

Hello!

Dr. Kerri Lemoie
Director, Digital Credentials Research & Innovation
Badgr / Concentric Sky
klemoie@concentricsky.com
@kayaelle (twitter & GitHub)
she/her/hers

Thank you for having me.

A Little bit about me:

I work on an Open Badges platform called Badgr at a company called Concentric Sky

My background is in technology. I worked as developer in e-commerce and then started looking for ways that I could use my tech skills to help others which led me to ed tech.

I'm one of the founding contributors to the Open Badges standard and over the years I've helped develop the specification, build badge issuing platforms, and consult on best practices for adoption of Open Badges.

The US election in 2016 led me to start thinking more about trust and the internet so I decided to pursue a doctorate in media psychology at Fielding Graduate University in Santa Barbara, California. Fielding is a psychology graduate school and I studied Media Psychology which is the study of how any type of media, including technologies, can affect or are affected by human behavior.

Right now I'm leading efforts to align education data standards with the W3C verifiable credentials model at the Verifiable Credentials in Education task force and also at IMS Global where we are working on Open Badges 3.0.

Today I'm going to present an abbreviated version of my dissertation but afterwards we can talk more about how this relates to verifiable credentials and open badges in education.

Determinants of Behavioral Intention
to Use a Self-Sovereign Identity
Digital Wallet: Extending the UTAUT
with Trustworthiness

Dr. Kerri Lemoie, Fielding Graduate University, Media Psychology

The title of my dissertation is: Determinants of Behavioral Intention to Use a Self-Sovereign Identity Digital Wallet: Extending the UTAUT with Trustworthiness

Please note that this research was done from an American's perspective so there is data that is particular to that country.

Agenda

- Internet Identity
- Self-sovereign Identity (SSI) & Digital Wallets
- Technology Adoption Models
- Trustworthiness & SSI
- Hypotheses & Analytical Model
- Research
- Results
- Limitations
- Take-aways & Future Research

Here's a brief look at the agenda for this presentation.

Because the research is based on some complex technology, I'm going to explain the reasons for the technology and a high level overview of how it works before I get into how adoption was studied.

The Internet doesn't have an identity layer.

So let's start here.

The Internet doesn't have an identity layer.

It was created to recognize machines, but it was not created with an identity layer for humans and organizations. There's been no inherent way to verifiably know who and what Internet users are connecting to

or how to verifiably identity themselves.

Offline ≠ Online

Offline and online identities are often intertwined.

For instance, we interact with governments, banks, and healthcare both in-person and online;

we connect with family & friends in-person and also through email, text, chat, and social media

But we compromise how we represent ourselves online because there is no way represent ourselves online exactly as how we'd like to be represented.

This is because we're beholden to the services & applications provided by others.

And this drastically reduces the agency we have over the personal data that represents who we are.

And this means...



We can't always trust who people say they are online.

It's inconvenient but also dangerous.

- Cross-correlation of data
- Privacy breaches & identity theft
- Commoditization of personal data

As platforms collect personal data, a potential trail is created for others to cross-correlate data and generate their own concepts about our identities.

Even when platforms have the best interests of their users in mind, and even when privacy policies and terms of use are clear and agreed upon, individuals are vulnerable to privacy breaches and identity theft.

Data brokers, whether legal or illegal, and online advertisers profit at a great disadvantage to individuals.

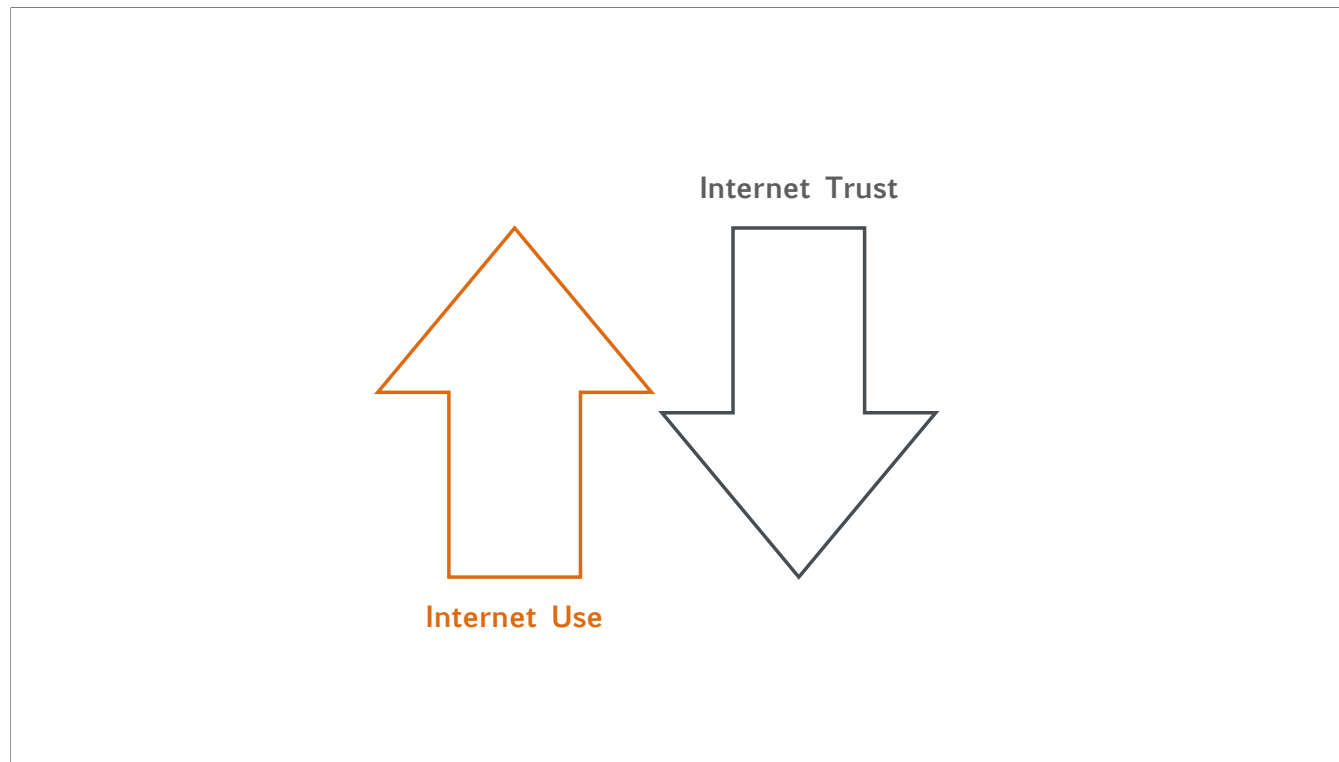
4.1 billion internet users (10% growth yearly)

It's worth noting that more than half of the world's population is online.

Each email address = 130 associated accounts

In the United States alone, each email address has an average of 130 accounts associated with it.

Sixty-four percent of Americans have online accounts associated with health, financial, and household data.



But as Internet use is increasing, trust is decreasing.

More than half of Americans have experienced a major data breach including fraudulent credit card charges, compromised personal data, and identity theft.

Many feel as though they do not have control over the data that is collected about them and that their personal information is not as secure as it has been in the past.

“If we do nothing, we will face rapidly proliferating episodes of theft and deception which will cumulatively erode public trust in the Internet.”

— Kim Cameron, *The Laws of Identity Problem Statement*

As Kim Cameron said in 2005,

“If we do nothing, we will face rapidly proliferating episodes of theft and deception which will cumulatively erode public trust in the Internet.”

Self-sovereign Identity

Self-sovereign identity is the next phase in digital identity and data management.

It has the potential to increase Internet trust by shifting how humans digitally represent themselves and increase the amount of control they have over their personal data.

This could have a reverberating effect across all online interactions.

but it's unknown if this nascent technology will be accepted and used.

The objective of this study was to better understand the factors may facilitate its adoption and the digital wallets that enable it.

But before we get to the research, I'll explain how self-sovereign identity works.

Persistent

Verifiable

Data-rich

Private

Self-sovereign identity is both a philosophy and combination of technologies that work together to produce persistent, verifiable, understandable, data-rich claims and provide individuals the ability to transact and share data about themselves privately.



Internet Technologies

Internet Standards

Cryptography

Blockchain

The technologies include data standards and protocols being incubated at the World Wide Web Consortium that define how identity data can be understood and verified called verifiable credentials and decentralized identifiers.

There are services that communicate, process, and deliver the identity data,

and there are applications called digital wallets that read, store, and present data on mobile devices and desktops.

Internet Technologies

Internet Standards

Cryptography

Blockchain

Cryptography is used to secure credentials and prove control over them.

Internet Technologies

Internet Standards

Cryptography

Blockchain

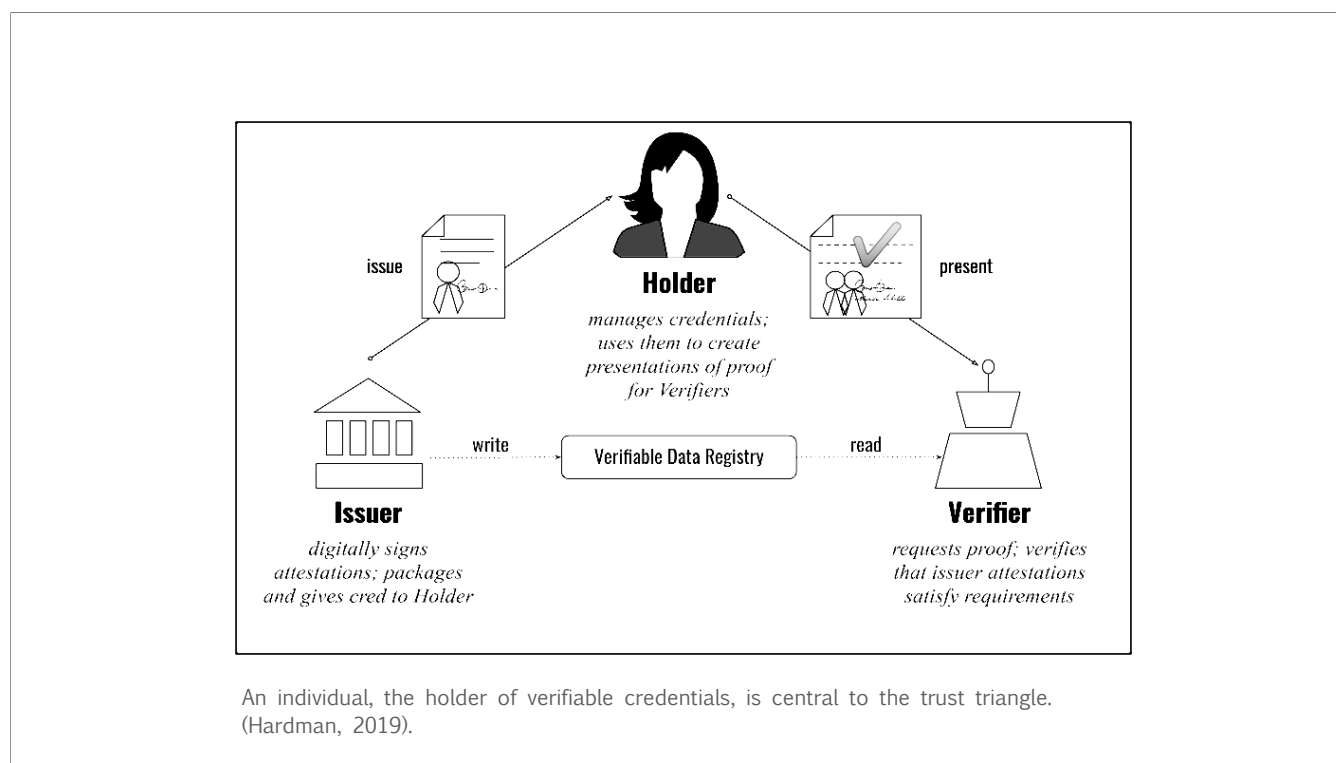
Blockchains, a type of distributed & decentralized databases that originated to store persistent, tamper-proof records of cryptocurrency transactions, are being used as a way to secure identities too.

How SSI Verifiable Credentials Can be Used

- Government IDs
- Educational & Occupational Credentials
- Application Authentication
- Universal Digital Library Cards
- Health & Immunization Records

Self-sovereign identity Verifiable credentials can be used for any type of credential. Projects being worked on include:

- Govt Ids like passports, drivers licenses, & birth certificates
- Educational & Occupational credentials like diplomas, certifications, & micro-credentials
- Application & website Logins
- Universal Digital Library cards
- Health & Immunization records such as vaccine passports which could potentially be in use by the end of this year



This image illustrates how an individual, who is the holder of verifiable credentials, may be at the center of a trust triangle.

Using the driver's license as an example, when a DMV issues a driver's license to an individual, the license can be both physical and also in the form of a verifiable credential.

The DMV issues the verifiable credential to the individual who stores it on the digital wallet app on their mobile phone.

When the individual is renting a car online, they can present the verifiable credential version of the license as proof of their age and ability to drive a car.

The rental car agency platform, as the verifier, reads the data in the credential and checks the verifiable data registry to ensure that the credential was issued by a valid DMV, that it's related to the individual presenting it, and that it hasn't expired, been tampered with, or revoked.

This trust triangle demonstrates that the license could be used online just as it could be used in person without the DMV being contacted directly for verification.



This is a mockup taken from the web page used in the research that shows what a self-sovereign identity digital wallet app may look like.

The issuer of a credential sends a unique link to the individual or displays a QR code that the individual can capture on their phone and accept in their digital wallet. In the wallet they can collect various credentials and from there, present them to verifiers.

Self-sovereign Identity Principles

1. Existence
2. Control
3. Access
4. Transparency
5. Persistence
6. Portability
7. Interoperability
8. Consent
9. Minimalization
10. Protection

Self-sovereign identity has 10 principles upon which the technology is based. These principles served as core concepts for this study so I will go through them briefly.

They are:

1. Existence: which asserts that every person on earth should have an identity throughout their lives no matter where they were born, where they live, their gender, socio-economic status, etc.
2. Control – Users must have control of their identities...They should always be able to refer to it, update it, or even hide it
3. Access – individuals should have unobstructed access to their identity data
4. Transparency – is how an identity system functions, is managed, and is updated must be publicly available and reasonably comprehensible
5. Persistence – Identity should exist as long as the individual wishes
6. Portability – identity data should be transportable from one app to another
7. Interoperability – the data must be exchangeable and understood wherever it is being presented
8. Consent – individuals must give permission for their data to be accessed or used
9. Minimalization – individuals should be able to "share only the least possible amount of data necessary to accomplish the task at hand

10. Protection – technology providers should protect data by maintaining the privacy and security of the data while it is created, transmitted, and authenticated.

Technology Adoption & Unified Theory of Adoption & Use of Technology (UTAUT)

To study the factors that affect the adoption of self-sovereign identity, I used a technology adoption theory called the Unified Theory of Acceptance and Use of Technology (UTAUT).

Technology adoption theories explore the motivations for technology adoption. These theories are rooted in behavioral factors including social, cognitive, emotional aspects.

These theories have assisted with organizational adoption of technologies and have also been applied to many consumer-based technologies and applications such as e-commerce sites, online banking, and mobile applications.

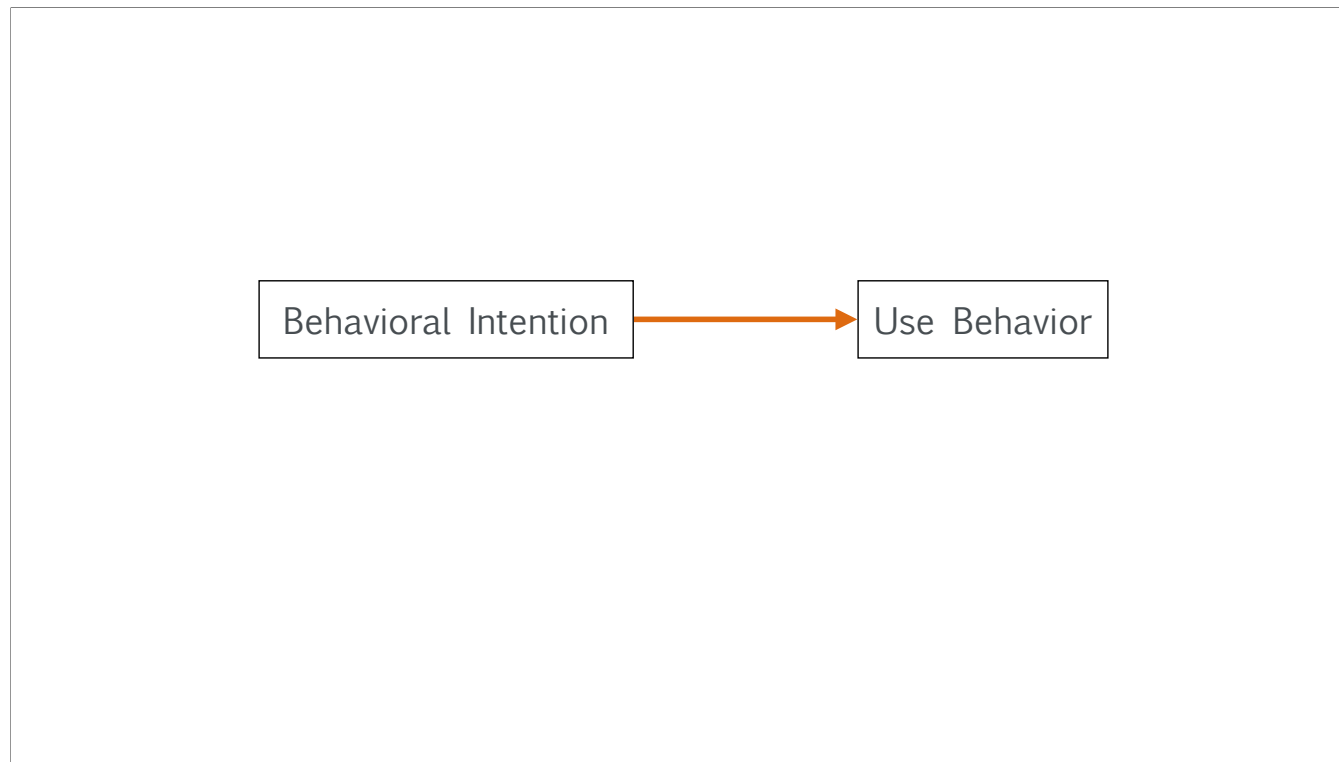
The UTAUT has been in existence for nearly two decades and has evolved since it was first developed to study the adoption of technology in organizational settings.

It's been adapted to accommodate various contexts and approaches to research of technology adoption including many types of consumer technologies.

<p>Theory of Reasoned Action (TRA) Attitude Toward Behavior, Subjective Norm</p>	<p>Motivational Model (MM) Extrinsic Motivation, Intrinsic Motivation</p>
<p>Theory of Planned Behavior (TPB) Attitude Toward Behavior, Subjective Norm, Perceived Behavioral Control</p>	<p>Technology Acceptance Model (TAM) Perceived Usefulness, Perceived Ease of Use, Attitude Toward Behavior</p>
<p>Combined TAM and TPB (C-TAM-TPB) Attitude Toward Behavior, Subjective Norm, Perceived Behavioral Control, Perceived Usefulness</p>	<p>Model of PC Utilization (MPCU) Job-fit, Complexity, Long-term Consequences, Affect Towards Use, Social Factors, Facilitating Conditions</p>
<p>Innovation Diffusion Theory (IDT) Relative Advantage, Ease of Use, Image, Visibility, Compatibility, Results Demonstrability, Voluntariness of Use</p>	<p>Social Cognitive Theory (SCT) Outcome Expectations-Performance, Outcome Expectations-Personal, Self-efficacy, Affect, Anxiety</p>

The UTAUT was formulated and validated based on the conceptual and empirical review of the eight technology acceptance models pictured here.

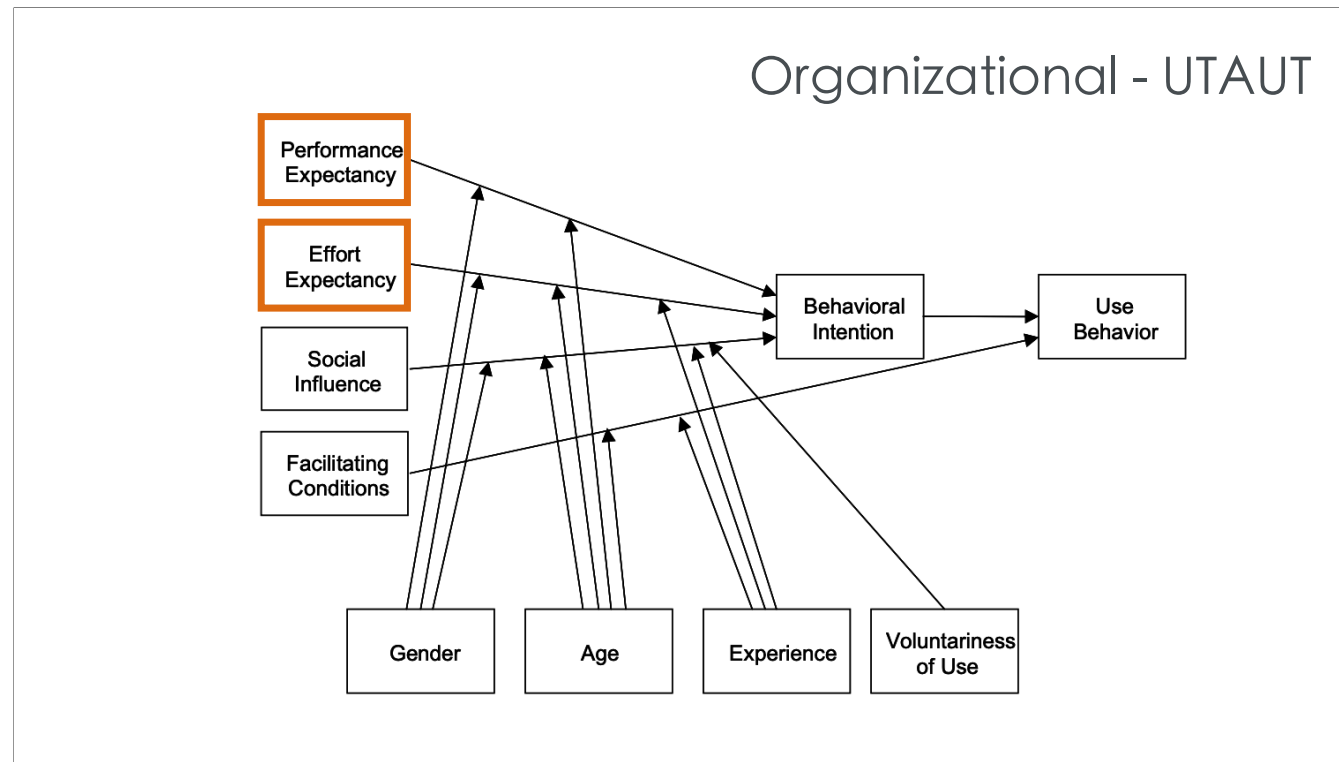
The highlighted constructs were synthesized into four determinants: performance expectancy, effort expectancy, social influence, and facilitating conditions.



The UTAUT is predicated on the significant positive influence of behavioral intention on use behavior based on the Theory of Planned Behavior and also, the Technology Acceptance model.

These theories contend that individuals make logical and reasoned decisions to engage in behaviors based on their intention to do so which can be influenced by

beliefs about the probable consequences of their behavior,
beliefs about the expectations of other people,
and beliefs about the factors that may enable or obstruct the behavior.



This figure of the original organizational focused UTAUT demonstrates the relationship I just described with the beliefs on the left that influence behavioral intention which then in turn influences actual use behavior.

My study explored two of the beliefs in the context of self-sovereign identity: performance expectancy and effort expectancy

Performance Expectancy – measures how much it is expected that technology may increase productivity or help individuals achieve what is important to them

Effort Expectancy – measures how much effort individuals believe it will take to use the technology

At the bottom of the figure are gender, age, experience and voluntariness of use. These are the moderators that were predicted to affect the relationships between the beliefs and behavioral intention.

Trustworthiness & SSI

Ability

Existence
Control
Portability
Interoperability
Minimalization

Integrity

Access
Transparency
Persistence
Consent
Protection

Benevolence

So how does trustworthiness fit into this picture?

Self-sovereign identity is intended to increase trust of the Web through compliance with its guiding principles. As a whole, the principles are well-meaning and were created to establish safer identity systems.

Individually, each principle establishes how self-sovereign identity applications should be more trustworthy.

There are three characteristics that explain the trustworthiness of an organization: ability, integrity, and benevolence.

Ability is the belief that the trustee, the organization, has the skills and understanding to perform the behavior expected by the trustor.

Integrity is the expectation that the trustee will follow the principles that have been agreed upon with the trustor.

Benevolence refers to the belief that the trustee intends to do good to the trustor.

This research proposes that the guiding principles of self-sovereign identity can be aligned with these characteristics.

This slide illustrates how the principles have been aligned for this research. Implied is an overarching alignment with benevolence because, overall, self-sovereign identity is intended to be a well-meaning approach digital identity.

Research Questions & Analytical Model

Behavioral Intention

This study applied the UTAUT model to explore the effects of perceived usefulness and perceived ease of use on behavioral intention to use a self-sovereign identity digital wallet.

It extended the UTAUT by adding trustworthiness as a direct determinant of behavioral intention and perceived usefulness.

This research was the first to use the UTAUT model to study behavioral intention to use a self-sovereign identity application.

It was also the first study to align the characteristics of trustworthiness to the self-sovereign identity principles.

The intention was to provide valuable insights to technology experts currently developing digital identity solutions and inform future research on acceptance of emergent technologies related to identity and decentralized technologies.

Since the technology can be implemented in many contexts, it was reasonable to establish this base literature so that it can be used for future research.

Because self-sovereign identity is a nascent technology, it had not been implemented broadly enough to research use behavior at the time of this study. For this reason, this research focused on behavioral intention specifically.

Research Questions & Analytical Model

- Which factors most significantly predict behavioral intention to use a self-sovereign identity digital wallet?
- Is trustworthiness related to the adoption of a self-sovereign identity digital wallet?
- Is there a relationship between perceived usefulness of a self-sovereign identity digital wallet and trustworthiness?

For this study, the UTAUT was used to form the following research questions:

Which factors most significantly predict behavioral intention to use a self-sovereign identity digital wallet?

Is trustworthiness related to the adoption of a self-sovereign identity digital wallet?

Is there a relationship between perceived usefulness of a self-sovereign identity digital wallet and trustworthiness?

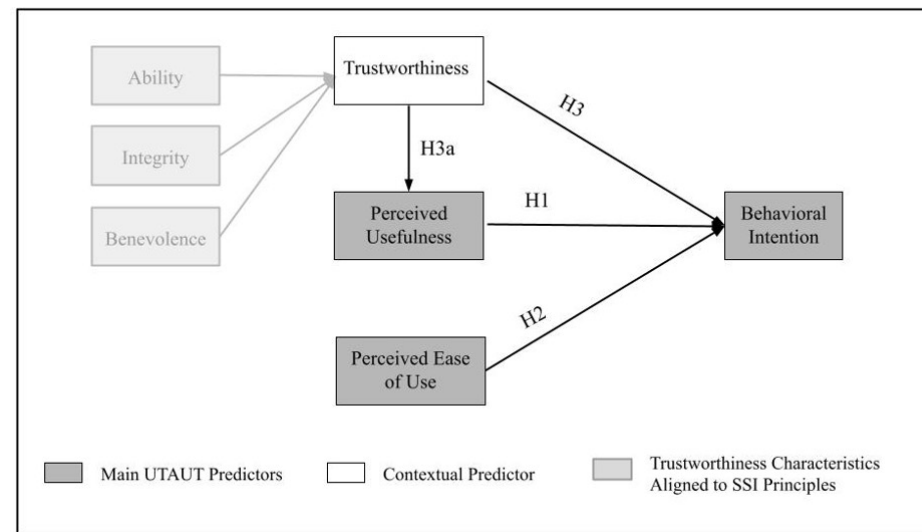
Hypotheses

- H1.** Perceived usefulness will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.
- H2.** Perceived ease of use will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.
- H3.** Trustworthiness will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.
- H3a.** Trustworthiness will have a positive effect on perceived usefulness.

Based on prior research, the following four hypotheses for this research were:

- H1: Perceived usefulness will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.
- H2: Perceived ease of use will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.
- H3: Trustworthiness will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.
- H3a: Trustworthiness will have a positive effect on perceived usefulness.

Hypothesized UTAUT Model with Trustworthiness



This figure is my hypothesized extended UTAUT model to research behavioral intention to use a self-sovereign identity (SSI) digital wallet.

It demonstrates each of the hypotheses:

Relationship of perceived usefulness and behavioral intention

Relationship of perceived ease of use and behavioral intention

Relationship of trustworthiness and behavioral intention

Relationship of trustworthiness and perceived usefulness

To the left are the characteristics that reflect trustworthiness

Research Design

- Quantitative
- Non-experimental
- Anonymous Survey
- 18+

This study used a quantitative, non-experimental approach that adapted and extended the UTAUT framework. An anonymous 3-part survey was hosted on Qualtrics using a Fielding Graduate University design theme.

It was restricted to persons 18 or older and because it was anonymous, online, and directed at adults, it was determined to be exempt from oversight by Fielding's IRB.

Three-part Survey

1. Demographic Questions (*Age, Location, Gender, Race, Education, Internet Proficiency*)
2. Embedded Webpage (*Design Fiction*)
3. UTAUT, Trustworthiness, & Open-ended Question

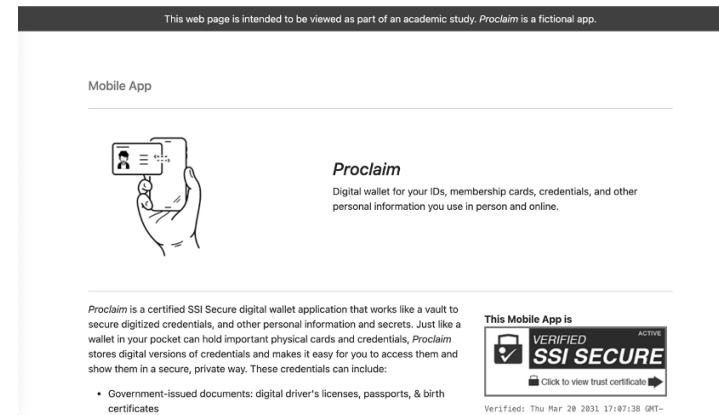
The survey was designed to:

- 1) ask demographic questions such as Age, Location, Gender, Race, Education. And also questions for participants to self-rate their internet proficiency.
- 2) present an embedded web page describing a digital wallet application of the future called, Proclaim leaning on a concept called design fiction that I will explain in the next slide,
- 3) ask questions about Proclaim related to main UTAUT factors, trustworthiness, and overall impressions of the app.

The measures for these questions were adapted from prior UTAUT research and the Consumer Trust and Trustworthiness–Beliefs Scale

Imagine it is the year 2031...

<https://proclaim.io/study>



Here's a screenshot of the embedded web page used in the study to describe a self-sovereign identity digital wallet. You can view this web page at proclaim.io/study

Design Fiction was used to introduce the webpage and its narrative.

Design fiction is a conceptual design tool used to present, explain, and prompt consideration of the implications of advances in technologies. It explains what the future could be like by transporting individuals through the use of narrative.

The instruction section preceding the embedded web page asked the participants to imagine it was the year 2031, ten years from now.

It went on to introduce digital wallets, how they were being used, and how this was different from the 2020's.

The web page explained the concepts of self-sovereign identity through relevant and routine use case examples and visuals.

Fictional screenshots of the Proclaim app were interspersed with descriptions.

Stories from users timestamped with dates in 2031 were included to provide a human perspective. These stories were positive and contextual but not intended to be persuasive since this web page was to be informational, not a marketing tool.

Content and imagery were presented as objectively informational as possible and the color palette was limited to white, black, and shades of grey to avoid brand association and semantic meanings.

Technical terms such as blockchain, interoperability, and standards were avoided so that the content could be accessible to a non-technical audience.

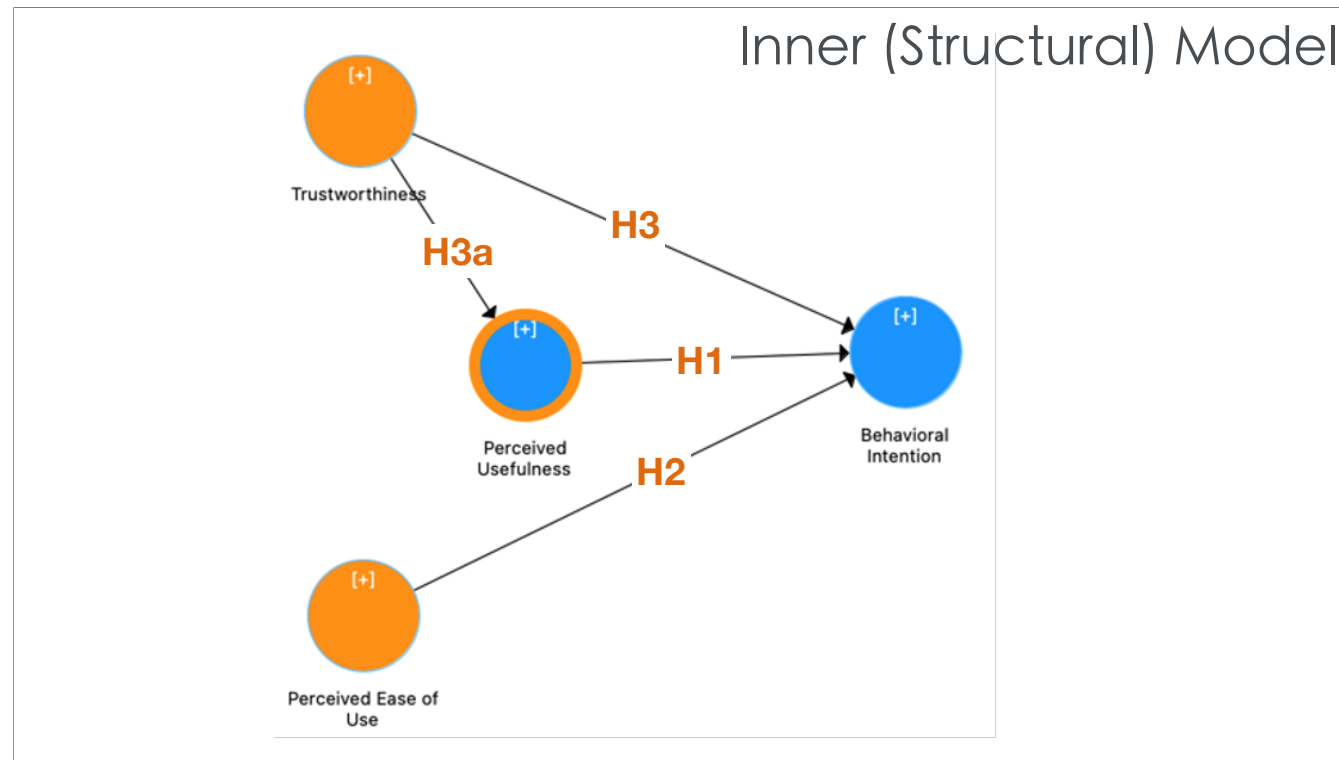
Application security was demonstrated by statements about encryption and privacy, and by displaying a clickable graphic that referenced a mental model of trust seals typically used on websites to indicate achieved security.

Research Data Analysis

Partial Least Squares Structural Equation
Modeling (**PLS-SEM**)

Based on prior UTAUT literature and the purpose of this study, Partial Least Squares Structural Equation Modeling (PLS-SEM) was used to analyze the data.

PLS-SEM is a commonly used modeling technique used to validate structured data and test the relationships between constructs. It allows researchers to estimate very complex models with many constructs and indicator variables, especially when the goal of the analysis is prediction.

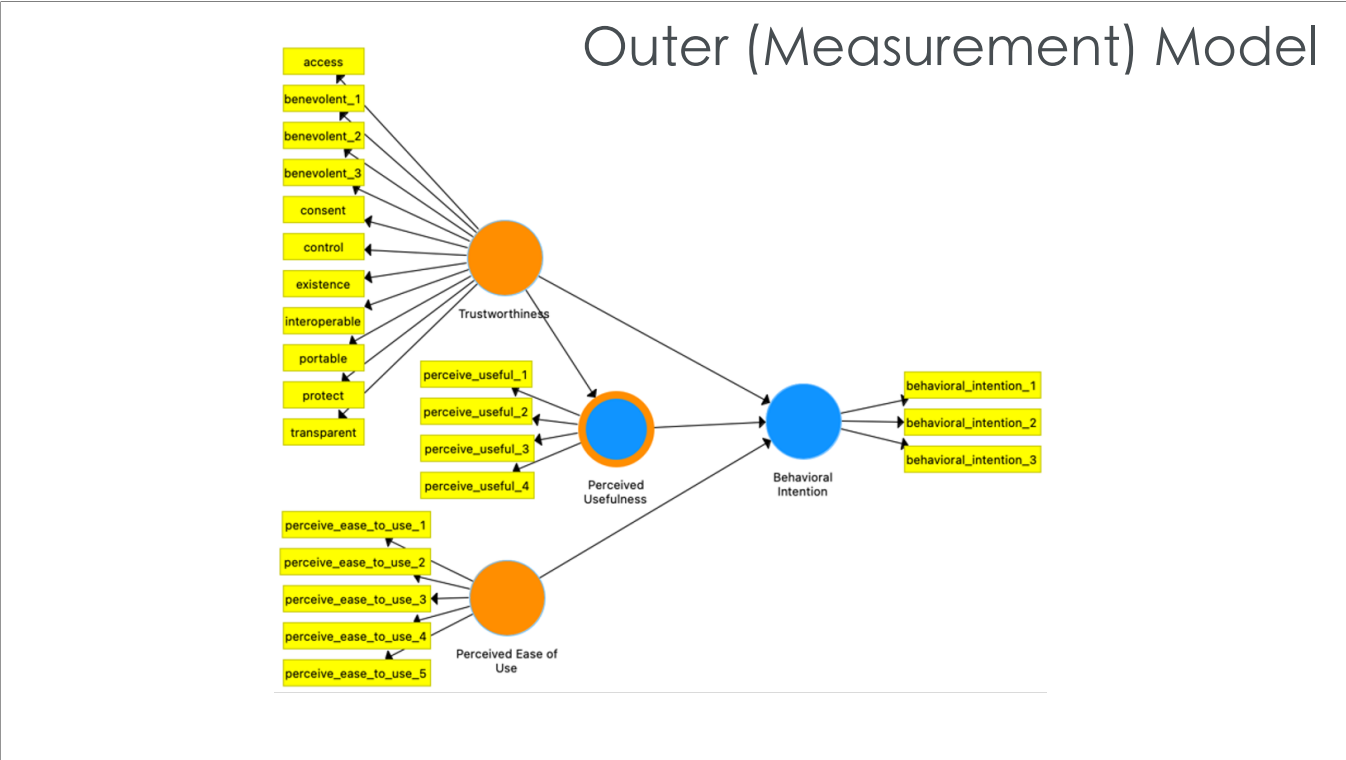


The foundation of PLS-SEM is its path model which is a diagram that displays the relationships of the variables involved in the hypotheses.

This figure displays the inner model which contains the latent variables and the connections between the variables, and as you may recall, looks much like the hypotheses figure I showed you earlier.

Behavioral intention is the primary endogenous construct since it is being explained by the exogenous constructs, perceived usefulness (H1), perceived ease of use (H2), and trustworthiness (H3).

Perceived usefulness is both an exogenous construct, explaining behavioral intention as well as an endogenous construct being explained by trustworthiness (H3a).



This figure is the measurement model or outer model and displays how the indicators (which are the yellow boxes) are related to each of the latent variables.

Each of the indicators represent the UTAUT & Trustworthiness questions taken by participants in the study.

Participants

- Minimum 103 participants
- Convenience sampling
- Internet users unfamiliar with the technology
- \$50 Amazon.com Gift Card Raffle

According to PLS-SEM guidelines a minimum of 103 participants were needed to achieve a statistical power of 80%.

Convenience sampling was used to recruit participants. This included targeted outreach to my network, friends and colleagues across the United States who were then asked to do targeted outreach themselves,

Postings were made on Reddit subgroups, to my Facebook timeline, NextDoor.com, and to a Facebook community group in Durham, NC.

To avoid experts in the field, the survey was not posted on LinkedIn or Twitter where I have more professional contacts in the self-sovereign identity field.

Participation was also incentivized by an offer to enter a raffle to win one of six \$50 Amazon.com gift cards.

Results

Demographics

- 381 participants (319 valid entries - 61 removed for missing values)
- 43% Gen X
- 70% live in the south
- 76% women
- 47% graduate or professional degree
- 51% average Internet Proficiency

Here are the demographics of the participants.

381 people took the survey but only 319 completed it,

43% were Gen Xers

70% live in the southern area United States

76% were women

47% had graduate or professional degrees

51% claimed they had average Internet proficiency

I would have preferred a more diverse group of participants and sought to do that but learned that sometimes convenience sampling leads to demographics that look like yourself.

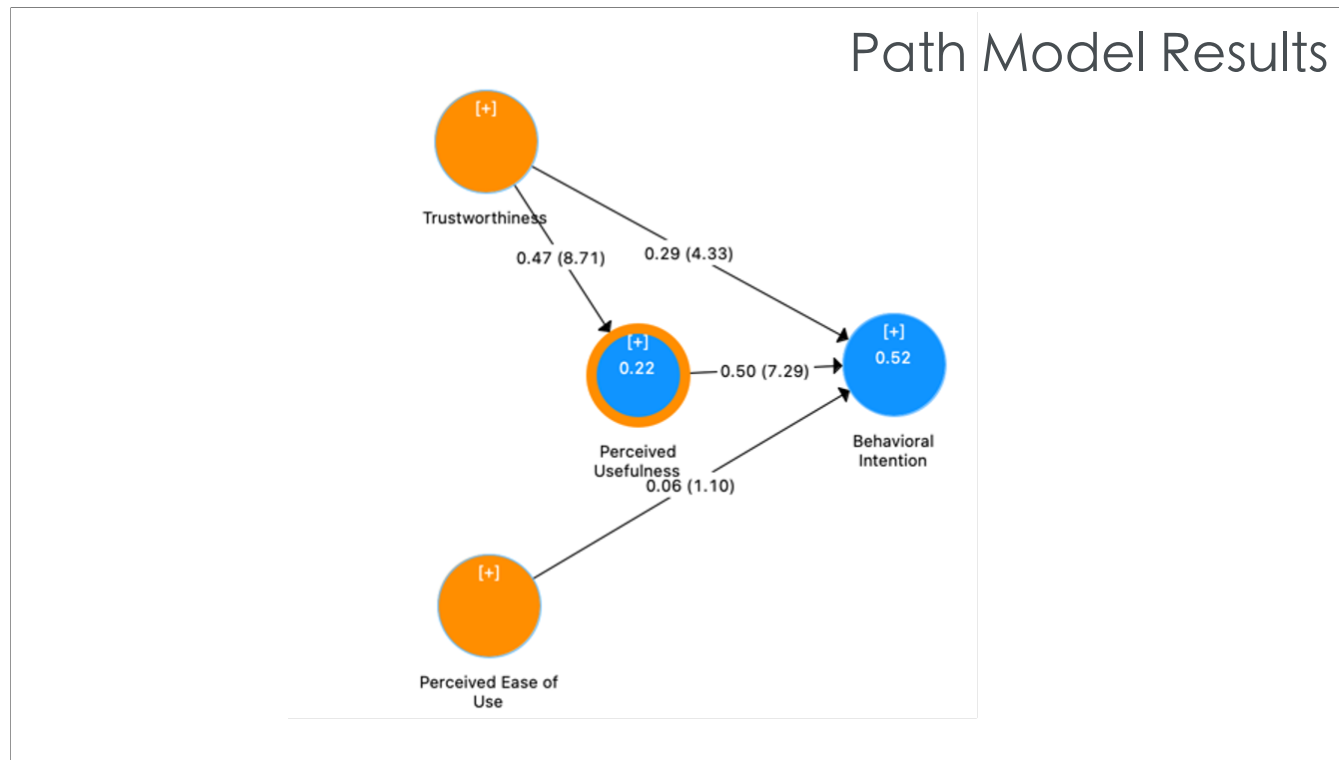
Results

Behavioral Intention

The results indicated that the participants overall did not have a strong intention to use the Proclaim application. However, they did not reject it but had a neutral response to it.

Millennials and those who considered themselves to have low Internet proficiency reported the strongest intention to use Proclaim.

This was not entirely unanticipated. Self-sovereign identity is not a familiar technology and digital wallet applications built on this model are not familiar to many.



This is the path model result. It demonstrates that

The relationship between perceived usefulness & Behavioral intention was found to be the strongest.

The relationship between Perceived ease of use & behavioral intention was found to be the weakest.

These results predict that it is likely that trustworthiness will contribute to adoption of self-sovereign digital identity wallets, but that perceived usefulness will play the biggest role in influencing behavioral intention.

Hypotheses

- H1.** Perceived usefulness will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.
- H2.** Perceived ease of use will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.
- H3.** Trustworthiness will have a positive effect on behavioral intention to use a self-sovereign identity digital wallet.
- H3a.** Trustworthiness will have a positive effect on perceived usefulness.

Hypothesis 1 was supported which as I mentioned indicated that perceived usefulness had a positive effect on behavioral intention. This aligns with prior research which found performance expectancy measures such as perceived usefulness, to be the strongest predictor of behavioral intention

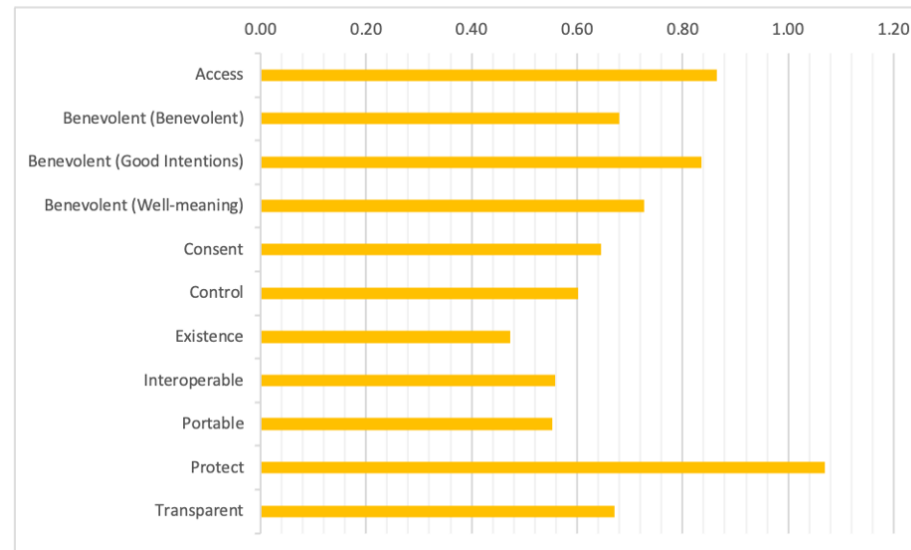
Hypothesis 2 was not supported indicating that perceived ease of use did not have a positive effect on behavioral intention. Participants in this study were unable to gauge the mental effort involved in using the application because they were limited to the narrative and images provided to them in the webpage and could not try it or see it in action for themselves.

Hypothesis 3 was supported indicating that trustworthiness had a positive effect on behavioral intention. However, the effect was weaker than perceived usefulness. This may suggest that trustworthiness of a digital wallet is less important to users than its usefulness.

Although self-sovereign identity is intended to provide a model for more trustworthy applications, at this stage it may be too early for that impact to be envisioned by potential users who likely do not have an understanding of how the technology works or how it is different from experiences with current internet applications.

Hypothesis 3a was supported indicating that trustworthiness had a positive effect on perceived usefulness. Research has shown that if a technology is considered to be capable and well-meaning, then the technology is also considered to perform as expected and, therefore, as useful.

Trustworthiness



The outer loadings for the trustworthiness indicators determine their contribution to trustworthiness.

Variables are considered to be stronger and more reliable if the outer loadings values of their indicators are closer to 1.

As seen in this chart, the protect & access principles are the strongest contributors to trustworthiness.

More than half of the trustworthiness indicators had outer loadings below the minimum accepted threshold. If this research was seeking to create a stronger trustworthiness construct for self-sovereign identity technologies, many of these would be removed.

However, there would not be enough remaining indicators to align with ability, integrity, and benevolence.

Also, since this exploratory study is intended to provide a base for future research, keeping the indicators as is provides the next study with a scaffolding upon which to adapt indicators for their context.

Take-aways

- Perceived Usefulness
- Ability vs Understanding
- Narrative Persuasion
- Access & Protection

Here are my take-aways.

Many of the participants perceived the application to be useful and convenient. They expected that it would protect their data, give them access to their data, and for the most part, have good intentions towards its users. These factors contributed to the result that perceived usefulness and trustworthiness could predict the behavioral intention to use an app such as Proclaim.

The principles aligned with ability may have contributed less to trustworthiness because the participants weren't able to evaluate if the creators of the Proclaim application had the competence to deliver on those principles.

This could be because the technology is new and not widely understood. Even those who consider themselves to have average or high Internet /computer proficiency likely do not have understanding of self-sovereign identity technology because it is so new and very much in development.

Experts in the self-sovereign identity industry have extremely high technology proficiency and implicit knowledge about how this technology works and its benefits. If the participants of this study were these experts, it is likely that ability would be a much stronger, if not the strongest, contributor to trustworthiness in this context particularly because their work is to ensure that the applications have the ability to perform what is expected of them.

The narrative approach to describing the application including the user stories may have played a role in the stronger contributions of integrity and benevolence to trustworthiness.

While the website describing the Proclaim application was not intended to be persuasive, it was presented positively with user stories that related to each of the functional descriptions.

Several participants noted in the open-ended text field at the end of the survey that they could relate to the user stories. Research has shown that narratives can be persuasive and change attitudes through transportation. When a narrative is self-referencing, individuals may become more immersed or transported which makes the narrative seem more real.

To increase adoption, this study would suggest an approach that focuses narrative on factors related to integrity and benevolence such as protection of and access to data. This may bridge the literacy gap while the technology matures.

Limitations

- Website
- Population of Participants
- Self-rating Internet Proficiency

Limitations of this study include

The constraint to a website to describe the Proclaim application versus using an actual application.

While the results indicated the power of narrative, by using a website the study limited which aspects of the UTAUT could be used, and limited the experience of the participants.

Also, while effort was made to ensure that the website was understandable and accurate, it was not possible to provide more in-depth explanations about the technology within the constraints of the study.

Explaining self-sovereign identity is challenging for the most experienced. The language does not yet exist to explain it in a way that is non-technical. Focusing the narrative on the benefits is a useful frame but without more in-depth understanding, it is challenging for many to recognize why this technology will be any better than what they are using now.

The second limitation is that the population of the participants was not representative enough of the population that could someday be using this application. In particular, the participants were mostly white, female, and highly educated. Research can be more effective when the sample is more diverse and balanced because it reflects more of the population of humanity.

The third limitation is that asking participants to rate their level of Internet / computer proficiency cannot be relied upon as a true assessment of their proficiencies.

It is acknowledged that this question provided no context and that Internet and computer proficiency is conceptually vast and subjective.

Also, there is a gap between understanding existing Internet technologies and nascent ones. One cannot rate proficiency of something they do not know exists. All of this was kept in mind while doing the exploratory analysis using the proficiency variable but should still be acknowledged as a limitation.

Future Research

- In-person Focus Groups
- Actual Digital Wallets
- Expand Upon the UTAUT

Future research should consider adapting this research to be with in-person focus groups with diverse participants, especially underserved populations who could greatly benefit from the agency and control that self-sovereign identity technologies intend to provide.

Also, as more applications like Proclaim come to market, research can be expanded to include use behavior introducing exploration into factors such as facilitating conditions, social influence, and moderators that apply to the technology and the specific contexts in which it is being used.

Thank You!