ESaPoNIS\100047

Verifiable Credentials: Finclusion Project

by

Karen Elliott, Kovila Coopamootoo, Dave Horsfall, Magdalene Ng, Tasos Spiliotopoulos, Han Wu, Aad van Moorsel

Newcastle University
contact: karen.elliott@newcastle.ac.uk or aad.vanmoorsel@newcastle.ac.uk


BILL & MELINDA
GATES foundation


The
Alan Turing
Institute

ACKNOWLEDGEMENTS

The Trustworthy Digital Infrastructure for Identity Systems project is led by the Turing Institute and is funded through a grant from the Bill & Melinda Gates Foundation.

The FinTrust Team is funded by the UK Engineering and Physical Sciences Research Council for the projects titled "FinTrust: Trust Engineering for the Financial Industry" (EP/R033595/1).

ABBREVIATIONS

DIDs	-	Decentralised Identifiers
FCA	-	Financial Conduct Authority
GFC	-	Global Financial Crisis
NHS	-	National Health Service
KYC	-	Know Your Customer
VCs	-	Verifiable Credentials

1. INTRODUCTION

Governments around the world are committed to supporting the roll out of national digital identities (IDs), but there exist many risks associated with scaling these systems at a national level. Building an ID system that meets developmental goals is a multifaceted challenge, and questions of trust are based around the complex interplay of socio-technical considerations, requiring multidisciplinary expertise. The 'trustworthiness' in digital IDs is multi-dimensional including characteristics concerning security, privacy, ethics, resilience, robustness and reliability.

Several high-level sets of principles have been defined by organisations like the World Bank Group's Identification for Development (ID4D) Initiative, in accordance with the Principles on Identification for Sustainable Development and other international standards. They provide a primer on why ID matters, the risks of ID systems, and the international stakeholders. Similarly, outline the critical principles that practitioners need to follow to ensure that ID systems are implemented responsibly. Such principles include robust, secure, and sustainable design, universal coverage, and accessibility, as well as strong governance and accountability frameworks. Yet, the existing technical implementations come with a set of trade-offs that need to be evaluated in a systematic way against the high-level design and implementation principles.

This report is the assessment of the work performed by The FinTrust team at Newcastle University in examining the potential of the combination of Decentralized Identifiers and Verifiable Credentials for the identification of vulnerable consumers in finance, and discusses possible implications that these technologies can have for the provision of tailored financial services and products. The UK financial regulator (FCA) has identified the protection of vulnerable customers as a key priority for the industry and has published appropriate guidance for financial firms, strongly encouraging them to treat vulnerable customers fairly. Four categories of characteristics are considered to constitute drivers of financial vulnerability—Health, Life Events, Resilience and Capabilities, the latest report finding that 53% of UK adults show one or more of these characteristics.

The analysis and results presented in this report are based on several pieces of work. First, (Spiliotopoulos et al., 2021), presented at the *Designing for New Forms of Vulnerability* workshop at the ACM CHI 2021 conference provide a position paper for the work in the Finclusion project. The second piece of work is a detailed design document by (Horsfall et al., 2021) which provides extensive documentation about the software platform, and is available from the authors. Thirdly, (Elliott et al.. 2021) is a precursor of this document, describing the outcomes of the expert interviews.

2. CHALLENGES

We explore the scalability of the identity software (which is based on Decentralized Identifiers and Verifiable Credential W3C standards), for vulnerable customers to understand the barriers

and pain points in existing system solutions. These include issues of poor (digital) connectivity and large amounts of users across diverse demographics to promote financial inclusion.

Furthermore, we examined the human and societal aspects of trust in above-mentioned identity technologies, in UK using the research methods of literature review, interviews with UK and international financial inclusion experts.

3. OBJECTIVES

We aim to enhance the privacy and security of national digital identity systems, with the ultimate goal to maximise the value to beneficiaries, whilst limiting known and unknown risks to these constituents and maintaining the integrity of the overall system. First, we identify one UK use case for financial inclusion (for instance in areas in the North-East of England) and garner international use case insights from our pool of experts who work on a global basis, to drive the research.

Second, produce a position paper investigating the potential of Verifiable Credentials for financial inclusion. In particular, we focused our research on identifying and addressing financial vulnerability and examined in detail the scenario of a customer interacting with their bank using VCs. This paper was published and presented in a workshop at a leading academic conference and is accessible to a broad community.

Third, create a user-centric design document of a scalable system for financial inclusion, using Decentralized Identifiers and Verifiable Credential open standards. Thus, producing a technology prototype in collaboration with industry that uses decentralised ID verification to present verifiable claims about users.

Finally, this report details insights from interviews conducted with UK and international experts on the human and societal trust issues related to Financial Inclusion technologies used in our prototype. The data from these interviews will expand our position paper ready for academic publication.

4. USE CASE/EXPERT CONSULTATION

To understand how financial institutions have approached vulnerability in light of the FCA guidance, we accessed stakeholders from the FinTech Ecosystem[1] (mainstream finance). In addition, spoke to stakeholders of the responsible lending sector, whose clients emanate from disadvantaged and vulnerable cohorts to understand this space from a business (mainstream and alternate) and client perspective. These perspectives informed creating a use case underpinning the development of the prototype (see Section 6).

[1] https://www.whitecapconsulting.co.uk/press-release/new-report-highlights-growth-potential-for-fintech-in-the-north-east/

First, we asked the mainstream stakeholders how their organisations perceived vulnerability and explored current procedures to identify the customer group. Current processes were reported as predominantly manual, based on customer phone conversations and chat messages with financial agents. Vulnerability is raised by the customer rather than the agent. A vulnerability can range from a lack of digital illiteracy to physical and sensitive conditions impacting an individual's financial capabilities. Customers willingly disclose physical conditions, such as blindness or deafness. However, in relation to more sensitive conditions e.g., a mental health issue, these are avoided premised on the associated social stigma. Whereas, for terminal illness or bereavement, customers again are reported as open and engaged in voluntary disclosure.

Second, once vulnerability was confirmed, what happened to the customer's accounts? The term "vulnerable" is replaced with "additional customer care and support" to avoid negative labelling of customers. In addition, "flagging" policies are used with reviews occurring every 12 months. To "flag" an account, customers and agents liaise to agree on the nature of the vulnerability, how these impact on their financial capacity, the support required and how customer data is stored and used by the institution (GDPR compliance). Flags are read by agents each time the customer accesses services with flexibility to assign an account manager if account arrears accrued and monitored every 3 months. If the issue is resolved the flag is removed. The customer can also request flag removal, and information is no longer stored (cf. GDPR). Thus, stakeholders purport to deliver flexible and tailored customer service for "vulnerabilities".

Third, we enquired, how the engagement process commences with customers in establishing vulnerability. Phone conversations are the current primary route. New functionality is being explored for sensitive conductions. For instance, in relation to mental health conditions, automatic notifications via the Vulnerability Registration Service[2] can inform stakeholders of a vulnerability disclosure with the consent of customers.

Fourth, to compare current processes and our verifiable credential technology, we discussed emerging solutions for disclosure: selective disclosure on external cards, or a dedicated vulnerability card. The stakeholder's response was negative premised on part of the design as a binary disclosure card i.e. "are you vulnerable – yes or no" was deemed inappropriate as with insufficient details, stakeholders claimed to be liable to operational risk. Indeed, selective (attribute) disclosure was viewed as aligned to suspicious frequent patterns of fraudulent behaviour. Yet, only approximately 30% of customers who are "vulnerable" are captured using the reported manual process.

For alternative stakeholders, algorithmic tools[3] are available to onboard customers ensuring that responsible lending is observed.[4] The response from these stakeholders emerged as technical and behavioural challenges. First, can decentralised ledger technology share profiles with third parties when the transaction data is used for credit decision-making processes. An "aggregation

[2] https://www.vulnerabilityregistrationservice.co.uk/

[3] https://prinsix.com/

[4] https://moneyline-uk.com/

hub" to consolidate the digital profiles and make them accessible for decisioning was suggested. The binary nature of the prototype was also questioned in ensuring how potential different verifiers of credentials i.e., landlords demonstrate digital transaction histories for "vulnerable" customers? Second, how do we motivate engagement to track their financial behaviour and how do we communicate the benefits to this cohort especially, as they may "trust" the anonymity of cash transactions or M-Pesa (i.e. Africa), where a credit history is unnecessary. Finally, for decision makers, what is the risk of collusion and fraud between verifiers such as landlords and individuals in creating fake profiles? Regulatory obligations are implied and how will the solution fulfil such obligations from the FCA around KYC ("know your customer")?

The above insights are useful consideration affording the team challenges to explore in the socio-technical space. However, for the purposes of prototype development, we focus on rich learning in current technological capabilities leaving the complex minutiae of business application to later recommendations for development. Below, we present the culmination of literature, discussion with stakeholders and direction captured a position paper underpinning the prototype design.

5. POSITION PAPER (Spiliotopoulos et al., 2021)

In order to investigate the potential of Verifiable Credentials (VCs) for financial inclusion, we focused our research on identifying and addressing financial vulnerability. Financial vulnerability is a broader concept that encompasses financial inclusion, that is, financial inclusion is a factor that mitigates vulnerability. The identification of vulnerable consumers is of great importance in the financial sector because it allows financial institutions to train staff, allocate resources and design products and services in a way that supports vulnerable populations. For this reason, the FCA has been tracking the vulnerability of consumers over time, together with other aspects of their financial lives. FCA's flagship consumer survey, the *Financial Lives* survey, has found that, before Covid-19, the number of UK adults showing one or more characteristics of vulnerability was decreasing, with this decrease largely attributed to improvements in digital inclusion and financial resilience. However, the latest results of this survey show that Covid-19 has reversed this positive trend in vulnerability and has disproportionately affected specific population groups, such as younger adults and the self-employed (Financial Conduct Authority, 2021a).

Our research was motivated by the FCA's latest report which provides *Guidance for firms on the fair treatment of vulnerable customers* in finance (Financial Conduct Authority, 2021b). This guidance identifies a vulnerable customer as "someone who, due to their personal circumstances, is especially susceptible to harm - particularly when a firm is not acting with appropriate levels of care". The guidance establishes the protection of vulnerable customers as a key priority for the industry and strongly encourages financial firms to treat vulnerable customers fairly. As stated in our introduction, exploring the four categories of characteristics that drive financial vulnerability – poor health, impact of life events, low resilience, and low capability.

We investigated the use of VCs and Decentralised Identifiers (DIDs) for identifying and supporting financially vulnerable consumers and published the work as a position paper (Spiliotopoulos et al., 2021) at the *Designing for New Forms of Vulnerability* workshop at the ACM

CHI 2021 conference. This paper examines in detail an overarching scenario that involves a customer interacting with their bank using VCs for different purposes and in different ways (e.g., both directly and via a revocable token), as well as the possible response and use of the vulnerability information by the bank. We focus our discussion on two key characteristics of this approach in this context, namely *self-sovereignty*, i.e., that people and businesses store and control their data on their own devices and provide these data only when someone needs to validate them, and *selective disclosure*, i.e., that only relevant private information is shared with interested parties in a privacy-preserving way. This work was presented and discussed at the workshop in the context of different approaches for addressing vulnerability and we gathered further comments and insights that fed into the later stages of the project. We also contributed to the creation of a collaborative output during the workshop in the form of a Zine – a creative and self-published magazine – around the concept of vulnerability. The final version of this Zine will be available in the future at the workshop website[5]. Premised on this position paper and prior discussions with industry to create a use case, we moved to prototype development.

6. SOFTWARE DESIGN SPECIFICATION DOCUMENT (Horsfall et al., 2021)

We created a software design specification document describing a structured collection of requirements to facilitate analysis, planning and decision-making in the development process. Our technical specification provides an implementation of the World Wide Web Consortium (W3C) standards for DIDs v1.0[6] and Verifiable Credentials Data Model 1.0[7] in an Azure environment, and was created to drive the discussion and evaluation of potential solutions for the use case of vulnerability in finance. We have defined a data model for a new Verifiable Credential type that maps the aforementioned drivers of vulnerability to attributes in a new Verifiable Credential type. This allows the presentation of tamper-evident claims that cryptographically prove who issued them, but without the need to disclose the specific details of the vulnerability about which the claim is made.

We define user roles, and the relationship between them to establish a triangle of trust between the Subject, the Issuer, and the Verifier. This trust model differentiates itself from other trust models by ensuring that the Issuer and the Verifier do not need to trust the repository, and that the Issuer does not need to know or trust the Verifier. Our software can issue Verifiable Credentials that attest information about users, who can then present the credential enabling claims to be verified. Through the aforementioned engagement with stakeholders, and extensive attention to consumer needs, we have defined user-centered workflows that vulnerable users may encounter when trying to access financial services. In order to assert claims about vulnerability criteria, a new credential type called ***VulnerabilityStatusCredential*** is defined, with schema built by extending existing vocabulary already available on the web at schema.org. We conducted interviews with partners in the financial industry who would verify these credentials to understand how they intend to request and consume them. To ensure

[5] https://www.thenewvulnerable.com
[6] https://www.w3.org/TR/did-core/
[7] https://www.w3.org/TR/vc-data-model/

interoperability of this credential, feedback from these sessions has been used to refine the credential type, schemas, and URIs for future use in the financial industry (see Sections 7 and 8 below).

The architecture leverages services from Microsoft that facilitate the creation, storage, and presentation of Verifiable Credentials on the Identity Overlay Network (ION)[8], which is a public DID overlay network. Two associated Node.js applications have been developed using the Microsoft VC Software Development Kit (SDK) that issue VCs to end users and verify VCs from end users. We now turn to discuss the second stage of expert interviews, evaluation of the prototype proposition, and recommendations from this project.

7. EXPERT INTERVIEWS

We had good access to stakeholders involved in technology, vulnerable customer engagement and financial inclusion aspects of the finance industry, such access is often a major barrier for research. The expert stakeholders agreed to conduct interviews to evaluate the VC prototype described in Section 6.[9] We conducted the semi-structured recorded interviews via Zoom because of Covid-19 restrictions, during the period May to June 2021[10]. Consent forms were distributed, signed, and returned prior to the interviews taking place (see Appendix I in (Elliott et al., 2021)). We used a cross-section of representative participants in the financial industry, as suggested by Denis et al., (2001). For availability and confidentiality reasons, we focused on five experts, details of their demographic information are displayed in Table 1 below, maintaining anonymity.

***Table 1**:* Financial Inclusion Experts (N=5)

Gender	Age	Education Level	Tenure in Finance
Female1	50+	MLIA (Dip) Finance	+40 years
Male1	50+	HND Business	+20 years
Male2	40+	Bachelor's degree	+15-20 years
Male3	40+	Post-graduate degree	+20 years

[8] https://github.com/decentralized-identity/ion

[9] Yin (2011) identifies gatekeepers who provide access and facilitation for qualitative research.

[10] Delays incurred due to the Covid-19 pandemic.

Female2	50+	Post-graduate degree	+20 years

Each interview lasted for approximately one hour with some variation, following the protocol designed by the team (see Appendix II in (Elliott et al., 2021)). We started our interviews by requesting participants to describe their experience within the financial industry. Next, presented the FCAs four characteristics driving vulnerability and walked participants through the verification architecture and process from the individual perspective, culminating in Figure 1, below. In short, the National Health Service (NHS, in our example) *issues* a credential. This credential (among other information) holds some attributes (date of birth, test date, disability, etc.). These attributes can be used to make claims about the holder (e.g., age > 18). The verifier (i.e. a bank) makes a request in order to *verify* a claim (i.e. enough information for a specific claim). We explained the caveat, that the Microsoft ION technology only permits the sharing of a full credential whereas, selective disclosure (see position paper) posits that only an attribute (or a predicate on an attribute) is required to verify a claim, thus preserving the privacy of the user (a future development). Our subsequent questions focused on evaluating the prototype from the expert's perspective to address our key research questions:

RQ1. How can we promote user adoption of DID and VC technologies in the financial sector?

RQ2. How can we maximise user disclosure of information in a privacy-preserving manner using VCs?

RQ3. How can financial firms use DID/VC technologies efficiently to improve support for vulnerable populations?

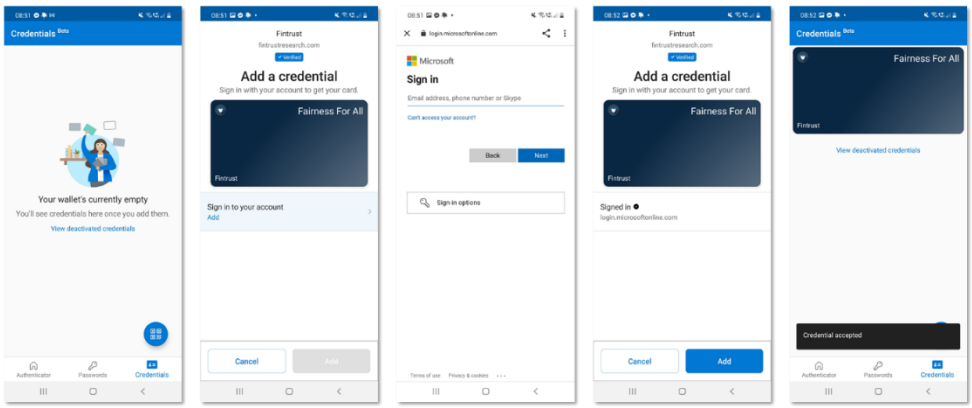

Figure 1: "mock-up" of VCs prototype wallet

Post-interview, the recordings were transcribed and to ensure participants retain maximum control over their information, transcripts were triangulated via verification with interviewees (Gioia et al., 2013). We have anonymised parts of the interviews included in Section 8 below, to

ensure that specific individuals cannot be identified from the data presented. All interviews were conducted by the co-investigator of the research team.

Following Strauss (1987) and Corbin and Strauss (2015), we analysed the subsequent data using a "process" coding approach utilising NVivo software (v.12). This is a cyclical approach, where the general meaning of the discussions conducted within the semi-structured interviews is initially categorised (initiation), structured around specific themes (focus) and then reviewed and encoded (axial coding). All the material was reviewed to check that we had grasped what was significant to the interviewee (respondent validation; see Charmaz, 2014). Subsequently, items were reduced into a more manageable form of themes or "sets" (Gioia et al., 2013). To further enhance the validity of our findings, we include in the results and discussion extensive verbatim descriptions of the expert's views, to reduce the impact of our own biases. Nevertheless, given that our study includes only a small number of expert interviews (N=5), we recognise concerns about validity remain justified and further work is certainly needed to generalise from the results. It was our intention to conduct focus groups and interviews with charities whose clientele experience financial vulnerability. However, the impact of Covid-19 delayed planned data collection, this is scheduled to take place post-conclusion of this project. We now present the findings of the expert interviews and conclude the report with recommendations.

8. FINDINGS

This section presents the participant responses to the DID/VC presentation premised on the expert's experience within the financial services sector specifically, seeking to improve vulnerability support and promote financial inclusion using technological solutions. Participants were asked to consider the question from both a business and community/individual perspective.

8.1. How can we promote user adoption of DID and VC technologies in the financial sector?

The challenge for the experts in terms of promoting adoption of the technologies in the financial sector is two-fold. First, persuading mainstream and alternate stakeholders that technologies would bring return on investment in investing in the technologies, training staff etcetera. Second, gaining the trust of customers to understand and use the application (e.g., a wallet function) to share credentials in the manner described in the prototype presentation. One expert, expressed concern that stakeholders would be reluctant to promote the technologies unless the regulators provided a clear indication that such innovation was recommended (at present the FCA vulnerability report is guidance not compulsory):

> "[I]t's also getting the FCA to acknowledge, approve, enhance their own requirements from a regulatory perspective for this, the adoption of this [technology]. I think that's absolutely key because as I say whether it's a fully regulated bank or a FinTech, who is sponsored by another third party, another issuer, how many of them are operating in this space? They won't move until the FCA has given its blessing and acknowledges and even promotes the application…But, I think even to pilot something, such as this would be very, very hard to do without the FCA approval"

(Male2, brackets added)

Both industry stakeholders and regulators are included in this description, thus, communication needs to be both internally to the stakeholders and to the broader general public by the FCA to facilitate and promote engagement with the technologies and associated benefits. The complexity added by these broader social actors therefore needs to be accounted for in relation to adoption via future collaboration with industry and regulators.

A further challenge was raised in terms of the financial stakeholders gathering information via such technologies and the customers being able to trust this party to ensure their data remained safe:

> "The banks haven't served the wider community well from the financial crash. And the whole reason why we've got open banking is to create more competition for all…if they [banks] are given information about a user and do you remember when aids was a big thing…people wanted to keep HIV private…if they had to disclose it from for a mortgage and things like that, and people didn't want to disclose it...with the credentials is, it depends what's in there...[t]rust is everything. And…fairness for all sounds trustworthy. I think it's a great title for it"
>
> (Female2, brackets added)

The challenge is compounded by the impact of the Global Financial Crisis (GFC, Pedersen, 2021) and recent instances where financial providers have breached regulatory rules around "know your customer (KYC)" leading to more stringent examination of how providers analyse customer data (i.e. Wirecard scandal).[11] This has resulted in "the issuers, financial institutions and fintechs being particularly… very, very nervous and very risk averse" (Male2) and mistrust by customers. An expert also raised concern over the cyber security aspect from the business perspective which could influence adoption of the technologies:

> "[H]ow do you ensure that I'm not a super-hot tech savvy guy? How do I or how does the bank know that I haven't hacked into it [VC] and have just increased my benefits from 30 pounds a month to 5000?"
>
> (Male2, brackets added)

These extracts show two key issues facing financial services providers and customers' trust in adopting technologies. On the one hand, the perspective to be compliant with the FCA regulatory expectations suggests providers are prepared to reserve caution to meet all users' needs. On the other hand, in adopting technologies to garner more customer information specifically, around sensitive "vulnerable" details, scepticism exists surrounding the banks motives, vested interests (Alford, 1975) and general mistrust of the sector (Edelman, 2019). From an academic perspective, the use of sandbox facilities in conjunction with the Turing Institute aligns with FCA regulations

[11] https://www.bbc.co.uk/news/world-europe-55004864

on technological developments. However, when promoting final versions raises awareness of a potential for resistance to adoption in the socio-technical space from providers and customers.

8.2. How can we maximise user disclosure of information in a privacy-preserving manner using VCs?

For financial services to provide care to vulnerable customers/users, the users will have to first, disclose the information pertaining to their vulnerability to the financial institution. However, as discussed in 8.1, this sector suffers from mistrust amongst customer and the general public (cf. Edelman, 2019) . Therefore, we wanted the experts to consider how we could reassure customers that the technology can move towards the concept of "self-sovereign identity" (Der et al., 2017) permitting the customer to control the disclosure of vulnerabilities to the financial institution. As part of the protocol, we asked the experts to reflect on two scenarios regarding facilitating disclosure afforded by the technology.

Scenario 1 purported that a national vulnerability scheme, e.g., the 'Fairness for All' scheme is approved and initiated by the FCA. In short, issuers of a verifiable credential may include financial firms, other firms (e.g. the NHS, universities) and professional individuals (e.g. private doctors). For example, after a visit to the NHS, the NHS will issue the "normal" VC with all the information that would be included in an NHS certificate, as well as a "Fairness for All" VC that has limited information (attributes) and is only intended to be shared with financial institutions. Thus, the 'Fairness for All' VC may say that the VC holder is not able to work for the next two months due to a disability but, will not disclose any further details about the disability. When the customer interacts with a bank, the bank simply asks for any 'Fairness for All' VCs with a message like "The bank would like access to your credentials based on the Fairness for All scheme – Accept Y/N" and the customer can decide whether to present the VC to the bank.

Scenario 2 concerned no public scheme exists as described above. Instead, when a customer interacts with a bank, a general mobile wallet application opens, and a request may appear as 'The bank would like access to your verifiable credential repository for the following information: Are you >= 18 years? Do you have a physical disability? Do you have mental health problems? And so forth, Grant access Y/N?" (see Appendix II in (Elliott et al., 2021)). We sought the experts' opinion on how best to communicate such questions, tenets of the scheme, the process, and benefits in preserving vulnerable information to the customer/user groups? Furthermore, based on the discussions featured in Section 4, would consideration of a "vulnerability flag" or "score" be appropriate for both financial institution and customer vulnerability disclosure needs?

In response, one expert felt that current systems provided under the open banking system introduced over the past five years in the financial sector could assist in the demonstration of benefits of disclosure (Omarini, 2018):

> "[W]hen you're talking about people being reluctant to identify themselves as…a vulnerability event. I was thinking…GDPR, there are different rules on the data and security. For example…we have basic, often very, very basic information on members, but if we started to ask questions such as and more personal questions around…whatever it is that is deemed to be sensitive data, then

> that increases data stored…I'm thinking maybe this is open banking at one level, and then maybe there's little offshoots of that, where almost, it's like an option, you can opt into providing the other information that's needed…saying this vulnerability factor?"
>
> (Female1)

In addition, the linkage between the move towards open banking and eventually open life was highlighted in communicating to customers/users the benefits of disclosure to improve individual financial journeys (Sclove, 2020):

> "A good comms plan around it [technology] to make it user friendly for everybody to understand. But it's pretty intuitive and I think that it could be adopted, I like the thinking about it from a comms point of view, fairness for all, because it's so important now that we have this democracy of life, but also, democracy of technology"
>
> (Female2, brackets added)

Specifically, examining the technological use case and benefits, an expert espoused their perspective on VC technologies and the eventual progress to self-sovereign identities:

> "There shouldn't be any difference between someone that is vulnerable or disabled, as tech enables people to be augmented with more conforming to normality, because tech starts to take those disadvantages away…you can promote being vulnerable [using this technology] in a way that is now enabling better service and better support"
>
> (Male1, brackets added)

Furthermore, stating that we should examine history to learn lessons from disability and vulnerability disclosure schemes without revealing the "full" credential, Male1 responded "I'll use the disabled blue badge[12] and the sunflower lanyard[13] examples – how do we modernize that, my experience with the blue badge, if I'm disabled, is all predicated on me being able to get access and fair access". Hence, as suggested, in future iterations, garnering trust and understanding within communities who already access the above schemes where credential attributes are commonplace, could assist in championing and advocating the benefits of using VC technologies. In short, the digitisation of the previous schemes to assist vulnerable cohorts.

An expert embedded within marginalised communities further supported the assertion of "vulnerability and inclusion by design" advocated by Male1. Citing that "we work with young people, probably about six to twelve, to do the equivalent of a random control trial (RCT) and saying, look, you know, this is what we want. This would be good to have our group as testers for such technology…you will have the support from people who want to be ambassadors or champions of what you're doing" (Male3). Furthermore, as this cohort utilises social media for communication channels, the expert confirmed their "followers" would trust the communication

[12] https://www.gov.uk/browse/driving/disability-health-condition
[13] https://hiddendisabilitiesstore.com/about-hidden-disabilities-sunflower

and awareness would be generated across the most affected groups promoting engagement with VCs. Similarly, the element of trust was raised as pivotal to engendering uptake of new technologies to cohorts where the presumption is a lack of "tech savviness" (Female1, brackets added). She continued, "we now talk to the majority of our members who do use this open banking, the majority have no problem with it whatsoever. You know, we're not talking on the marginal anymore, people are fine with it. I think because we are trusted with them (customers)".

From these excerpts, the difficulty perceived in relation to how to engage the target marginal and vulnerable groups, shows history and collaboration as a design mechanism to generate trust and adoption is feasible. Whether this causes complexity for the financial institutions who as we found are risk averse in the post-GFC era is beyond the scope of this project but raises areas of research to be explored around the concept of democracy and technology (Sclore, 2020). We turn to our final question.

8.3. How can financial firms use DID/VC technologies efficiently to improve support for vulnerable populations?

Finally, we asked the experts to posit themselves as leading a financial institution and imagining how they could improve the support for vulnerable populations by their organisation. What would be required based on their experience in introducing technologies.

Our expert (Male1) continued with the theme of "vulnerability by design" in advocating taking lessons learned from the development and implementation of open banking which culminated in application programme interfaces (APIs) becoming understood and accepted technologies by financial providers (mainstream and alternative) and customers.[14] He suggested that firms could "start with the principles of open banking, open, trusted custodian convener, independent, mutual, all of those things are not for profit. All those things that engender trust." Simply put, there is a route to implementation not too devoid of the recent open banking experience that applied to VC technology could assist financial firms understand how to better identify and support vulnerable customers. Furthermore, the "digital divide" must also be brought into consideration, the VCs solution is premised on technological access however, a workaround may be revealed in working closer with the communities in this cohort (Male1, 2, 3 and see van Dijk, 2019).

In addition, it was revealed that a mainstream provider had been in discussion with one expert in this regard. "A bank was asking that particular question about just sharing the passport number, nothing else. And by that passport number, it will be read and confirmed by the bank" (Male3). He suggests that the mainstream banks are aware that such technologies are under development and that this change is expected to come hence "very much aware of what's going on" based on this incident. Moreover, if financial providers support using technologies to reduce the stigma of "vulnerabilities" the use of "providing that sense of empowerment" is the key word to garner support from communities and for this question, will improve the mistrust of financial

[14] PSD2 regulation - https://www.fca.org.uk/news/press-releases/fca-finalises-revised-psd2-requirements

institutions to take the lead or collaborate in this space. A point raised where the VCs could pivotally empower a sector in society involving females. As this expert, consults within communities if financial institutions used the VC technologies to afford females a "voice and just…listen[ed] to them, and how they feel about their finances, they want to be, on top of things, generally, even if they haven't got money…this will be welcomed by these women" (ibid.). It could be suggested that the concept of self-sovereign identity releasing attributes of credentials if offered by banks, as reported from this expert, would enable firms to "get this message across, the best way to do it is in the communities where these vulnerable people live and die" (Male1). Likewise, those dealing with vulnerable communities and providing responsible lending, the VC technology was viewed as an "extension of the open banking" innovation and no problems were envisaged in their network of similar providers improving their existing provision in supporting vulnerable customers (Female1). Moreover, all experts viewed the prototype as positive, including the title "Fairness for All" which was tackling the "upstream problems" to design better vulnerability solutions. For the purposes of this report, the main themes created following the process detailed in Section 7, are displayed in Figure 2, below.

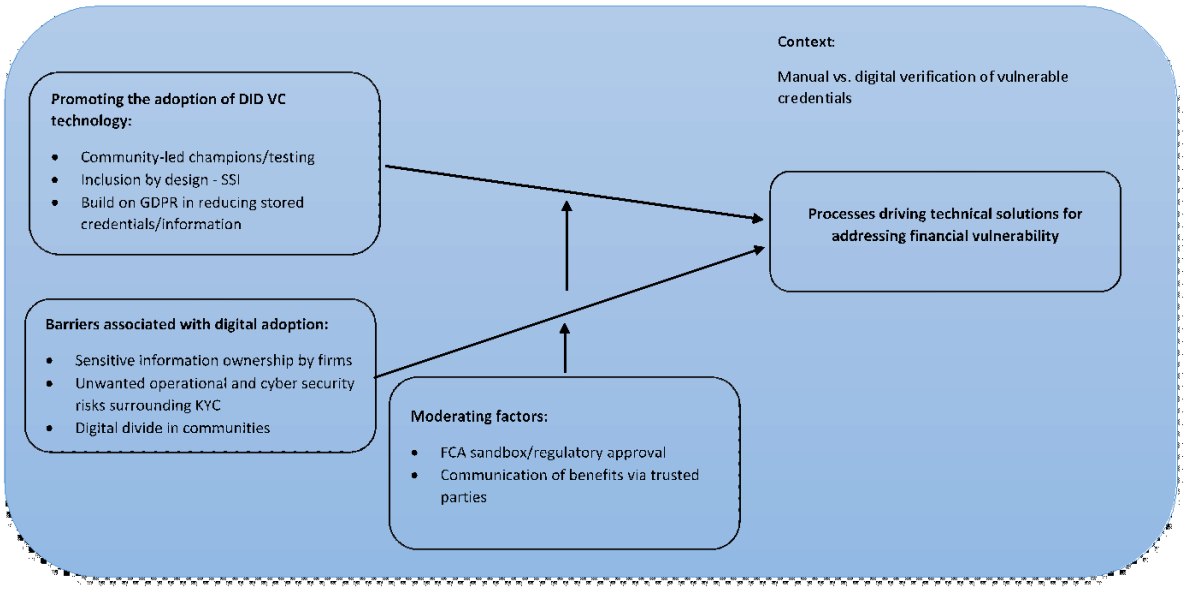

Figure 2: factors affecting procedures for technical solutions addressing financial vulnerability

9. CONCLUSION & RECOMMENDATIONS

This report presents the work performed by the FinTrust team at Newcastle University in examining the potential of combination of Decentralized Identifiers and Verifiable Credentials for the identification of vulnerable consumers in finance, and discusses possible implications that these technologies can have for the provision of tailored financial services and products. The UK financial regulator (FCA) identified the protection of vulnerable customers as a key priority for the industry and has published appropriate guidance for financial firms, strongly encouraging them to treat vulnerable customers fairly. We worked with financial industry stakeholders to

examine the four categories of characteristics that are considered to constitute drivers of financial vulnerability—Health, Life Events, Resilience and Capabilities. Initially, we asked stakeholders what processes were in place to identify and support "vulnerable" customers. What emerged is that current protocols within the mainstream stakeholders are manual, capturing only an estimated 30% of "vulnerable" customers. This leaves an opportunity for technologies to improve identification of vulnerabilities and thus support provided to these groups, and generate broader financial inclusion.

Premised on initial stakeholder insights, we performed a review of associated literature and FCA guidance in producing the position paper (Section 5, (Spiliotopoulos et al., 2021)), simultaneously developing the prototype technical guidance (Section 6, (Horsfall et al., 2021)). Once the prototype was developed and could be illustrated via presentation, a series of stakeholder expert interviews were conducted (Section 7, (Elliott et al., 2021)). The insights in relation to implementing the prototype and projecting towards self-sovereign identities are revealed Section 8 and Figure 2. Simply put, for the wider adoption of these technologies, it is important that the industry seeks both technical and regulatory support from government bodies such as the FCA. A first step was published in February 2021 examining UK digital identity and attributes trust network[15] and discussion of forthcoming FCA sandbox on digital identities in September 2021.[16] Similarly, based on our small sample, the industry can draw from the experience and previous practices of schemes (such as open banking) to increase user uptake of these technologies, we suggested key areas for future research.

Based on the empirical work described in this report and the technology insights obtained from the implementation (see also (Horsfall t al., 2021)), we outline a set of recommendations for researchers and practitioners in the financial sector when considering the combination of DID and VC technologies.

1. The design detailed in (Horsfall et al., 2021) relies on the Microsoft Identity Overlay Network, which has a number of implications with respect to the interoperability that need to be considered when using DiD and VC for financial inclusion or other applications
2. Trust in the DiD and VC software platform requires a deep analysis depending on the use case. For instance, trust in the system requires trust in the credentials and if crednetials can be obtained without strong safeguards, this would weaken the trust one can place in the overall system.. The way credentials are issued may depend on the platform implementation and needs t be thoroughly understood to judge the appropriateness of the solution for a desired application.
3. Following from the previous point, deep analysis of the trust features of DiD and VC software is an urgent and important research topic. Such analysis may demonstrate that additional governance approaches may need to be integrated with DiD/VC platform to assure that trust can be justifiably placed in the services that use the platform.

[15] https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework
[16] https://www.fca.org.uk/firms/regulatory-sandbox/regulatory-sandbox-cohort-7

4. The industry can draw from the experience and practices of previous technological solutions (e.g., open banking) to increase user uptake of these technologies.
5. In terms of Corporate Digital Responsibility, businesses should be upfront to the customers about the use of data, for example by making it clear that they follow GDPR-compliant practices. Similarly, businesses should communicate the benefits of information disclosure, for example by explaining how this information can enable better service and support in a privacy-preserving way. Research methods should consider multiple stakeholder, including but not limited to end-users.
6. As the responsibility is often placed on the user to make decisions about their identity, it is important for researchers to study users' understanding and practices around DIDs and VCs specifically. Similarly, further research is required to gauge users' current understanding and practices around the privacy implications of using DID and VC technologies, as well as to investigate the most suitable way of communicating the privacy benefits of this combination of technologies.

REFERENCES

Alford, R. R. (1975), Health Care Politics: Ideological and Interest Group Barriers to Reform, Chicago, IL: University of Chicago Press.

Charmaz, K. (2014). Constructing grounded theory, 2nd ed., Thousand Oaks, CA: Sage.

Corbin, J., and Strauss, A. (2015). Basics of qualitative research: Techniques and procedures for developing grounded theory, Thousand Oaks, CA: Sage.

Denis, J. L., Lamothe, L., and Langley, A. (2001). The dynamics of collective leadership and strategic change in pluralistic organizations, *Academy of Management Journal*, 44:809–837.

Der, U., Jähnichen, S., and Sürmeli, J. (2017). Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution https://arxiv.org/ftp/arxiv/papers/1712/1712.01767.pdf

Edelman (2019). 19th Annual Trust Barometer: Financial Services. Available at: https://www.edelman.com/research/trust-in-financialservices-2019 (Accessed: 24 June 2019).

Elliott, K., Spiliotopoulos, T., Coopamootoo, K., Horsfall, D., Ng, M., and Van Moorsel (2021), A. *Expert Feedback on Financial Inclusion Project Work,* available from the authors

Financial Conduct Authority. (2021a). Financial Lives 2020 survey: the impact of coronavirus. Retrieved from https://www.fca.org.uk/publication/research/financial-lives-survey-2020.pdf

Financial Conduct Authority. (2021b). Guidance for firms on the fair treatment of vulnerable customers. Retrieved from https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf

Gioia, D. A., Corley, K. G., and Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology, *Organizational Research Methods*, 16:15–31.

Horsfall, D., Van Moorsel, A., Coopamootoo, C. Ng. M., and Spiliotopoulos, T (2021). *Using Verifiable Credentials to identify vulnerable customers in finance--Software Design Specification (SDS) Document*, available from the authors

Omarini, A. E. (2018). Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future, *International Business Research,* 11(9): 23-36.

Pedersen, N. (2021). Financial Technology: Case Studies in FinTech Innovation, London: Kogan Page.

Sclove R. (2020). Democracy and Technology: An Interview with Richard Sclove from Beth Simone Noveck. *Digit. Gov.: Res. Pract.* 1, 1, Article 5: 6 pages. https://doi.org/10.1145/3368273

Spiliotopoulos, T., Horsfall, D., Ng, M., Coopamootoo, K., van Moorsel, A., & Elliott, K. (2021). Identifying and Supporting Financially Vulnerable Consumers in a Privacy-Preserving Manner: A Use Case Using Decentralised Identifiers and Verifiable Credentials. In Designing for New Forms of Vulnerability workshop at CHI 2021. http://arxiv.org/abs/2106.06053

Strauss, A. (1987). Qualitative analysis for social scientists, Cambridge: Cambridge University Press.

van Dijk, J. (2019). The Digital Divide. Cambridge: Polity.

Yin, R. K. (2011). Applications of Case Study Research, Thousand Oaks, CA: Sage.