Please quote as: Göppinger, S. M. M., Meier, A., Elshan, E., Malekan, O. & Leimeister, J. M. (2024). Beyond Trial and Error: Strategic Assessment of Decentralized Identity in US Healthcare. International Conference on Information Systems (ICIS), Bangkok, Thailand.

# Beyond Trial and Error: Strategic Assessment of Decentralized Identity in US Healthcare

*Completed Research Paper*

## Introduction

The healthcare system of the United States (US) is considered inefficient, accounting for a sizeable 18.3% of the country's gross domestic product (GDP) (CMS.gov, 2023). Yet, it ranks lower than many other countries in terms of various performance metrics (Tanzi & Lu, 2018). An immense volume of digital data, from clinical to reimbursement data, circulates through the system, establishing it as a data-driven domain. For effective functioning of the system, these data must be readily and securely accessible, editable, and trustworthy, yet this is currently not the case (Hasselgren et al., 2020). As a result, a range of well-documented issues associated with security, privacy, and confidentiality; data quality; identification, authentication, authorization (IAM); and interoperability have emerged (e.g., López Martínez et al., 2023; Yusof et al., 2008) contributing to the inefficiencies. Besides the widely discussed conflicting interests among healthcare stakeholders (Ozdemir et al., 2011), the equally critical but seemingly neglected issue of inauthentic data can be considered a culprit of impeding seamless data movement.

In technical discourse, authenticity refers to securely attributing data to a source (National Institute of Standards and Technology, n.d.). Securely attributing data to a source means that the data's provenance can be verified and its integrity can be ensured, with integrity defined as data that has not been tampered with, revoked, or expired (Ruff, 2023). Authenticity becomes pertinent only when data is not independently verifiable or when the verification process is costly, as is typically the case in digital interactions to date (Smith, 2021). Thus, as we shift to digital realms, ensuring data authenticity becomes challenging, resulting in surging transaction costs (Timberg, 2015). Decentralized digital identity (ID), or simply decentralized ID[1], enables solutions for the persistent challenge of maintaining trustworthiness over distance, positioning it as a breakthrough for resolving many data flow issues in US healthcare. Although the concept of identity is elusive and definitions vary widely by discipline and context, this paper views ID simply as a means of providing the authenticity of data by uniquely identifying its source or provenance (Ruff, 2023). A source is any identifiable actor, such as individuals, organizations, and software agents (Reed & Sabadello, 2021). The notion of decentralization can be understood as an implementation strategy (Windley, 2023) for providing ID or, in other words, data authenticity. However, emerging information systems (ISs) frequently encounter high deployment failure rates within healthcare (Safi et al., 2018), often due to mismatched use cases or pervasive contextual barriers (e.g., Yaraghi et al., 2015), incurring human, economic, and technological progress costs (e.g., Agarwal et al., 2010; Ammenwerth & Shaw, 2005). This situation is worsened by an increase in the complexity of ISs and their deployment environments (Maylor et al., 2013), such as with decentralized ID, which constitutes a transformation in today's communication infrastructure and its power balances (Preukschat & Reed, 2021). Structured approaches, such as use case assessments, enhance the likelihood of successful IS deployment by amplifying the understanding of what constitutes successful deployment and aiding in the selection of appropriate use cases (Cresswell, 2016).

Despite growing organizational interest in decentralized ID, structured frameworks in this realm remain scarce. To address the lack of systematic, methodological support for practitioners, we propose the following research question (RQ):

> ***RQ:*** *Which socio-technological factors determine the amenability of US healthcare use cases to decentralized ID?*

[1] Often, the term *self-sovereign ID (SSI)* is applied in lieu of decentralized ID. This paper uses the latter term, as decentralized ID encompasses more than just the SSI application, which merely concentrates on autonomy, independence, and censorship resistance (Preukschat & Reed, 2021; Windley, 2023).

To address this RQ, we conducted a Participatory Action Research (PAR) study (Baskerville, 1999). We developed a framework for assessing decentralized ID use cases in US healthcare, utilizing primary data from expert interviews, a survey, a workshop, and an Open Space conference. To that end, this study's main output is the Decentralized ID Amenability Assessment (DIAA) toolkit, which comprises the DIAA framework, a multi-media companion guide, and a live resource wiki, aiding in the population of the framework. The DIAA framework consists of a preparatory stage, followed by two tiers, with the first evaluating the potential suitability of decentralized ID as a solution for a particular use case based on theoretical analysis alone and the second addressing contextual circumstances, acknowledging that while a novel IS may seem fit for purpose, implementation challenges can arise.

From a theoretical perspective, our framework provides a structural and conceptual basis that researchers can adapt and extend to guide empirical research or as a foundation for developing further decision-support systems in decentralized ID by facilitating a better understanding of decentralized ID and the socio-technical change it brings about. From a practical perspective, the framework advances healthcare stakeholders' knowledge of critical components for successful decentralized ID deployment, enhancing informed decision-making and planning of respective decentralized ID projects.

The remainder of the paper is organized as follows: The next section examines decentralized ID as a potential solution for US healthcare data exchange challenges, segueing into exploring this study's related work. Subsequently, the methodological approach for the framework development, grounded in PAR, is articulated. The findings focusing on the DIAA toolkit are then delineated. The discussion includes the contributions of our work to scholarly research and its relevance for US healthcare stakeholders and the decentralized ID community. The paper concludes with a summary and outlook.

## Conceptual Foundations of Decentralized Identity in US Healthcare

There is no universally accepted definition of decentralized ID, and its full range of capabilities remains somewhat obscure (Allen, 2016; Cheesman, 2022). Efforts have been undertaken to outline first principles and architectural considerations for decentralized ID deployment. For instance, Cameron (2005) outlined seven laws essential for the effectiveness of digital ID systems designed to enable secure digital interactions. Additionally, Allen (2016) identified ten principles: control, transparency, portability, consent, existence, access, minimalization, interoperation, persistence, and protection. They have become a reference standard in the field. Lastly, researchers and practitioners, including Mühle et al. (2018), Windley (2023), and the Trust over Internet Protocol (IP) (ToIP) Trust Spanning Protocol Task Force (2023) proposed architectural components of a decentralized ID system. Drawing on this prior scholarly and practical work, a working definition of decentralized ID can be established. It is proposed that:

> Decentralized ID refers to *the concepts, ideas, architectures, processes, and technologies that facilitate authentic digital relationships that are inclusive, instigate power-structure changes, and are collective-action- and network-dependent to reach their full potential.*

This encapsulates three crucial characteristics of decentralized ID. First, decentralized ID allows for *authentic digital relationships* due to its "protocological" (p. 309) nature, as coined by Windley (2023). Instead of relying on a centralized administrative authority, digital interactions are mediated through a protocol. The protocol enables decentralized ID to be heterarchical, or peer-to-peer, rather than hierarchical, which prevents any one actor from controlling the system; private by design; and instantly verifiable. It is *inclusive* due to its unifying nature: It is universally encapsulating, allowing any actor to build a context-specific ID system that can seamlessly interoperate with other context-specific ID systems rooted in the same fundamental components and framework (Windley, 2023). The architectural modularity and flexibility of the system make it easy to enable context-specific ad-hoc decentralized ID use cases. Further, it is posited that inclusiveness is inherent in decentralized ID's description as *concepts, ideas, architectures, processes, and technologies*, which suggests that its implementation is not contingent on a specific technology but on its first principles (Cucko & Turkanovic, 2021), as outlined by Allen (2016), for instance. Due to authentic and inclusive digital relationships, decentralized ID *instigates power-structure changes* from the networks' centers to their edges. The combination of the characteristics of instigating power structure changes and being *collective-action- and network-dependent to reach its full potential* indicates decentralized ID's deployment challenges. Unlike the more traditional model of developing and deploying solutions, where actors independently develop and market a solution that may or may not be for their own use (Christensen, 2013), decentralized ID requires collaboration among multiple actors to address a

complex, shared problem that is beyond any one actor's capabilities to be solved alone. This collaborative approach underscores decentralized ID as more of "an agreement rather than a technology or system" (Windley, 2023, p. 427). Further, scaling decentralized ID across use cases is imperative for its value extraction, as its worth proliferates with greater network capability.

# Related Work

First, we lay out empirical work relevant to the development of a decentralized ID use case assessment framework before discussing our theoretical lens and units of analysis.

## *Empirical Context*

While structured approaches for assessing and selecting use cases are suggested to improve the success rates of ISs (Cresswell, 2016), there is no framework for evaluating use cases for decentralized ID, let alone one customized for healthcare – a sector with numerous domain-specific needs (Burns, 2021). Thus, we consulted broader formative IS deployment frameworks specific to healthcare and decentralized technologies and partner selection and fit frameworks of the inter-organizational relationships' literature, given decentralized ID's success hinging on collaborative action.

Many assessment frameworks for health ISs (e.g., Cresswell et al., 2020; Greenhalgh et al., 2020; Yusof et al., 2008) are derived from generic IS assessment frameworks, such as the IS success model (DeLone & McLean, 1992), the task-technology fit (TTF) model (Goodhue & Thompson, 1995), and the IT-organization fit model (Morton, 1991). These frameworks aim to initiate and guide discussions regarding the deployment of ISs, with a noted preference for qualitative rather than quantitative metrics. Transitioning to decentralized IS assessment frameworks, research appears to be narrowly focused on blockchain. Publicly accessible use case assessment frameworks specific to decentralized ID seem to be non-existent. Blockchain use case assessments range from simple decision trees or flowcharts to complex decision matrices (e.g., Almeshal & Alhogail, 2021). Sidelining the overly simplistic decision trees and flowcharts that lack practical usefulness, Labazova (2019) developed a use case assessment for evaluating blockchain implementations in which she explicitly incorporates the implementation environment, assigning greater importance to ecosystem considerations. Erol et al. (2021) advanced these methods further by integrating a quantitative dimension into their assessments. Lastly, given decentralized ID's collaborative nature, the inter-organizational relationships literature provides partner selection and fit assessments revolving around varying degrees of partner compatibility and fit success factors, including resource complementarity, strategic fit, organizational fit, operational fit, cultural fit, and human fit (e.g., Child et al., 2019; Cummings & Holmberg, 2012). Cummings and Holmberg's (2012) framework for inter-organizational partner selection and fit has been particularly influential, notable for its selection criteria that underscore the significance of acknowledging the dynamic nature of numerous parameters.

## *Actor-Network Theory*

To establish a solid theoretical foundation for the proposed decentralized ID use case assessment framework and elucidate the theoretical grounding of the above-mentioned empirical studies, we undertake a brief review of theories from IS research related to IS deployment. The evaluation of health IS deployment often employs socio-technical approaches, and in this context, our study primarily adopts actor-network theory (ANT) as its key theoretical lens. Additionally, we utilize other theoretical frameworks from IS literature (i.e., theory of the diffusion of innovations, unified theory of acceptance and use of technology, TTF, expectancy theory, institutional theory, theory on alignment and misalignment, theory of institutional logics, network effects theory, theory of social planning, and general theory of action systems) to supplement ANT, addressing its limitations and facilitating theoretical triangulation in our study. ANT aims to unravel how diverse actors connect, making up a unified whole, referred to as a *network*, and how such systems develop and attain temporary equilibrium or the absence thereof. The theory's most controversial assumption is rooted in the principle of general symmetry (i.e., that both human and nonhuman entities are equally considered actors with agency and can cause change in another actor's action) (Law, 1992), rendering it a socio-technical network (Amsterdamska, 1990). ANT posits that the inclusion or exclusion of an actor in the network affects its overall functioning, as observed in technology deployment within

organizations (Callon et al., 1986). The inherent structure of stable networks, typically concealed, becomes noticeable with the introduction of change (*punctionalization*) (Law, 1992). In response, ANT has developed notions like *translation* to decipher the development of networks. Translation involves bridging different actors within a socio-technical network by delineating their roles, establishing the nature of their interactions, and contextualizing their engagement (Callon et al., 1986). ANT is widely applied to explore IS deployments in healthcare (e.g., Cresswell et al., 2011; Cresswell et al., 2010; Doolin & McLeod, 2005), yet it faces significant criticisms. These include the loose definition of its vocabulary, such as *network boundaries* (e.g., Sayes, 2014) (which Latour (1999) defends as intentional to allow for flexible definitions, ensuring ANT's applicability across time and space), neglect of researcher influence on networks, its emphasis on micro-level processes over the macro-context impact on IS adoption (McLean & Hassard, 2004), and its broad, descriptive nature that inadequately explains how exactly actors influence IS introduction within networks (Wacker, 1998). Still, we selected ANT as the theoretical foundation for this study due to its effectiveness in understanding the complex and dynamic nature of reality in healthcare, which involves multiple stakeholders and technologies. This dynamic setting is expected to undergo significant changes by introducing a new IS (Mol, 1999). Further, ANT aids in mapping actors and their relations and acknowledges the existence of multiple realities (Mol, 1999), from which follows that the introduction of ISs is defined by the context in which they are embedded. Lastly, contrary to frequent criticism, ANT enables a granular approach to network analysis, diving into the micro-processes to then permit a broadening of the view to draw more general conclusions about social processes (Cresswell et al., 2010). As a result of the foregoing, ANT seems particularly useful for guiding data collection, as it enables researchers to locate pertinent network actors linked to the IS under investigation and trace their relationships (Cresswell et al., 2010), providing a systematic approach to analysis. To mitigate its shortcomings, we provide precise, study-specific theory-informed definitions of network actors and network boundaries, as intended by ANT proponents (Latour, 1999), recognize and acknowledge our unavertable influence and impact as researchers within PAR (Cresswell et al., 2011), and consult supplementary theoretical lenses to inform the data analysis of IS deployment in US healthcare – a common approach in studies applying ANT (Cresswell et al., 2011) and deemed acceptable in the more general literature, as long as they are compatible and uphold their respective theoretical assumptions (Sovacool & Hess, 2017).

Drawing on ANT and its complementary theoretical approaches facilitates the framing of units of analysis in terms of their level of abstraction and scope. We adopt two primary units of analysis: a use case perspective (setting the level of abstraction) and a system perspective (setting the scope). Use cases describe a set of joint actions or, in other words, a sequence of processes by actors to achieve a certain goal, comprising tasks and dictating the order of these tasks (Jacobson, 2004). Thus, in this study, we define use cases as task- or process-related opportunities for deploying decentralized ID across the US healthcare system. Our approach extends beyond viewing use cases as mere isolated processes or tasks; we analyze them within the broader operational environment of the US healthcare system, which sets the analysis's scope. We aim to examine potential decentralized ID use cases across the entire US healthcare system, including all relevant stakeholder groups, instead of focusing on a sub-section of it. In that context, we categorize *actors* as both human (i.e., individuals, for-profit and non-profit organizations, and federal agencies) and nonhuman (i.e., intermediaries modifying the dynamics among two or more actors such as decentralized technologies) in accordance with ANT principles (Law, 1992; Sayes, 2014). These actors collectively constitute networks, which we refer to as *ecosystems*. Adopting Adner's (2017) ecosystem-as-structure view, which defines ecosystems as structures where actors interact to realize a value proposition, we recognize the need for adaptation in the decentralized ID context, focusing on use cases instead of value propositions. Thus, we present the following ecosystem definition, adjusted from Adner (2017):

> *An* ecosystem is *the alignment structures of the multilateral set of actors that need to interact in order for the use case to materialize and be addressed.*

Tying together these concepts, the healthcare apparatus can be viewed as composed of multiple interdependent ecosystems formed by connecting human and nonhuman actors centered around a specific decentralized ID use case. To complete the picture, so-called *trust boundaries* surround actors. Trust boundaries determine the degree of confidence required by an actor and, accordingly, the level of risk they are prepared to accept to interact with another actor within a specific context (Windley, 2023). While within the trust boundary, the evidence to provide the required confidence is sufficient, appropriate, and persuasive

enough for the evidence-requiring actor to engage in interactions with the evidence-providing actor (Perry, 2021), beyond the trust boundary, it is not. Presently, the requested data to provide the level of confidence required for entering into digital relationships is often inauthentic. As a result, organizations must go to great economic lengths to establish these trust boundaries.

# Methodology

Initially, we specify the research objective and approach in light of the PAR paradigm and then detail the exact steps taken to design a framework for assessing decentralized ID use cases in US healthcare.

## *Positioning the Research Approach in the Action Research Paradigm*

Action research (AR) is a qualitative research approach that comprises a set of practices, including PAR, that seek to bridge the gap between theory and practice to identify actionable solutions to pressing problems faced by a social organization. Action researchers work collaboratively with the affected individuals, who, as collaborators, become an integral part of the study (Baskerville, 1999). Despite its limited representation in IS literature (Peak et al., 2011), this study adopts this interventionist research approach, deemed most effective for methodology development (Baskerville & Wood-Harper, 1996). AR offers a structured framework for testing new techniques and is particularly apt for addressing complex, real-life socio-technical issues, as supported by recent studies. For instance, Engel et al. (2023) used AR to develop and test a model for assessing the amenability of generic use cases to cognitive automation, serving as a methodological guide for our work. Our goal to devise and test a method for determining the amenability of healthcare use cases to decentralized ID, thus makes AR an ideal choice. Within the wide spectrum of AR, this study employs PAR. PAR establishes research subjects as co-researchers, combining the action researchers' expertise in the research methodology and ISs theory with the subjects' practical theory obtained through their experience in the researched environment (Baskerville, 1999).

## *Action Research Stages*

Regardless of its form, AR is conducted in the iterative stages of (1) diagnosing, (2) action planning, (3) action taking, (4) evaluating, and (5) specifying learning (Susman & Evered, 1978). Table 1 provides a detailed account of the specific research steps undertaken in this study in each of the different (P)AR stages.

| **PAR stage** | | **Research steps** |
|---|---|---|
| 1 | Diagnosing | (i) Semi-structured expert interview study and coding (Gläser & Laudel, 2009) with healthcare stakeholders: providers, payers, payviders, federal agencies, health IT vendors, clinical data exchanges, academia, manufacturers, emerging technology companies, and cross-stakeholders (n = 15)<br>(ii) Qualitative patient survey and coding (n = 25) (Gläser & Laudel, 2009) |
| 2 | Action planning | (i) Workshop with eight (healthcare) decentralized ID experts<br>(ii) Eight additional semi-structured decentralized ID and healthcare expert interviews and written feedback from a non-healthcare decentralized ID expert, including first framework feedback<br>(iii) Open Space conference sessions on the framework (n = +40) |
| 3 | Action taking | (i) Six semi-structured briefing interviews with suitable healthcare stakeholders from the diagnosing stage: payvider, federal agency, health IT vendor, manufacturer, emerging technology company, and patient organization<br>(ii) Application of framework in the respective healthcare organizations |
| 4 | Evaluating | (i) Six semi-structured debriefing interviews with healthcare stakeholders from the action-taking stage<br>(ii) Application of framework in the education sector |
| 5 | Specifying learnings | (i) This thesis<br>(ii) DIAA toolkit<br>(iii) PAR result presentations in decentralized ID community |

**Table 1. Overview of the Research Methodology**

Adhering to rigorous AR tradition, we initially established a formal research agreement (Baskerville, 1999). Subsequently, in the diagnosing *(PAR stage 1)*, we sought to identify the key issues hindering the effective implementation of ISs in US healthcare to substantiate the need for a decentralized ID use case assessment

framework. Since decentralized ID has not yet been widely introduced in healthcare or other industries, there are few decentralized ID projects to study. Therefore, the ISs examined were expanded to include those with similar characteristics to decentralized ID. Accordingly, the dependent variable of the diagnosing was defined as *barriers to successful deployment of ISs that share one or more characteristics with decentralized ID*. To avoid the pitfalls of liberal AR, overly focused on implications for subjects while neglecting scientific knowledge production and fiduciary duty to the research community, the problem statement was grounded in theoretical foundations (Baskerville, 1999; Baskerville & Wood-Harper, 1996).

To initiate the PAR project, we selected the PAR team. Using ANT to inform the sampling, we mapped the operations, actors, and relationships within the US healthcare system. Given the study's focus on system-wide use cases, this approach enabled us to pinpoint relevant stakeholder groups and invite their representatives to participate in the research. Candidates were screened according to organization type and size, and by experience, to ensure coverage of all stakeholder groups and diversity, giving the project a broad conceptual basis. By employing this purposeful sampling approach (Patton, 2002), we recruited a PAR team of 15 healthcare experts from 15 US-based healthcare organizations and 25 patients.

Empirical data from the stakeholders on the problem definition and the need for a use-case assessment was gathered through one-on-one semi-structured expert interviews and a qualitative patient survey. In preparation for the data collection, we developed a *hypothetical model of the causal mechanism*, following the approach of Gläser and Laudel (2009). For the semi-structured interviews, following predefined guidelines, we inquired about organizational data types, the primary data flows and problems in the US healthcare system, deployment challenges of health ISs, and implications of failed deployment.

Additionally, to account for the patients' perspective, we conducted a qualitative survey. The decision to carry out a survey instead of undertaking patient interviews and thus diverging from a consistent data collection approach across all stakeholder groups is grounded on Braun et al.'s (2017) assertion that qualitative surveys can offer a broader and more inclusive perspective compared to other methods of qualitative data collection. Further, surveys provide focused data, which is valuable when collaborating with non-experts, such as patients, who may deviate from the primary subject during an interview as they are uncertain of what information to share (Braun & Clarke, 2013).

We selected the study sample from the general US population, assuming that everyone in the US is eventually a patient. We applied a convenience sampling strategy (Patton, 2002), and collected the data through both an electronic and a hard-copy survey. The electronic survey was coded using Qualtrics and administered via Prolific to obtain the desired demographic characteristics of the sample. The hard-copy survey was provided to reduce the sampling bias that relates to the digital divide, which is inherent in online surveys (Agarwal et al., 2009). The survey comprised a set of eight open-ended topic-based questions. The participants provided information on the data they commonly share with various healthcare stakeholders, the issues associated with data collection, their level of trust in these stakeholders, the influencing factors of trust, and how they educate themselves on privacy and security features of technology. Further, they were asked to report the factors that contribute to their trust in technology and their willingness to share their personal health information once for the purpose of inclusion in a system accessible by all healthcare players upon their consent. To account for potential confounding factors, we followed Anderson and Agarwal's (2011) approach, gathering additional information on the respondents' emotions toward their current health status, the number of yearly medical visits, technological proficiency, their exposure to media coverage about security and privacy breaches, and their interest in technological innovation. The survey also included a screening question and collected relevant demographic information, including gender, age, health insurance status, and actual health status as measured by instances of chronic conditions. To minimize the common method bias often found in self-reported data, we adopted procedural mitigation measures exemplified by Anderson and Agarwal (2011). Further, we conducted a pilot test with five study participants, representing 20% of the target sample (i.e., 25). As a result, we slightly modified the survey. The demographics of the sample somewhat reflected that of the US population in terms of gender and age.

We transcribed the interviews, prepared the qualitative survey data in Excel, and extracted, processed, and analyzed the data from both collection methods, in accordance with the qualitative content analysis method developed by Gläser and Laudel (2009), which is considered particularly well-suited for expert interviews. We used the same coding approach for the survey to ensure coherence. We shared the findings with the interview partners, asked for feedback to rectify any misconceptions, and inquired about supplementary information that could be useful in the subsequent action-planning stage.

In the action planning *(PAR stage 2)*, the PAR team, guided by theoretical and conceptual frameworks, planned the solution to the problem identified in the diagnosing stage. The goal of change was to equip healthcare decision-makers with the ability to assess the amenability of specific processes or tasks to decentralized ID, initially prioritize those use cases that are less resistant to decentralized ID, and anticipate and address potential deployment challenges to reduce the likelihood of failure. Thus, in search of decentralized ID-specific amenability factors (AFs) that explain and predict the likelihood of successful deployment of decentralized ID, we set the *amenability of healthcare use cases to decentralized ID* as the dependent variable. Successful deployment was measured in terms of *system-wide adoption* and *value-adding use* within a set timeframe. This indexing was motivated by the fact that the literature commonly describes socio-technical change in terms of an actor adopting and utilizing technology (Sovacool & Hess, 2017). System-wide adoption was determined by *perceived critical mass*: The point at which decentralized ID adoption decision-makers and users have the perception of whether the decentralized ID solution has a critical mass of users through interactions with others (Lou et al., 2000). However, since adoption does not guarantee an IS's value-adding use (Lin et al., 2019; Ozdemir et al., 2011), value-adding use served as a second parameter, which refers to the realization of an IS's maximum potential within a specific context upon adoption. We selected a virtual workshop as the setting for the action-planning stage to emphasize the participatory aspect of PAR. In preparation, we researched theories related to the adoption and use of new technologies. This research supplemented a review of current formative IS use case assessments, both generic, healthcare- and decentralized technology-specific, and partner selection and fit frameworks for inter-organizational collaboration. Drawing on this scholarly work and the theory-informed problem statement that resulted from the diagnosing stage, we identified an initial set of constructs for a decentralized ID use case assessment framework. The workshop aimed to contextualize this initial set by identifying decentralized ID-specific constructs. Considering the nascency of decentralized ID, we expanded our PAR team by adding five decentralized ID experts, bringing the total to eight. Six of the eight decentralized ID experts also had a background in healthcare, while the remaining two came from other industries. Following the workshop, the developed decentralized ID use case assessment framework underwent multiple initial evaluation rounds. First, we conducted five additional individual 60-minute interviews with decentralized ID experts from the extended PAR team. Second, we presented the framework to three external decentralized ID and healthcare experts for feedback through interviews of similar length. Another expert offered written feedback due to time constraints. Third, we convened two sessions at the Internet Identity Workshop (IIW) 37 in Mountain View, California, where experts around all things related to digital ID gather bi-annually, to discuss the DIAA framework. Together, these initial framework evaluations served as a *proof-of-concept*, following Nunamaker et al. (2015), and sought to discern the comprehensiveness, ease of understanding, and potential practical usefulness of the framework. We incorporated the suggested improvements into the subsequent drafts of the framework.

We approached the workshop's empirical data analysis analogously to the healthcare expert interviews of the diagnosing stage. The hypothetical model and search grid were adjusted, such that they reflected the constructs identified in the review process of existing formative IS use case assessment frameworks. Using the logic of extant formative IS assessment frameworks, we sorted the long list of constructs into two groups: critical assessing and comprehensive assessing constructs of decentralized ID amenability. We consolidated the longlist of constructs, which resulted in a use case assessment framework for decentralized ID that encompasses the most relevant constructs in light of current literature.

In the action taking *(PAR stage 3)*, the planned action is put into effect to solve the issues identified during the diagnosing (Baskerville, 1999). In the context of this research study, the developed assessment framework was applied across six US healthcare stakeholder groups. The objectives were to test its effectiveness, usefulness, and user-friendliness and whether any patterns could be discerned in terms of use case amenability. Not all healthcare stakeholders of the diagnosing stage took part in the action taking. The developed use case evaluation framework is beneficial only to the core healthcare stakeholder groups and not to those in supporting functions such as academia or consulting. Further, the framework's intended audience is organizations, not individuals, as specified below; thus, we consulted a patient organization instead of individual patients. Lastly, certain stakeholders were under severe time constraints, necessitating a replacement. The action taking took the form of 30-minute briefing calls with the representative of each stakeholder group to provide an overview of decentralized ID, explain the framework, and discuss potential use cases for decentralized ID applications in their organizations, settling on one upon which to test the framework. Subsequently, the stakeholders received the framework as an analytical tool in Excel format and

a companion guide as a textual reference manual to facilitate the assessment. They had approximately one week to complete the framework in their own time, allowing for potential team discussions.

Upon completion of the intervention phase, an evaluation *(PAR stage 4)* of its results is to be conducted (Baskerville, 1999). Concerning this study, we held separate 15-minute to one-hour debriefing calls with each action-taking participant to assess the framework's usability and discuss the outcome of the DIAA framework. If the study participants were pressed for time, written feedback was used as a substitute for an interview. Additionally, to demonstrate the applicability of the DIAA framework in non-healthcare domains, we are currently examining it in the skills-based hiring and advancement sector. This sector-external evaluation may lead to derivative decentralized ID use case assessment frameworks.

While throughout the entire PAR process, the PAR team must remain informed and up to date on the latest insights from the study, the final phase *(PAR stage 5)* involves explicitly documenting the lessons learned and sharing them with the scientific research community and the PAR team (Baskerville, 1999; Baskerville & Wood-Harper, 1996). Following this ethos, we shared the acquired knowledge with the IS research community, the US healthcare system stakeholders, and the decentralized ID community. The PAR study culminated in the creation of this paper for the IS research community and the DIAA toolkit for practitioners. Further, we presented the study's findings in working groups of the decentralized ID community, including the Credentials Community Group of the World Wide Web Consortium (W3C).

## Results

Figure 1 presents the resulting main artifact of this paper, the DIAA framework. It supports practitioners (i.e., US healthcare organizations, including for-profit companies, not-for-profit institutions, and federal agencies) and researchers in qualitatively and, to some degree, quantitatively evaluating the amenability of healthcare use cases to decentralized ID during the early stages of decentralized ID exploration. It is accompanied by a multi-media companion guide in the form of a textual reference manual and a screencast intended to introduce the framework and assist in navigating it, and a live resource wiki, offering supplementary resources to aid in populating the framework and provide a jumpstart for potential decentralized ID implementation.

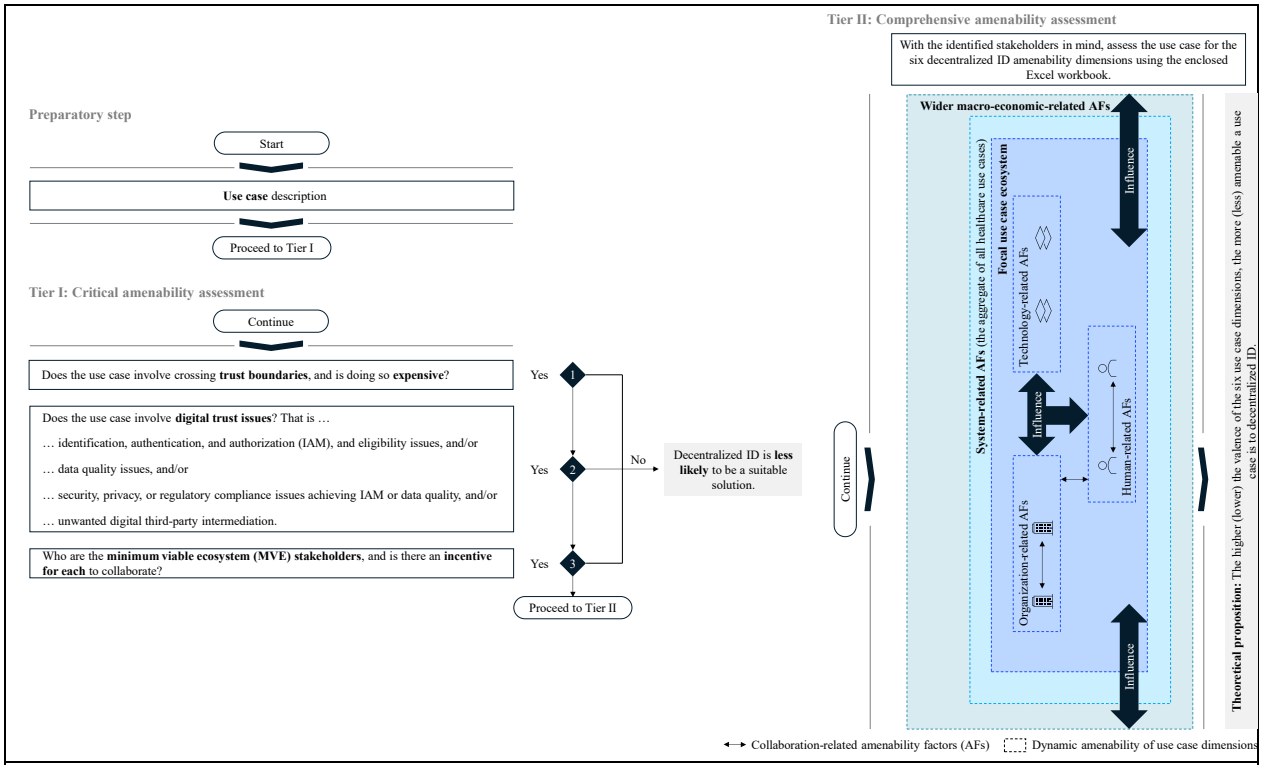


**Figure 1. The DIAA Framework**

The empirical study revealed a total of 77 standardized socio-technical AFs that need to be considered when assessing use cases' characteristics for their amenability to decentralized ID. These AFs were categorized into two separate tiers: the *critical amenability assessment* and the *comprehensive amenability assessment*. The AFs in the first tier evaluate the appropriateness of applying decentralized ID for a healthcare use case based solely on theoretical effectiveness. The second-tier AFs consider contextual factors, acknowledging that although a socio-technological innovation might seem promising in theory, practical challenges may emerge during its implementation (Flessa & Huebner, 2021). The division into two tiers offers an early assessment exit point. If Tier I yields negative results, it is not recommended to advance to the deeper use case evaluation of Tier II. The latter tier makes the amenability of use cases quantitatively measurable and offers in-depth qualitative insights into the use cases that are potential decentralized ID candidates. This tier is structured around six use case dimensions that primary data collection and prior scholarship studies have shown to be relevant for assessing decentralized ID amenability. Tier II is founded upon the following theoretical proposition:

> *The higher (lower) the valence of the six use case dimensions, the more (less) amenable a use case is to decentralized ID.*

The dependent variable *amenability of US healthcare use cases to decentralized ID* should be viewed as a matter of degree, not kind, as it is continuous and not discrete. Hence, a negative assessment outcome does not imply that the use case is not amenable to decentralized ID but rather that positive outcomes signify greater amenability and, thus, a higher likelihood of system-wide, value-adding deployment. A use case's amenability can also evolve since its parameters might change over time. The assessment is intended to be completed through a collaborative effort between two organizational divisions – as applicable: a technology division, knowledgeable about the organization's IS (henceforth referred to as *Tech Division*) and a commercial division, knowledgeable about the market in which the organization operates (henceforth referred to as *Commercial Division*). While these two divisions may conduct the assessment together in one sitting, its format allows for asynchronous collaboration. Provided that the assessment results are promising, the findings can be presented to the organization's senior executives or analogous positions for further discussion. Following that, it is recommended to engage in conversations with other *minimum viable ecosystem* (MVE) stakeholders – that is, all actors integral for the respective use case to materialize and be addressed – to explore the decentralized ID concept and its potential applicability since successful deployment usually depends on collective action and network effects, as highlighted above.

### *Preparation and Critical Amenability Assessment*

The framework opens by prompting the organization to articulate the use case it aims to explore as a preparatory step. A precise description of the use case facilitates the assessment by providing clear use case delineations, which is particularly useful given that two different divisions may populate the framework asynchronously. The responsibility for writing the use case description depends on its origin. If the endeavor is initiated by the Tech Division, that division is responsible for preparing the use case description. Conversely, if initiated by the Commercial Division, that task falls on it.

The completion of the preparatory phase leads to Tier I, which allows organizations to efficiently assess the theoretical suitability of decentralized ID for a specific use case. Critical evaluation questions are utilized to achieve this. Three sections are presented in a flowchart format, posing yes/no queries largely. Advancement to Tier II of the framework requires at least one positive answer in each section. The first two sections are directed toward the Tech Division, as they contain more technical questions. The last section is directed toward the Commercial Division, as it pertains to the dynamics of the healthcare market. The first decision point examines whether a use case involves the transfer of digital trustworthiness across trust boundaries, introducing the concept of trust boundaries discussed above. Investing in decentralized ID infrastructure may prove cost-effective in the long run for stakeholders who find trust boundary establishment and maintenance costly by providing authentic data that increases confidence and facilitates trustworthy digital interactions, as demonstrated in one of the post-workshop follow-up interviews:

> *[With decentralized ID, I can now with the] same small cost … verify that or create that confidence. The economic cost is now a sub-second software thing that does it digitally …, verifies a cryptographic signature, versus me hiring a set of people that makes phone calls and sends emails to people to say, 'Hey, did this person really do with you what they say here [that] they did?'* (Interview E1_APII)

While decentralized ID infrastructure may be employed by actors within a trust boundary, the high upfront investment associated with its introduction may not be justifiable in an environment where a centralized technological solution would suffice. Echoing the sentiments of others, one workshop participant expressed, *"'is it a problem that is shared within his [chief executive officer (CEO)'s] network by the other CEOs?' Because if it is only his problem, then he can probably solve it with some central standard technology"* (Workshop E2_APII). Thus, the framework is directed toward use cases involving multiple organizations rather than those limited to a single organization.

Proceeding to decision point two, this framework section explores whether the focal organization encounters any relevant digital trust issues that could be resolved by decentralized ID. The digital trust issue's *relevance* threshold is subjective to the assessing organization's use case. It refers to the costs (e.g., financial expenditures, time expended, and effect on user satisfaction) associated with the organization's current way of (1) verifying and proving ID, authenticity, authorization, and eligibility and (2) achieving use-case-appropriate data quality (3) in a secure, privacy-preserving, and regulatory-compliant manner. Lastly, this section inquires about the organization's use and preference for interaction intermediaries, as they often play a role in establishing and maintaining trust boundaries. Together, these sections on digital trust queries essentially represent US healthcare's primary data flow concerns.

The terminal section of Tier I focuses on addressing the collaborative-action- and network-dependent characteristics of decentralized ID, making it more relevant to the Commercial Division. Effective decentralized ID use cases involve multiple actors facing the digital trust issue in question. Therefore, this section prompts organizations to compile a list of the MVE stakeholders. Based on that list, they are asked to evaluate whether each MVE participant has an incentive to collaborate in jointly tackling the use case. If there are no incentives, persuading MVE stakeholders, particularly direct competitors, to participate in the initiative may prove to be an insurmountable task.

### *Comprehensive Amenability Assessment*

Provided that a use case is theoretically a good fit for decentralized ID, the next level of examination introduces the various contextual factors that may impede its successful deployment. The study's methodological approach revealed six mutually influencing socio-technical dimensions that determine a use case's amenability to decentralized ID: human-related, organization-related, and technology-related use case dimensions at the micro level; system-related and collaboration-related use case dimensions at the meso level; and wider macro-economic-related use case dimensions at the macro level. An additional but separate seventh cross-cutting temporal dimension considers how these evolve. The six use case dimensions are described by a collective total of 61 AFs. Each AF is traceable back to prior scholarly work and insights derived from the primary data collection. Following Maylor et al.'s (2013) approach, where relevant, the AFs are formulated as challenges to ascertain the extent to which a given use case conforms to the determinants of successful decentralized ID deployment. For example, instead of prompting, "There *is* a clear organizational understanding of what decentralized ID can and cannot do," the AF asks, "The organization *can* be clearly informed about what decentralized ID can and cannot do." A negative response to this statement represents a non-trivial challenge, revealing low amenability to decentralized ID deployment along that AF. Similar to Tier I, some AFs are targeted toward the Tech Division and some toward the Commercial Division. The Tech Division exclusively handles the technology-related use case dimension, while the Commercial Division, with healthcare market knowledge, exclusively addresses the organization-related, system-related, and macro-economic-related use case dimensions. Both the human-related and collaboration-related use case dimensions contain individual AFs for each respective division.

In terms of determining the valence of a use case's amenability to decentralized ID, each AF is rated with respect to how well a use case aligns with the statement described by each of the AFs. The rating scale ranges from -2 to 2, with one-unit increments, where a rating of -2 indicates strong misalignment, 0 is neutral, and 2 denotes strong alignment. To ensure the framework's flexible application across various use cases and account for an organization's dynamic context, flexibility is considered in two ways. First, practitioners assign a weight to each AF that, based on their best judgment, reflects its relative relevance to the use case. Second, the six use case dimensions are balanced against one another to reflect their relative relevance to the use case, resulting in a final amenability score. A final score of 0 corresponds to a factor of 1. In accordance with the theoretical proposition, a final score above 0 corresponds to a factor above 1, indicating an amplification of a use case's amenability. Conversely, a final score below 0 corresponds to a factor below

1, suggesting a reduction in a use case's amenability to decentralized ID. An amenability summary chart portrays the amenability scores of each use case dimension, with an exemplary chart showcased in Figure 2. Although the manifestation of these dimensions may be subject to change over time, the quantitative component of the tool is static. The absence of dynamic scoring resulted from the action-taking and evaluation phases, in which practitioners emphasized the need to streamline the tool's complexity. Nonetheless, to still account for dynamism in decentralized ID projects, a time factor was qualitatively incorporated by prompting organizations to contemplate and record expected future changes for each AF.

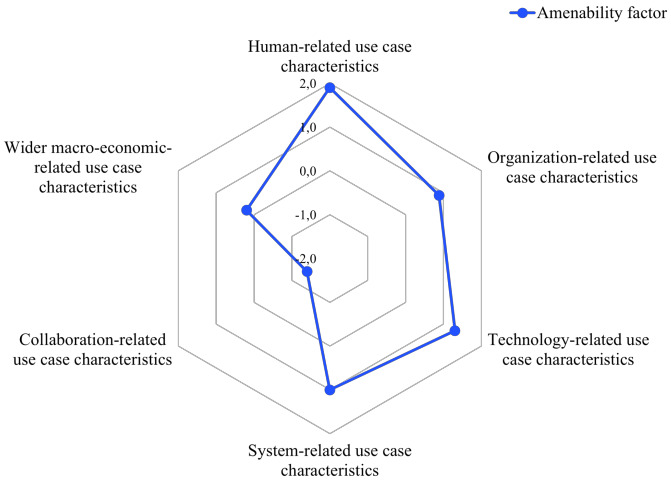


**Figure 2. Exemplary Amenability Summary Chart**

In the following, the six dimensions and their corresponding AFs are presented in turn. On the micro-level, the dimension of human-related use case characteristics deals with AFs at the level of organizational IS decision-makers and end-users of a potential decentralized ID solution. The definition of an end-user varies depending on the use case. For instance, in the case of a front-end application of decentralized ID, the adopter and user system may refer to healthcare professionals, patients, or caregivers. For back-end implementations, there is typically no tangible end-user, rendering this use case dimension inconsequential. The adoption of decentralized ID may encounter resistance from decision-makers or end-users who have had negative experiences with similar ISs or if certain job positions are to be reevaluated, potentially impacting their necessity in a decentralized ID-adjusted structure. Further, end-users may be hesitant toward the new system if it is expected to change or increase their workflow or workload, respectively, in the case of healthcare professional-facing solutions, or if additional work is required from patients and caregivers in the case of patient-facing solutions. This dimension also includes perceived security and compliance concerns, which appear to significantly influence the likelihood of adoption, regardless of the decentralized ID's objective security and compliance features and capabilities. Lastly, this dimension considers whether end-users can participate in the design of decentralized ID applications and whether the generational divide can be addressed, increasing a use case's amenability.

The dimension of organization-related use case characteristics focuses on an organization's capacity and readiness for decentralized ID infrastructure. For an organization to effectively manage the deployment of a system that fundamentally alters its infrastructure, the endeavor ought to align with its strategy, and the organization ought to possess the necessary resources, educate its employees on the capabilities and the limitations of this novel IS, obtain internal sponsorship, demonstrate risk tolerance, and display a willingness to collaborate with and rely on other stakeholders. Further, despite the shift in data handling paradigms, it was found crucial that the project does not necessitate significant organizational and cultural changes or an overhaul of the operating processes. Additionally, an organization should be able to make adoption decisions independently, without relying on confirmation from other companies, as is often the case with providers who are at the mercy of health IT vendors; adjust its investment appraisal frameworks to enable comparison of premises, such as decentralized ID, with alternative, more conventional investments that are easier to stack-rank based on a clear return on investment; and modify its expectations of an immediate change and instead adopt a phased approach to realizing the benefits of decentralized ID.

The technology-related use case characteristics dimension examines the technical aspects of decentralized ID deployment. It involves assessing the technical maturity and planned properties of decentralized ID solutions, the organization's current tech stack and operations, and the necessary technical knowledge and support for utilizing a decentralized ID solution. The technology dimension also assesses whether the use case involves a front-end or back-end application. As discussed above, for a mere back-end application, end-user adoption is less of a concern, increasing the likelihood of successful deployment due to reduced exposure to potential resistance to adoption and usage.

Widening the perspective to the meso-level, the dimension of system-related use case characteristics considers the dynamics of the US healthcare system affecting the use case at large. The focal point of this expanded context relates to the prevalence of the identified digital trust issues among healthcare stakeholders, the market's demand for remedies to such concerns, and the requirement for the existence of a decentralized ID infrastructure from business partners. The more widespread the issues, the more probable it is to convince other stakeholders to cooperate on a resolution. Similarly, if customers are requesting solutions to problems that decentralized ID appears to be a natural fit for solving, or if business partners who have adopted decentralized ID are urging the focal organization to adopt such systems as well for seamless integration, an increase in the amenability of a use case for decentralized ID is suggested.

The dimension of collaboration-related use case characteristics pertains to the inter-organizational relationships that appear to be critical for initiating efforts to tackle the use case with decentralized ID infrastructure and achieving a fully functional, scalable, and ubiquitous solution. Many of the collaboration-related AFs are not novel to decentralized ID; they are frequently present in partner selection and fit frameworks described in the literature on inter-organizational relationships. For instance, collaboration-related AFs include the compatibility of the MVE stakeholders' resources, strategies, cognitions, organizational structures, operations, cultures, employees' backgrounds and experiences, and tech stacks. Additionally, it is important for MVE stakeholders to share a common vision and scope of the project, possess similar innovation capabilities, including budget availability, and be willing to collaborate on an equal footing to ensure proportional risk and output based on respective inputs. Other factors to consider are MVE risk aversion, anticipated changes in power structure and disintermediation, perverse incentives, and competing interests. If these factors register high and prove intractable, they are expected to decrease a use case's amenability. Given the importance of mandates and enforcement in healthcare, regulatory interest and support play a crucial role as well.

Lastly, on the macro-level, the dimension of wider macro-economic use case characteristics opens the lens even further by considering the broader non-healthcare institutional and sociocultural context. This domain covers the media and public perception of decentralized ID, whereby a positive opinion of decentralized technologies is beneficial for successful deployment. It also covers federal and state regulatory frameworks – not limited to the healthcare sector – which are frequently in conflict with each other, thereby possibly impeding the effective deployment of decentralized ID infrastructure.

Overall, it bears to mention that the use case dimensions are interrelated, as is typical for socio-technical systems. A certain rating in one dimension will frequently impact those in others. For example, in the case of a back-end decentralized ID application, many of the human-related AFs become irrelevant.

## Discussion

Having developed, operationalized, tested, and evaluated a first-of-its-kind decentralized ID use case assessment framework for healthcare organizations to select suitable use cases, we strive to make the following contributions to research and practice while also acknowledging this work's limitations.

Regarding theoretical implications, this study situates itself in the emerging academic discourse on decentralized ID, drawing from the literature on ISs, health services, and inter-organizational collaboration. As for prior empirical work, the assessment framework draws inspiration for its logic and structure from formative (health) IS assessment frameworks, decentralized IS suitability frameworks, and partner selection and fit frameworks for inter-organizational collaboration discussed above. For instance, it adopts those frameworks' thought processes of tier structuring, models their flexibility and shift from static to dynamic assessment tools by considering the evolution of a use case's AFs over time – even if only in a qualitative manner – and takes guidance for categorizing the AFs. Further, prior empirical work enhanced this study conceptually by drawing indicators and constructs from this scholarly work, providing a frame for anchoring

the empirical data. This study's framework exceeds the constraints of prior models, maintaining both depth and breadth. While not making this trade-off naturally leads to a longer, more complex framework, which Cresswell et al. (2020) criticize for diluting a tool's utility, we accept this point of critique since decentralized ID is a novel concept that is inherently intricate and lacks intuitiveness for the uninitiated. Lastly, this study's numeric scoring system advances present health IS assessments. While some practitioners may have concerns about quantifying such rather subjective evaluation processes, Cummings and Holmberg (2012) suggest that some form of quantification can aid in revealing and examining underlying assumptions, particularly in the early stages of potential undertakings.

Pertaining to the study's contribution to the theoretical knowledge base, first, it complements and further specifies prior theoretical efforts to explain decentralized ID by presenting its purpose, definition, and distinguishing attributes. The pursuit of such a level of precision has been neglected in both research and practice, resulting in scattered academic dialogue fraught with a plethora of ill-defined terms, each conveying multiple interpretations (e.g., Allen, 2016; Cameron, 2005; Mühle et al., 2018; Windley, 2023). Second, we offer a fresh perspective on the extant theories that aim to explain socio-technical changes by examining them from a new approach to ISs: decentralized ID. This work casts a novel perspective on ANT's principle of translation (Callon et al., 1986). The DIAA framework underscores ANT's declaration that the intrinsic properties of a nonhuman actor, such as an IS, are not key factors in its diffusion. Instead, it is the IS's network interactions that are mission critical (Callon et al., 1986). In that vein, the present study finds that contextual factors are central to socio-technical change, as indicated by the second tier of the framework. Nevertheless, the study also argues that the role of an IS's innate nature (which is reflected in Tier I) should not be disregarded by ANT prematurely. An IS being fit for purpose is a fundamental prerequisite for its diffusion (Rogers, 2003), and if ANT considers this to be a tacit assumption, it should be explicitly stated. Additionally, this study adds nuance to ANT by examining socio-technical change through the use case layer, which focuses on the specific application and context of an IS rather than solely on the IS itself. Due to the potential variation in influencing networks or MVEs and their dynamics based on the use case, a more nuanced perspective is suggested to be necessary.

Regarding practical contributions, the DIAA framework serves primarily as a decision support tool for US healthcare practitioners seeking to determine the amenability of a use case to decentralized ID in the initial stages of a potential decentralized ID project, where they are becoming acquainted with decentralized ID as a concept without considering or committing to particular implementation options, such as certain technology types. The derivative functions of the tool include the cultivation of a deeper understanding of decentralized ID as an evolution and extension of traditional ISs by explicitly delineating the socio-technical factors critical for successful deployment by identifying potential use-case-specific challenges and managing them to minimize adverse effects on decentralized ID initiatives. As such, it also serves as an expectation management tool, mitigating the bandwagon effect of opportunistic adopters, heralding decentralized ID as a panacea, leading to ill-conceived projects, which may inevitably founder. Conversely, the tool may also serve as a summative assessment framework for retrospectively explaining project failures. Additionally, it empowers practitioners to walk away from adopting decentralized ID before expending resources on implementation planning. Lastly, while the toolkit does not offer insights into architectural design options for a given use case, it facilitates more informed decision-making in planning corresponding endeavors.

The study is not free of limitations, which, however, provide avenues for future research. First, regarding the DIAA framework development, we attempted to form a heterogeneous and all-encompassing empirical database with research participants representing different stakeholder groups, company types, divisions, hierarchical levels, demographics, and areas of expertise, certain personal and organizational biases may still exist within the collected data set. Further, even though we considered our data collection to have achieved theoretical saturation, gathering input from additional healthcare stakeholders and decentralized ID experts could potentially reveal further insights, AFs, and use case amenability dimensions. Future studies may benefit from increasing the number and heterogeneity of PAR participants to ensure the framework's validity and exhaustiveness. Second, regarding limitations in the evaluating phase, to further ensure the framework's validity, as well as its applicability and robustness, the DIAA framework's evaluation should be expanded to include more healthcare use cases. These studies could also involve reverse engineering implemented solutions to test the framework's applicability. Furthermore, the framework

evaluation concentrated on gauging perceptions of user-friendliness, perceived utility, and the inclination to use it. It did not examine the actual success of decentralized ID initiatives in which the DIAA framework was applied. A future research project could accompany an organization throughout the entire deployment process, utilizing the framework in all its suggested applications to examine its effectiveness.

## Concluding Remarks

This PAR research project aimed to support healthcare organizations in making more structured and informed decisions about the suitability of deploying decentralized ID for specific healthcare use cases and in guiding the implementation process if deemed appropriate. Therefore, we developed a decentralized ID use case assessment framework comprising the socio-technological factors that help explain why some US healthcare use cases are more or less amenable to decentralized ID.

Decentralized ID is still a nascent notion, although it is built upon components that have been around for decades. Healthcare may be among the initial beneficiaries of the dawn of this new era, given its data-driven nature, the type and severity of its data flow problems, and its centrality to present-day economies. However, the impact will extend far beyond, reaching almost every field in society and business, as the digital world permeates all aspects of modern life. To date, decentralized ID remains primarily conceptual, with limited practical implementations. There is still a lot to be discovered, and individuals involved ought to be modest enough to recognize the limits of what we know. Before any solutions capable of scaling and becoming mainstream can be built, it is imperative to ask the right questions, continually circling back to the primary, overarching query of what exactly is being aimed for. Bridging the gap between theory and practice, this study is an attempt to aid researchers and practitioners in jointly posing the right questions to generate workable solutions that can transition this still largely conceptual new era into tangible reality.

## References


Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. *Journal of Management*, 43(1), 39-58.

Agarwal, R., Animesh, A., & Prasad, K. (2009). Research note – social interactions and the "digital divide": Explaining variations in internet use. *Information Systems Research*, 20(2), 277-294.

Agarwal, R., Gao, G., Desroches, C., & Jha, A. K. (2010). Research commentary – the digital transformation of healthcare: Current status and the road ahead. *Information Systems Research*, 21(4), 796-809.

Allen, C. (2016, April 26). The path to self-sovereign identity. *Life With Alacrity*. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

Almeshal, T. A., & Alhogail, A. A. (2021). Blockchain for businesses: A scoping review of suitability evaluations frameworks. *IEEE Access*, 9, 155425-155442.

Ammenwerth, E., & Shaw, N. T. (2005). Bad health informatics can kill – Is evaluation the answer? *Methods of Information in Medicine*, 44(1), 1-3.

Amsterdamska, O. (1990). Surely you are joking, Monsieur Latour! *Science, Technology, & Human Values*, 15(4), 495-504.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469-490.

Baskerville, R. (1999). Investigating information systems with action research. *Communications of the Association for Information Systems*, 2(1), 1-32, Article 19.

Baskerville, R. L., & Wood-Harper, A. T. (1996). A critical perspective on action research as a method for information systems research. *Journal of Information Technology*, 11(3), 235-246.

Braun, V., & Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*. Sage.

Braun, V., Clarke, V., & Gray, D. (2017). Innovations in qualitative methods. In B. Gough (Ed.), *The Palgrave handbook of critical social psychology* (pp. 243-266). Palgrave MacMillan UK.

Burns, L. R. (2021). *The U.S. healthcare ecosystem: Payers, providers, producers*. McGraw Hill.

Callon, M., Law, J., & Rip, A. (1986). *Mapping the dynamics of science and technology: Sociology of science in the real world*. The Macmillan Press.

Cameron, K. (2005, May 11). The laws of identity. *Identity Weblog*. https://www.identityblog.com/?p=352

Cheesman, M. (2022). Self-sovereignty for refugees? The contested horizons of digital identity. *Geopolitics*, 27(1), 134-159.

Child, J., Faulkner, D., Tallman, S., & Hsieh, L. (2019). *Cooperative strategy: Managing alliances and networks* (3rd ed.). Oxford University Press.

Christensen, C. M. (2013). *Innovator's dilemma: When new technologies cause great firms to fail*. Harvard Business Review Press.

CMS.gov. (2023). *NHE summary, including share of GDP, CY 1960-2021 (ZIP)*.

Cresswell, K. (2016). Evaluation of implementation of health IT. *Evidence-Based Health Informatics*, 222, 206-219.

Cresswell, K., Williams, R., & Sheikh, A. (2020). Developing and applying a formative evaluation framework for health information technology implementations: Qualitative investigation. *Journal of Medical Internet Research*, 22(6), e15068.

Cresswell, K., Worth, A., & Sheikh, A. (2011). Implementing and adopting electronic health record systems: How actor-network theory can support evaluation. *Clinical Governance: An International Journal*, 16(4), 320-336.

Cresswell, K. M., Worth, A., & Sheikh, A. (2010). Actor-network theory and its role in understanding the implementation of information technology developments in healthcare. *BMC Medical Informatics and Decision Making*, 10(1), 67.

Cucko, S., & Turkanovic, M. (2021). Decentralized and self-sovereign identity: Systematic mapping study. *IEEE Access*, 9, 139009-139027.

Cummings, J. L., & Holmberg, S. R. (2012). Best-fit alliance partners: The use of critical success factors in a comprehensive partner selection process. *Long Range Planning*, 45(2-3), 136-159.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research*, 3(1), 60-95.

Doolin, B., & McLeod, L. (2005). Towards critical interpretivism in IS research. In D. Howcroft & E. M. Trauth (Eds.), *Handbook of critical information systems research: Theory and application* (pp. 244-271). Edward Elgar Publishing.

Engel, C., Elshan, E., Ebel, P., & Leimeister, J. M. (2023). Stairway to heaven or highway to hell: A model for assessing cognitive automation use cases. *Journal of Information Technology*, 0(0), 1-29.

Erol, I., Ar, I. M., & Ozdemir, A. I. (2021). Assessing the feasibility of blockchain technology in industries: Evidence from Turkey. *Journal of Enterprise Information Management*, 34(3), 746-769.

Flessa, S., & Huebner, C. (2021). Innovations in health care – A conceptual framework. *International Journal of Environmental Research and Public Health*, 18(19), 10026.

Gläser, J., & Laudel, G. (2009). *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen* [Expert interviews and qualitative content analysis as instruments of reconstructive studies] (3rd ed.). VS Verlag für Sozialwissenschaften.

Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly*, 19(2), 213-236.

Greenhalgh, T., Maylor, H., Shaw, S., Wherton, J., Papoutsi, C., Betton, V., Nelissen, N., Gremyr, A., Rushforth, A., Koshkouei, M., & Taylor, J. (2020). The NASSS-CAT tools for understanding, guiding, monitoring, and researching technology implementation projects in health and social care: Protocol for an evaluation study in real-world settings. *JMIR Research Protocols*, 9(5), e16861.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences – A scoping review. *International Journal of Medical Informatics*, 134, 10.

Jacobson, I. (2004). Use cases – Yesterday, today, and tomorrow. *Software & Systems Modeling*, 3(3), 210-220.

Labazova, O. (2019). Towards a framework for evaluation of blockchain implementations. 40th International Conference on Information Systems, Munich, Germany.

Latour, B. (1999). On recalling ANT. *The Sociological Review*, 41(1_suppl), 15-25.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice*, 5(4), 379-393.

Lin, Y.-K., Lin, M., & Chen, H. (2019). Do electronic health records affect quality of care? Evidence from the HITECH act. *Information Systems Research*, 30(1), 306-318.

López Martínez, A., Gil Pérez, M., & Ruiz-Martínez, A. (2023). A comprehensive review of the state-of-the-art on security and privacy issues in healthcare. *ACM Computing Surveys*, 55(12), 1-38.

Lou, H., Lou, W., & Strong, D. (2000). Perceived critical mass effect on groupware acceptance. *European Journal of Information Systems*, 9(2), 91-103.

Maylor, H. R., Turner, N. W., & Murray-Webster, R. (2013). How hard can it be?: Actively managing complexity in technology projects. *Research-Technology Management*, 56(4), 45-51.

McLean, C., & Hassard, J. (2004). Symmetrical absence/symmetrical absurdity: Critical notes on the production of actor-network accounts. *Journal of Management Studies*, 41(3), 493-519.
Mol, A. (1999). Ontological politics. A word and some questions. *The Sociological Review*, 47, 74-89.
Morton, M. S. S. (1991). *The corporation of the 1990s*. Oxford University Press.
Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80-86.
National Institute of Standards and Technology. (n.d.). *Glossary: Authenticity*. Retrieved October 14, 2023 from https://csrc.nist.gov/glossary/term/authenticity
Nunamaker, J. F., Briggs, R. O., Derrick, D. C., & Schwabe, G. (2015). The last research mile: Achieving both rigor and relevance in information systems research. *Journal of Management Information Systems*, 32(3), 10-47.
Ozdemir, Z., Barron, J., & Bandyopadhyay, S. (2011). An analysis of the adoption of digital health records under switching costs. *Information Systems Research*, 22(3), 491-503.
Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Sage.
Peak, D. A., Guynes, C. S., Prybutok, V. R., & Xu, C. (2011). Aligning information technology with business strategy: An action research approach. *Journal of Information Technology Case and Application Research*, 13(1), 16-42.
Perry, S. (2021). Trust assurance in SSI ecosystems [Livebook]. In A. Preukschat & D. Reed (Eds.), *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Manning.
Preukschat, A., & Reed, D. (2021). Why the internet is missing an identity layer – and why SSI can finally provide one. In A. Preukschat & D. Reed (Eds.), *Self-sovereign identity: Decentralized digital identity and verifiable credentials* (pp. 3-20). Manning.
Reed, D., & Sabadello, M. (2021). Decentralized identifiers. In A. Preukschat & D. Reed (Eds.), *Self-sovereign identity: Decentralized digital identity and verifiable credentials* (pp. 157-188). Manning.
Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
Ruff, T. (2023). IIW 37 book of proceedings. Internet Identity Workshop 37, Mountain View, United States.
Safi, S., Thiessen, T., & Schmailzl, K. J. (2018). Acceptance and resistance of new digital technologies in medicine: Qualitative study. *JMIR Research Protocols*, 7(12), e11072.
Sayes, E. (2014). Actor-network theory and methodology: Just what does it mean to say that nonhumans have agency? *Social Studies of Science*, 44(1), 134-149.
Smith, S. (2021). Authentic chained data containers (ACDC). *GitHub*. Retrieved November 15, 2023 from https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/ACDC.web.pdf
Sovacool, B. K., & Hess, D. J. (2017). Ordering theories: Typologies and conceptual frameworks for sociotechnical change. *Social Studies of Science*, 47(5), 703-750.
Susman, G. I., & Evered, R. D. (1978). An assessment of the scientific merits of action research. *Administrative Science Quarterly*, 23, 582-603.
Tanzi, A., & Lu, W. (2018). *Reverse engineering the Bloomberg U.S. health care index*. Bloomberg. Retrieved October 3, 2023 from https://www.bloomberg.com/news/articles/2018-09-27/reverse-engineering-the-bloomberg-u-s-health-care-index?embedded-checkout=true
Timberg, C. (2015). *Net of insecurity: A flaw in the design*. The Washington Post. Retrieved October 8, 2023 from https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/
ToIP Trust Spanning Protocol Task Force. (2023). *Mid-year progress report on the ToIP trust spanning protocol*. Trust over IP. https://trustoverip.org/blog/2023/08/31/mid-year-progress-report-on-the-toip-trust-spanning-protocol/
Wacker, J. G. (1998). A definition of theory: Research guidelines for different theory-building research methods in operations management. *Journal of Operations Management*, 16(4), 361-385.
Windley, P. (2023). *Learning digital identity: Design, deploy, and manage identity architectures*. O'Reilly.
Yaraghi, N., Du, A. Y., Sharman, R., Gopal, R. D., & Ramesh, R. (2015). Health information exchange as a multisided platform: Adoption, usage, and practice involvement in service co-production. *Information Systems Research*, 26(1), 1-18.
Yusof, M. M., Kuljis, J., Papazafeiropoulou, A., & Stergioulas, L. K. (2008). An evaluation framework for health information systems: Human, organization and technology-fit factors (HOT-fit). *International Journal of Medical Informatics*, 77(6), 386-398.