A Design Science Approach to Investigating Decentralized Identity Technology

Janelle Krupicka
William & Mary

Follow this and additional works at: https://digitalcommons.odu.edu/covacci-undergraduateresearch

Part of the Computer and Systems Architecture Commons, Databases and Information Systems Commons, Data Storage Systems Commons, Digital Communications and Networking Commons, Information Security Commons, OS and Networks Commons, Science and Technology Studies Commons, Software Engineering Commons, and the Systems Architecture Commons

https://digitalcommons.odu.edu/covacci-undergraduateresearch/2024spring/projects/13

This Paper is brought to you for free and open access by the Undergraduate Student Events at ODU Digital Commons. It has been accepted for inclusion in Cybersecurity Undergraduate Research Showcase by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.
A Design Science Approach to Investigating Decentralized Identity Technology

Janelle Krupicka, W&M

CoVA CCI Undergraduate Research Program Spring 2024

Abstract

The internet needs secure forms of identity authentication to function properly, but identity authentication is not a core part of the internet’s architecture. Instead, approaches to identity verification vary, often using centralized stores of identity information that are targets of cyber attacks. Decentralized identity is a secure way to manage identity online that puts users’ identities in their own hands and that has the potential to become a core part of cybersecurity. However, decentralized identity technology is new and continually evolving, which makes implementing this technology in an organizational setting challenging. This paper suggests that, in the future, decentralized identity research should focus on practically and usability by using the design science paradigm. By considering the organizational challenges in implementing a decentralized identity management system, decentralized identity technologies will improve and become more widely adopted, making the internet more secure for individuals and organizations.
Introduction

In the offline world, institutions create and issue standardized identity documents, like passports and drivers’ licenses. In the online world, identity systems vary in trustworthiness and effectiveness. Online users keep track of multiple logins, certificates, etc. and when they need to verify their identity, they often still need to upload a picture of their physical ID card. A picture of a user’s ID card is something that the user owns, which is one form of identity verification online. Other forms of identity verification include “something a user knows,” like a password, “something that qualifies a user,” like a fingerprint, and “something the user can do,” like a signature (Idrus et al. 2013). These forms of identity verification address the authentication component of identity online, which corroborates a form of identity to a specific user. Secure information systems use multiple forms of identity verification to allow a user to authenticate; for example, requiring a password and a fingerprint check. Beyond authentication is authorization, which determines whether an authenticated user is permitted to access a specific component of an information system (Idrus et al. 2013). Identification, authentication, and authorization are core parts of information systems and essential to ensure the integrity of the online world, which makes them a key focus of cybersecurity research and implementation.

Despite the importance of identification, authentication, and authorization online, all forms of identification systems include some security risk. Authentication in identity systems makes the internet secure and usable, but it is not a fundamental part of internet technology. Identity systems experts argue that the internet requires an identity layer to center identification, authentication, and authorization in the design of the online world (Zaeem et al. 2021). This identity layer would exist on top of the OSI network stack in both a symbolic and technical way, meaning that it would vary from the existing layers, but address the core functionality of a
network layer. Proponents of an internet identity layer explain that describing it as a network layer illustrates that identity should be a core part of the internet, rather than an afterthought (Zaeem et al. 2021). With an internet identity layer, users could keep track of which companies have their identity information, easily prove their identity, and choose to share certain aspects of their identity online and not others. An overarching identity layer is a lofty goal given that the internet is decentralized, but existing without this layer is a constant risk. Current online identity management systems can make sharing and organizing identity convoluted, but they can also expose user information and provide a cyberattack surface to maliciously access user and organization data.

Centralized databases storing user login and personal information are a target of cyberattack, as are user passwords accessed through phishing and other attacks (Weigl et al. 2023). This potential for cyberattack threatens the financial stability of the companies and institutions that use those databases. From a user perspective, these centralized databases can be dangerous on a more personal level when users’ lose control of their data online. In many cases, the entities storing personal information are trusted by users, but there are still risks of user data being sold or tracked across the internet. Internet users may choose to forgo individual website logins in favor of logging in with their Single-Sign-On account, Google account, etc. to decrease the number of logins they need to keep secure. However, these alternative logins allow the parent company to track user data beyond its own digital products, which is a concern to privacy sensitive users (Weigl et al. 2023). The security concerns of centralized databases and alternative logins can be addressed with better cybersecurity infrastructure and policy, but they can also be addressed at the root: the identity management system itself. A properly designed internet identity layer could alleviate cybersecurity threats for users and companies alike.
Self-Sovereign Identity (SSI), also known as decentralized digital identity, is a solution to security concerns with current identity management systems and could serve as the internet’s identity layer. Because SSI is decentralized, users hold onto their own forms of identity (online account, IDs, etc.) in the form of verifiable credentials (VCs), rather than storing their identity information in centralized databases owned by other organizations. Parts of those credentials (excluding personal data) are stored on a decentralized store, often a blockchain ledger, which makes it possible to verify that a VC represents the identity it claims to represent without violating user privacy (Bolgouras et al. 2022). Rather than verifying user login information with a centralized login database, SSI users present their account credential to login to a website, for example. The credential issuer and the credential verifier do not need to communicate with each other to verify that the credential is valid: it’s decentralized. SSI and VCs are user-centric and have the potential to secure private information across the internet, but they are complicated to implement and explain. VC technology is continually evolving and would benefit from a focus on usability and easy implementation in future technical iterations in order to truly address the need for an internet identity layer (Ishmaev 2020).

**Literature Review**

Ideas for a decentralized blockchain based form of digital identity emerged in 2015, but VCs were still not widely adopted in 2023 (Čučko and Urkanović 2021; Pava Díaz et al. 2023). Part of the delay in VC and SSI adoption is due to the large variety of VCs with different use cases and communities, which make it difficult for one kind of decentralized identity credential to become standard (Barbereau et al. 2023). Despite semantic and structural differences between different VCs, all VCs address the same fundamental requirements and require the same types of technology. Zaeem et al. name the core principles of VCs: “Provability, Interoperability,
Portability, Pseudonymity, Recovery, Scalability, Security, and Usability,” (2021 pg. 130) and the practical requirements for implementing a SSI system with VCs:

“1) Issuer Discovery  
(2) Connection Creation  
(3) Credential Creation  
(4) Verification with Credentials  
(5) Backup/Recovery  
(6) Derive/Share Credentials  
(7) Sunset/Delete/Revoke Credentials” (2021 pg. 130-1).

Essentially, users have to be able to prove their identity, users have to securely receive credentials and communication, and verifiers have to trust that a decentralized proof of identity is valid. On a more practical level, users need a digital wallet to store their VCs and manage their identity and both users and verifiers need access to the distributed ledger where VC information is stored to complete the verification process (Abraham et al. 2020). The cryptography required to authenticate a credential based on information from a distributed ledger is complex, which also contributes to the delay in VC adoption (Barbereau et al. 2023).

It can be helpful to imagine a specific scenario involving SSI and VCs to better understand the meaning behind the technology. For example, an employee could hold an employee VC. When the employer, or credential issuer, decides to issue an employee ID credential to the employee, or credential holder, the issuer and holder first create their own decentralized identifiers (DIDs). DIDs are unique identifiers that act as public keys in asymmetric key cryptography for signing credentials to a distributed ledger and securely sending credentials, credential requests, and credential proofs. In the case of issuing an employee ID credential, the employer and employee both have DIDs and secret private keys that relate to their DIDs, which makes it possible to secure their communications and credentials (Abraham et al. 2020). To issue a credential, the employer prepares an outline of the credential that defines the credential fields and writes that outline to a node on a distributed ledger, using their DID to sign
the outline (Zaeem et al. 2021). Then, the employer can create a credential based on the existing outline with the specific employee’s information and the employee’s DID. The employer and employee establish a connection based on their DIDs and the employer sends the employee the credential, which is only valid for the employee’s DID.

In this example, after the credential has been issued, the employee holds the credential in their digital wallet until a verifier, like a work email server, requests proof that they are an employee. The employee and email server establish a connection with their DIDs and the email server prepares a proof request using the credential outline that the employer published on the distributed ledger. The employee receives the proof request along with information about who is requesting their information so that they can make an informed decision about sharing their personal information. If the employee trusts the email server, they can send back a proof of employment based on the proof request the server sends. The server can validate the proof request with cryptography by using existing information on the distributed ledger (Richter et al. 2023). The employer-employee-email server example is more straightforward than many real implementations of VCs, but all VC interactions work in structurally the same way as this example.

In addition to the decentralized, privacy preserving aspects of VCs, the power of VCs and SSI comes from the versatility of the technology. VCs could provide a secure solution for e-prescription management; they could improve SSO models; they could help banks address Know Your Customer requirements; they could track carbon footprint through supply chains; and they could provide a digital version of driver’s licenses and health care cards (Schlatt et al. 2023; Johnson et al. 2023; Soltani and Nguyen 2018; Shams et al. 2023; Zaeem et al. 2021). Along with a variety of use cases for VCs, there are also a variety of types of VCs, like the
World Wide Web Consortium (W3C) standard JSON VC and the AnonCreds VC developed by an open source community (Laborde et al. 2020; Richter et al. 2023). VC types distinguish themselves through their handling of add-ons to the original VC structure. For example, AnonCreds VCs allow for selective disclosure, which allows credential holders to choose which aspects of a credential they share with the verifier (Yamamoto et al. 2022). AnonCreds can also be verified using a Zero Knowledge Proof (ZKP) where the verifier asks a question of the holder (e.g. are you of legal age?) and the holder is able to provide a trusted answer to that question without providing any specific personal information (e.g. their date of birth) (Richter et al. 2023).

Existing literature on VCs and SSI focuses on technological add-ons, like selective disclosure and ZKP, and advancements in cryptography for VCs (Pava Diaz et al. 2023).

Credential architecture also needs to include a form of credential revocation before the credential design can reasonably be put into use. In other words, it needs to be possible for a credential issuer to take a credential back from the holder when it reaches an expiration date or when the credential is no longer valid. When identity is stored in a centralized database, revocation is straightforward, but it is not so for decentralized identity. SSI technologists have addressed credential revocation by incorporating expiration dates into credentials that makes it impossible to validate a credential after a certain date. Additionally, some kinds of credential architecture include a revocation registry separate from the registry used to store DIDs and credential outlines. When a credential is revoked, the information is added to the distributed revocation registry and all credentials need to be cross-examined for revocation (Richter et al. 2023). In the case of the Sovrin distributed ledger network, the revocation registry is present on the main registry alongside DIDs and credential outlines (Naik and Jenkins 2021). Searching
revocation registries can become an expensive task, which is why improving revocation is a focus of SSI technologists.

Literature on SSI and VCs primarily focuses on VC architecture and specific use-cases, but fails to address user experience with decentralized identity and institutional challenges of implementing a decentralized identity management system. In 2021, Ćučko and Urkanović conducted a bibliometric study on SSI and identified an emphasis on validation research, solution proposals, architectures, and framework in the literature, “while just a few papers address the methods, protocols, patterns and specifications” of SSI (2021 pg. 139023). Pava Díaz et al. conducted a similar bibliometric study in 2021, which was published in 2023, and found the top 15 most cited papers on SSI, which all focus on the general VC and SSI framework (2023). Proof that institutions and users would benefit from SSI was absent from both Pava Díaz et al. and Ćučko and Urkanović’s literature surveys. Relatedly, Ishmaev argues that there may not be enough motivation on the part of institutions to switch to a decentralized structure, given that companies and governments benefit from storing and tracking identity data (2021). Pava Díaz et al. and Ćučko and Urkanović’s bibliometric research does not contain literature between 2021-2024, which means that it missed literature written by Weigl et al. that addresses SSI from an institutional perspective (Weigl et al. 2023). Weigl et al. analyzes SSI by considering how it relates to theories on the Social Construction of Technology and identifies the requirements institutions will have to fulfill to implement a decentralized identity system (2023). Given the gap in SSI literature on usability and user-experience, a potential research area emerges on the practicality of how organizations and institutions would implement SSI and whether leaders at those institutions believe that SSI would benefit their users. This focus on the usability of SSI and VCs from a leadership perspective (i.e. what does an organization need to implement SSI?
Does it make sense for an organization to implement SSI? What makes it difficult for organizations to implement SSI?), broadens the research that Weigl et al. conducted on institutions by expanding SSI concepts for institutions and organizations beyond the Social Construction of Technology.

**Methodology**

This methodology aims to address the gaps in the literature on decentralized identity by focusing on the practicalities of implementing a decentralized identity management system on an organizational level, including SSI infrastructure and end-user usability. Both Weigl et al. and Satybaldy et al. cite usability and practicality as primary obstacles to widespread adoption of SSI (2023; 2024). Usability and practicality can best be tested by implementing SSI technology in a real organization and tracking the obstacles and successes with the implementation, thus providing data to SSI technologists to improve decentralized identity on the organizational side.

Design science, as proposed by Hevner et al., provides a methodology for implementing a new technology into an organization, tracking its progress, and improving the technology (2004). Hevner et al. describe this new technology as an artifact in the context of design science and explain the seven guidelines for conducting design science (2004). The end goal of design science is “to create ‘what is effective,’” while still offering “clear and verifiable contributions” to existing research on the artifact, and to be “presented effectively both to technology-oriented as well as management-oriented audiences” (Hevner et al. 2004 pg. 98; pg. 83). Because the goal of this methodology is to bridge the gap between technology-oriented and management-oriented audiences through the effective application of decentralized identity technology, design science is the right choice for conducting future research on decentralized identity management systems.
To achieve a robust design science-based study, researchers need to design a decentralized identity management system to test in design science, which is made difficult by the variety of different verifiable credential formats, proving strategies, and software architectures (Satybaldy et al. 2024). In design science, the technology being tested is the artifact; in this case, the artifact is a new employee identity management system that allows employees to login to work-related digital products using an employee verifiable credential. This identity management system would be based on existing decentralized identity frameworks and VC formats. In order to determine whether this employee VC management system, the artifact, achieves the goals of decentralized identity, researchers should consider enforcing and proscribing constraints that define decentralized identity technology. Weigl et al. offer an enforcing constraint for decentralized identity management: “a software application to hold users’ credentials, the so-called digital wallet” and a proscribing constraint: “centralization, because a decentralized infrastructure is a basic design prerequisite for SSI” (2023 pg. 11). These enforcing and proscribing constraints are broad requirements, but they serve as a benchmark for measuring whether an artifact for decentralized identity management fits the goal of SSI design science research.

Beyond preliminary enforcing and proscribing constraints, implementing an entire VC decentralized system on an organizational level is an unwieldy task, which is why companies and open source communities have developed frameworks for decentralized identity management that organizations can build on top of. Satybaldy et al. explain the Hyperledger Aries, Affindi, and Veramo frameworks, which provide an API library for users to reference to create DIDs, issue credentials, verify credentials, and more (2024). To properly combine the ideas of design science with existing decentralized identity management technologies, this methodology
proposes that future researchers choose an SSI framework to build on top of by building an application to handle the business logic by calling from a frameworks’ API. This business logic application will allow organizations and researchers to iteratively improve VC usability, while still addressing potential challenges with these existing frameworks, which will benefit the technologists who aim to improve them.

In design science, researchers develop a relationship with an organization willing to test their artifact and continuously improve the artifact’s effectiveness for the organization, while incorporating scientific rigor through thorough testing and by considering existing research. Researchers may find many use-cases for VC and decentralized identity in the testing organization, one of which presents VC as a replacement for employee single-sign-on (SSO) where employees carry employee credentials rather than SSO logins. Replacing an organization’s employee SSO system with a decentralized system is a good place to start the artifact testing process with that organization because it is internal to the organization, which minimizes risks with clients, and because employees will already be accustomed to a unique identity management system if their organization uses a SSO system. Johnson et al. propose a VC-based SSO replacement to address security issues with typical SSO implementations and this SSO replacement could be implemented with the design science process (2023). Current SSO systems “[rely] on a central entity,” which “risks a single point failure” (Johnson et al. 2023 pg. 25). Additionally, due to the centralized nature of SSO systems, an “attacker may monitor a user’s traffic” through the SSO system (Johnson et al. 2023, pg. 25). A decentralized identity solution removes these risks on employee SSO systems and secures employee and company information and privacy. However, companies will need to weigh the benefits of decentralized identity management with the drawbacks of having less control over their employees’ data. By
developing a decentralized SSO system for employee sign-on using an existing decentralized identity management framework, which can be partially based on the research done by Johnson et al., the design science process can reveal whether a company would be motivated to implement a decentralized identity system.

Design science is a set of guidelines for conducting research in the Information Sciences domain, rather than a set of precise steps for researching a new technology. Because the specifics of conducting research in the design science paradigm is open to interpretation, this methodology proposes a specific progression that aligns with the ideals of design science and the current gaps in SSI research. First, researchers should conduct in-depth interviews at multiple companies and organizations about their current employee SSO system and identify problems. Although researchers should focus the implementation of the VC artifact in only one or two organizations, decentralized identity literature will benefit from qualitative data from many organizations on identity management problems on an organizational level and organizations’ responses to the idea of decentralized identity management. Next, researchers should build the initial business logic application on top of a SSI framework for a decentralized employee SSO system with VCs, after thoroughly researching the frameworks and existing examples of business logic applications for SSI. After the researchers develop the application and identify an organization willing to test it, they should begin the rigorous testing and feedback process for the artifact. The testing stages of this research should not be isolated to feedback from employees on the system, but should also encapsulate any problems encountered as the organization’s IT department implements the new VC based system. Researchers should iteratively improve the identity management system based on employee and organizational feedback, as much as is possible while using an existing framework. Some problems will likely be caused by the framework itself,
rather than the identity management application, which should be noted by researchers. If researchers follow the guidelines of design science throughout this research process, the result will be an effective decentralized identity management system as well as much-needed data on the nature of decentralized identity management systems in organizations.

**Conclusion**

When organizational leaders attempt to switch to a decentralized identity management system to address security issues with their centralized systems, they are likely to encounter obstacles in setting up a distributed ledger, determining which type of VC to use, finding a digital wallet that is user friendly, and any number of other obstacles. These practical challenges of implementing a decentralized identity management system stifle the new adoption of VCs and SSI, even when these new technologies could bring benefits to users and organizations (Satybaldy et al. 2024). Not only is practicality and usability missing from technological implementations of VCs, but it is also missing from the literature focused on VCs and SSI (Čučko and Urkanović 2021). This paper proposes a new focus in the literature on the practical application of decentralized identity technology through the paradigm of design science. Design science emphasizes iterative engineering that focuses on the effectiveness of a particular technology for a specific organization, which means that the real problems of that organization are rigorously addressed. For design science to address the practical considerations of VC systems, research needs to incorporate feedback on how the systems are integrated into organizations’ IT departments, step-by-step. In other words, future research needs to address the question: how can decentralized identity systems be easier for organizations to implement? Reimagining an organization’s employee SSO system to be decentralized using design science is
a good starting point for putting practicality and usability at the forefront of decentralized identity management research.

Current forms of centralized identity authentication do not protect user privacy or organizational cybersecurity, whether it is because user data is trackable by companies or because identity data is stored in centralized databases that are targets for cyber attacks. Decentralized identity spreads identity management out across the internet by allowing users to hold their own identity credentials, making it more difficult to attack and allowing users to determine when to share their identity. It is apparent that there is a need for a standardized decentralized identity management system interwoven with the core functionality of the internet to address identity authentication, but current decentralized identity management systems are convoluted and miss many practical needs. This paper addresses the gaps in SSI research in terms of practicality and usability and proposes a form of research, design science, that can help develop more usable SSI solutions, which is important given the cybersecurity risks of current authentication solutions. Decentralized identity technology is a growing domain filled with fascinating cryptography and philosophical breakthroughs on the structure of the internet, but the practicality of the technology must be developed to achieve the full benefit of this new internet identity system.
References


