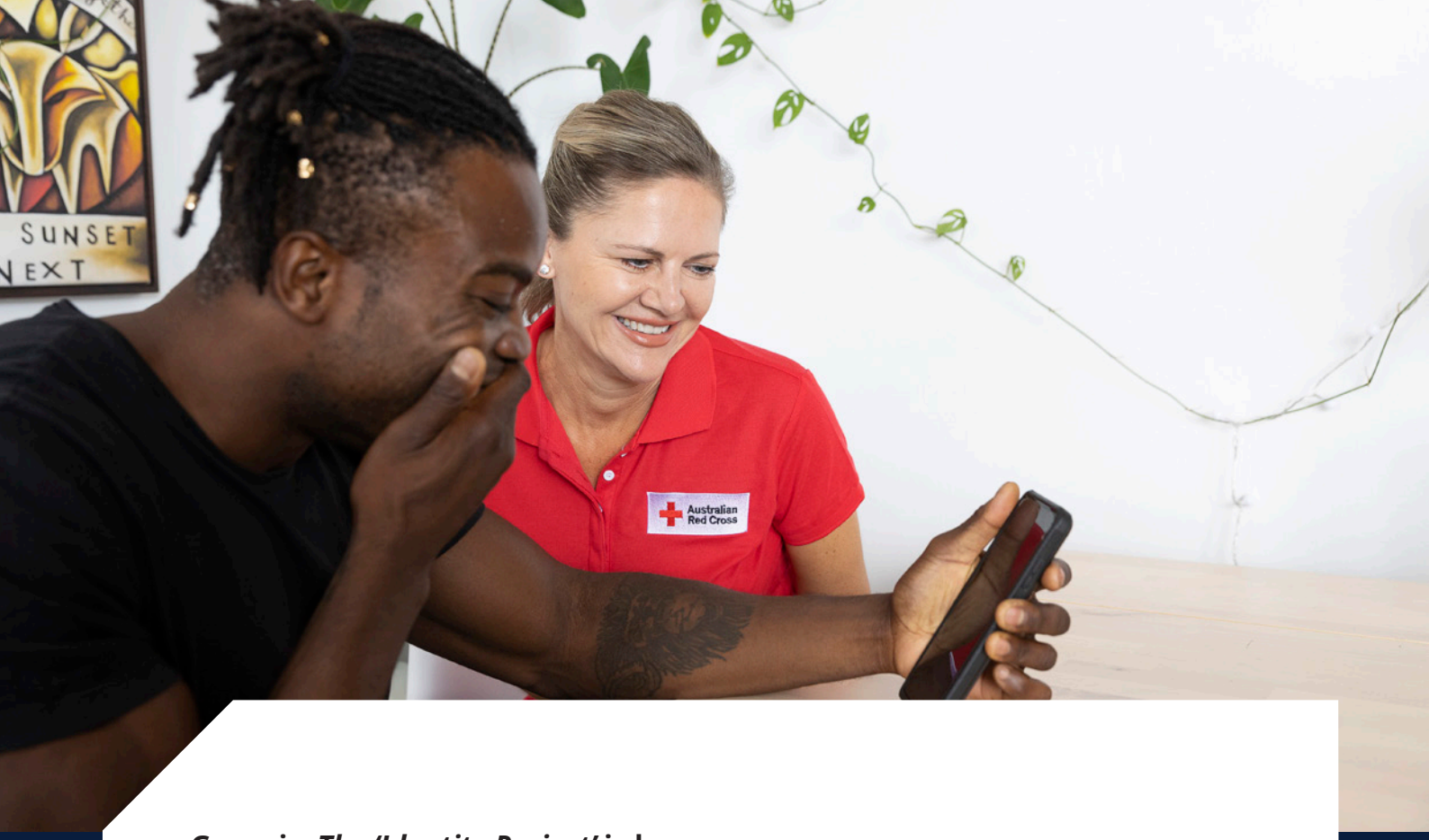
This approach is increasingly common; Canada's decentralised federated governance structure was a catalyst for the development of the Pan-Canadian Trust Framework. This innovative approach shows how central and regional public institutions can establish a coherent approach to identification. A similar approach has also been taken in Australia, where the Australian government has created the Trusted Digital Identity Framework (TDIF), which outlines specific rules and standards for all providers and services within Australia's digital ID system.

The importance of digital identification is increasingly recognised as a global concern. The United Nations links digital identification to legal identity and its associated rights and entitlements. The UN Secretary General has urged the development of digital ID technologies as 'digital public goods' that form the core public infrastructure of future states and economies.

The efforts of these large public institutions demonstrate that digital ID has clearly been deemed an essential element of the digital transformation of the public and private sectors, one that requires a careful balance of the data necessary to participate in an increasingly digital society, with an attention to the protection of people's information and data in the future.

Methodology

Caribou Digital interviewed 12 people, including members of ARC, the Trust Alliance, and Traverse, to obtain a complete overview of events and gain a better understanding of the project. Additionally, the case study drew on documents provided by Traverse and other desk-based research surrounding digital ID.



Genesis: *The 'Identity Project'* is born

ARC started to explore the role of digital identity in the humanitarian sector through its Volunteering Directorate and International Strategy and Influencing teams in early 2018. Framed by a global conversation about digital identity, participation in a series of technology-oriented 'futures' workshops, and concerns about safeguarding communities from abuse by humanitarian workers, there was interest in exploring these problems in the immediate contexts within which ARC worked. This led to a focus on identity management for volunteering, particularly the opportunity to remove structural barriers and administrative burdens.

Around the same time, there was a leak of sensitive data from one of ARC's third-party vendor platforms, PageUp, which increased the organisation's awareness of the risks inherent in centralised identity data stores. As a senior ARC leader stated: 'There is a lot of risk around data, and if their data had been compromised that would have been a large issue.' With that in mind, ARC began to explore innovative techniques to improve the data protection of their clients and volunteers, mindful of the concerns with the intersection of digital identity and migration. From this ideation phase came the 'Identity Project.'

During the initial phases of the project, ARC examined different technologies it could use. There was already interest in blockchain from the futures workshops, and collaboration with a technology and design consultancy with experience in decentralised and Web3 technologies led ARC to commission them to design a platform based on blockchain and verified credentials. The focus for the project at this stage was to explore how these technologies could support credential and identity management for the volunteer workforce.

The Identity Project looked deeply into digital identity and verifiable credentials to understand how the technology worked and to explore applications and partnerships with relevant organisations. From the insights gained through this initial phase it was clear that, in addition to Traverse as the identity technology solution, an alliance of partners who would trust Traverse and each other in order to share credentials was required. The Trust Alliance was established to meet this need.

Selection and implementation of the solution

The unique organisation of Traverse: Towards a commercially viable startup

ARC structured Traverse in a unique and strategic way, which ultimately restrained the initiative's movement and forward progress. ARC wanted Traverse to be able to move quickly, like a startup for-profit enterprise, and placed the initiative in a unique space within ARC's bureaucracy.[2] This allowed Traverse to be removed from ARC's day-to-day operations. Additionally, ARC organised the initiative with an eye towards the project's future commercial viability. While commercial viability was a desired outcome for the project from the outset, the implementation of the initiative highlighted that it was unclear how this goal could be accomplished.

A number of problems were identified for which a digital ID could be a solution

The problem space around personal data and identification is broad. While ARC defined its initial focus as the movement of volunteers between organisations, it still struggled to find clear routes to deploying the digital identity solution. Importantly, the scope for the problem space was largely limited to ARC's work in Australia. Efforts to engage with the wider IFRC movement had only limited success, though once Traverse was under development there was an initial conversation with Kenyan Red Cross about its work on digital identification. However, according to the development team, there was a sense that the problems they were solving, despite being identity problems, were very different.

One problem that Traverse identified was the inability of volunteers to quickly move and work between different nonprofit organisations due to significant obstacles, such as extremely long and bureaucratic onboarding processes. This became a major issue when disasters struck and organisations needed to quickly send volunteers to the emergency. Additionally, trends showed that in recent years volunteers have moved between nonprofits more frequently, meaning that those volunteers had to go through long onboarding processes multiple times. Requirements such as police checks and 'working with children checks' (WWCCs) must be completed by each of these organisations, leading to strains on the volunteer, as well as on the organisation's resources and time. The process that ARC and all nonprofits use now consists of long onboarding processes, time-consuming police checks and WWCCs, and confusing national versus state standards. This seemed like a clear need and a problem that aligned with Traverse's focus on solving volunteer identity and credential management.

Verifiable credentials and blockchain selected as the solution to the problem of volunteer management

Following an exploration of the utility of building a cross-functional credentialing tool, Traverse landed on verifiable credentials as the best solution to the problems of volunteer identity vetting and management. The technology was seen as a good fit for two reasons: its robust security aspects and its ability to verify credentials in real time. In addition to addressing the problem of volunteer management, there was a belief the technology could help solve the data security issue as well. A lead figure in the development of the project noted that 'you can still attack a decentralised database but the attack vector is smaller because it is distributed.' Additionally, the blockchain technology could allow an organisation to verify credentials instantaneously with minimal manual steps, which would save time and resources. ARC engaged a technology and design consultancy to build a prototype that would facilitate volunteers' movement, and together the consultancy and ARC landed on a proof of concept.

However, the decentralised technology approach also became a barrier. Although there was a shared belief that verifiable credentials and decentralised technologies could help achieve the security goals and identification management objectives, in practice the technologies became a hindrance, as the potential partners struggled to understand the value of blockchain. There was also a tension between a practical need for Traverse to focus on humanitarian use cases and the broader Web3 agenda. Consequently, ARC brought product development resources in-house for efficiency and to explore whether a more established, Web 2.0-type approach might overcome the barriers to adoption.

Critical elements to solving the identity problem: Traverse and the Trust Alliance

When Traverse examined the potential for digital identity and credential use, it encountered the reality that the value of a credential is primarily determined by the party that relies on it as proof of identity or status (the 'relying party'). If the credential is not accepted by both the holder and the relying party, then the credential has only limited value. Therefore, a crucial component of Traverse's efforts to develop a useful digital identity product was finding a way for credentials to be accepted by other organisations. This introduces the second pillar that emerged from the Identity Project: the Trust Alliance.

The Trust Alliance, a multi-sector collaboration committed to shared principles of 'do no harm', humanity first, and open ecosystems, was launched by ARC in July 2019 as a response to the insights gathered from the Identity Project. Open ecosystems would be a critical component if blockchain credentialing was to become a reality. Stakeholders would implement stakeholder engagement activities to grow membership and build momentum for decentralised identity.

In 2020, the Trust Alliance focused on establishing the governance structure for credentialing within its member network, which became the first Trust Alliance Credentials Framework. The Framework included guidance for registering a credential user, issuing a credential, and verifying a credential issuer using a blockchain ledger, which made the credentials cryptographically secure. The acceptance of this format of digital ID by a large number of organisations was recognised as crucial for the decentralised credential to gain legitimacy and trust, and thus utility.

The Trust Alliance Credentials Framework clearly laid out how decentralised ID could be used at a technical level by these organisations. The partnership between the Trust Alliance and Traverse was key for the coordination of both of their efforts. However, Traverse found that the Trust Alliance could not move quickly enough to establish the pathway for other organisations to start accepting credentials; while organisations might have trusted one another, they feared legal and reputational consequences if something went wrong. As a result, the process was slow-moving as establishing trust between participating organisations required regulatory and policy changes. It was recognised that this was likely to take more time than ARC's funding for Traverse provided. Traverse needed to move faster to demonstrate viability. Traverse turned to existing ARC partners and processes to identify opportunities and problems that Traverse might help solve.

Partnerships are critical to identity systems

With the Trust Alliance not able to provide use cases quickly enough, Traverse realised that it needed to find its own use cases to test and validate its product. To do this, it used some of its existing networks in the education sector, while exploring other networks that could be potential fits. Traverse had a startup mindset: quick to pursue new opportunities and attempt to develop and sell its product to the market. This approach and pace continued to be at odds with the institutions and organisations the initiative was able to partner with. Partners that Traverse pursued included

healthcare institutions, organisations within the education and training sector, and departments within ARC. Despite this, Traverse struggled to obtain commercially viable partnerships (with partners who would pay to use the product) due to lack of confidence in its unproven product and competition from more established technology companies that had existing, proven digital identity applications.

One of the partnerships Traverse pursued was with a set of healthcare institutions. It started by examining the ways a set of medical clinics currently provided centralised training for all their medical staff, enabling those staff members to work at multiple facilities within the same healthcare network. This model was similar to the one that the Trust Alliance hoped to facilitate, and therefore seemed to be a close fit. Traverse found that the clinics did not have an adequate system in place to verify that nurses and staff had completed this shared training. The clinics were manually verifying someone's credentials each time, which was costly and resource-intensive. Traverse deduced that the clinics could use verifiable credentials and blockchain to quickly verify a volunteer or staff's credentials. The clinics were interested in what Traverse had to offer but believed it might be too big of a risk to take on the new product. The organisations wanted the product to be fully developed and to exist in the wider market with other use cases before they came onboard.

Another similar use case that Traverse identified was in the education sector. Traverse recognised that there was a need for students to be able to share their school credits across different universities in the event that they wished to transfer or get recognition for prior learning. One local Australian university was interested in the product but preferred to wait until the product had proven market success. Also, other credentialing organisations were already present in the market, such as Credly, with a proven product and customers using a more familiar, centralised technology platform. Therefore, this partnership was unsuccessful.

Another partnership was with departments within ARC. Traverse worked directly with the Volunteer department and examined how the product could be used within the Migration Programs and the Emergency Services departments. Volunteer Services was where Traverse had the most traction, concrete engagement, and feedback. The Volunteer Operations team shared details of its onboarding system and identified where Traverse could potentially help. A senior figure in Volunteer Operations highlighted that 'the pilot that we did wasn't to see if we could make the police check process easier, it was to see if once that police check process was done, could we get those credentials into Traverse's system.' Traverse eventually found that the volunteers and internal staff valued convenience over the ability to self-manage data. The blockchain technology was too complex, unfamiliar, and nuanced to roll out in the Volunteer Operations department. A senior volunteering leader pointed out that ARC already had a complex onboarding system in place that they were not looking to replace, which meant it was hard to find the right place to fit Traverse's new technology and system. Traverse also worked directly with the Emergency Services department to examine how its product could help with the delivery of services. The grant team was interested in the product after dealing with Australia's worst bushfires on record in the summer of 2019–20 and the allocation of grant funds to the victims of the fires. Traverse saw this as a possible opportunity to evaluate how digital ID might serve as proof that a bushfire had affected a victim's home and unlock the grants and insurance.

However, after several days of research and ideation that generated increasingly complex technological solutions to the problem of collecting and distributing digital ID in an environment with unreliable electricity and internet, the team realised the problem had already been solved with the most basic of technologies. They discovered that a year earlier a group of emergency responders had solved most of the problem by printing the forms on carbon paper notepads that didn't need Wi-Fi. They concluded that there are times when the most low-tech solution can be just as useful as anything a computer can come up with.

Why did ARC stop Traverse?

Adoption and commercialisation

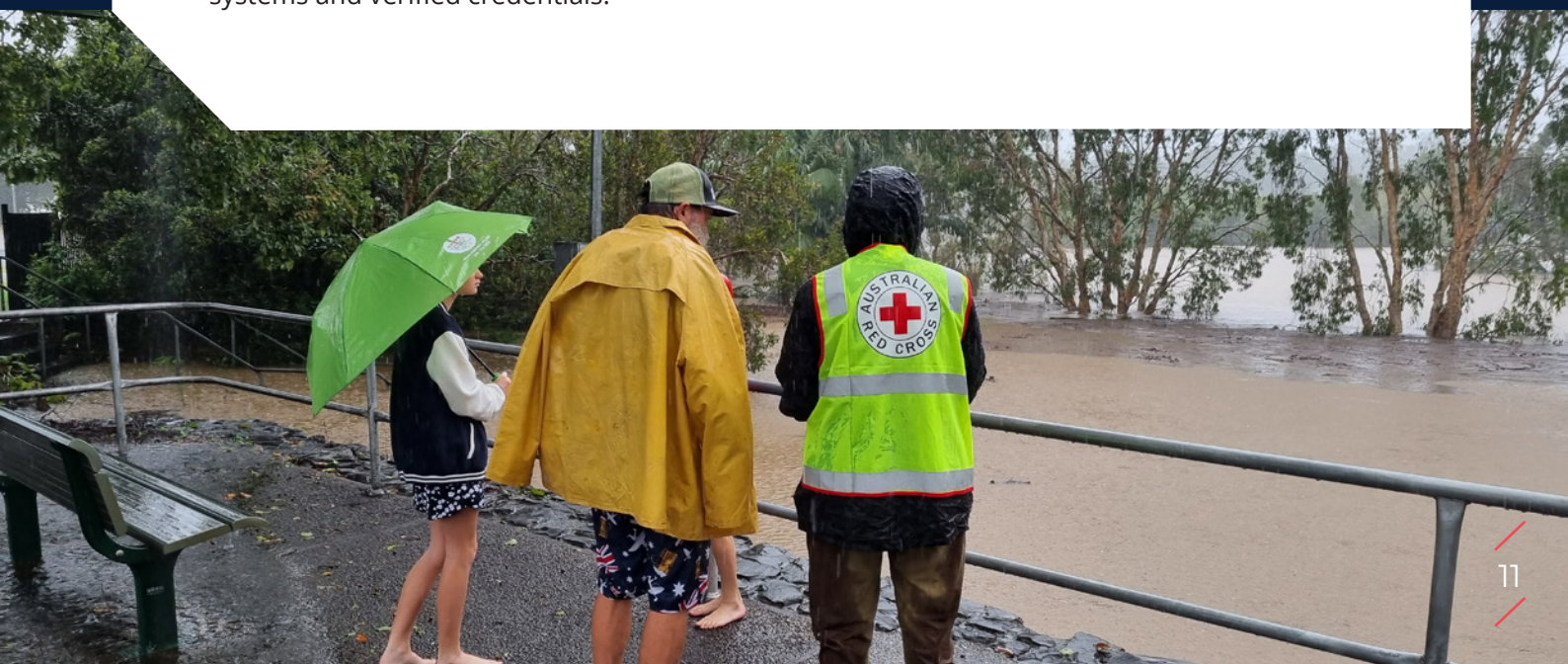
In late 2021, Traverse was formally shut down by ARC. Traverse had set out to solve a complex set of problems, and while the initiative produced important learnings and created new intellectual property, connections, and networks for ARC, the organisation decided to stop the initiative because it could not solve two fundamental challenges it faced. First, the Trust Alliance was not able to enrol any users who would take the risk of trusting the credentials held in the wallet. Second and relatedly, Traverse had competing visions of success and was unable to establish a route to commercialisation.

Trust and risk issues limited adoption

Technology products, particularly digital identity technologies, require users to trust them to achieve intended purposes. ID systems generally, and digital credentials specifically, are intended to address the issue of trust between transacting parties: that the person presenting the credential is who they say they are or that the claim they make (for example, about a status or qualification) is true. For a party to rely on a credential, it must trust that the credential is reliable and legitimate. Traverse and the Trust Alliance found that organisations commonly do not trust credentials issued by other organisations.

A further obstacle to achieving the trust required was the challenge of getting the right organisations to commit to the initiative. The Traverse team engaged with the sector through the Trust Alliance (partners included RedR Australia, Oxfam Australia, Care Australia, Engineers without Borders, some community-based organisations) and the wider IFRC network (through presentations,including at the IFRC's data and digital week in 2020). Although this led to a number of pilots, it did not lead to the adoption of credentials in practice.

Barriers to translating engagement and pilots to commitment, according to one lead figure in the initiative, included getting the right people at partner organisations and the wider IFRC network to join the authorising environment, as well as the technology itself. As one figure put it: 'It took us a while to stop talking to people about why blockchain and start talking about the problem this might help solve.' The Trust Alliance continues to work through these challenges and build the necessary ecosystem and community to enable the use of decentralised identity systems and verified credentials.



Tensions between commercialisation and humanitarian goals

The stakeholders involved with Traverse held divergent views on the fundamental goal of the project, essentially, whether the priority was to solve a humanitarian need or to develop a commercially viable technology business. The goals around commercial viability were ultimately at odds with meeting humanitarian needs in areas like volunteering, migration, identity support, and emergency services.

Some stakeholders believed Traverse needed to at least be financially self-sustaining, whilst others believed it should generate profit as a return on ARC's investment to further support ARC's mission. However, Traverse struggled to identify a pathway to any form of commercial return, because it focused on the humanitarian sector and was competing against established commercial identity solution providers. The humanitarian sector is limited in size and resources, which makes developing products designed exclusively for it challenging as a commercial proposition. Stakeholders, such as the technology consultancy, believed that the mandate should have been broadened to include less of the humanitarian sector—even though this was explored unsuccessfully in the education and healthcare sectors. Additionally, there was a good deal of existing competition in the credential sector; organisations such as Credly and Accredible sell their products to multiple industry sectors, and even though they do not provide the portability that Traverse offered, they meet the minimum requirements of the clients who purchase their products and services.

Learnings

Digital identity systems are technology solutions to trust and can only be developed at the speed at which trust is established. ARC found that developing a technology solution can only proceed at the pace at which trust is developed. This means that any identity system requires an appropriate governance framework and authorising environment for verifiable credential technologies to be used.

Innovation and the ability to 'fail safely' is challenging when dealing with cutting-edge technology, especially for resource-constrained organisations. Instead, it might be more useful to focus on establishing private and public partnerships that are on the forefront of cutting-edge technology. A member of the Trust Alliance echoed this, underlining that technological innovation requires freedom to fail and experiment, a luxury that humanitarian organisations often do not have. Although the Trust Alliance was intended as a route to achieve this, the path to establishing the credential framework was longer than ARC and Traverse could support.

Digital ID as a set of processes is broader and covers more use cases than any single technology can support. Although there were initial conversations with others in national societies working on digital identification, such as the DIGID program at the Kenyan Red Cross,[3] Traverse concluded that these were very different: 'They used different technology, to solve a different problem, for a different group of people, with different needs. The only things they really had in common was Red Cross branding and the word "Identity."' There does remain, however, a significant number of efforts to find innovative applications of technology to support the different processes of identification, within both the IFRC and the wider humanitarian community. One learning for the IFRC would be to explore within the

IFRC—and possibly the wider humanitarian community—whether there are specific problems shared by a sufficient number of Red Cross National Societies or programmes within the many identification processes that a defined digital identity technology could help solve. This could take the form of a concerted program of working sessions and communications channels with other societies in order for them to share project experiences and challenges. This might help identify a shared problem for which a partnership or even Federation-wide initiative is the right approach to developing digital technology solutions.

Innovation happens at the pace of the slowest mover. ARC was unable to move as quickly as Traverse's startup style required. Its new working style provided learnings, which included setting a different pace and expectations for ARC. The team, which saw themselves as a high-performing product team, was put in an environment where there was minimal product development and product strategy, because ARC is geared towards the delivery of programs and services rather than product-like most humanitarian organisations. Additionally, the Trust Alliance worked similarly to ARC in that it made progress slowly. To support such longer-term technology and process developments, there is an urgent need for patient capital to invest into innovation and experimentation in the sector without 'fear of failure.' The Modular Open Source Identity Platform (MOSIP) is a case in point; supported with long term core funding from foundations such as the Gates Foundation, Omidyar Network, and Norwegian government, it is now one of the most adopted 'digital public goods' in the national identity space.

The best solution does not necessarily have to be the most high-tech solution. The humanitarian sector's focus on specific problems means innovation needs to be problem-led rather than solution-led. For example, if vulnerable people do not have the best internet capacity, a better solution could be using simpler, lower-tech solutions.

Set the right expectations from the beginning. There were conflicting expectations among different stakeholders. Some of the learnings around this concern setting the right expectations from the beginning and even framing Traverse as more of an experiment. During an interview conducted with one of the project's founders, there seemed to be a lack of coherence with the overall goal of the project and Traverse's mandate. Despite the clear focus on volunteering identity and credential management, there was a sense that the project was also focused on the wider 'global identity problem' that framed the initial support for the project. Some Traverse stakeholders reflected that these lofty philosophical goals were confusing, since their mandate concerned specifically supporting the onboarding and management of volunteers and staff, while other project sponsors felt that Traverse had focused too narrowly on the Human Resources technology problems space.

Future opportunities

Most of the people interviewed for this study feel there was a lot of potential for blockchain and verifiable credentialing technology, but that it was three to five years away from the point where it will be widely used and recognised throughout various sectors. Traverse highlighted that, in relation to its benefits, the resources required to develop and maintain blockchain technology were too high for humanitarian actors, such as the Red Cross. However, others stated that as the technology becomes more established and the associated costs and resources decrease, the application of digital ID in the humanitarian sector will become more viable.

Regardless, humanitarian actors should look for partnerships with companies that already have technological capabilities and utilise their expertise, rather than establishing in-house resources. ARC and the overall humanitarian sector should consider whether it is appropriate to be technology innovators—with all the cost and risk involved—or instead rely on existing tried and tested technology that has already been proven in the market (noting that these have their own costs and risks associated with them). However, to make the most of such partnerships, humanitarian organisations need to build their knowledge and capabilities to be an informed procurer of technology partners and technology products and services.

Additionally, as the technology is rolled out across the public and private sectors, policy and regulatory reform will make uptake easier. For example, in Australia there's a real possibility that in the future there will be useful policy changes that will make WWCCs and police check credentials more standardised and create an easier onboarding flow for volunteers. Traverse ran into issues with difficult police check processes and WWCCs that were not standardised throughout the country and changed from state to state. This may also mitigate several of the legal and compliance risks that the Trust Alliance encountered while trying to develop trust relationships between organisations.

Another significant opportunity for humanitarian organisations is to create lasting and meaningful partnerships with companies and startups that are at the forefront of cutting-edge blockchain digital ID technology. As mentioned above, the humanitarian sector should consider to what degree partnerships could decrease risk, reduce the cost of projects, and increase the adoption of new products through other networks. Engaging the right partners, understanding their motivations, and developing a shared agenda or set of objectives can help create space for careful innovation. Technological innovation requires freedom to fail and experiment, which is not a luxury or mandate that the Red Cross has. But through partnerships and working with affected communities, humanitarian organisations can customise proven technologies, which will bring innovative technological applications to safely and ethically support ARC's work to meet the needs of the people and communities it serves.

Glossary

blockchain technology: Blockchain technology is a decentralised digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. It is a system of recording information that is difficult to hack.

digital identity: Digital identity is digitised information on an entity used by computer systems to represent an external agent, which could be a person, organisation, application, or device.

police check: A police check is an official document issued as a result of a background check by the police or a government agency.

verifiable credential: Verifiable credentials are an open standard for digitally sharing information currently found in physical credentials, such as passports or licences. They can also represent things with no physical equivalent, such as ownership of a bank account.

Web3: Web3 is the third generation of internet services. It is based around the principles of using cryptography to provide trust and storing data in a distributed rather than centralised fashion.

working with children check (WWCC): A working with children check is an ongoing assessment of a person's eligibility to work or volunteer with children, which involves checking a person's national criminal history and other disciplinary and police information.

Endnotes

[1] Established by ARC, the Trust Alliance is a multi-sector collaboration of organisations committed to shared principles of 'do no harm', humanity first, and open ecosystems to support the use of secure, user-centred, and controlled digital identity systems.

[2] As an endorsed brand of ARC.

[3] The Kenya RC Digital ID work was focused on cash transfer for people without official ID. Additional information on the work can be found at https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf