

**LEARNING TO TRUST: EXPLORING THE RELATIONSHIP BETWEEN USER  
ENGAGEMENT AND PERCEPTIONS OF TRUSTWORTHINESS IN SELF-  
SOVEREIGN BLOCKCHAIN SYSTEMS**

by

Zakir Suleman

B.A., The University of British Columbia, 2015

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF  
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF LIBRARY AND INFORMATION STUDIES

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

THE UNIVERSITY OF BRITISH COLUMBIA  
(Vancouver)

August 2022

© Zakir Suleman, 2022

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, a thesis entitled:

LEARNING TO TRUST: EXPLORING THE RELATIONSHIP BETWEEN USER ENGAGEMENT AND PERCEPTIONS OF TRUSTWORTHINESS IN SELF-SOVEREIGN BLOCKCHAIN SYSTEMS

---

submitted by Zakir Suleman in partial fulfillment of the requirements for

the degree of 

---

Master of Library and Information Studies

in 

---

Library and Information Studies

---

**Examining Committee:**

Dr. Victoria Lemieux, Professor, School of Information, UBC

---

Co-Supervisor

**Additional Supervisory Committee Members:**

Dr. Heather O'Brien, Professor, School of Information, UBC

---

Co-Supervisor

## Abstract

Blockchain can be characterized as a technology that enables social trust between actors. In Satoshi Nakamoto's original vision, trust emerges through transparency, as the technology allows for expert users to verify any transaction by consulting a shared ledger. However, for lay users the technology itself can be quite opaque. Further, in private, permissioned medical blockchain applications, transparency can conflict with the need for confidentiality. This leaves an open question of how blockchain can enable social trust in these situations. Research on blockchain technology points to the importance of user experience design as providing a foundation. What then is the relationship between how users experience blockchain systems and how they may come to trust them? While there is some research exploring how user experiences with blockchain systems influences trust, the relationship between the front-end design of these systems, user engagement, which has been a major focus of user experience design for non-blockchain systems, and user trust in blockchain and distributed ledger systems has not explored previously. To address the gap in this nascent area of literature, this study presents original exploratory research on the relationship between user engagement and the user's perception of trustworthiness with MYPDx, a prototype blockchain system that utilizes self-sovereign identity principles to enable patients to share genetic and other biomarker information with healthcare researchers. This research utilizes multiple methods to explore the relationship between user engagement and users' perception of blockchain system trustworthiness, utilizing survey and interview data gathered during usability testing with a diverse sample of users (n=20). A strong positive correlation was established between the extent to which users found the system engaging and assessed the system to be trustworthy. The extent to which MYPDx was seen as usable was most strongly correlated with

users' assessment of its trustworthiness. Analysis of the research data indicates that users undergo a process of learning about the system through engagement, employing indicators from the system's user interface to assess whether to trust the system. This study explores this interaction in more detail, presenting a theoretical picture of this phenomenon and design principles to inform future design and research.

## **Lay Summary**

If an online platform is designed with users' security and control in mind, do users notice or care? How do users learn to trust unfamiliar systems? This research explores how users assess whether systems are trustworthy, specifically exploring user experiences within the context of a new blockchain-based system called MYPDx that enables users to securely share biological information to enable important research into new cures and treatments for diseases. This research found that there is a correlation between how a system positively engages users and whether users feel comfortable in placing their trust in the system. It was observed that users go about learning about unfamiliar systems through engaging with these systems, and that this learning process then enables users to make assessments of trustworthiness of the system. This research presents ideas to inform the research and design of engaging blockchain-based systems in which users feel comfortable placing their trust.

## **Preface**

The identification of the research problem, review of literature, design of the research program and analysis is all the original intellectual product of the author, Zakir Jamal Suleman. This thesis is based on research conducted while the author worked as part of a large, collaborative research team developing and piloting MYPDx. The research team of MYPDx was led by Dr. Victoria Lemieux and included Hoda Hamouda, Danielle Batista, Trinh Nguyen, and Henry Kan. MYPDx is developed in partnership between Molecular You, Stonepaper, Blockchain@UBC. The author helped review the design of the usability protocol used in the MYPDx study and helped to recruit and schedule participants for this research, including contacting Insights West for additional recruiting help. The usability protocol contained in Appendix C was primarily the work of Hoda Hamouda, with contributions by Trinh Nguyen, Danielle Bautista, Henry Kan and the author of this study. Henry Kan and the author were responsible for conducting all user testing as part of the MYPDx pilot. Henry Kan, an undergraduate student in Cognitive Science, wished to gain experience of being a part of both the usability testing and research this author was conducting, and so participated in much of the interviewing and data collection. However, the author of this study was present in every interview and user test, and collected all the survey data and conducted all interviews, with help from Henry Kan. The author of this study was responsible for all data cleaning, organization, and analysis of both qualitative and quantitative outputs. All writing and research for this thesis was conducted by this author, recognizing the disclosures above, with editing from both Dr. Lemieux and Dr. O'Brien. The research conducted was covered by UBC Ethics Certificate number H18-02127, from the UBC Behavioral Research Ethics Board.

## Table of Contents

<b>Abstract .....</b>	<b>ii</b>
<b>Lay Summary.....</b>	<b>v</b>
<b>Preface .....</b>	<b>vi</b>
<b>Table of Contents.....</b>	<b>vii</b>
<b>List of Tables.....</b>	<b>xi</b>
<b>List of Figures .....</b>	<b>xii</b>
<b>List of Abbreviations .....</b>	<b>xiii</b>
<b>Acknowledgements .....</b>	<b>xiv</b>
<b>Dedication.....</b>	<b>xv</b>
<b>Chapter 1: Introduction.....</b>	<b>1</b>
1.1 Background.....	6
1.2 Molecular You Personal Data Exchange (MYPDx) .....	11
1.3 Research Problem, Aims, Goals, and Questions .....	15
<b>Chapter 2: Literature Review .....</b>	<b>19</b>
2.1 General Notions of Trust.....	19
2.2 Trust and Technological Systems.....	20
2.3 Trust and Blockchain Technology.....	27
2.4 Use, Usability, User Experience, & User Engagement.....	33
2.5 The Design of Blockchain Systems.....	41
2.6 Theoretical Framework .....	52
<b>Chapter 3: Methodology .....</b>	<b>57</b>

3.1 Introduction .....	57
3.2 Research Philosophy .....	57
3.3 Methods .....	58
3.4 Recruitment & Participants .....	63
3.5 Procedure.....	65
3.6 Quantitative Analysis .....	67
3.6.1 Instruments .....	68
3.6.1.1 Trust Measures .....	68
3.6.1.2 User Engagement Measures .....	69
3.7 Qualitative Analysis .....	70
<b>Chapter 4: Findings.....</b>	<b>74</b>
4.8 Measures of Trust and User Engagement.....	74
4.8.1 Reliability Analysis .....	76
4.8.2 Descriptive Statistics of the Trustworthiness and Engagement Scales .....	79
4.8.3 Correlation between Engagement and Trust .....	81
4.9 Qualitative Results.....	83
4.9.1 Users' conception of Trust in SSI systems.....	83
4.9.2 Risk as fundamental to Trust.....	87
4.9.3 Reward.....	94
4.9.4 Engagement as Learning Process .....	96
4.9.5 Experience of Engagement as Information for Assessment.....	99
4.10 The influence of the design of SSI systems on user trust and user engagement .....	104
4.10.1 'Technology' as Conceptual Model .....	105

4.10.2	Social layer as relevant to assessment .....	108
4.10.3	Information as Tool and Object of Trust .....	111
4.10.4	Relevant Design Elements for Assessment .....	114
4.10.4.1	Modality .....	115
4.10.4.2	Information Architecture .....	117
4.10.4.3	Organizational Assurances .....	124
4.10.4.4	Visual indicators .....	127
4.11	System Elements Supporting Trust and Engagement .....	128
<b>Chapter 5:</b>	<b>Discussion .....</b>	<b>132</b>
5.12	The Relationship between Trust and Engagement .....	132
5.13	The Relationship between Design and Trust .....	137
5.14	The Relationship between Engagement and Design .....	140
5.15	Design Implications .....	141
5.16	Research Implications .....	145
5.16.1	Design of Blockchain Systems .....	145
5.16.2	Trust .....	149
5.16.3	User Engagement .....	158
5.17	Limitations .....	160
5.18	Future Work .....	163
5.19	Contributions .....	165
<b>Chapter 6:</b>	<b>Conclusion .....</b>	<b>167</b>
<b>References:</b>	<b>.....</b>	<b>168</b>
<b>Appendices</b>	<b>.....</b>	<b>183</b>

<b>Appendix A: Consent Form and Pre-Survey Questions .....</b>	<b>183</b>
<b>Appendix B: Usability Test Protocol .....</b>	<b>190</b>
<b>Appendix C: Interview Protocol .....</b>	<b>206</b>
<b>Appendix D: Post Task Survey.....</b>	<b>207</b>

## List of Tables

Table 1 Propensity to Trust Correlation Matrix .....	76
Table 2 Reliability Analysis .....	77
Table 3 User Engagement Factors.....	80
Table 4 Trust in a Specific Technology Factors.....	81
Table 5 Trust and Engagement Correlation Matrix.....	82

## List of Figures

Figure 1 McKnight et al.'s Validated Model of Trust in a Specific Technology .....	26
Figure 2 Lemieux's Model of Trust in Distributed Ledger Technologies .....	31
Figure 3 Methodology .....	61
Figure 4 Data Collection Workflow .....	66
Figure 5 MYPDx Handshake Process .....	85
Figure 6 Sign Up for Research Study .....	94
Figure 7 Adding Biomarkers to Blockchain Wallet App .....	114
Figure 8 Biomarker Credential Confirmation .....	115
Figure 9 MYPDx Browse Page .....	119
Figure 10 MYPDx Page – MYHI.....	120
Figure 11 Esatus Wallet Proof Request.....	121
Figure 12 Notification examples .....	129

## **List of Abbreviations**

### **Blockchain and Distributed Ledger Technology Abbreviations**

**DLT:** Distributed Ledger Technology

**SSI:** Self-Sovereign Identity

### **Design Abbreviations**

**IA:** Information Architecture

**TSDE:** Trust Supporting Design Element

**UX:** User Experience

### **Engagement Abbreviations**

**AE:** Aesthetic Appeal

**FA:** Focused Attention

**PU:** Perceived Usability

**RW:** Reward

**UE:** User Engagement

### **Trust Abbreviations**

**FUN:** Functionality

**HE:** Helpfulness

**RE:** Reliability

## Acknowledgements

To paraphrase Deleuze & Guattari, many of us wrote this thesis. And since each one of us was already multiple, there really *was* quite a crowd (Deleuze & Guattari, 1988). I wish to thank both of my supervisors for their contributions to this work. I want to thank Dr. Victoria Lemieux for her guidance, mentorship, and support, without which this project would not be possible. Dr. Lemieux provided invaluable kindness and support when I was lost in this project and has helped me to become a better scholar. Thank you. I want to thank Dr. Heather O'Brien for her enduring patience and crucial guidance during the process of learning the skills I needed to produce this research. I grew as a scholar under her guidance by leaps and bounds, and I am profoundly thankful to her for her kindness.

Thank you to MyPDx, Mitacs Accelerate, and Canada's Digital Supercluster for funding different parts of this research. Thank you to the MYPDx Team, especially Hoda Hamouda, Henry Kan, Danielle Bautista, and Trinh Nguyen. Special thanks to Henry for being by my side conducting this research, and Hoda for her experience and direction. I want to thank Paul Bucci for his support and encouragement, which helped me to feel I could actually do this work. Thank you to Ashley Welsh, who helped me to resolve imposter syndrome I didn't even know I had. I want to thank my ancestors on both sides. It's within my family history to choose new directions in quick succession. I want to thank my parents, for teaching me how to be and how to be better. I also want to thank my brother, for his love. Finally, I want to thank my enduring and loving partner, Davida MacBain who helped to make me, and this, what they are. Unfortunately, I can't split a graduate degree into fractions. If I could, a sizable portion of this would be hers.

## Dedication

To whomever cares either enough about me, or this topic, to be reading these words: *thank you for being a part of this desiring machine. May the things that we desire also come to be. May all beings find liberation from suffering.*

## **Chapter 1: Introduction**

As users of computer systems, we are increasingly living in a reality in which every service we use online relies on sharing information about ourselves. This information is often personal: our phone numbers, where we live, or our browsing habits. This information is also often sensitive, including details about our needs, wants, and desires expressed (explicitly or implicitly) through our actions online. Most importantly, this information is often identifying. It involves our emails, usage data, names, social security numbers, or demographic information that can be used to uniquely identify us and the things we do online. This information is often used for purposes unknown to us and may be stored in ways of which we may be unaware. Within the realm of E-Health, a number of influential and important fields of science and medicine rely on one particularly identifying and sensitive type of personal data called “omic” data. Omic refers to the combination of genetic, metabolic, proteomic, microbiome phylum data and other “biomarkers” that can be analyzed from individual blood samples (Vailati-Riboni et al., 2017). The word omics refers to fields of study in the biological sciences that end with -omics, including genomics, proteomics, and metabolomics (Vailati-Riboni et al., 2017). Specific omic data points are called “biomarkers” and give medical professionals a snapshot of individuals’ metabolic processes at the cellular level. This level of analysis provides important insight into the processes that cells undergo to stay alive, grow, and respond to threats (Vailati-Riboni et al., 2017). Biomarkers from individuals are combined to form large data sets, and are then manipulated using machine learning, data mining, and other methods of computational analysis to derive deep insights into the structure of viruses, potential therapeutic treatments, new medical interventions, and studies about the efficacy of treatment regimens (Lin & Lane, 2017, Huang et al., 2017).

To underscore the value of this field, it's worth considering the role of omics science in the context of the COVID-19 Pandemic. Omics science was essential to the rapid response of scientists around the world to the virus and the development of the novel mRNA vaccines against the SARS-CoV-2 virus, and its subsequent variants. At the start of the COVID-19 pandemic, genomics-based approaches were crucial in quickly mapping the structure of the virus and developing insights into its epidemiology (Lu et al., 2020, Ahluwalia et al, 2020). These insights were essential to the development of public health plans at the international and national levels (World Health Organization, 2020b). Many readers will have had a direct experience with omics science through reverse transcription polymerase chain reaction tests (colloquially, 'PCR tests'), which were used in the testing regimes in many countries at the beginning of the pandemic before antigen testing became widespread. PCR tests are one application of transcriptomics, and have been crucial to the data collection, virus surveillance, and planning regimes of countries around the world (World Health Organization, 2020a). Later, multi-omics played a central role in helping expedite the development of a vaccine by quickly analyzing many potential therapeutic approaches against the (now identified) structures of the virus (Muthuramalingam et al., 2020) and analysis of the responses of patients to trial COVID-19 vaccines (Singh et al., 2021). These approaches helped in part to drive the unprecedented speed of the development of the SARS-CoV-2 MRNA vaccines (such as those developed by Moderna and Pfizer) for use in human subjects and have had a massive impact on mitigation of the potential harm of the COVID-19 pandemic (Singh et al., 2021). In the future, vaccinomics and adversomics have the potential to provide crucial insights into differing individual reactions to vaccines, both in terms of effectiveness and potential adverse effects at the individual level (Omersel & Kuželicki, 2021). We can see then how omics science has already had

an impact on our lives. The role of omic science in the development of this globally lifesaving vaccine underscores the emerging value of the field.

The same possibility for rich analysis that helps omics science further human health at a macro scale also drives advances in personalized health. Due to the power of omics-based analysis techniques, omics science offers a variety of benefits for personal health, including personal prediction of the likelihood of disease, screening for potential hereditary conditions, personalized diet and fitness planning, as well as the development of new drugs and treatment therapies for a range of illnesses (Bencharit, 2012). Most importantly, this insight can be gained from one blood sample. However, given the level of analysis possible from one biomarker sample, patients would be well justified in being cautious with sharing their biomarker information. One blood sample, compromised by bad actors and leaked online, could be used to derive all of the above insights for negative ends or be used by unscrupulous companies to affect insurance premiums. At a more basic level, it's hard to imagine many people would be comfortable openly sharing with strangers information that has the potential to reveal family histories of mental illness or hereditary disease. Users would be quite right to question if they trust that the goals and behaviour of the researcher with whom they are sharing their information encapsulates their interests; that is, that the healthcare researchers' work will somehow be of benefit to them directly or indirectly, and that the researcher will handle or use their information in a way that does not harm their interests (Hardin, 2002). In short, the amount to which participants trust researchers is a relevant consideration for the omic sciences.

In our current digital world, trusting relations between social actors, such as between individuals sharing their biomarker information and researchers using that information to identify diseases or to develop novel therapies, is mediated through technology, systems or platforms. Such

systems or platforms often serve as a proxy representation of the trustworthiness of the interacting parties and employ mechanisms that constrain the behaviour of interacting social actors. As such, users' perceptions of the trustworthiness of a system or platform itself is an important, indeed, necessary, precondition to the existence of trusting social relations between social actors.

The architecture and technologies comprising today's information systems are complex and difficult for most users to understand, and users' digital literacy can vary widely. Further, when it comes to medical data, recent scholarship has found that breaches of health records are increasing rapidly in frequency and magnitude (Seh et al., 2020). In one local example, the health records of up to 15 million patients were exposed when LifeLabs, a Canadian medical diagnostic services company, was the subject of a ransomware attack in 2019 (Abedi, 2019). LifeLabs conducts over 100 million laboratory tests in a year (LifeLabs, 2021). Yet because the health information it collects is digitized and centralized, it represented a lucrative target for hackers, who extorted the company for the return of the patient information they had access to (Abedi, 2019). In the current digital environment, sharing a blood sample becomes just another form of digitized information we share in order to access important services, as part of a trend toward the totalizing quantification of as many aspects of human experience as possible (Haraway & Wolfe, 2016).

Users are likely more comfortable sharing information in other ways online and do so every day. We share information online about our lives on social media, have our data scraped through cookies to access "free" newspaper articles, or use services like Google federated identity to sign into new services. Like these forms of information, biomarker information is a kind of uniquely identifying, sensitive, and personal information. However, biomarker information is clearly even more sensitive than this usage data, as it gives professionals the ability to gain insight into even more 'personal' processes that are occurring in the body at a cellular level. Far beyond identifying

us with our birthdate or even political views, health records contain information about our pre-existing health conditions and family medical histories, about our past and (potentially) future health (Webster, 2020). While there are clear benefits to omic science, as it relies on patients sharing their biomarkers with researchers, could one design a system that would enable users to not have to simply accept the risk of potential breaches of their most sensitive data, and enable the large-scale medical benefits we've seen through the COVID-19 Pandemic? Under what conditions might users feel that they have meaningful control over their data, and trust researchers they've never met with their genetic information?

One potential solution is through systems built on blockchain technology, a technical architecture built to enable social trust through decentralized, immutable, cryptographically secure records of value. Through Bitcoin, that first gave rise to and used blockchain technology, Satoshi Nakamoto envisioned a way for unknown individuals to trust each other to achieve important social goals. Similarly, MYPDx, the system at the heart of this study, envisions a way for users to be able to trust researchers with the information that enables medical breakthroughs.

However, even though blockchain technology was designed to enable social trust, it is a category of technology that must still gain the trust of users. As such, blockchain systems must provide indicators that signal to users that it and those using it can be trusted. This is challenging, first, because blockchains, being a novel class of technology, employ complex underlying technologies, such as distributed computing and cryptography. This makes it difficult even for technologically savvy individuals to assess trustworthiness within a given blockchain implementation, let alone lay users. The novelty of the technology also means that clear indicators of trustworthiness are not necessarily available to import from similar systems. Secondly, through its original association with Bitcoin, blockchain technology is intimately linked to

cryptocurrencies. Given that such currencies have been connected with scams, fraud and criminal activity, some users associate blockchain technology with criminal activity rather than trustworthiness (Voskoboynikov, 2020). So, while blockchain systems are designed at a technical level to encourage users to place their trust in such systems, users might have good reasons to perceive even a technically reliable and very difficult to breach system as untrustworthy. Hence, while blockchain is theoretically and technically capable of creating verifiable trust between actors exchanging valuable information (whether money or biomarkers), it is not clear how blockchain system designers can communicate to users that a system *can* be trusted as a mediator of their social interactions, and further, whether or not such a system would be seen by users to be trustworthy. Thus, even though blockchain technology represents a potential solution to the problem of user trust in the privacy and security of digital health records (Lemieux et al., 2021), this potential has yet to be fully realized.

## **1.1 Background**

First proposed by Satoshi Nakamoto in his 2008 whitepaper, a blockchain is an open, immutable, and distributed ledger, recorded on a decentralized cryptographic hash chain, shared between peers (Nakamoto, 2008). Blockchains are designed to enable actors to agree on a shared record of the “truth” without a trusted third party and are often used to store records of valuable information. For example, decentralized finance applications of blockchain technology such as Bitcoin rely on blockchain technology to keep a shared record of the transactions of financial exchanges (Nakamoto, 2008). At a basic level, a blockchain is a cryptographic hash chain of records, which are added following a consensus algorithm by authorized peers (Nakamoto, 2008). While different applications may use different kinds of cryptography, in essence a cryptographic hash function

takes some data as an input and produces a collision resistant output (Swan, 2015., p. 1 – 6). A collision resistant output means that there is only one unique answer to the function hashing the specific data. This implies that any changes to the data in question will change the output of the cryptographic hash function. Because the values of each record of transactions (or ‘block’), is ‘chained’ together, an alteration to one record alters all subsequent records, ensuring that any tampering with the original input data is evident (Swan, 2015., p. 1 – 6). Immutability is considered a core characteristic of blockchain records, which assures their integrity and security through making any tampering computationally difficult and evident to observers (InterPARES, 2017; ISO 2019). Within blockchain technologies, the chain itself is distributed among peers within the system, which all have a common record of the chain. These nodes can then add to the record following the rules outlined in the system’s consensus algorithm. This helps to further ensure the security and validity of the record by ensuring that any attempt to change the ledger must be authorized by validated nodes. The ledger also aligns the incentives of all users to keep a correct record of their own (and therefore everyone else’s’) value, be that value monetary or social. This is understood to incentivize the group to reject malicious changes to the ledger and maintains the veracity of the blockchain. In summary, blockchain technology is designed to enable trusted, immutable records of transactions stored in accessible, decentralized, distributed, automated ledgers.

While decentralized finance blockchain implementations like Bitcoin focus on the transaction of value in the form cryptocurrency, the technology can also be used in cases where there is a need to store, protect, and use important records while maintaining integrity (Lemieux, 2016 & 2022). One potential use case is in the storage and use of an individual’s biomarker information (Lemieux et al., 2020). There is an emerging literature in the nascent area of

blockchain studies exploring attempts to store, share, and utilize health records through different blockchain implementations (O'Donoghue et al., 2019; Zhang et al., 2017; Guo et al., 2018; Kaur et al., 2018; Xia et al., 2017). Within this area of research and design the value of blockchain technology outlined above is inverted, such that the transparency of some blockchain ledgers systems may work against them. Instead of affording trust, the promise of a transparent, unchanging record of information shared between every user on the network may not inspire trust, particularly when the information being stored on-chain is individual genetic information. Indeed, it is hard to imagine a situation where most users would be comfortable storing information about family histories of mental illness, heart disease, or diabetes, in a public, shared record.

Several blockchain solution designs seek to overcome this difficulty by utilizing private, permissioned blockchains. In private, permissioned blockchains those using the system must have authenticated identities to use the system and be authorized to perform certain actions. As such, while these systems also rely on a cryptographic hash chain of records, the integrity of the chain is not ensured solely by decentralization or offering transparency to all users. It is ensured by more traditional security guarantees such as identity and access management, and off-chain governance. For this reason, private permissioned blockchains are often most appropriate where there are only a few necessarily trusted actors within a single organization or set of organizations. Within private blockchain systems, only authorized actors can write to and access the ledger, and are governed by off-chain, real world governance mechanisms. One benefit of this more conventional governance structure is that it enables compliance with regulatory standards within professionalized industries, such as in medical research.

While private, permissionless blockchains mean that individuals' sensitive personal health information is not wide open to public scrutiny, such systems still generally operate by means of

recording interactions between peers in an immutable ledger. As such, there is still a risk that sensitive personal health information can be leaked to system users or administrators, for whom the information is not intended. One solution to this issue is to keep the personal information off chain and record only a hash of it on chain as part of a transaction. This solution has a number of limitations, however. First, information leakage is still possible. Knowledge that an individual has participated in a certain type of transaction (e.g., research studies on diabetes) still can reveal sensitive information even if the details of the transaction remain confidential. For example, the leaking of a transaction recording that an individual has consented to meet with a mental health practitioner, even if the details of their conversation during a meeting remain private, would still constitute a breach of sensitive personal information. Secondly, with quantum computing and cryptanalysis rapidly developing, in the future one-way hash functions may be able to be reverse engineered to reveal the input data, at which time the content of confidential records could be made public. Thirdly, linkages between on-chain transaction records, or “ledger records,” and off chain information can be computationally fragile, and result in broken links which makes later interpretation and checking of the integrity of the information quite difficult or even impossible.

One promising variant of blockchain technology that addresses a number of the above-noted challenges can be found in blockchain protocols that support Self Sovereign Identity (SSI). SSI as a concept seeks to change the current “identity paradigm” of the internet - a paradigm which SSI proponents argue represents both a “usability disaster” and a security risk for both users and organizations (Tobin et al., 2017, p.3). In the current internet identity paradigm, users are required to manage ad-hoc digital identities across many different internet services (Van Bokkem et al., 2019). As Tobin et al. write, current internet identity approaches mean that “the user doesn’t have their own consolidated digital identity, they just have tens or hundreds of fragments of themselves

scattered across different organizations, with no ability to control, update or secure them effectively” (Tobin et al., 2017, p.5). To solve this fundamental issue, Tobin et al. argue to reorient digital identity around SSI, such that:

The individual (or organization) to whom the identity pertains completely owns, controls and manages their identity. In this sense the individual is their own identity provider—there is no external party who can claim to “provide” the identity for them because it is intrinsically theirs (Tobin et al., 2017, p.8).

In his writing, Christopher Allen identified ten foundational principles in designing SSI systems (Allen, 2016). For our purposes, the three most significant principles include the SSI being **portable**, such that no third party controls a user’s identity and it can be moved as the user sees fit, being **controlled** by the user, such that they can control who can see what parts of their data for what purposes, and that the information that is disclosed must be **minimized**, such that the information that is shared is the minimum possible amount needed for the task at hand (Allen, 2016). While SSI has been implemented without blockchain technology in the past, and is not the only blockchain application that stores private information off-chain, blockchain-enabled SSI addresses important problems for the user. Firstly, decentralizing information ensures that users are not reliant on third parties to “give” them their digital identities. Secondly, the cryptographic hashing functions and consensus algorithms of blockchain systems ensure that the information has integrity and is very difficult to tamper with. Finally, SSI blockchain systems minimize the amount of information that needs to be identified about an individual for performance of a given function or delivery of a specific service, achieving minimization (Mühle et al., 2018). This enables users

to grant selective access to their information to other parties without the need to transfer that information or to disclose more information than is necessary to that partner. For example, a user could use an SSI system to verify they are of legal drinking age to a bartender to without needing to share their name, address, or any other identifying information.

## **1.2 Molecular You Personal Data Exchange (MYPDx)**

SSI has been recently applied in the development of Internet of Things (IoT) devices (Gebresilassie et al., 2020) and ridesharing apps (Bothos et al., 2019). In recent work, Lemieux et al. (2021) extend the use of blockchain-enabled SSI from its application in identity management to support sharing personal health information for personalized health research. The proposed system, called MYPDx, implements an SSI-based solution designed to enable privacy preserving and secure sharing of personal health data (Lemieux et al., 2021). This application is designed with the goal of fundamentally respecting users' right to privacy and aims to provide users "with the same level of choice and control over the sharing of their data as they would expect over the sharing of their bodies" (Lemieux et al., 2021 p. 8). The solution architecture is informed by the principles of privacy by design and self-sovereign identity, such that the system:

Is designed to ensure that the identity of data owners is never revealed to researchers, no personal health information is ever recorded or stored on the blockchain to prevent conflicts with privacy laws and reduce the potential for privacy breaches, and data owners remain in control of their personal health information at all times, revealing only as much information as they feel comfortable with given their assessment of the risk-benefits of the transaction (Lemieux et al., 2021, p. 13).

To achieve this, the system utilizes Hyperledger Indy/Aries, an open source blockchain framework, focuses robustly on information governance policies, and ensures that all research projects on the platform meet the rigorous standards of a university Research Ethics Board (REB) (Lemieux et al., 2021). Importantly, throughout this process of contributing biomarker information to a research project, the identity of the data owners is never revealed to researchers, and no personal health information is ever recorded on-ledger. This system is designed to enable data owners to maintain control of their information and only share as much information as they feel comfortable with to researchers, with confidence.

Within MYPDx, the content of the distributed ledger (e.g., public keys of issuers) are shared across a set of permissioned nodes coordinated following a Practical Byzantine Fault Tolerant consensus algorithm. Roles (e.g., individual user/patient, researcher, REB member) can send verifiable credentials, containing verifiable claims (a kind of cryptographically authentic statement), to other roles through the use of software agents. Hyperledger Indy/Aries also employs privacy-enhancing techniques, such as selective disclosure and zero knowledge proofs, that enable agents to prove they have certain claims without disclosing the content of those claims. Each role in the system has a decentralized identifier (DID) which is used to facilitate a connection and communication channel between peers. The public DID's of verifiable credentials issued to individuals are stored on the ledgers and used to verify the authenticity of the data itself. For example, that one researcher from a particular university is associated with a particular research project. This data is then issued by individuals as verifiable credentials, which assert machine-readable statements about the roles. For example, a verifiable credential might assert that that a

project has received REB approval, or that a user has added a particular biomarker to their personal digital health wallet.

From the perspective of users, MYPDx is primarily comprised of a web-based platform and a wallet app. Within the platform, each user has an individual mobile health wallet, in which they can store specific biomarker data. Throughout this process, users utilize this blockchain wallet to scan QR codes on a web-based platform to approve connections between the ledger and their wallet. Researchers use the same platform to request REB approval for their research, and store REB approval as a verified credential within their own cryptographic wallets. This credential can be verified by any users interested in the project to demonstrate that the project has approval. Once a research project has approval, the researchers then use the platform to advertise their projects and recruit participants. Their posting includes detailed explanations of the specific goals and nature of the research project, whether the project has REB certification, which university or corporation the study is affiliated with, the desired demographics of participants, the terms and conditions of the study, and the specific biomarkers needed for the research.

Users on the platform can then find research projects they might want to participate in, learn about the goals of the project, and check if the project has REB certification. If they want to participate in a project, users can initiate an anonymous verification process to check if they meet the study's requirements for demographics and biomarkers using zero knowledge proofs. This enables only the information needed to verify the individual's eligibility to be shared. For example, if a study about diabetes was looking for participants of a specific ethnic background, this process would allow the researchers to check whether the declared ethnic background of the participant was correct for the study without requiring the individual to reveal their actual background. Once determined to be eligible, users can then review a copy of the terms and conditions for the study

and save a copy of the terms in their blockchain wallets for future reference. Finally, users can choose to share their data with the researchers and receive a reward from the researchers for participating.

MYPDx addresses the concerns about both medical blockchain-based applications and SSI systems by using an SSI-based framework to guide the development of a blockchain-based system. The goal of the system is to ensure that users data is private by design and enables greater and more granular control of this important information by actively involving users and obtaining their consent in multiple stages of the process of sending their genetic information. In addition, by not storing medical information on-chain, and utilizing minimizing techniques like zero knowledge proofs, the system attempts to minimize the potential for the data breaches that are increasingly common in other medical systems. Ultimately, MYPDx is designed with the goal of enabling ethical and private sharing of some of the most sensitive personal data imaginable to enable the demonstrated and far-reaching benefits of omics science. Within the area of blockchain studies, there is emergent work on blockchain applications for the management of health records (Guo et al., 2018, O'Donoghue et al., 2019, Jin et al., 2019) data standardization and security in a cloud computing environment (Kaur et al., 2018, Xia et al., 2017) and decentralized apps for patient access to health records (Zhang et al., 2017). There is also burgeoning scholarship on prototype SSI applications within blockchain-enabled healthcare technology (Houtan et al., 2020). However, several things are novel about the MYPDx application both within the context of blockchain enabled health record solutions and blockchain enabled SSI work. Firstly, within the system there is no single identifier which can be traced back to the user. This helps to ensure the further disintermediation of individuals and their data and helps to preserve anonymity and security. Secondly, parties who access user information must have REB approval and conform to REB

standards to be able to receive biomarkers from interested users. From the user’s perspective, users are given information about who is requesting the use of their data to inform their decision to share their omic information. Users are also able to share the minimum amount of data needed to fulfill the purpose of the research, and most importantly, personal data is not transferred, recorded or stored on ledger, further ensuring privacy. Finally, the approach taken by the MYPDx architecture is fundamentally novel in treating health records like other kinds of identity information, using SSI architecture to address privacy concerns with health records (Lemieux et al., 2020).

MYPDx is therefore designed to ensure user privacy and security at the architecture level, while enabling users to assert control over the sharing of their highly sensitive information. However, while the solution architecture here may be novel for numerous reasons this does not necessarily mean users can or will perceive the system as trustworthy. Most users who may want to interact with a system like MYPDx are lay users and won’t necessarily understand or be able to check whether the technical architecture of this blockchain system is trustworthy. Further, blockchain has a negative reputation with many users (Voskoboynikov, 2020). How do users understand blockchain systems to be worth trusting, and what elements of these systems are relevant to their trust? If a system like MYPDx is secure by design, will it matter to user trust?

### **1.3 Research Problem, Aims, Goals, and Questions**

Research in the area of user trust in blockchain-based systems is sparse (Elsden et al., 2018, Voskoboynikov et al., 2021) and very little scholarship has been conducted on the way that the front-end design of blockchain systems influences user trust (Zavolagina et al., 2020). Thus, we are left with the question: if we design a system that is more secure for users to share sensitive information, how can we make users aware that it exists? We know from the field of human

computer interaction that the front-end of a system is the user's first point of contact and is deeply influential on their experience with and perception of the system as a whole (Norman, 2013, Hazenhal, 2011, Doherty & Doherty, 2018, Fallman, 2007). Yet, the small body of research on the user experience of blockchain systems shows that the experience of users has some effect on how users trust blockchain systems, but this effect has not been shown to be causal (Voskoboynikov et al., 2021, Zavalakina et al., 2020). What remains to be discovered is exactly how the front-end design of a blockchain system, and more specifically the experience users have, informs how users come to trust a system. And, even if they do trust the system, what components of the system design contribute to users' perception that a system is trustworthy? We know from HCI research that user experience can be influential on user trust, and that specific elements of the interface and experience can be isolated as being specifically influential. (Söllner et al., 2012, Hoffman & Söllner, 2014, Söllner et al., 2016b). There is also a rich vein of research in Information Science exploring how engagement is a rich way of exploring user experience as a process and product, which has been generative in research in a variety of domains including e-learning, social media, marketing, gaming, and most notably, digital health (O'Brien & Toms, 2008, O'Brien & Toms, 2010, O'Brien & Toms, 2013, O'Brien, 2016b, Doherty & Doherty, 2018). Building on these literatures, this study aims to explore the relationship between the design of blockchain-based SSI systems and user trust, utilizing MYPDx as an artifact for design-based research (Fallman, 2007). This research posits that user experience, specifically user engagement with the system, may be relevant to how users trust blockchain systems. As such the objectives of this research are as follows: 1) To explore what, if any, relationship exists between how systems are designed and the way users come to trust blockchain-based systems, 2) To identify elements of design that affect users' decision to trust a system, 3) To identify what elements of the design affect users' experience

of engagement with blockchain systems, specifically MYPDx. These research goals are formulated into the following research questions:

*RQ1: What is the relationship between user assessments of trustworthiness and user engagement in SSI systems?*

*RQ2: What elements of the design of SSI systems influence user trust in the system?*

*RQ3: What elements of the design of SSI systems influence user engagement?*

Through exploring these research questions, this study aims to contribute knowledge to the under-researched intersection of user experience design and user trust in blockchain-based systems by adding to the one relevant study published to date in this area. While the technical design of blockchain systems is well studied, the user experience or front-end design of blockchain systems remains a niche area of inquiry. Secondly, this study seeks to contribute to development of a theoretical understanding of the relationship between user experience and user trust in blockchain systems, which to the knowledge of this researcher has not been previously explored. This intersection is a crucial area of inquiry both theoretically, and to inform future design work. This research also seeks to extend the body of research on user engagement to the domain of blockchain technology, as it remains to be demonstrated whether the construct holds in this new environment. In addition, as will be discussed, this research extends work from the Management Information Systems field into the domain of blockchain studies, with the goal of providing theoretical contributions to the theory of trust in a specific technology (McKnight et al., 2011). Finally, this research seeks to develop practical implications that can guide the design of future blockchain-based systems. In exploring how users come to trust systems like MYPDx, it is hoped that insights

developed will be useful for designers seeking to show that systems which are trustworthy by design are indeed trustworthy to lay users.

To answer these questions, this research employs multiple methods iteratively as part of a usability study conducted by the MYPDx team. Within the methodology, quantitative and qualitative data are gathered from surveys and interviews with 20 lay users conducted after completing a usability testing protocol with the system. This data was then analyzed iteratively using Spearman's rho and conventional content analysis to develop insights into the above questions. This study begins with a review of relevant literature from the Management Information Systems, Information Science, and Human Computer Interaction fields, and the nascent area of blockchain studies. This review focuses on relevant methodological and theoretical considerations for the proposed work, focusing on the selection of relevant constructs of trust and engagement. The following section outlines the methodology, including the selection of participants, specific instruments used, and the proposed integration of multiple methods. The findings section is organized following the above research questions, seeking to answer these questions by integrating the quantitative and qualitative analysis to present preliminary answers. The discussion section delivers answers to the above questions and discusses the implications for theory in the fields reviewed. Finally, the findings section presents relevant implications for design to guide future iterations of similar systems.

## **Chapter 2: Literature Review**

In this chapter, literature from the fields of Human Computer Interaction, Management Information Systems, Information Science, and the nascent area of blockchain studies is explored to develop a conceptual framework which will inform the methods of data collection and analysis used to answer the study's research questions. This section begins by providing a robust notion of the concepts of 'trust', 'engagement', and 'use', and by exploring how users may come to find blockchain systems trustworthy.

### **2.1 General Notions of Trust**

To begin, we first need a robust conceptualization and definition of trust. We can begin by noting that there are clearly different kinds of trust. Take for example the trust one has in a parent compared to the trust one has in a surgeon. While both can reasonably be called 'trust,' they are both relevant in different contexts. We may trust both to take care of us when we are sick, or to remember our birthdate, but for different reasons. It is also worth noting that these are different applications of the word 'trust.' When we say that we 'trust' that the sun will come up, we 'trust' someone's passport information, and we 'trust' that our smartphones will work, we use the term 'trust' in a different sense than when we talk about 'trusting' a surgeon. In exploring such a ubiquitous and commonly used concept as trust there is the potential to fall into linguistic traps wherein a concept is inconsistently applied to dissimilar contexts based solely on patterns of linguistic usage. As such, it is important to specify what kind of trust we are talking about here. The kind of trust that is of interest to this research has a specific context: a new kind of blockchain system for sending and receiving omics information. The type of trust of interest to this research

is the trust of new users in this system, who have never interacted with the system before. The object of trust, or the thing that is hoped to ensure the users' trust, is the system (understood here as the system itself, rather than the provider of that system). The relationship of trust we are talking about here then is specifically the trust that users are willing to place in a blockchain-based system after interacting with it. With the nature of trust we are interested in specified, we can then explore the kind of theoretical grounding needed for this research. Firstly, we need a theoretical understanding of user trust in technology. Secondly, we need an understanding of what relevant considerations may be for user trust in blockchain systems, more specifically.

## **2.2 Trust and Technological Systems**

There is a rich vein of research on users trust in systems within the field of Management Information Systems (MIS). This research primarily focuses on e-commerce systems, variously exploring user trust in organizations (Mayer et al., 1995), the effect of trust on models of technological adoption (Gefen et al., 2003), the relationship of trust between users and non-human technical artifacts (McKnight et al., 2011), and user beliefs about the trustworthiness of online tools (McKnight et al., 2002). In an interdisciplinary meta-analysis of empirical literature on trust in e-commerce systems, Beatty et al. (2011) synthesized several notable strains of discussion about trust. As Beatty et al. (2011) note, the relationship between the customer and retailer in an e-commerce environment hinges on trust, whereby users “must entrust their personal information to an organization they know only from images displayed on a computer screen” (Beatty et al., 2011, p.2). In e-commerce situations, trust is occurring between the vendor of an e-commerce website (e.g., Amazon) and the user, rather than between sellers on a particular platform or between the website and the user (Beatty et al., 2011, McKnight et al., 2011). In general, risk is understood to

be a fundamental component of trust within this literature, such that trust is always understood to arise in the context of some risk to the user(s) (Beatty et al., 2011). As such, much of the scholarship attempts to accommodate for the relationship between trust and risk, whereby the choice to trust someone or thing implies a calculation of the risk of doing so (Beatty et al., 2011, p.6, Mayer et al., 1995).

Trust as a concept is understood within the MIS field to have cognitive (sometimes called calculative), behavioral, and emotive dimensions which are explored differently across the literature (Beatty et al., 2011). Trust can be placed in individuals (individual trust), organizations (institutional trust) or be a general feature of an individual's outlook (generalized trust) (Gefen et al., 2008). In the context of e-commerce research, generalized trust is typically thought of as an antecedent of trust in a specific system, and institutional trust is understood to be focused on the various structural assurances (e.g. the "undo button") within a system, such that an action or functionality can be reliably carried out by users (McKnight et al., 2002, McKnight et al., 2011, Gefen et al., 2008). The majority of work in this area attempts to explore different antecedents of trust understood as beliefs that influence dispositions to action, and generally are framed with one of the pre-eminent models in the field such as the Technological Acceptance Model (TAM) (Venkatesh & Bala, 2008, Beatty et al., 2011). Usefulness, risk, reputation, integrity, and ease of use have been explored as influential antecedent factors of trust in e-commerce environments (Beatty et al., 2011). Of these factors, usefulness and ease of use emerge as important antecedent features of the design of e-commerce systems to influence user trust (Beatty et al., 2011). In addition, the reputation and integrity of the online seller have been identified as important to how the user understands the relative risk of using an e-commerce platform, where risk is understood

to both negatively and positively influence trust (Beatty et al., 2011). Conversely, the usefulness of a system is understood to be the single biggest influence on future use (Beatty et al., 2011).

While it is possible to synthesize developments within the various antecedents found in the MIS literature on trust in information systems (Beatty et al., 2011, Meeßen et al., 2019, Söllner et al., 2016a), aspects of this theoretical perspective would make it difficult to use within the context of the proposed research questions. Specifically, there is a trend within the MIS literature that operationalizes trust in a system as the intention to ‘use’ a system. This vein of literature utilizes users self-report data about their beliefs about the system to be indicative of their trust in the system *and* their future likelihood to use the system. However, we can imagine scenarios where users may trust a system but still not use it, and, conversely, they might use a system without necessarily trusting it. Further, this research conflates behaviors, intentions, and trust with actual use. Work in this vein therefore potentially confounds identification of factors that may improve our understanding of the antecedents of users’ placing their trust in systems (Meeßen et al., 2019).

To understand this conflation, we can explore foundational work in the field by Gefen et al. (2003). In their 2003 paper, Gefen et al. present a theoretical synthesis of trust with the Technological Acceptance Model, a central model in the field of MIS. The Technological Acceptance Model itself relies on the Theory of Reasoned Action which separates beliefs and actual behaviour by treating beliefs as predictive of future behaviour (Gefen et al., 2003, p. 60, Davis, 1989, Venkatesh and Bala, 2008). Within Gefen et al.’s (2003) work, trust is understood as the set of beliefs of a user about a system, separated from intentions to use a system, which is further divorced from the use of that system. Therefore, a user is understood to trust a system *and* to be likely to adopt the system if they believe it to be trustworthy, without ever necessarily using the system. This work therefore conflates the constructs of perceived trustworthiness, trust,

behavioral intentions, and actual use of technologies (Beatty et al., 2011, p.10, Meeßen et al., 2019). Indeed, the authors readily admit that they conflate the concepts of trust and trustworthiness without giving indications of how to resolve this distinction (Gefen et al., 2008, Söllner et al., 2016a). They also understand ‘use’ to be operationalizable by the same beliefs that operationalize trust, such that use follows from the same beliefs that indicate trust. (Gefen et al., 2008, Söllner et al., 2016a). Importantly however, this perspective does not account for a variety of other potential moderating factors on use including assessments of risk, or importantly for this study, variations in the design and structures of specific systems. This issue extends to later work by the same authors, which relies on the same conceptualizations (Gefen et al., 2008, Söllner et al., 2016a). Indeed, this conflation of trust-related concepts runs through much of the MIS literature on trust in general (Meeßen et al., 2019) As Beatty et al. note, “many authors...treat use of a resource as an operationalization of trust in that resource” (Beatty et al., 2011, p.8). As such, much of the vendor-based trust literature in this field is conceptually ill-suited to the task of examining how specific user experience design decisions might affect user trust in a specific system or platform (Meeßen et al., 2019).

In contrast to vendor-based trust literature, McKnight et al. present a technology-based model of user trust in e-commerce (McKnight et al., 2002, p.336) that does not conflate these concepts, making it suitable for use in this study. This model is understood to be the most significant technology-focused MIS theory of user trust in the literature and has been used as a foundation for an important and ongoing vein of subsequent research on trust in technology within the MIS field. (Beatty et al., 2011, Meeßen et al., 2019, Gefen et al., 2016, Theilsch et al., 2018, Lankton et al., 2015). Within McKnight et al.’s work, trust is understood not as an intention to use a system, but rather the beliefs formed by users about the system after using it, and the actions the

users are willing to take based on those beliefs (McKnight et al., 2002). McKnight et al. conceptualize trust in terms of the initial interaction users have with a technology (McKnight et al., 2002). Within McKnight et al.'s (2002) model, trust is understood as a phenomenon that exists between two actors in a relationship and initial trust refers to trust with an unfamiliar trustee. Within McKnight et al.'s (2002) concept of this relationship, two actors start without enough information or affective investment in each other, and so both parties engage in a process of learning whereby both engage in a trust building behavior such as disclosing personal information, and by means of their engagement, assess the trustworthiness of the other actor based on the consequences of that action (McKnight et al., 2002, p. 335-336). Within initial interactions with a technology, users' perceptions of an interface are understood to be among the factors relied upon to make inferences about the trustworthiness of an application (McKnight et al., 2002). McKnight et al. use this foundation to develop their theory of trust in a specific technology (McKnight et al., 2011).

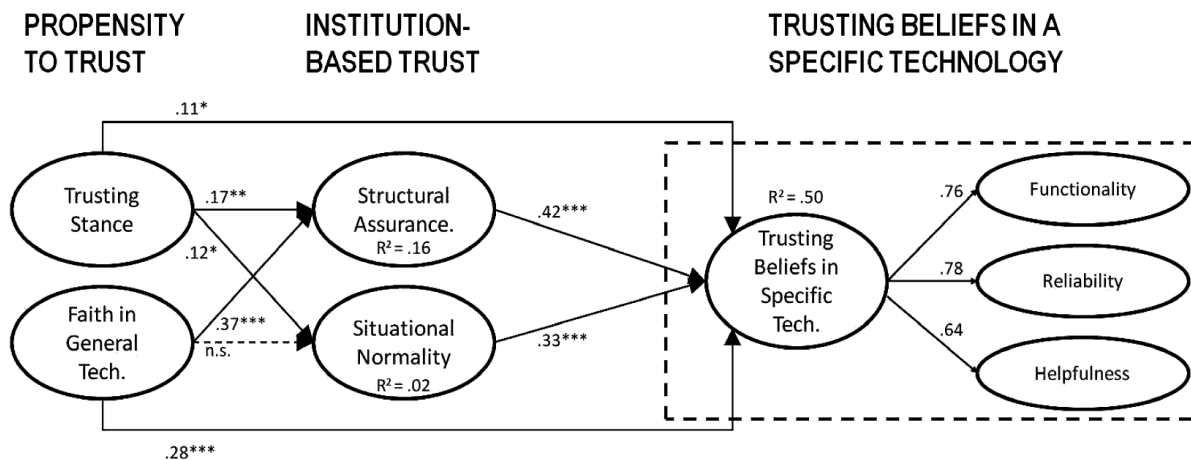
Within their foundational paper on user trust in a specific technology, McKnight et al. (2011) outline a model in which a user's general propensity to trust is mediated by their general trust in the 'institutional environment' (or technology platform) in which they are engaging. In so doing, McKnight et al. focus their work on operationalizing trusting beliefs focused exclusively on a technology, rather than the vendor offering a particular technology-enabled service or other organizational aspects of a technology platform (McKnight et al., 2011, Meeßen et al., 2019). McKnight et al. theorize and then empirically validate a structure of user trust in a specific technology by showing that users' trusting beliefs in the reliability, functionality, and helpfulness of a technology are significantly correlated with user's future usage intentions (McKnight et al., 2011, Meeßen et al., 2019). This interaction and the perceptions of users about a technology are

formed through the interaction of users with the system, and are understood to change from an initial “calculus-based trust” – based on the ways in which the system is seen to conform to the traits of a similar system such that it is reliable and functional and helpful in supporting a user to achieve their goal - to a “knowledge-based trust” founded on a history of successful interactions over time (McKnight et al., 2011). In this way, a user’s interactions with a system are understood to influence the formation of user’s trusting beliefs about the specific technology, and following the TAM, their future adoption or use of the system (McKnight et al., 2011). McKnight et al. outline two sets of constructs within their model that influence user trust in the system: the users’ ‘general propensity to trust’ and the ‘institutional environment’ or technology with which they interact.

General propensity to trust is composed of two constructs: the degree of an individual’s general beliefs about the reliability of technology (General Faith in Technology), and the degree to which an individual believes that positive outcomes will result from technology (Trusting Stance) (McKnight et al., 2011, p.6). The institutional environment in which the users engage is understood to be composed of two constructs as well: the degree of user belief that needed structural conditions are present (e.g., technological features, governance structures, legal frameworks) to ensure a successful outcome in using a given technology (Institution-Based Trust), and the degree to which a user believes that a digitally-mediated situation is normal, and favorable to complete a certain task (e.g., users recognize and are familiar with an interface similar to Adobe Photoshop, in a new environment) (McKnight et al., 2011, p.7). These attributes influence the trusting beliefs of an individual in a specific technology, understood as their beliefs in a technology

to have the capacity to complete a required task (Functionality), the feedback and general guidance given by a technology relative to the user's goal (Helpfulness), and the expectation that a technology will achieve the user's goals consistently and predicably (Reliability) (McKnight et al., 2011, p. 9). These influence the trusting intentions of the user (or their likelihood to adopt the technology) which in turn influence the actual trusting behaviors of the user.

The model of trust in a specific technology presents validated constructs for measuring user trust in technology based in a theoretical foundation that avoids the conceptual confusion of other



**Figure 1 - McKnight et al.'s Validated Model of Trust in a Specific Technology**

work in the MIS field pertaining to use. This presents multiple tools that are of use to the current research agenda. Firstly, McKnight et al.'s work offers a theoretical foundation for understanding user trust that has been operationalized and empirically tested. As such the work offers a quantitative way of measuring a validated construct of user trust. This quantitative measure will be adapted and used in the proposed research to provide a measure of user trust. However, while the questionnaire in McKnight et al.'s work has been adapted and used in other contexts (Beatty et al., 2011, Meeßen et al., 2019, Theilsch et al., 2018, Lankton et al., 2015) as an explicitly context and system-specific measure of user trust, it has not been validated within the context of blockchain

systems. Therefore, while this questionnaire will be adapted in the current study to measure the construct of user trust, there is a need to perform additional analysis about the reliability of this scale within this new context. Secondly, McKnight et al.'s work presents a theoretical grounding for understanding trust that is sensitive to users' interactions with a new kind of a specific technology in a way that differentiates 'use' from 'beliefs' about the system in relationship with user trust. This theoretical grounding creates a foundation for qualitative analysis by relating users' experiences with technology to their trust in that technology.

However, there are a few areas in which additional theoretical considerations are needed to proceed with this research. Firstly, because the research focuses on the design of a novel blockchain-based SSI system, there is a need to review the literature on blockchain systems for additional theoretical and design considerations that may be relevant to this new technological context. Secondly, because users are unlikely to be familiar with using a blockchain-based system for sharing genomic information, there is an open question of what (if anything) situational normality or structural assurances would look like in this context. In addition, as is noted elsewhere, the MIS literature does not distinguish trustworthiness from trust, though McKnight et al. do note a difference between initial and knowledge-based trust (McKnight et al., 2011, Meeßen et al., 2019). Finally, there is still a need for a picture of how 'use' and 'user experience' is relevant to user trust. These concerns will be addressed through a review of literature from the HCI field, as well as recent work exploring the design and research of blockchain systems

### **2.3 Trust and Blockchain Technology**

To orient ourselves to the theoretical considerations of the type of system under examination, we can turn to recent work that theorizes trust in blockchain-based systems. In their book *Searching*

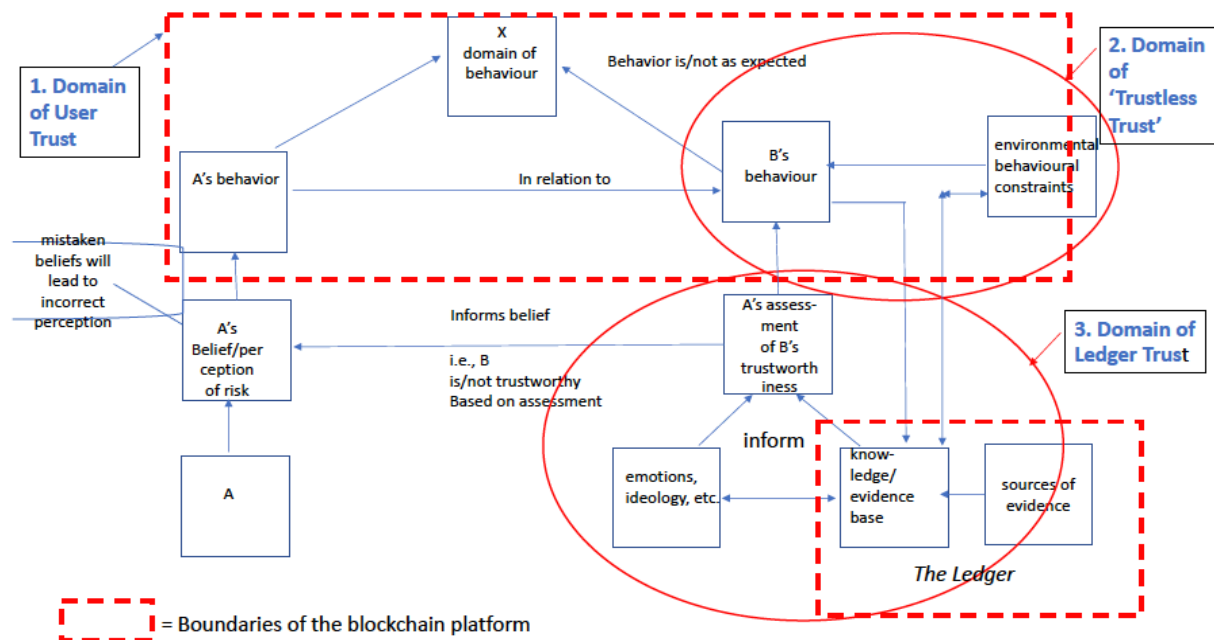
*for Trust*, Lemieux expands upon their work in blockchain studies to present a theory of trust in blockchain systems connecting it to trust in society more generally (Lemieux, 2022, Lemieux, 2016, Lemieux, 2017). This work builds upon previous work by Lemieux & Feng that theorizes blockchain as a socio-informational-technical system (Lemieux & Feng, 2021). Within this work, Lemieux & Feng propose “an integrative multidisciplinary ontological framework” that synthesizes emergent theory with the goal of better describing, assessing, and designing future blockchain and distributed ledger systems (Lemieux & Feng, 2021). Lemieux & Feng argue that blockchain systems, as socio-informational-technical systems, function as a kind of complex system, one that helps to achieve social trust (Lemieux & Feng, 2021). Partly building on Bruno Latour’s Actor Network Theory, blockchain systems are understood to have social, informational and technical ‘actants’, assembled into ‘layers’ in Lemieux & Feng, that are represented in the final design artefact and enable the operation of the system as a whole (Latour, 2005, Lemieux & Feng, 2021). As a complex socio-informational-technical system, blockchain systems require a social system, comprised of actors (as nodes) to be able to trust other actors or at least be sure that their actions are reasonably constrained, to encapsulate the interests of the other party (Lemieux & Feng, 2021; Lemieux, 2022). As such, the motivations, intentions, capabilities, power dynamics, behavior, values, and constraints of actors within the system become a relevant consideration for assessing and designing new blockchain systems (Lemieux & Feng, 2021). This trust is “usually mediated through an informational layer,” namely the records of value created on, and added to, the blockchain ledger (Lemieux, 2022). The ability to write to this ledger, the constraints on actors, and, indeed, the system itself are all enabled through an instantiation of a technical architecture. The technical layer, which is usually focused on as the sole provider of trust within blockchain literature, is understood instead to function as a kind of internal governance on the space of

permissible actions of actors within the system (Lemieux & Feng, 2021). Following the systems theory framework developed by Von Bertalanffy, Lemieux and Feng posit these three layers as unstable sub-systems within a complex system that interact, enable, and constrain each other (Lemieux & Feng, 2021, Von Bertalanffy, 1950). This entails thinking of the model as a kind of dynamic, rather than a deterministic or descriptivist theory. As Lemieux writes, “To attempt to understand blockchain purely in terms of the computational technologies...is to miss the mark by focusing on the wrong abstraction layer” (Lemieux, 2022).

Lemieux utilizes this model as a starting point for their recent theoretical work on trust in blockchain systems (Lemieux, 2022). Within this work, Lemieux explores trust from an interdisciplinary set of perspectives, outlining a framework of trust based on the philosopher Russell Hardin’s conception of ‘encapsulated interest’ (Lemieux, 2022, Hardin, 2002). Within this conception, trust is defined as a “a three-part relationship that exists when a trustor trusts a trustee with respect to a specific domain of activity” (Lemieux, 2022, Hardin, 2002). On Hardin’s conception, trust exists between two actors when an actor is motivated by a belief that their interests are included in what another actor values, such that A trusts B to X (Lemieux, 2022, Hardin, 2002). This trust is necessarily grounded in a relationship between actors that both actors wish to maintain. Because of this relationship, the Actor A can be sure that Actor B will be motivated to encapsulate Actor A’s interest, such that Actor B will reliably achieve some outcome desired by Actor A. Trust is understood here as a cognitive phenomenon, and therefore fundamentally related to the beliefs and knowledge that an actor has (Lemieux, 2022). Risk, drawing on the MIS literature, is understood as a fundamental component of trust, and a way in which actors make themselves vulnerable (McKnight et al., 2011, Lemieux, 2022). Because trust is epistemic and cognitive in nature, risk is ultimately a kind of information asymmetry between

the trusting actor and the trusted actor, whereby the trusted actor knows their own motivations and goals better than the trusting actor (Lemieux, 2022). Based on this asymmetry, the trusting actors must make themselves vulnerable. Through multiple interactions with a trusted actor, trusting actors gain more information to inform their assessment of the trustworthiness of the trusted actor. This information forms the trusting actor's beliefs about the trusted actor and can be based on "their own interests in a matter, the trustee's interests and likely behaviour in relation to the trustor's interests, the trustee's trustworthiness (i.e., whether the trustor perceives that the trustee is likely to behave as expected), and the trustor's perception of the impact if the trustee does not behave as expected" (Lemieux, 2022). Borrowing from McKnight's work, this picture of trust also notes that this information is filtered through a variety of cultural, contextual, and personal features, including "human cognitive biases, the trustor's emotions, the trustor's political ideology, and the trustor's values" (Lemieux, 2022).

Finally, trustworthiness and trust are distinct concepts within Lemieux's work. Trustworthiness is understood to be epistemic and defined as the belief that an actor *is likely* to behave as expected, and in the interest of the trusting actor (Lemieux, 2022). Trustworthiness is understood as a part of users' assessment of a particular system, and distinct from trust, which is one actor's belief that another actor *will behave* in a manner that encapsulates their interests (Lemieux, 2022). Trustworthiness and trust have a necessary but not sufficient relationship, such that trust necessitates trustworthiness, but trustworthiness can exist without trust. Following this, it is possible for a system to be trustworthy, but not trusted. This distinction becomes important for Lemieux when they outline how this picture of trust interacts with blockchain systems as socio-informational-technical systems. When it comes to trust in blockchain systems, Lemieux outlines



**Figure 2 - Lemieux's Model of Trust in Distributed Ledger Technologies**

that there are three distinct and interrelated aspects of the system, broadly corresponding to their three -layer model. These are user trust, trustless trust, and ledger trust. Turning first to ledger trust, Lemieux argues that because blockchains are ultimately distributed ledgers, and therefore a kind of record, they can be profitably analyzed using archival theory (Lemieux, 2016). While discussions of blockchain trust often speak solely about the ‘technology’ enabling trust in actors in an unprecedented way, Lemieux notes that records have long been a foundation for human interpersonal trust by extending our cognition and memory (Lemieux, 2022). Lemieux argues that one key difference between a blockchain ledger and other forms of record keeping that track value is that power in enforcing the authenticity of a record comes from a singular source in conventional records (e.g., the state, a bank) whereas blockchain ledgers have power relationships encoded into the ledger, making power “endogenous” to the blockchain system (Lemieux, 2022). This allows records on the ledger to be a source of final, definitive, and immutable claims about a state of affairs under certain conditions (Lemieux, 2022), providing an epistemic basis for the assessments

of the user about the trustworthiness of other actors with whom they might be transacting using the system (Lemieux, 2022).

Finally, and most relevant to this research, Lemieux outlines a third area of trust in blockchain systems called ‘user trust’, in which the blockchain system mediates trust in both other users and the ledger (Lemieux, 2021). Because blockchain technologies are an emerging technology, many users simply lack an understanding of the basic structures that constrain and enable user behaviors, ensuring the quality of the ledger. In addition, blockchain systems can be implemented in a variety of ways. Because of this, user trust in blockchain systems is theorized as being mediated by users’ interactions with a ledger’s user interface and their experience with using the system. Or, if they lack direct experience, “by what they learn from others about the use (or imagined uses) of these technologies” (Lemieux, 2022). Therefore, the reputational aspects of actors within a blockchain system become more important. As Lemieux writes, “trust in the designers, sponsors, or users of blockchain systems will affect perceptions of the trustworthiness of blockchains as a category of thing” (Lemieux, 2022). Building on work by McKnight et al. in the MIS literature, these perceptions are understood to be formed through an interaction with other users and the technology through the interface (McKnight et al. 2011, Lemieux, 2022). As such the knowledge needed to form trusting relationships is mediated by the experience and interactions of users with a particular system. In Lemieux’s model this perception of the system becomes a key piece of information that informs users’ knowledge about the system. This information is in addition to other factors influencing users’ perception of risk that influence users’ willingness to rely upon blockchain systems in interactions with social peers.

Relying upon McKnight et al.’s (2011) and Lemieux’s (2022) work, we have a more comprehensive picture of the relevant considerations for user trust within technological systems,

and blockchain systems more specifically. Lemieux's work offers a rich theoretical grounding for qualitative analysis of the blockchain-based system under examination. However, while Lemieux offers a picture of how users' experiences with, and use of, blockchain technology may be relevant to their trust in these systems, the model is focused both a different problem (system design) and different questions than the questions asked by this research. This research is concerned with understanding the relationship between trust and engagement in information systems, and how users come to trust these systems. While we now have a working definition of user trust, and an understanding of theoretical considerations for user trust in blockchain technology, we are still in need of an expanded definition of 'use' to build on McKnight et al.'s work (2011). Further, while both the work of McKnight et al. (2011) and Lemieux (2022) examine how users' interactions with technology are relevant to trust, neither offers a concrete theoretical picture of the relationship between users, use, usability, experience, interface, interaction, and technology. To gain a better understanding of the relationship between human beings and technology we can turn to research from the field of Human Computer Interaction (HCI) and Human Information Interaction (HII) which will be reviewed below.

## **2.4 Use, Usability, User Experience, & User Engagement**

Similar to MIS, the HCI field conceives of the way users interact with or 'use' technology in terms of a normative outcome. While in MIS the focus is often the adoption of technology by users (or an ongoing and sustained interaction) as the desired outcome, in HCI the concept of usability (a desirable or efficient interaction) has been a primary goal of design and research (Quiñones & Rusu, 2017). We should note the slight shift in the concept of 'use' here. In the MIS literature use is discussed in reference to the adoption of the system in the future, or the way the interactions

with the system have informed users' trust (e.g., in McKnight's work). However, there is not a clear sense of how the interaction occurs, and how aspects of a system influence the experience of users. This is where we can profitably move to the concept of usability as a more robust way of talking about use. While these concepts are also raised by McKnight as being relevant to the trust of users in systems, work in the HCI literature theorizes both the relationship between system and user and gives insight into which aspects of the system are relevant to this experience (McKnight et al., 2011, Schneiderman et al., 2016).

We can define usability as the “extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” (ISO, 2019). It is important to note here how the concept of usability is fundamentally connected with the way in which systems support being used by individuals for particular goals, and the way in which users are supported to achieve their goals. Indeed, the concept of usability has changed over time, moving from a conception of a usable system as efficient, easy to learn, and error tolerant, to being accessible for diverse users and sensitive to their contexts (Fallman, 2011, Schneiderman et al., 2016, Quiñones & Rusu, 2017). While it may center on different goals, user groups, and context of use, usability still describes the extent to which a system helps achieve a certain objective. The quality and content of those objectives is frequently described within the language of user experience.

Within HCI there has been a movement away from earlier conceptions of usability as a primarily quantifiable phenomenon which can be improved towards one normative goal, toward user experience as a subject of both research and design (Fallman, 2011, McCarthy & Wright, 2004, Doherty & Doherty, 2018). User experience can be defined as a “user's perceptions and responses that result from the use and/or anticipated use of a system, product or service” (ISO,

2019). User experience focuses on the quality of a user's experience with every aspect of a system including the organization, technology, interface, and information (Norman, 2013). The unit of analysis here is the experience of the users, understood as an emergent phenomenon arising from the integration of perception, motivation, action and cognition into "an inseparable, meaningful whole" (Hazenhal, 2011). Building on concepts from cognitive science, users and designers are understood to have mental models, sometimes called conceptual models<sup>1</sup>, of how a particular system works (Norman, 2013). Mental models can be defined as "an explanation, usually highly simplified, of how something works. [The model] doesn't have to be complete or even accurate so long as it is useful [to end users]" (Norman, 2013, p.25). Users develop mental models of a given system based on what they can do with it relative to their goals (affordances), what they can't do with it (constraints), and what is being indicated to them about how to use the system (signifiers) (Norman, 2013). Designers are understood to have their own conceptual models, in their case about how the system they are designing works and can be used to achieve some goal by end users. Within the context of users' interaction with design artifacts then, designers' conceptual model of a way that a system can be used is conveyed to users through their experience of utilizing the system, mediated through the affordances, constraints, and signifiers of the current design of the system (Norman, 2013). An imperfect and iterative process of communication, user experience literature prioritizes the consistent iteration of design artifacts to better support the goals of users and ways users actually use a system (Norman, 2013). User experience as a concept is focused on outcomes of the interaction of a user with a system, much like usability. However, within user

---

<sup>1</sup> Confusingly, the term conceptual model and mental model are used without clarity within Norman's work and within influential design systems like the Apple Human Interaction Guidelines (Norman, 2013). While the idea of mental models pre-date the use of conceptual models by Norman in a design context, I have decided to use the term mental model to refer to the user's model of the system and conceptual model to refer to the model of the system built by designers for clarity.

experience research the focus can be either qualitative or quantitative, and often takes into account the differing social and normative contexts of groups of users' interactions with technology (O'Brien & Toms, 2010). For example, user experience designers of a system might have a more usability-focused goal of reducing the amount of errors users make with an interface, or a more experience-focused goal of improving the way in which users feel connected to a medical practitioner through an E-health portal. User experience researchers and designers explore how these two goals are meaningfully related; while usability focuses on the behaviors of use, user experience focuses on the cognitive and emotional aspects of use, as well as behavioral aspects (Hazenhals, 2011).

Within user experience there are different normative goals that can be designed for, such as greater accessibility. Recently work in HCI has centered on user engagement as a robust way of structuring and measuring the process of user experience, as well as a goal for design (Doherty & Doherty, 2018). User engagement as a concept is described and measured in a variety of ways across disciplines and therefore the exact relationship of user engagement to user experience differs widely (O'Brien, 2016a). Within the field of Information Science, O'Brien and Toms have worked to synthesize these different approaches in their Process Model of User Engagement, within which engagement is understood as a quality of user experience with a system (O'Brien & Toms, 2008). O'Brien et al. have further worked to refine the concept of engagement through a body of interdisciplinary work over the last decade (O'Brien & Toms, 2008, O'Brien et al., 2018, O'Brien et al., 2020). O'Brien et al. define user engagement as "a quality of user experience characterized by the depth of an actor's cognitive, temporal, affective, and behavioral investment when interacting with a digital system" (O'Brien et al., 2018). As such, user engagement represents a framework and measurement tool for the quality and character of a user's experience of using a

particular digital system, along multiple dimensions. This model of engagement, and the subsequently developed User Engagement Scale (O'Brien et al., 2018), have been widely applied and refined for over a decade. This conception of engagement has been explored in the areas of e-commerce, online news, online video, education, haptic and consumer applications, social media, and video games, and is supported by scholarship in the disciplines of Information Science, Human Information Interaction, Information Retrieval, and Human Computer Interaction, among others (O'Brien, 2016b, O'Brien & Toms, 2013, O'Brien & Toms, 2010, Doherty & Doherty, 2018).

To move forward with engagement as a concept we will need to understand why and how it is used. For O'Brien & Toms, user engagement (UE) is understood as a fundamentally dynamic process, mediated by the context, user, and content under examination (O'Brien, 2016a). UE is also understood as a product of people's interactions with computer mediated environments and can be measured as such (O'Brien, 2016b). Following the process model, engagement is theorized as a continuum from shallow to deep, with distinct stages that can be influenced by the context of use, the needs of users, and the nature of the interaction (O'Brien, 2016a). O'Brien & Toms outline these stages as the point of engagement, engagement, disengagement, and re-engagement (O'Brien & Toms, 2008). At the point of engagement, a user starts to interact with the system, either to achieve some goal or to pursue some interest and is spurred to become invested in their interaction with the system by the aesthetic or novel interface, rather than manipulating it in a mechanistic or routine way (O'Brien & Toms, 2008). This initial engagement (and subsequent reengagement) is facilitated by contextual factors, such as the user having sufficient time and ability to manipulate the system, the aesthetic appeal of the interface, and the novel presentation of the interface (O'Brien & Toms, 2008). The engagement stage is then maintained when the system provides sufficient feedback, control, and customization, as well as enabling the user to lose track of time

while also maintaining relevant awareness of other users (O'Brien & Toms, 2008). Users then disengage for various reasons, such as when issues arise with the system's usability, an inappropriate level of challenge is presented, the user becomes distracted, or they simply choose to disengage. At this stage a user can have positive or negative affect about their interaction with the system (O'Brien & Toms, 2008). In either case, a user may then re-engage with the system (O'Brien & Toms, 2008). As such, UE is understood to be both a process and a product of user interactions of computer mediated environments (O'Brien, 2016a).

Within this definition, usability can be understood to be necessary but not sufficient for user engagement, such that an engaging user experience is enabled by a usable system, but a usable system is not necessarily engaging (O'Brien, 2016a). UE is understood as one particular quality of UX among many, and is understood to be a spectrum, ranging from highly engaging to minimally engaging (O'Brien, 2016a). The level of engagement, high or low, and quality of engagement along affective, cognitive, and behavioral dimensions is important to the robust understanding of user experience that engagement represents.

Since first proposing the process model, O'Brien et al., have operationalized the attributes from the scale to develop, validate, and test their User Engagement Scale (UES-LF) and its short form (UES-SF) (O'Brien & Toms, 2010, O'Brien, et al., 2018). Both the model and scale focus on the interaction between the user and technology, and the user's perspective of their engagement with a technology (O'Brien, 2016b). While recent years have seen the development of a variety of methods to measure engagement including behavioral metrics (e.g., page visits) and neurophysiological techniques (e.g., eye tracking) (O'Brien et al., 2016b, Doherty & Doherty, 2018), the UES relies on a subjective self-report of the user's experience of engagement using a validated series of closed questions (O'Brien, 2018). The UES has been described by scholars in

the HCI discipline as “one of the most thorough attempts to develop an understanding of user engagement within the literature” (Doherty & Doherty, 2018). Initially composed of six factors, O’Brien et al. have restructured and validated a four-factor version of their UES scale based on attributes of the process model (O’Brien & Toms, 2010, O’Brien, 2016b, O’Brien et al., 2018). The factors of the current UES-LF are aesthetic appeal, focused attention, perceived usability, and reward (O’Brien et al., 2018). The factors are broken out into items that attempt to capture the concept of UE within the user’s experience of a system (O’Brien et al., 2018). The scale gives an overall score for engagement for a given user-system interaction, based on the levels of the four factors of engagement within their experience of using the system (O’Brien, 2016a).

In many studies that utilize the UES the scale is administered to participants either during or after an interaction with a system (O’Brien, 2016b). Attempts to apply the UES to a new context must be mindful not only of the way that the UES relates to the relevant attributes of the user experience under study, but also to how the system under study presents contextual factors that require the UES to be re-evaluated for use in a new context (O’Brien et al., 2018). The reliability and validity of the scale have been widely tested by its applications in both O’Brien and Tom’s work, and the work of other researchers (O’Brien, 2016b). As such, while the UES may be “flexible, appropriate, and useful” in investigating user engagement across several areas of study, it is important to measure each factor separately with other relevant factors when applying the scale, rather than solely relying on a summative engagement score (O’Brien, 2016b). In addition, it is important to be clear on the specific unit of analysis, scope, and relevant antecedents and attributes of engagement for measuring engagement within a specific context (O’Brien, 2016b). Its wide application suggests that the UES has strong generalizability, though it is not often used

in its full form, but rather used in conjunction with other theoretical and domain specific measurements and theories (O'Brien, 2016b).

To return to the goals of this research, as 'use' is undertheorized within the MIS literature, there is a need for a robust and validated measurement and model of how users utilize technology to explore what, if any, relationship there may be between the design of systems and how users come to trust them. The User Engagement Scale (O'Brien et al., 2018) and Process Model of User Engagement (O'Brien & Toms, 2008) represent the outcome of a decade of inquiry, theory building, and empirical validation, and thorough attempts to understand user engagement within the HCI and HII literature (Doherty & Doherty, 2018). This research utilizes the User Engagement Scale as a measure of users' interactions with and experience of the system under examination (O'Brien et al. 2018). This research also uses the process model of user engagement (O'Brien & Toms, 2008), and its subsequent refinements (O'Brien et al., 2016b) as a theoretical grounding for understanding how users use, interact with, and ultimately engage systems.

Now that we have established a theoretical basis for measuring and understanding user trust and user engagement in a way that is sensitive to the design of systems, we still need to review the state of the literature in the proposed area of study. Specially, research that explores the role of front-end design in creating trustworthy blockchain enabled systems. We can start by noting that the area of blockchain design, and specifically the area of designing for user trust in blockchain systems, is a nascent and emerging area with little available published literature to date. This work intends to contribute to this emerging area.

## **2.5 The Design of Blockchain Systems**

Within work by Lemieux, systems are understood to have a social dimension to their design, and long-term effects which are networked and ultimately political in nature (Lemieux, 2022, Lemieux & Feng, 2021). While obliquely discussed in the MIS literature, technology within the HCI field is widely understood to have social sub-systems, goals, elements, and effects that are intervened upon by the choices of designers and researchers (Watson & Karrufa, 2021, Baxter & Sommerville, 2011, Clemmenson, 2021). It is common within HCI research to focus on some aspect of design within the context of the research question, exploring how design processes or changes effect some variable or phenomenon. This can take the form of the testing of a design through empirical methods, creating new design artifacts which attempt to address some issue, goal, or design fiction, or of creating iterative prototypes to explore a conceptual problem (Fallman, 2007, Watson & Karrufa, 2021, Söllner et al., 2012). The goal of this work is often to produce typologies, or to produce what are called “implications for design,” which can inform the creation of future systems or research (Sas et al., 2014, Elsdén et al., 2018). However, there has been minimal overlap between Human Computer Interaction research and research about blockchain based systems to date. In general, the discussion of the design of blockchain systems within the literature usually refers to design of the overall solution architecture of a system, rather than front-end elements with which the user interacts (Guo et al., 2018, O’Donoghue et al., 2019, Jin et al., 2019, Kaur et al., 2018, Xia et al., 2017, Zhang et al., 2017, Houtan et al., 2020). The intersection of HCI with blockchain studies is therefore currently a niche area within an emergent field. To this researcher’s knowledge at the time of writing, there are currently very few studies which explore the relationship between the front-end design of blockchain systems and trust, and no literature which

explores the relationship between user engagement and trust in blockchain-based systems. The available literature is explored here.

We will begin with the work of Sas & Khairuddin, who have conducted multiple studies into the phenomenon of user trust created in (or through) blockchain-based technologies (Sas & Khairuddin, 2015, Khairuddin et al., 2016, Sas & Khairuddin, 2017, Khairuddin et al., 2019). In their 2015 paper, Sas & Khairuddin develop a research framework for exploring Bitcoin from an HCI framework, relying on work from the MIS field to explore user trust, including the foundational work by McKnight et al. (2011) that will be utilised in this research (Sas & Khairuddin, 2015). Within the Bitcoin ecosystem, Sas & Khairuddin's framework identifies relationships between social trust, institutional trust, and technological trust, with each of these types of trust having fundamentally different objects while being theorized to depend on the technological layer of the system and the trust placed in the technology itself (Sas & Khairuddin, 2015). Sas & Khairuddin (2015) identify four different stakeholders within the Bitcoin ecosystem: users, merchants, governments, and miners, and apply this framework to their specific goals and needs to form a research agenda. The researchers then go on to develop this agenda through their later work, exploring trust in Bitcoin from the perspective of miners (Khairuddin & Sas, 2019) and users (Khairuddin & Sas, 2016, Sas & Khairuddin, 2017, Khairuddin et al., 2019). Through their research on trust in Bitcoin, Sas & Khairuddin have explored the area thoroughly, creating a research framework (Sas & Khairuddin, 2015), exploring how users conceive of trust and issues with trust in Bitcoin (Khairuddin et al., 2016, Sas & Khairuddin, 2017, Khairuddin & Sas, 2019), even creating design artifacts to explore and co-create blockchain architectures with non-technical Bitcoin users (Kairuddin et al., 2019).

Within this work, we can collect a few findings that are relevant to the proposed research. Firstly, Khairuddin et al. (2019) demonstrate that users' have mental models of blockchain systems architecture, and that these models change with exposure to information and relevant aspects of the design. Secondly, Sas & Khairuddin (2017) outline that even users of Bitcoin who rely on its "algorithmic authority" as an object of their trust within the ecosystem still look for reputational information about other actors to mitigate potential risks, indicating that there is a social layer to trust in Bitcoin for users. Based on this finding, they further argue for a more robust reputational system for users as a design implication of their work (Sas & Khairuddin, 2017). Sas & Khairuddin's work is robust, mature, and presents design-focused findings. However, while the focus of this scholarship is similar to the research proposed here, there are two primary limitations on the relevance of Sas & Khairuddin's work for the current study. Firstly, their theoretical framework is strongly focused on Bitcoin and user relationships to this cryptocurrency through wallet apps and other transaction platforms. As such, it is minimally generalizable to the current work that focuses on an SSI blockchain-based application in healthcare. For example, their theory of user trust in Bitcoin relies on the technology of the system (public permissionless blockchain) to ensure social and institutional trust (or what in Lemieux's framework of trust in blockchain systems is called 'trustless trust'). This type of trust is not relevant in the context of this study because MYPDx uses a private, permissioned chain and off-chain governance measures between already trusted nodes (e.g., universities, hospitals). Further, the same features that ensure user trust in Bitcoin, such as transparency, have been shown elsewhere to be a key problem for the viability of systems that transact private health information in which patient privacy is essential (Guo et al., 2018, O'Donoghue et al., 2019, Jin et al., 2019). Therefore, this theoretical work cannot be seen

as necessarily relevant to user trust in the kind of blockchain implementation under examination in this research.

Secondly, the focus of this work is primarily on the architecture level of the design of systems, focusing either on users' perceptions of the architecture that are relevant for trust (Sas & Khairuddin, 2015) or exploring how a design artifact could specifically improve users' mental models of the technical architecture, where an understanding of the specifics of how blockchain technologies are implemented (private/public keys, consensus algorithms, decentralization, etc.) is understood to be relevant to user trust (Khairuddin et al., 2019). However, this research holds as an open question what if any role the technology of blockchain systems has in users' perception of the trustworthiness of systems, seeking to explore what aspects of the design of blockchain systems are relevant to user trust, including the user interface and experience design, not solely the technical architecture. Further, while the architecture of blockchain-based systems has been shown to be important to users' trust in Bitcoin, it's not certain that this will be the case in health-related blockchain systems, and therefore using this theory within the proposed research would unnecessarily restrict the focus of any findings. While technological trust is understood within Sas & Khairuddin's work as a fundamental dependency for other kinds of trust, it's not clear that this would be the case in the context of sending omic information to a researcher where social trust (e.g., with a specific doctor or researcher) or institutional trust (e.g. with a particular company or university) are likely independent of trust users may have in Hyperledger Indy/Aries. Indeed, given the vastly different goals (e.g. privacy vs. transparency) and architecture between public permissionless blockchain systems like Bitcoin and private, permissioned blockchain systems like MYPDx, it's not clear that the technical architecture of the system will be necessarily important to user trust. Therefore, while treating similar subject matter, this literature is used for purposes of

this study as important context that may be relevant to the implications of this research, rather than forming a part of the theoretical orientation of the research.

While some work has attempted to explore the intersection of users and blockchain systems from an HCI perspective, as one of the most mature and recognized blockchain-based application areas, much of this work focuses explicitly on cryptocurrencies. Elsdén et al. created a typology of blockchain applications to guide future research (Elsden et al., 2018). Echoing Sas & Khairuddin, Elsdén et al. also noted that if blockchain is meant to create trust between actors solely by virtue of its architecture, there is a central question of how to demonstrate the trust-preserving nature of the technology and prove the trustworthiness of a system to the end user (Elsden et al., 2018). Here ‘demonstrating facts to the user’ presumes a non-specialist user, to whom one cannot demonstrate the validity of the code or cryptographic credentials that underly the blockchain system (Elsden et al., 2018). This work also raises the question of how to provide users with scrutable parts of the process of transacting on the ledger (Elsden et al., 2018). Similar issues surrounding how information is conveyed to a lay user were raised in an interview study of Bitcoin users by Gao et al., in which users’ felt they needed to understand more about how Bitcoin works than other forms of financial transactions (Gao et al., 2016). The same study noted that a perception of Bitcoin as being complicated or difficult to understand stopped users from using Bitcoin (Gao et al., 2016). Recent work by Voskoboynikov et al. (2020) has documented similar perceptions of non-Bitcoin cryptocurrencies, connecting this lack of information and lack of clear tools to help users learn with the diverse number of crypto wallets available to lay users (Voskoboynikov et al., 2020). Users were observed to be mitigating risk through their behaviors, based on the specific perceived risks associated with a given cryptocurrency (Voskoboynikov et al., 2020). The study noted that despite the diverse interfaces users interacted with, cryptocurrency wallets were united

as a class of technologies by the scenario of their usage, the user experience, and the behavior of users trying to mitigate risk (Voskoboynikov et al., 2020). The study is notable for connecting the role of the user experience to user's perceptions and baseline usability of the blockchain system under study. As they write, Crypto wallets "have usability problems. Combined with misconceptions about cryptocurrencies' building blocks, these UX problems result in barriers that are hard to overcome" (Voskoboynikov et al., 2020, p. 609). Abramova et al. (2021) build on this work, using a cluster analysis to derive three psychometric profiles of cryptocurrency users: 'Hodlers', 'Cypherpunks', and 'Rookies'. Echoing McKnight et al.'s (2011) theory of trust in a specific technology, Abramova et al. show that these three clusters all have differing assessments of relative risk in using crypto wallet based on prior knowledge, literacy, and experience, including their ideological orientation, digital literacy, familiarity with blockchain, and self-efficacy (Abramova et al., 2021). This study also suggests (though does not explore) that adjusting the UX of a particular app based on how meeting the needs and behaviours of the developed user profiles could be a profitable way of trying to cater to the level of functionality and information provided to users in order to improve the overall usability of cryptocurrency apps (Abramova et al., 2021).

Finally, and most relevant to the proposed research, there are three studies which most directly explore the role of UX based on the design of blockchain systems in influencing user trust (Eskandari et al., 2015, Voskoboynikov et al., 2021, Zavolagina et al., 2020). Firstly, in their study of Bitcoin clients, Eskandari et al. (2015) conducted six cognitive walkthroughs to identify potential issues for users. The walkthroughs, conducted by experts familiar with cryptocurrencies rather than lay users of blockchain solutions with native cryptocurrencies, note that the technical metaphors employed by the clients (e.g., 'coins', 'wallet', 'address') may confuse users by either obfuscating or oversimplifying the actual operations of the client (Eskandari et al., 2015). They

also note that highly technical language (e.g., “no free outputs to spend”) had the potential to be confusing, particularly for lay or novice users (Eskandari et al., 2015). These issues, along with a general lack of guidance, were identified by experts as potential barriers to the adoption of blockchain technology (Eskandari et al., 2015). However, it is important to note that while cognitive walkthroughs are a proven method of usability testing, they involve expert testers, not actual users, and so should be contextualized in terms of their validity. While also focusing on cryptocurrency, the finding that language is an important area of analysis for user trust in blockchain systems will inform the analysis of this work.

Secondly, in a thematic analysis of 2,522 app-store reviews of cryptocurrency wallet applications, Voskoboynikov et al. explored how UX can positively or negatively influence the user perceptions of the trustworthiness of blockchain systems. The study found that negative UX compromises the trust of users in crypto wallet apps, and that UX/UI issues were often deeply problematic for users due to the technicalities of blockchain systems (Voskoboynikov et al., 2021). Voskoboynikov et al. (2021) noted that poor UX leads users to question the motives of developers and apps, where it was often interpreted by users as indicating incompetence or bad intent on the part of the developer. This work suggests that not only are users’ perceptions of trustworthiness of cryptocurrencies related to users’ perceptions of the motivations and incentives of other users of a system, but they are also related to users’ perceptions of motivations and incentives of the developers or designers of the system (Voskoboynikov et al., 2021). While this may be a feature of the cryptocurrency space, which is known for scams or fraudulent behavior, this connection between the way that users assess the intentions of developers or designers as part of their assessment of a system’s trustworthiness is particularly important for the proposed research. This empirical finding echoes work by Lemieux (2022), which understands the design of the social sub-

system of blockchains as relevant to user trust. Voskobochnikov et al. (2021) also note that there are both general and domain-specific usability issues at play in the UX problems experienced by users. For example, in instances where apps froze or crashed, a common problem with many apps, users reported an outsized negative consequence, namely access to their funds. Voskobochnikov et al. (2021) also note, echoing Eskandari et al.'s (2018) work and McKnight et al.'s (2011) theory, that users import mental models from non-crypto contexts into using crypto wallets and have insufficient information about how blockchains work, leading to confusion about what to expect. They propose that a guide or tutorial would be helpful to resolve this issue (Voskobochnikov et al., 2021). Unlike other work in the area, Voskobochnikov et al. (2021) also propose concrete, UX-design focused changes, specifically advocating both for the use of proven usability heuristics and the development of domain-specific heuristics to guide the design of cryptocurrency wallets. They note for example that using the Nielsen/Norman usability heuristics, which include 'error prevention' as a heuristic of good design, if used at the prototyping stage, might prevent users from losing cryptocurrency (Voskobochnikov et al., 2021, Nielsen & Molich, 1990).

While this work is promising, like the vast majority of other usability-focused blockchain research it is solely based on cryptocurrency wallet apps, which have their own architecture specific quirks and design specific issues. As mentioned above, the management of health records has been one area of blockchain research in which a system's transparency through a public ledger is not a desirable (or ultimately relevant) aspect of the technological design. (Guo et al., 2018, Donoghue et al., 2019, Jin et al., 2019) In addition, while Voskobochnikov et al.'s (2021) work derives generalizable UX insights for cryptocurrency wallets as a category of technology from aggregated user data, like Eskandari et al. (2015), Voskobochnikov et al.'s work does not involve gathering data from actual users about a specific platform. For more specific methodological

considerations for the proposed research we can look to promising work by Zavolagina et al. (2020) that relies on usability testing, involving users in the design process of a non-cryptocurrency application of blockchain, with a focus on the relationship between UX and trust.

Within the area of HCI, one vein of trust-related research focuses on the analysis and development of trust supporting design elements, or TSDE's (Söllner et al., 2016b) which are developed from theory and iterative user testing (Söllner et al., 2012, Hoffman & Söllner, 2014, Söllner et al., 2016b). An example of a TSDE might be a visualization of information about friends' activity, or a general rating system for resorts within a travel app (Hoffmann & Söllner, 2014). In this work, trust in a system is understood to be able to be influenced through the development and investigation of trust supporting design elements (Söllner et al., 2012). For example, in a study of 143 participants in a redesign of a restaurant booking app to encourage greater trust, the system redesign (in keeping with the TSDE's of understandability and information accuracy) increased self-reported user trust in the system (Hoffman & Söllner, 2014). In their recent work Zavokolina et al. (2020) evaluated a blockchain-enabled car re-selling platform using TSDE's. Like MYPDx, the blockchain system under examination was based on a private, permissioned blockchain ledger. Called Cardossier, it was created and maintained by a consortium of academic, corporate, government agencies and regulatory bodies in Switzerland (Zavolagina et al., 2020). Cardossier asked users to trust the platform with a variety of personal information about the history of their cars and driving habits to enable information parity between car sellers and buyers. In the study, adoption of the system was understood to be hindered by the lack of familiarity with blockchain systems, lack of expertise with using blockchain technology, and privacy concerns (Zavolagina et al., 2020). Through an iterative process of design and evaluation with 22 participants, Zavolagina et al. (2020) found that TSDE's that gave users

information and context about the partners, without overloading them with information, helped to increase trust. Specifically, informative videos, FAQ's, and the logos of partner companies improved user trust for 22 users assessed by an iterative process of interviewing, surveys, and workshops (Zavolakina et al., 2020). Users who were unfamiliar with the blockchain system looked for indicators of the trustworthiness of that system, as well as evidence that the system would work as intended. Zavolakina et al. noted that, unlike applications that rely on AI technology, it was not useful to “blackbox” and hide how the system works from the user to avoid overwhelming them (Zavolakina et al., 2020). Instead, it was important that the right level of information was communicated to the users, relying on data, and communicating the rationale for using blockchain technology. Users also looked for information about the participation and interests of consortium members, which allowed them to extend their trust in the institutions to the system when sharing their information (Zavolakina et al., 2020). Based on their findings, the researchers argue that trust in blockchain systems for new users was passed upwards through the layers of the system for new users, that is, from the blockchain technology to the organizing consortium of business and government bodies to the particular partner implementing the Cardossier platform (Zavolakina et al., 2020). The interface of the system serves then as the primary point of contact, and the way that trust is communicated and developed with the system. Based on this theory, Zavolakina et al. (2020) argue that the correct TSDE's could support the trust of users in this context.

This review of UX-focused user trust research in blockchain presents important considerations that will inform the theoretical framework of the proposed research. Work by Voskobochnikov et al. (2021) lays the groundwork for this study, in connecting negative UX to a lack of user trust within blockchain-based applications (Voskobochnikov et al, 2021) Further,

Voskoboynikov et al.'s work (2021) provides limited evidence for a connection between users experience with the interface of blockchain-based applications and the trust users place in both other users and social actors within the system. Work by Sas & Khairuddin is also understood to be foundational to the theoretical orientation of this study, identifying that users of blockchain systems have mental models about the system's architecture which are relevant to their trust and change with new information and design (Sas & Khairuddin, 2015). Further, Sas & Khairuddin's work provides empirical support for the idea that social trust and institutional trust, rather than solely technological trust, may all influence user trust in blockchain systems such that users need additional assurances about the system and actors within a system before being able to trust blockchain systems (Sas & Khairuddin, 2015). Most relevant to this study however is the work of Zavalakina et al. (2020), which demonstrates that iterative changes to the front-end design of a non-cryptocurrency focused blockchain system can have an impact on user trust. Echoing McKnight (2011), Lemieux (2022), Sas and Khairuddin (2015) and Voskoboynikov (2021), users in the study were observed to look for information about other actors and institutions within the system as part of their assessment of the system's trustworthiness (Zavalakina et al., 2020). Also worth noting for the proposed research is that users of the Cardossier system, as another novel non-cryptocurrency implementation of blockchain technology, looked for information about the system and actors to inform their trust in the system (Zavalakina et al., 2020). Echoing McKnight et al. (2011) users also are looking for indications that the system will work as intended from the information they gain through interacting with the system's interface. While there are important theoretical distinctions between the MIS, HCI, and blockchain focused research reviewed, there appears to be the potential to synthesize an initial theoretical framework which will inform this research. This review of UX-focused research into user trust with blockchain systems work

provides us with a series of relevant findings that can inform the theoretical framework and analysis of this research.

## **2.6 Theoretical Framework**

In outlining the theoretical framework for this research, we can begin by collecting a few aspects of the theories of McKnight et al. (2011) and Lemieux (2022) to create our theoretical foundation for user trust in blockchain systems. While McKnight speaks to a theory of trust in a specific technology, Lemieux outlines how trust may work within blockchain systems, the kind of technology under examination in this research. Lemieux focuses on how aspects of the design of systems (at the level of the architecture) are relevant for users' assessment of trustworthiness and eventual trust. However, Lemieux's work is currently a theoretical model, having yet to be empirically validated. Here, McKnight et al.'s theory of trust in a specific technology, as a validated and influential approach to measuring user trust in technology, can bring an empirically tested measurement of user trust as a construct which is theoretically compatible with Lemieux's work as a model of trust in this specific technology. The theories are compatible on several levels, indeed, Lemieux's theoretical framework of user trust explicitly incorporates parts of McKnight et al.'s framework (Lemieux, 2022). Both scholars understand trust to be primarily cognitive, connected to the process of knowledge formation that users develop from information gained through interacting with a system to achieve some goal (Lemieux, 2022, McKnight et al., 2011). Lemieux, like McKnight et al., holds that the perceptions of users about a system influence users' knowledge and trusting beliefs about a blockchain system (Lemieux, 2022, McKnight et al., 2011). Further, both McKnight et al. (2011) and Lemieux conceive of trust as a relationship between two parties involving inherent risk, though Lemieux brings much additional detail about the nature of

this trusting relationship and distinctions between ‘trust’ and ‘trustworthiness’ (Lemieux, 2022). As Lemieux’s work incorporates McKnight’s theory in their model, and both understand trust as inherently involving risk, being relational, and primarily as cognitive in nature, and, furthermore, are sensitive to how users’ interactions with a system over time influence trust, they are suitable for the proposed research and are complementary theoretical approaches. The proposed research then will adopt both McKnight et al.’s theory of trust in a specific technology and Lemieux’s model of trust in blockchain systems as a theoretical basis for understanding trust. This research uses McKnight’s validated quantitative measurement of trusting intentions and theoretical orientation to measure users’ trusting beliefs in the focal system for this study (i.e., MYPDx). Both McKnight and Lemieux’s work provide a theoretical foundation for the qualitative analysis, where McKnight’s work is understood to pertain to user trust in technology in general and Lemieux’s work introduces technology-specific considerations for MYPDx, as a blockchain-based socio-informational-technical system.

We can now move on to outline our theoretical grounding of ‘use’ within this research. While we have adopted McKnight et al.’s theory as a way of measuring and theorizing trust, this theory requires a definition of ‘use’. As explored above, because ‘use’ within McKnight et al.’s (2011) theory can refer to the usability of the system, the overall user experience, or the process of user engagement of a user interacting with a system, McKnight’s theory speaks to the relevance of design to user trust but does not present a robust way of measuring it. McKnight et al.’s theory is sensitive to the design of systems only through the factor of Structural Assurance, which treats the design of systems as a measurement of to what extent users feel that the right “structures” are in place to ensure they successfully achieve their goals using a specific system (McKnight et al., 2011). The lack of definition about what these structures are and how they relate to the elements

of the design of the system make it difficult to conduct a quantitative or qualitative analysis solely from this factor. In general, without robust conceptions or definitions of use, usability, and user experience, and their relationship to the design of systems, implications generated from the use of McKnight's scale are difficult to contextualize in a valid, generative way that can inform or analyze system design. Here, this research utilizes literature from HCI and Information Science literature to provide a theoretically rich, operationalized, and generalizable conceptual framework for this research. While we have differentiated between use, usability, and user experience above, the concept of user engagement offers a theoretical foundation and tools for measuring and analyzing users' experience of using a system along multiple dimensions (O'Brien et al., 2016b, O'Brien et al., 2018). Further, it has been validated in numerous contexts and shown to be generalizable (O'Brien et al., 2016b). Importantly, the process model of user engagement explicitly foregrounds the way that the design of systems influences the overall experience of users in relationship with their specific goals, enabling a detailed analysis. Within this research, user engagement is utilized to quantitatively measure the way in which MYPDx users are engaged by the system. The quantitative measurements of user trust and user engagement will be analyzed for potential correlations. In addition, O'Brien & Toms' (2008) process model of user engagement, and subsequent refinements (O'Brien et al., 2016a, O'Brien et al., 2016b) are used to ground the qualitative analysis of how user's experience of using the current design of MYPDx relates to their assessments of the system's trustworthiness.

As McKnight et al. write, future studies are needed to examine "the dynamic interplay between users' trust in human agents that build a system, human agents that introduce a system, those that support a system, and the technology itself." (McKnight et al., 2011, p.16). This research seeks to contribute to meeting this need, while contributing to the small body of literature on this

topic area. Rather than positing a relationship between user engagement and trust, this research aims to inductively explore what (if any) relationship may exist between user engagement and trust in blockchain-based SSI systems designed for health data sharing. Within the MIS literature, initial user adoption of a technology is understood to be largely related to cognitive-based trust, which is based on the user's assessment of technological and social factors when deciding whether to use a system for the first time (McKnight et al., 2002). Following the MIS literature, trust is always accompanied by an assessment of risk (Beatty et al., 2011). The risk in this case is how the system will preserve the security, portability, and minimalization of their information, following the goals of SSI systems (Tobin et al., 2017). Trust is conceived of as an emergent property of the relationship between the system and the user (Lemieux, 2022). Trusting beliefs of the user in a specific technology are understood to be based on an assessment of the functionality, helpfulness, and reliability of the system to keep users' omic information safe from bad actors (McKnight et al., 2003, McKnight et al., 2011). In addition, there are relevant concerns that users may have about the institutions and other actors involved that will need to be addressed as relevant to their trust in the system as a whole (Sas & Khairuddin, 2018, Lemieux, 2022). There has been shown to be a connection between the quality of user experience with blockchain-based systems and user trust (Voskoboynikov et al., 2021, Sas & Khairuddin, 2018). The quality of the engagement of the user with the system is therefore hypothesized to affect in some way the trust of the user in that system, in the context of the development of perceived trustworthiness of, and eventual trust in, the system. The quality of engagement is also understood to be meaningfully related to aspects of the front-end design of the system that are relevant to the users' experience of focused attention, aesthetic appeal, perceived usability, and reward (O'Brien et al., 2018). As such, this work seeks to examine what aspects of the design of MYPDx are relevant to users' assessments of trustworthiness and

user engagement. Understanding the initial interaction of the user with the system in terms of the process model gives us a way to more robustly understand the role that the interface plays in enabling users to see the system as trustworthy. This work operationalizes engagement using the UES developed by O'Brien and Toms (O'Brien & Toms, 2010, O'Brien et al., 2018). As such, the study is interested in how new users of SSI systems engage with a system and how aesthetic appeal, focused attention, perceived usability, and reward, as the four factors of the UES-SF may relate to the user's assessment of the trustworthiness of the system (O'Brien et al., 2018). It is hypothesized that the way that the system presents information to users, the indicators it gives about its architecture, and information it conveys about other users and institutions within the platform will be relevant to user trust in the system. (Zavolakina et al., 2020, Voskoboynikov et al., 2021). The quality and accessibility of the language used in this system (e.g. few technical terms) may also be an important determinant of users' trust in this system (Eskandari et al., 2018). Ultimately, information that conveys to users that the system works as intended to achieve their goals is hypothesized to be relevant to user trust (McKnight et al., 2011, Lemieux, 2022, Zavolakina et al., 2020).

## **Chapter 3: Methodology**

### **3.1 Introduction**

This chapter outlines the methodology used by this work, including the research philosophy, recruitment strategy for participants, plan for analysis, and instruments used.

### **3.2 Research Philosophy**

This section begins by outlining the research philosophy used in this work. Taking as foundational work by Bruno Latour (2012), Langdon Winner (1980), and Deleuze and Guattari (1988), this work asserts that technology has a rich and co-constitutive social dimension, whereby technical artifacts are actants with social agents to construct reality. This work maintains the sensitivities Bruno Latour outlines in his work on Actor Network theory, whereby technologies are active participants in dynamic systems and networks that are constitutive of reality (Latour, 2012). Broadly, the main move taken from Latour in the proposed research philosophy is to do away with the ‘modernist’ distinction between subjective and objective when examining user’s experiences with technology (Latour, 2012). Instead, there are many actants and materials in dynamic relationship, whereby “the social” is not wholly constitutive of reality, nor is the ‘objective’ object (Latour, 2012). Both afford and constrain in relationship with the social context of a technology’s conception, design, and usage to co-constitute the ‘subjective’ dimensions of a technology’s effect on individuals or populations (Latour, 1993). As such, artifacts are also understood to have ‘politics’, by virtue of the embedded assumptions and values of the designers that create them, which embody assumptions of power and authority and are embedded in features of the overall design, architecture, and business model enabling the system (Winner, 1980). Lastly, this work

draws on Deleuze and Guattari (as does Bruno Latour) to introduce a sensitivity to the way in which the topography of the dynamic networks that Latour describes is itself constitutive both of political reality and power relationships, and always changing, creating, rupturing, and creating again into new arrangements with new potentials based on the power relationships and pre-existing connections (Deleuze & Guattari, 1987). As such, in aiming to describe a socio—informational-technical phenomenon, this work asserts that its findings will be descriptive of one set of relations, with the goal of informing the next set of relations, taking the form of subsequent prototypes or iterations in this design area. Overall, following Latour, Deleuze and Guattari, and Winner, the orientation of the research philosophy used in this work can be described as broadly pragmatist, in keeping with other strains of design-focused research (Winner, 1980, Deleuze & Guattari, 1987, Piirainen, 2010, Latour, 2012). Within this philosophy, the value of the truth claims made through the knowledge created by this research is not understood to be true through their reference to an ultimately knowable and objective reality (objectivism) nor a subjective and constructed reality (constructivism). Rather, it recognizes “that there are many different ways of interpreting the world and undertaking research, that no single point of view can ever give the entire picture and that there may be multiple realities” (Saunders et al., 2012).

### **3.3 Methods**

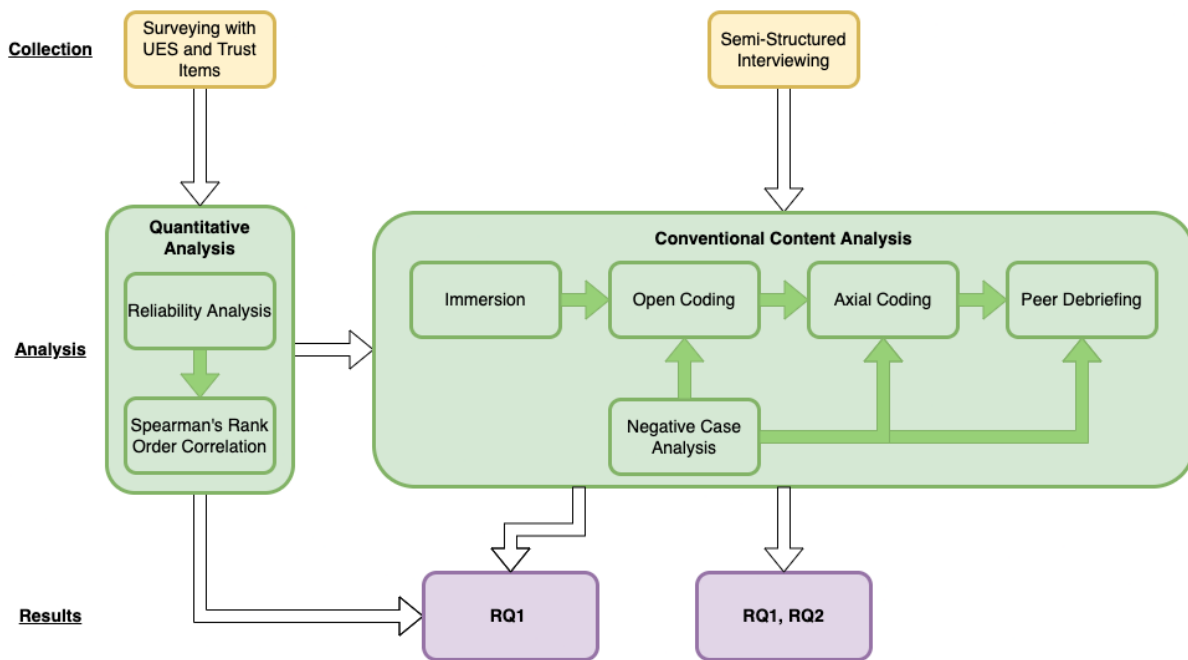
This work employs multiple methods to investigate the phenomenon under examination as part of a usability study. Usability studies are a common research method within the field of Human Computer Interaction and are used in academic and commercial contexts to generate information about the way individuals interact with technology, often for the purpose of improving a specific product or system (Fan et al., 2020). The phenomenon being explored here, both within the

category of the technology (blockchain-based systems), the specific kind of implementation (blockchain-based health information sharing systems) and the relationship itself (trust in a specific technology and user engagement) have not been explored in prior literature. Therefore, the methodology adopted by this research is exploratory (Patten & Newhart, 2017), attempting to describe and theorize about the phenomenon under examination with reference to the data gathered, rather than relying solely upon validating existing theory.

This research was conducted as an embedded member of the MYPDx research team usability study. The team was conducting a usability study to inform the next iteration of the MYPDx prototype. This research was conducted as part of that usability study, utilizing multiple additional methods to explore the research questions. Specifically, surveys and semi-structured interviewing were utilized concurrently, after users had completed the usability test protocol developed by the MYPDx team. Measures taken from the literature on trust in a specific technology, as well as the User Engagement Scale – Short Form (UES-SF) were used to measure the trust and engagement of users respectively through the administered surveying, and to inform the questions asked during the semi-structured interviews. The quantitative and qualitative data was gathered concurrently and analyzed iteratively, utilizing descriptive and inferential statistics and conventional content analysis. The results of quantitative analysis informed the development of categories and direction and observation through the multiple rounds of qualitative content analysis.

It may be asked why this research utilizes validated measurements of both trust and of user engagement respectively for quantitative measurement and qualitative analysis but takes an exploratory approach. This approach was chosen because neither of these measurements have been in prior work tested with blockchain technologies. Further, both the theories emphasize the context

sensitivity of their respective measures to the specific technology and domain under examination (O'Brien, 2016a, McKnight et al., 2011). Therefore, to assume that these scales can be used deductively within this context would be a methodological error caused by asserting the applicability of these scales to a new area without prior evidence. Instead, these measures have been adopted within this exploratory research to help define an otherwise largely undefined phenomenon. The term multiple methods is used consciously here in recognition of discussions in the field of mixed methods research and the methodological norms of usability studies. Usability studies regularly incorporate multiple qualitative and quantitative methods based on the context of the research questions, business needs, and situational constraints (Fan et al., 2020, Tarkkanen & Harkke, 2019). The term “multiple methods” is used in recognition of recent methodological discussions that more thoroughly contextualize the practice within the philosophy, methodology, methods, and community of research of ‘mixed methods research’ as a field (Clark & Ivanokov, 2016). The primary rationale here for using multiple methods was the added value of triangulation and complementarity between methods to enhance the overall validity of the results in the contexts of exploring a phenomenon that does not have a strong foundation within the literature. As Clark



**Figure 3 - Methodology**

and Ivanokov write, “complementarity occurs when researchers need quantitative methods to describe general trends about variables and qualitative methods to illustrate the details of those trends” (Clark & Ivanokov, 2016 p.7). Within this work, the quantitative data and analysis was used to establish the ‘what’ of this research, namely the presence and strength of a relationship between trust and user engagement, and the associated factors of each construct within this context. The findings of that analysis established the existence of the phenomenon under examination, and qualitative analysis was used to establish the ‘why’ and add a richer theoretical picture of the phenomenon. In this way the methodology seeks to improve the validity of its findings through triangulation and complementarity between multiple methods. The methods are used to elucidate different aspects of phenomena being investigated while providing a holistic understanding and ultimately more grounded recommendations for future designs.

Non-probabilistic purposive sampling was used to recruit 20 participants using advertisements in REACHBC, a local health-research portal and using the help of a local research firm, Insights West, for recruitment of study participants. Users were asked to participate in usability testing for a new iteration of the MYPDx prototype. Before being interviewed, participants were asked to complete a survey, including demographic questions ([see Appendix A](#)). All research was conducted remotely with participants during the COVID-19 Pandemic, using Zoom and LetsView to mirror and record the users' computer and phone screens. As part of the usability study being conducted by the MYPDx Pilot Team, participants were asked to complete tasks with the system while using a think aloud protocol (Boren & Ramey, 2000) ([see Appendix B](#)). This experience constituted their only interaction with the system prior to data collection. Users were then interviewed by the researchers ([see Appendix C](#)), and another survey was administered after the interview, comprised of items from the UES-SF and items adapted from McKnight et al.'s (2011) work ([see Appendix D](#)). Data was collected from recorded semi-structured interviews with participants conducted after the tasks from the usability study were completed, and from surveys administered to participants after the interviews.

The data analysis took a convergent approach, establishing the existence and features of the phenomenon being explored using quantitative analysis, then using qualitative analysis to help develop nuanced and structured theoretical insights. The quantitative data collected was analyzed with descriptive and inferential statistics using SPSS statistical software to answer RQ1 (*What is the relationship between user assessments of the trustworthiness of a system and user engagement in SSI systems?*) and indicate possible answers for RQ2 (*What elements of the design of SSI systems influence user trust in the system?*) and RQ3 (*What elements of the design of SSI systems influence the user engagement in the system?*) based on the valence and strength of the relationships between

the two constructs and associated factors. These relationships indicated areas of interest for further exploration through subsequent qualitative analysis. The interview data collected consisted of video recordings and transcripts of semi-structured post-session interviews conducted with participants. This data was analyzed using Nvivo (Online version, release 1.5) qualitative analysis software. Data was also analyzed from the usability test recordings in situations where the topics under discussion were relevant to the goals of this study or were more generative than the content of the interviews themselves. An iterative method of conventional content analysis including negative case analysis and peer debriefing was used to analyze the interview data to add nuance to RQ1 and answer RQ2 and RQ3.

### **3.4 Recruitment & Participants**

Participants for this study were selected using non-probabilistic, purposive sampling. This method was chosen given the exploratory and theory-building goals of this study and is in keeping with sampling methods of similarly-focused HCI research (Lazar et al., 2017). The goals of this sampling were to select a diverse population along the axes of gender, ethnicity, education, age, and employment, so as to better mirror the general population, while specifically recruiting participants who had a lived experience of the healthcare system. Exploratory research with a small sample size can run the risk of sampling an overly homogenous population, particularly if convenience or snowball sampling is used (Lazar et al., 2017, Linxen et al, 2021). Participants were therefore selected to achieve a demographically diverse, though ultimately not a representative sample, to attempt to mitigate this threat to validity. Four participants were recruited through a call for participants posted on a local health research portal (REACHBC). However, close to the start date of the research, the number of appropriate participants responding through

the research portal was insufficient. The remainder were recruited by a local polling firm (InsightsWest), which was contracted by the research team. Participants recruited by the firm answered a demographic survey before participating, using occupation categories employed in recent research in the field based on similar demographic survey work used by Ambramova et al., and ethnicity categories adopted from the Canadian 2016 Census categories (Ambramova et al., 2021, Government of Canada, 2017). Categories were treated as inclusive, allowing participants to give multiple answers to more accurately account for intersecting and hybrid ethnic identities (Westbrook & Saperstein, 2015). Participants received honorariums in the form of an Amazon gift card in recognition for their time. Participants were all healthy at the time of this study.

In total, 20 participants were recruited between the ages of 20 and 75, with lived experience interacting with the Canadian healthcare system. The majority of participants were between the ages of 20 and 34 ( $n=9$ , 45%), with 25% between 45 and 64 ( $n=5$ ), 15% between the ages of 35 and 44 ( $n=3$ ), and 15% between the ages of 65 and 74 ( $n=3$ ) years old. Half of the participants were female ( $n=10$ , 50%) and there were nine male participants (45%) and one non-binary participant (5%). A strong majority of participants indicated their ethnicity as ‘White’, among multiple possible options ( $n=15$ , 68%). Of these 15 participants that indicated ‘White’ as an ethnic identity, two (10%) indicated additional ethnic identities, (White and South Asian; White and Japanese). While 32% ( $n=7$ ) of participants indicated they had a visible minority ethnicity, no participants indicated multiple visible minority ethnicities. ‘South Asian’ ( $n=3$ , 14%) was the most prevalent minority ethnicity represented in the sample, followed by Chinese ( $n=2$ , 9%) and Japanese ( $n=1$ , 5%). Only one participant indicated their ethnic identity as Indigenous, Métis, or Inuit ( $n=1$ , 5%). Of the twenty participants, 55% of participants were employed (‘employed professional’,  $n=9$ ; ‘self-employed/freelancer’,  $n=3$ ), 25% indicated they were current students

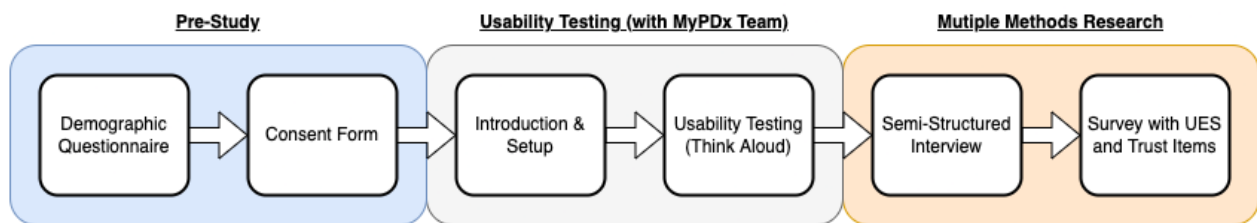
( $n=5$ ), and 15% ( $n=3$ ) were retired. Notably, of the five participants who were current students, all were familiar with the biomedical sciences and research methods, either through their course work or through conducting research themselves. This is further discussed in the “Limitations” section. Most participants indicated that the highest degree they had attained was an undergraduate degree ( $n=10$ , 50%); 30% ( $n=6$ ) had completed some college or university schooling, and the remainder had attained a Master’s ( $n=3$ , 15%) or a PhD degree ( $n=1$ , 5%).

### **3.5 Procedure**

Participants were sent a consent form ([see Appendix A](#)) and administered a pre-intervention questionnaire to complete before their interview session. This questionnaire included demographic questions, questions regarding participants’ familiarity with blockchain technologies, and questions focusing on the participant’s generalized trust ([see Appendix A](#)). As mentioned above, this research was conducted by the study author as an embedded member of the MYPDX research team’s usability testing. Participants were first asked to complete a usability resting protocol ([see Appendix B](#)) with the current iteration of the MYPDx prototype as part of the MYPDx team’s usability testing, and then completed a semi-structured interview ([see Appendix C](#)) and a survey for this research ([see Appendix D](#)). This research was conducted remotely using Zoom video conferencing software and LetsView screen mirroring software to observe how participants used their phones and internet browsers to interact with the MYPDx platform. The usability testing protocol was the only context in which participants of this research were exposed to and gained experience using the system. Within the protocol, users were given a brief overview of the goals of the system and were helped to set up all the associated technology for the remote session. Users were then asked to complete tasks with the system including connecting a mobile blockchain

wallet to the MYPDx web platform, browsing studies on the platform, sending biomarkers to participate in a study, and receiving rewards as verified credentials using a mobile blockchain wallet ([see Appendix B](#)). The usability testing employed a think aloud protocol, asking users to verbalize their thought process in using the system while encouraging users to experiment with the system rather than asking researchers for the correct answer.

Once participants had completed the user testing protocol, they were then guided through a semi-structured interview following a pre-established protocol to capture their experience of using the system ([See Appendix D](#)). Some items asked participants to reflect explicitly on their sense of the system’s trustworthiness, and what parts of their experience with the system informed that perception (e.g. *“What aspects of MYPDx made you feel more assured that the system was trustworthy/not trustworthy?”*). Other questions asked about users’ previous experiences with other technologies (e.g. *“What kind of system did this most remind you of?”*) or understanding of



**Figure 4 – Data Collection Workflow**

how the system worked (e.g. *“How did you feel about having to approve each aspect of the information you were sharing?”*). Once the interview was completed, a survey was administered to participants comprised of the items from the UES-SF, items adapted from McKnight’s work on trust in a specific technology, as well as questions about the likeliness of users to share their information with the system ([see Appendix C](#)).

Each usability session was conducted by two members of the MYPDx Pilot team, Zakir Suleman, the primary researcher and author of this research, and Henry Kan, the secondary

researcher. The researchers took turns conducting the usability testing following the MYPDx protocol. Once the protocol was completed, the semi-structured interviews were conducted by either the primary researcher, or the secondary researcher with follow ups and queries from the primary researcher where appropriate. The primary researcher administered the post-session survey for all participants. Once the survey and interviews were complete the primary researcher gave all participants a high-level overview of blockchain technology to answer any lingering questions for participants. These conversations were for the benefit of participants and were not included in the qualitative data for analysis. Recordings of the sessions, the users' browsers and smartphone screens, and transcripts were recorded for analysis.

### **3.6 Quantitative Analysis**

Quantitative data was collected from surveying participants interacting with the MYPDx prototype and analyzed with descriptive and inferential statistics. The survey was administered to participants after completing a usability testing protocol with MYPDx. The survey data collected was then analyzed using SPSS 27 statistical software. To start with, separate reliability analyses were conducted to ensure the dimensionality of the two constructs under examination, ensuring that the instruments were performing as expected within this new context of examination. Next, the data was analyzed using descriptive statistics to establish potential relationships between the different factors of engagement and user trust. Finally, Spearman's rank order correlation was conducted to determine the valence and strength of possible correlations between the constructs and their associated factors. This research attempts to discover whether there is a correlation between these previously unlinked factors to establish the existence of a relationship while keeping room for additional theory to be built. The valence and strength of the relationships between the

two constructs and associated factors was used to answer RQ1, and to indicate what relationships and factors were of interest for further exploration through subsequent qualitative analysis.

### **3.6.1 Instruments**

#### **3.6.1.1 Trust Measures**

Within this research, we focused on exploring whether the user's experience of engaging with an SSI system for sharing health information affects the user's assessment of the trustworthiness of that system. To explore this, measures for trustworthiness were adapted from McKnight et al.'s construct of trust in a specific technology (McKnight et al., 2011). The construct of trust in a specific technology is understood to be predicted by two factors: propensity to trust and institution-based trust. *Propensity to trust* measures a user's general tendency to be willing to depend on technology and is comprised of faith in general technology (FGT) and trusting stance (TS) (McKnight et al., 2011). *Institution-based trust* measures the belief that outcomes will be successful due to the presence of supportive situations and structures, and is comprised of structural assurance (SA), and situational normality (SN) (McKnight et al., 2011). A user's propensity to trust has been shown to predict their formation of institution-based trust, which in turn has been shown to predict their trusting beliefs in a specific technology (McKnight et al., 2011). Within McKnight et al.'s work, *trusting beliefs in a specific technology* are understood to be predictive of future post-adoptive use of a system, and is comprised of the user's assessment of the reliability (RE), helpfulness (HE), and functionality (FUN), of the system (McKnight et al., 2011).

Items for measuring users' trust in a specific technology in the current research were adapted from McKnight et al.'s work (2013)(discussed further in [Section 3.1.6.1](#)), for this context

and involved altering wording for the specific technology being explored. Six questions were asked to measure propensity to trust factors, which were included in a pre-session questionnaire. Five questions were asked to measure institution-based trust, and six questions were asked to measure the trusting beliefs of participants. These questions were administered in a post-interaction survey. The questions were rated on a five-point scale from 1 (strongly disagree) to 5 (strongly agree). In addition to the measurements of trust from McKnight, participants were also asked their willingness to share personal information with MYPDx as a system on a 5-point scale from 1 (strongly disagree) to 5 (strongly agree). This item was generated independently from the MIS literature on trust. This question is not meant to measure trust, but rather to measure the assessment of trustworthiness made by participants.

### **3.6.1.2 User Engagement Measures**

The user engagement scale short form (UES-SF) was used to measure engagement (O'Brien et al., 2018), and administered as part of the post usability study survey. The construct of engagement measured has four dimensions: aesthetic appeal (AE), perceived usability (PU), reward (RW), and focused attention (FA) (O'Brien et al., 2016a). The UES-SF comprises 12 questions, three for each factor, that can be used to generate information about the roles of differing factors in the overall experience of a user's engagement (O'Brien et al., 2018). The questions were unchanged from the wording outlined in guidance from O'Brien et al. on administering the scale. The questions were rated on a five-point scale from 1 (strongly disagree) to 5 (strongly agree), apart from the three questions capturing perceived usability which were reverse coded, following guidance from the literature (O'Brien et al., 2018).

### 3.7 Qualitative Analysis

The qualitative results of this study are used to generate further insights in answering RQ1, and to answer RQ2 and RQ3. Qualitative data was collected from semi-structured interviews, conducted after participants used MYPDx to complete assigned tasks as part of a usability test protocol. The interview data was collected remotely during the COVID-19 pandemic to ensure participant and researcher safety. Qualitative data collected consisted of video recordings and transcripts of the post usability test interviews conducted with participants, and an iterative method of conventional content analysis was used to analyze the interview data to answer RQ2 and RQ3. Conventional content analysis was chosen as the goal of describing a phenomenon as this new area of research requires a sensitivity to the specific dynamics of the new context of SSI blockchain systems, and in keeping with an inductive approach that builds on what is observed in the data (Bengtsson, 2016). Further, the approach is sufficiently lightweight compared to more comprehensive approaches such as grounded theory while still generating rich insights into a phenomenon (Hsieh & Shannon, 2005). Finally, Hsieh & Shannon note that conventional content analysis is usually used to describe a phenomenon “when existing theory or research literature on a phenomenon is limited” (Hsieh & Shannon, 2005, p.1279). Both McKnight et al. (2011) and O’Brien et al. (2016a) emphasize the context sensitivity of their respective constructs. In the case of work by O’Brien et al., the concept of engagement is understood to differ in different contexts due to the interplay of the four engagement factors within the experience of a user with the specific system under study (O’Brien et al., 2016a). Within McKnight et al.’s work, trust is understood as trust in the ability of a specific technology to reliably ensure a favorable outcome in the context of specific risks, such that the construct of trust in a specific technology differs between technologies or even different versions of a similar class of technology (e.g. Microsoft’s Excel software as distinct from Apple’s

Numbers software) (McKnight et al., 2011). It is in keeping with the methodological perspectives of the theoretical foundation of this research to undertake a mixed (or more specifically, multiple) method(s) of analysis to explore these research questions.

Nvivo (Online version, Release 1.5) qualitative data analysis software was used to review and code the interview data. Following the guidance from Hsieh and Shannon (2005), two successive rounds of open and then axial coding were applied to the interview data. Negative case analysis and peer debriefing were also used to improve the validity of the qualitative analysis. Initially, notes taken during the sessions were combined with reviewing the transcripts and recordings of the interviews to achieve immersion in the text. Next, the text was analyzed using open coding, whereby small units of meaningful text were isolated for their meaning, themes, or context, and labelled as codes (Bengtsson, 2016). The initial codes developed iteratively, changing as needed to incorporate new potential instances. Once this first round of coding was complete, all the text within each code was examined to ensure the internal homogeneity and external heterogeneity, and further refined to develop clusters of categories and where appropriate, themes. (Bengtsson, 2016, Hsieh & Shannon, 2005). For example, within the parent code “Users look for indicators to inform their sense of trust” were two sub codes: “Indicators of authority and authenticity” and “Modality and handshake process”. The code “Indicators of authority and authenticity” included statements such as “if it's health information... I would kind of expect to see some sort of waiver or some sort of information at the beginning (P3)” and “I think that it's important to have an ethics board certificate and the self-attested proof would be important (P7)”. The parent code “modality and handshake process” included statements such as “I sort of decide to share...I can stop at any step and say, okay, you know, I don't think it's a good idea for me...it doesn't, you know, the data doesn't get sent with one click (P1)”, and “plus that you know you're

stepping through all those different steps, where you have to agree to do this and it looks like if at any point you don't like it, you could back out (P5).”

At this point, the findings from the quantitative analysis were used to inform the deductive elements of the second, axial round of coding. Where appropriate and analytically useful, codes were reorganized to better reflect the relationships between the trust and engagement constructs, including relationships between associated factors. For example, initial codes such as “usability problems”, and “assessing trustworthiness based on sense of control” were reorganized under a parent code of “perceived usability” in recognition that both codes spoke to different ways in which the usability of the system influenced user trust in the system (a relationship that emerged in the quantitative analysis). However, the analysis of the interview data indicated that this effect may be positive or negative, depending on the users’ experiences with the system. Wherever needed, the explanations developed in the initial coding were modified to better reflect emerging codes and were adjusted to reflect any negative cases and the structures of the codes were altered accordingly. The interviews were then re-coded using the revised coding scheme.

It has been noted that credibility can be a potential issue when conducting conventional content analysis, thus, an iterative negative case analysis approach was taken when analyzing this data (Hsieh & Shannon, 2005). During the initial coding, a series of provisional explanations were developed (Given, 2008). These explanations attempted to explain the observed structure, context, and relationships between trust and engagement. In instances where divergent phenomena were observed, the explanations were revised to include the unique findings, and then tested by how well they described the relationship between trust and engagement for subsequent cases (Givens, 2008a). In addition, peer debriefing was incorporated during the analysis process to help ensure the validity of the analysis and representativeness of the data collected (Hsieh & Shannon, 2005,

Bengtsson, 2016). The peer reviewer holds a Doctorate in Science Education, was unfamiliar with the project, and regularly designs and implements mixed methods research in their academic and professional work. Once a third iteration of the coding scheme was developed, a peer debriefing session was conducted following established guidelines (Given, 2008b). In this session the codes, categories, themes, and relationships were discussed with the knowledgeable peer who provided feedback on the analysis and provided critique and support where appropriate. Based on this session, the structure and categories of the codes were revised, finalized, and used as a basis for the analysis used to answer RQ1, RQ2, and RQ3.

## Chapter 4: Findings

This chapter outlines the findings of this research organized into sections by the research questions.

The questions asked by this research are:

*RQ1: What is the relationship between trust and user engagement in SSI systems?*

*RQ2: What elements of the design of SSI systems influence user trust in the system?*

*RQ3: What elements of the design of SSI systems influence user engagement?*

As outlined in the methodology section, multiple methods are used to answer each question, and are reported appropriate to the quantitative or qualitative method with reference to how the methods are mixed within the analysis. At the end of this section, the results are synthesized to give a fuller picture of the phenomenon being explored. Further discussion of the results of this research and their relationship to the literature can be found in the Discussion section. In order to answer RQ1, we first need to establish the existence of the constructs under examination within a novel context, speak to the reliability of the measurements used, and then establish what, if any, relationship exists between user assessments of trustworthiness and user engagement within MYPDx.

### 4.8 Measures of Trust and User Engagement

Within this study, quantitative methods were used to establish the existence and quality of a relationship between user assessments of trustworthiness and user engagement. Quantitative data

was gathered from surveying participants using the UES-SF and adapted items from McKnight et al.'s (2011) work on trust in the MIS field.

Specifically, quantitative data about user's sense of the system's trustworthiness was gathered using adapted items from McKnight et al.'s (2011) work on trustworthiness. The construct of trust was comprised of three factors (helpfulness, functionality, and reliability), which were measured by two items each (see Appendix C). The trust items used in this survey relied upon a five-point rating scale. Participants indicated their agreement with the items from 'strongly disagree' (1), to 'disagree' (2), 'neither agree nor disagree' (3), 'agree' (4), and 'strongly agree' (5). For the trust factors, the mean overall trust score was 4 (agree) ( $M=4.07$ ,  $n=40$ ). The data collected for all the responses for each of the factors had a negative skew, with reliability having the most dramatic skew.

The User Engagement Scale Short Form used a five-point rating scale with a total of 12 items. Participants indicated their agreement with the items from 'strongly disagree' (1), to 'disagree' (2), 'neither agree nor disagree' (3), 'agree' (4), and 'strongly agree' (5). In keeping with guidance on best practices in the use of the UES-SF, the three questions measuring the Perceived Usability factor were reverse coded (O'Brien et al., 2018). Within the UES-SF, there were a total of 12 questions administered to 20 participants for a total of 240 data points. The total engagement scores were calculated by taking the average of each individual's responses, following instructions on using the scale (O'Brien et al., 2018). There were no missing values within the data collected from the UES-SF.

#### 4.8.1 Reliability Analysis

A reliability analysis of the trust and engagement subscales was conducted to ensure they were functioning as intended in this research, given the novel context of their application, and the adaptation of the trust scale. Cronbach's alpha was calculated for propensity to trust ( $\alpha = .685$ ,  $M = 3.925$ ,  $SD = 0.72$ ), comprised of two factors (trusting stance and faith in general technology), each comprised of 3 items respectively (see Appendix C). Cronbach's alpha was also calculated for institution-based trust ( $\alpha = .834$ ,  $M = 20.60$ ,  $SD = 3.25$ ), which is comprised of two factors (situational normality and structural assurance), each composed of two and three items respectively (see Appendix C). Finally, Cronbach's alpha was calculated for trusting beliefs ( $\alpha = .835$ ,  $M = 24.45$ ,  $SD = 3.98$ ) comprised of three factors (reliability, functionality, and helpfulness), each comprised of two items (see Appendix C).

**Table 1**

*Reliability Analysis*

	$\alpha$	Mean	SD	Mean of Inter-item Correlation	SD of Correlation
<b>Trust in a Specific Technology Factors</b>					
<b>Propensity to Trust</b>	0.685	3.93	0.724	0.388	0.324
<b>Institution-Based Trust</b>	0.834	4.12	0.902	N/A	N/A
<b>Trust in a Specific Technology</b>	0.835	4.08	0.954	N/A	N/A
<b>Engagement Factors</b>					
<b>Focused Attention</b>	0.576	3.65	0.936		
<b>Reward</b>	0.693	4.267	0.634		
<b>Perceived Usability</b>	0.866	3.383	1.166		
<b>Aesthetic Appeal</b>	0.897	3.367	0.863		

While there is disagreement about the specific value of Cronbach's alpha that is considered to indicate a sufficient level of consistency; in general, 0.7 is understood to be an acceptable value (Tavakol & Dennick, 2011). The value for propensity to trust fell below that value. In arguing for

the sufficient consistency of this value in this novel context, it is worth noting that McKnight's trust in a specific technology construct is an established construct within the MIS field and has been validated in different contexts by McKnight's team, and others (McKnight et al., 2011; Gefen et al., 2014, Söllner et al., 2016a). Common practice when addressing a below 0.7 alpha coefficient as a measure of the value of an alpha for a measurement scale is to review the correlations between the scale items and the total score for that scale, and then to remove items that lower the alpha value (Tavakol & Dennick, 2011). However, in this case there are so few items within each scale that removing items risks compromising the validity of the overall constructs, as validated by previous research. Without removing scale items, another way to ensure unidimensionality is to calculate the mean inter item correlation value and measure the distribution of the inter-item correlation values (Clark & Watson, 2016). A mean inter-item correlation value of between .15 and .50, and a distribution where the majority of the correlation values group close to the mean between .15 and .50 is understood to indicate unidimensionality (Clark & Watson, 2016). The mean inter-item correlation values were calculated for the propensity to trust factor (see Table 2):

**Table 2**

*Propensity to Trust Correlation Matrix*

	<b>M (SD)</b>	<b>TSQ1</b>	<b>TSQ2</b>	<b>TSQ3</b>	<b>FGTQ1</b>	<b>FGTQ2</b>	<b>FGTQ3</b>
<b>TSQ1 – My typical approach is to trust new technologies until they prove to me that I shouldn't trust them</b>	3.66 (.816)	1					
<b>TSQ2 – I usually trust a technology until it gives me a reason not to trust it</b>	3.80 (.941)	.672	1				
<b>TSQ3 – I generally give a technology the benefit of the doubt when I first use it</b>	4.06 (.593)	.299	.288	1			
<b>FGTQ1 – I believe that most technologies are effective at what they are designed to do</b>	4.20 (.560)	.392	.021	.368	1		
<b>FGTQ2 – A large majority of technologies are excellent</b>	4.13 (.833)	.218	.100	.293	.338	1	
<b>FGTQ3 – I think most technologies enable me to do what I need to do</b>	4.26 (.457)	.067	.138	.584	.122	.097	1

The mean inter-item correlation value was .388, and the standard deviation of the correlation matrix was .324. As the internal reliability of these was shown to be between .15 and .5, and the construct of trust in a specific technology has been validated more extensively elsewhere (Söllner et al., 2016a), the propensity to trust scales are understood to be sufficiently unidimensional in the context of this research. The score from the trusting beliefs factors was taken as sufficiently representative of the participants' assessment of the trustworthiness of MYPDx within this new context. The scores from the factors of trust in a specific technology adapted from the work of McKnight et al. (2011) were then used as a measure of participants' assessment of the trustworthiness of the MYPDx system in this research and used to explore the relationship between engagement and trustworthiness.

A reliability analysis was also conducted on the four factors from the UES, which are each comprised of three items (see Appendix C). Cronbach's alpha was calculated for aesthetic appeal ( $\alpha = .897$ ,  $M = 3.367$ ,  $SD = 0.863$ ) perceived usability ( $\alpha = .866$ ,  $M = 3.383$ ,  $SD = 1.166$ ), reward ( $\alpha = .693$ ,  $M = 4.267$ ,  $SD = 0.634$ ), and focused attention ( $\alpha = .576$ ,  $M = 3.65$ ,  $SD = 0.936$ ). However, reward and focused attention fell below an acceptable level of reliability in this context.

The User Engagement Scale factors have been extensively validated for use in a variety of contexts including online search, news, and online gaming, and have also been used to conduct HCI research with similar methodologies (O'Brien, 2016a; O'Brien et al., 2018). As mentioned before, one way to ensure unidimensionality is to calculate the mean inter-item correlation value and measure the distribution of the inter-item correlation values (Clark & Watson, 2015). In this instance, correlation tests were run between the total score for reward and focused attention against the items within their respective subscales. Spearman's rho values for the three focused attention items with the mean value for focused attention were all positive, and moderate to strong (FAQ1

$\rho = .660$ , FAQ2  $\rho = .685$ , FAQ3  $\rho = .840$ ). Spearman's rho values for the three reward items with the mean value for reward were also positive, and moderate to strong (RWQ1  $\rho = .692$ , RWQ2  $\rho = .962$ , RWQ3  $\rho = .684$ ) (See Appendix C for the wording of the items). As the internal reliability of these measures were all moderate to strong, and the engagement scale has been thoroughly validated in diverse contexts (O'Brien, 2016a), the score from the trusting beliefs factors was taken as sufficiently unidimensional and appropriate to measure the participants' experience of engagement in this context.

#### **4.8.2 Descriptive Statistics of the Trustworthiness and Engagement Scales**

The average engagement score was 3.37 indicating a moderate overall level of engagement in users' experiences of using the system ( $n=240$ ) ( $SD = 0.988$ ) (see Table 3). Responses for aesthetic appeal, reward, and focused attention were negatively skewed, with reward having the most dramatic negative skew. Due to both the type of variable (ordinal) and the skewness of the data, the median values are used as the measure of central tendency. Reward had a median value of 4 (somewhat agree) and the lowest standard deviation ( $M = 4.27$ ,  $SD = 0.634$ ), indicating that the majority of participants felt their experience of engaging with MYPDx was characterized by the presence of perceived rewards associated with using the system. Perceived usability had a median value of 4 (somewhat agree) on a 5-point scale, but the largest standard deviation ( $M = 3.383$ ,  $SD = 1.166$ ) as well as a bimodal distribution, indicating that participants had divergent perceptions of the usability of the system: while some participants felt the system was insufficiently usable, most felt that it was usable. This distribution will be explored further in the Discussion chapter. Focused attention had a median value of 4 (somewhat agree), and a standard deviation of 0.936 ( $M = 3.65$ ), indicating that most participants' experience of MYPDx involved an aspect of focused

attention, though not strongly. This finding is also perhaps unsurprising, as think aloud protocols like the one used in this study have the potential to negatively impact users' immersion in a system (O'Brien et al., 2020). This will be further discussed in the Discussion and Limitations sections below. Aesthetic appeal had a median value of 3 (neither agree nor disagree) on a 5-point scale, indicating that the aesthetic appeal of MYPDx was not a significant factor in participants' experience of using MYPDx ( $M = 3.36$ ,  $SD = 0.936$ ).

**Table 3**

*User Engagement Factors*

	<b>Median</b>	<b>Mean</b>	<b>Mode</b>	<b>Standard Dev.</b>
<b>Reward</b>	4	4.267	4	0.634
<b>Perceived Usability</b>	4	3.383	4	1.166
<b>Aesthetic Appeal</b>	3	3.367	3	0.863
<b>Focused Attention</b>	4	3.650	4	0.936
<b>Total Engagement</b>	4	3.370	4	0.988

In terms of trustworthiness, reliability had the highest median value with 5 (strongly agree) on a 5-point scale, as well as the lowest standard deviation ( $M = 4.375$ ,  $SD = 0.807$ ), indicating that a strong majority of participants perceived the system as reliable, with few outliers (see Table 4). Functionality had a median value of 4 (somewhat agree) on a 5-point scale, indicating that a majority of participants felt that MYPDx was sufficiently functional to guarantee success when using it ( $M = 4.275$ ,  $SD = 0.847$ ). Helpfulness had a median value of 4 (somewhat agree) on a 5-point scale, and the highest standard deviation ( $M = 3.575$ ,  $SD = 1.010$ ), indicating that while a slight majority of participants felt MYPDx offered help when needed, for some participants MYPDx was not seen as helpful. This finding will be explored further in the Discussion chapter.

**Table 4***Trust in a Specific Technology Factors*

	<b>Median</b>	<b>Mean</b>	<b>Mode</b>	<b>Standard Dev.</b>
<b>Helpfulness</b>	4	3.575	4	1.010
<b>Functionality</b>	4	4.275	5	0.847
<b>Reliability</b>	5	4.375	5	0.807

#### 4.8.3 Correlation between Engagement and Trust

User engagement and trust were first graphed to examine whether they had a monotonic relationship. Because the data being analyzed was ordinal and paired, and there was a monotonic relationship between the variables, Spearman's rank order correlation was used to analyze the correlation between the two variables (total engagement and total trustworthiness) and their respective dimensions (see Table 5). Within the experience of users interacting with MYPDx, overall engagement and trust had a significant, strongly positive correlation ( $\rho = .848$ ). Engagement was most strongly correlated with helpfulness, as a factor of trust in a specific technology ( $\rho = .804$ ), then by reliability ( $\rho = .737$ ). There was a moderate correlation between engagement and functionality ( $\rho = .553$ ). Trust was most strongly correlated with Perceived Usability ( $\rho = .705$ ), and moderately correlated with Reward ( $\rho = .658$ ) and Aesthetic Appeal ( $\rho = .626$ ). Focused Attention ( $\rho = .510$ ) and trust, while still moderately correlated, was the weakest relationship.

**Table 5***Trust and Engagement Correlation Matrix*

		<b>RW</b>	<b>PU</b>	<b>AE</b>	<b>FA</b>	<b>Overall Engagement</b>
<b>RE</b>	Correlation Coefficient	.645**	.564**	0.393	.688**	.737**
	Sig (2-tailed)	0.002	0.01	0.087	0.001	0
<b>FUN</b>	Correlation Coefficient	0.432	0.413	.550*	0.315	.553*
	Sig (2-tailed)	0.057	0.07	0.012	0.176	0.011
<b>HE</b>	Correlation Coefficient	.578**	.706**	.588**	0.365	.804**
	Sig (2-tailed)	0.008	0.001	0.006	0.114	0
<b>Trust Score</b>	Correlation Coefficient	.658**	.705**	.626**	.510*	.848**
	Sig (2-tailed)	0.002	0.001	0.003	0.022	0

In addition, an inter-factor correlation matrix was created to summarize the relationships between trust and engagement factors (see Table 5). Notably, helpfulness and perceived usability were found to be strongly correlated ( $\rho = .706$ ), as were reliability and reward ( $\rho = .645$ ). Finally, correlations between the expressed willingness to share information (the assessment item) and engagement and trust were analyzed. The single item measuring participants' willingness to share information with MYPDx was strongly correlated with their positive assessment of the trust factors, specifically the system's reliability ( $\rho = .863$ ) and functionality ( $\rho = .806$ ). Of the engagement factors, a willingness to share information was moderately correlated with reward ( $\rho = .632$ ) and focused attention ( $\rho = .601$ ), but not significantly correlated with aesthetic appeal ( $\rho = .345$ ) or perceived usability ( $\rho = .318$ ).

Returning to RQ1, we can note firstly that the constructs were understood upon analysis to be operating as intended within a novel context. Secondly, we can note that there was a strong, positive correlation between user assessments of trustworthiness and the engagement of users

interacting with this blockchain-based system, based on the quantitative analysis. Of the constructs of trust and engagement used here, perceived usability was strongly correlated with perceived trustworthiness and engagement was strongly correlated with helpfulness. There was also a strong correlation between the way that users perceived the system to be usable and how users felt the system to be helpful. These relationships, as well as other significant findings from this analysis, give us an initial picture of the phenomenon we are exploring here.

## **4.9 Qualitative Results**

Where the quantitative results demonstrate the existence and quality of a relationship between the trust and user engagement constructs, qualitative analysis was used to bring theoretically rich descriptions of the relationship being explored. Findings from the quantitative analysis were used to help structure the coding process, which derived inductive themes. These themes were then grouped and structured for internal homogeneity and external heterogeneity. The following themes are most relevant to the relationship between trust and user engagement in SSI systems: a general picture of users' conception of trust in SSI systems, including risk being understood as fundamental to trust and reward as a mitigating factor for trust in risky contexts, and user engagement emerging as a process of learning, with users' experiences of engagement being used as information to inform their assessment of trustworthiness.

### **4.9.1 Users' conception of Trust in SSI systems**

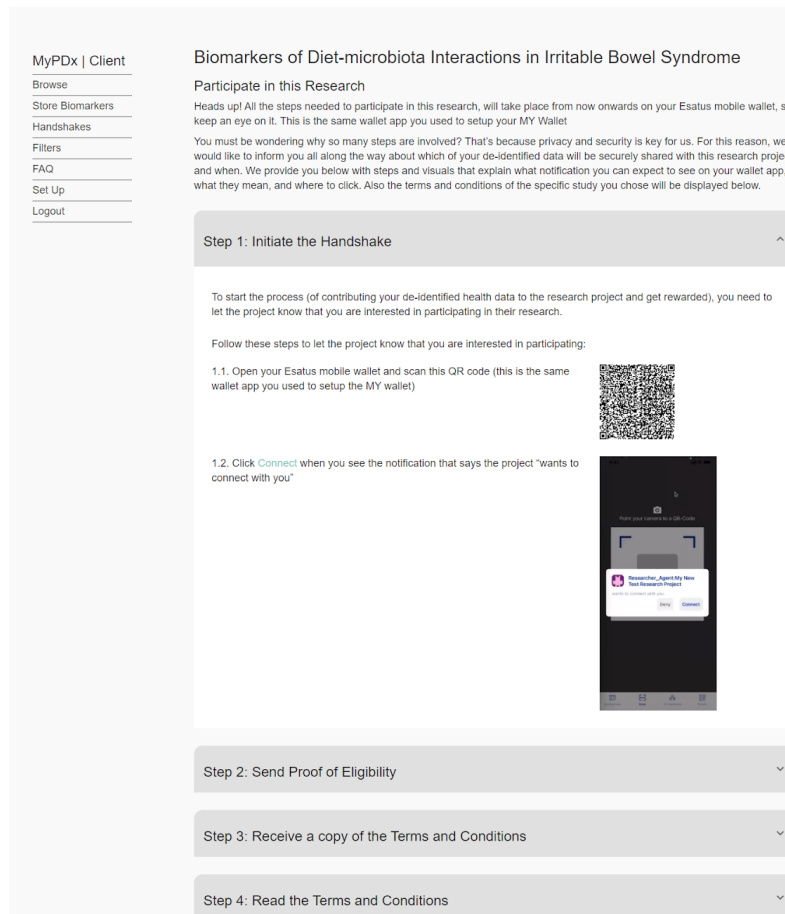
In order to answer what the relationship between trust and engagement was for users, we begin with an exploration of how users conceived of the potential trustworthiness or untrustworthiness of the system. The common conception that emerged from a strong majority of users was that they

felt the system was trustworthy when it had whatever attributes they felt were necessary to mitigate risk, based on specific aspects of the system. Notably, trust was not founded solely (or at all, for a majority of users) on the use of blockchain technology as the basis for MYPDx SSI system. A strong example of this characterization of trust came from participants who specifically spoke to how their experience of the technical architecture of the system contributed to their sense of trust in the system overall. When asked about what made MYPDx trustworthy, P1 said:

I'm having to scan QR codes that only I would have access to. So that's nice to know. And the two-factor authentication. First, you're just checking your eligibility, and there's an entire process that goes through you [to send your data]. Nobody else can do that. Yeah, I imagine it'd be hard to access (P1).

When asked to elaborate on why my MYPDx would be difficult to access, they provided a metaphor of the QR codes being “like a wall. Every QR code you have to scan is like a wall that= you have to go through that you only have the key for. If you have your phone and your app, and you've got that sorted (P1). In this example the user’s experience of using their wallet app to send transactions to the system (by scanning QR codes) is foundational to their sense of the system being trustworthy. The metaphor used here is very telling and speaks to how the user’s experience of the system’s architecture (mediated through the interface) reinforced their conceptual model. With MYPDx, users were asked to scan QR codes on the MYPDx website with their wallet app to transact with the blockchain used by the system and received notifications when different transactions were completed (see Fig. 5). Notably, the user doesn’t mention “blockchain technology” as a justification for trust. Instead, their experience of the system’s technical

architecture helps form a conceptual model of the system connected to technologies with which



**Figure 5 – MYPDx Handshake Process, using the scanning of QR codes**

they are already familiar, which is used as a justification for trust. The user also spoke of a potential risk that was being mitigated by the architecture of the system, namely that their data might be accessed by other people. Their experience of the system's security and understanding of how to use the system leads them to trust that the system couldn't be accessed by anyone other than them, contributing to their assessment of the system as being trustworthy.

For a majority of users, the assessment of trustworthiness was not ongoing, but instead looked like a one-time decision based on relevant information. Users would engage with the system and, once having learned enough about what they felt were relevant aspects of the system to mitigate risk, make a decision about whether the system sufficiently mitigated risks or presented

rewards. As one user said, “I think you need to be initially 100% confident the system is going to work and from there on you’re done (P5).” This sentiment was echoed directly by other users: “my thought was once I did it the first time, I was already two feet in. (P14).” While a majority of users assessed the system once, a minority of users also spoke to a desire for more convenience once they felt the system was trustworthy. This was expressed most clearly by one participant:

Q: Did having to go through all the steps, and having to send each piece of information individually make you feel more in control of the information that you were sharing?

P11: Not really... I think, once you are aware of the biomarkers, when you're ready to just share the information you don't need as much like, when you're ready to go you're good, you know?... the first time, or the first couple times going through it you're getting used to it and you're like ‘okay these are the steps involved,’ but say you've been using it, and say I've gotten my blood tests done and my markers are changed and I'm sharing my data. After that it'd be a little annoying.

Here the user specifies that there is a difference between using the system for the first time and using the system regularly, where after one is “ready to share the information” the process of sending biomarker information securely by scanning QR codes with the wallet app (as they say, “steps”) was less important to the user than then potential lack of convenience over time. Similar sentiments were echoed by other users. For example: “once I start this whole process, I know what it is about. I know that I want to participate in the research and I know that I have to share some information. I just feel like I was checked too many times (P13).” However, it is worth noting that while the majority of users spoke to their assessment of trustworthiness being a one-time

assessment, the explicit desire for more convenience after the system was trusted was only expressed by a minority of users.

Throughout these examples then we can see that trust among the users interviewed was conceived of as a one-time assessment, based on their experience with the system, after which a user's priorities in using the system could change. In the case of some users, like P11 above, the priority then became about the relative usability and convenience of using the platform, rather than its trustworthiness. They had acquired sufficient information from previous interactions to already have determined that the system was trustworthy and feel comfortable placing trust in it.

#### **4.9.2 Risk as fundamental to Trust**

One theme that emerged was the relationship of trust to risk. Almost all interviewees spoke to how they assessed risks and rewards related to using the system as part of their assessment of the system's trustworthiness. In this relationship, in order for the system to be trustworthy it had to mitigate the perceived risks associated with using it. In situations where the system was deemed to be still risky, the system then had to present sufficient rewards to users that they were willing to use the system despite the risk.

Users also spoke to a shared understanding of risk. Almost all users were concerned that the information they were being asked to share through the platform could be used and accessed by unauthorized or malicious actors. We can see the conception of trust as being meaningfully connected to mitigating risk in a comment made by one participant about their assessment of the system as trustworthy:

Yes....really at the end of the day, what sort of a negative impact would that have if they got a hold of [my biomarker data]? What on earth would they be able to use that info for? Right? So I thought about it, and then, [I thought] ‘yeah, I think I’m okay with it.’ There are still couple little like, you know, ‘should I or should I not?’ but, the benefits for me far outweighed the negatives (P20).

We can see in this example how the user clearly located the risk of using the system with unauthorized access to their biological data. The user then deliberated about the potential risks to them of using the system based upon their knowledge of what those risks might be. Finding that they aren’t aware of any potential negative effects from a scenario in which their data is breached, they then weigh that risk against perceived “benefits” to make an assessment of the system’s trustworthiness. This sentiment was echoed in almost all interviews with participants, indicating a consensus among participants that the system was inherently risky to use, as it required sharing their information online with unknown researchers. Many users also attributed risk to the sensitivity of biological data.

Overall, the biomarker information participants were asked to share was perceived as particularly risky. As one user put it: “I share my health card number with my doctor. My name, phone number, whatever email, like that's one thing, but I think what freaks me out is putting like biological data online that's really where it takes a shift for me (P2).” This user stated that it was the combination of both biological data and sharing that information digitally that was at issue. Further, within the online environment, biological data was seen by this user as distinct from more common identifying information such as an email address. Indeed, this connection between digital biological data and risk and reward was made even more explicit by the same user: “It seems like

the more information that you're providing, a little bit more money should be...offered in return because it does feel like you're offering up more of yourself, your data, your information (P2).” Biological data is understood as risky because it is unique and more deeply identifying than an email address or even health card number; it represents some part of the user's “self”, understood as being meaningfully related to “data” and “information.” Therefore, sharing this information carries more risk for the person it identifies. This was echoed by another participant, who spoke about the riskiness of using MYPDx, saying:

How is this information accessible? I mean it'd be nice to know who's viewing it, who has access to it... I think people want reassurance. You know, people may start to put in information and then feel hesitant because they're looking at it and think like ‘who's actually going to find out that I have some syndrome?’ you know things like that... Maybe make it clear how this information can be used, what are the benefits of sharing the information, a lot, besides just the rewards? (P3).

This user also locates the risk of sharing information with unwanted actors viewing the user's biological data, specifically for the ability of that data to identify diseases the user may have or be at risk of developing. Sharing biomarker data then becomes risky, based on how it uses aspects of the biology to identify specific individuals. This potential identification has negative social consequences for users, which the user understood, asking for information about the potential benefits to try to influence their assessment. We can also note that both P2 and P3 echo a common sentiment of making trade-offs between benefits and the risk of using the system

In these examples, then, we can note a common picture of risk's relation to trust. Users understood that there was risk to using the system both through sharing information online, and the nature of that information. Users then looked for ways the system mitigated those risks (e.g., by ensuring their security), or offered benefits, as part of their assessment of the system's overall trustworthiness relative to their understanding of their personal risk.

The awareness of risk online came from two sources: firstly, past experiences with the risks of sharing information online, which were connected to assumptions users brought into the session with MYPDx. For example, one user said “[My TurboTax] account was hacked and like the TurboTax people were freaking out and we spent two hours on the phone with them.... Other than like the actual official government websites I'm pretty much like assuming that anything can be hacked into (P3)”. Secondly, users' awareness of risk came through knowledge they had gained indirectly through other sources: “I think these days, some security data leaks and things like that it's a real issue for people. There's been you know, historical leaks... information can leak out quite easily...information gets hacked (P3)”. Similar pre-session experiences and information about online risks with sharing personal information were noted explicitly by every user in this study and used to inform each individual's assessment of the relative risk of using MYPDx.

Though risk was understood to be inherent to sharing information online for the majority of users, the concern about the severity of that risk depended in part on who the data was shared with. As part of the knowledge that users brought to their assessment, users spoke of various biases toward the likelihood that different kinds of organizations would provide security for their information online. A majority of users were more willing to trust a university, non-profit, or a government rather than a corporation with their information. In some cases, the only organization that was seen to keep data private and safe was the government:

The second you log into your email, the second you log into Facebook, the second you open an app on your phone, like 99% of the time, your data is just, like, out there.... I mean other than, say, like your government, like the [Canada Revenue Agency] website, and you know, doctors' websites, other than those basically any website you log into or any app that you open, you might as well be assuming that everything's out there (P11).

In some cases, the involvement of a corporation was enough to make users want to limit whether they shared their information: "If it's for the greater good...testing for information on vaccines...then, yes. If it is for let's say towards development of a new drug that will bring profits for the company...I don't know if I want to be part of that (P18)." For some users, this was tied explicitly to the ability of insurance companies to base their premiums on biomarker data: "This kind of stuff worries me a bit... when all your health data is out there, an insurance company could gain access to your medical records or your information online; it may impact folks getting their life insurance (P7)." In both instances users indicated that the profit motive of the corporations was an issue for their desire to share their information.

Users adopted different perspectives in the face of this perceived inherent risk to sharing information with MYPDx. In some instances, users spoke to their experience with sharing other forms of personal information online, often with reference to security enhancing behaviors. For example, one user who "had [their] email hacked before (P11)" said, "so I think I would want stronger security settings. That'd be the first thing I look at." It's worth noting in this quote that the user took a pragmatic approach to risk. Having had a pre-existing data breach, their response was not to avoid engaging with services online or sharing information online completely, but instead

to assess the system's ability to protect them and speak to what they would need to feel comfortable using it. Indeed, an attitude of pragmatism in the face of the inescapability of sharing personal information to use online services pervaded many of the conversations with users. One user spoke to this quite eloquently, saying:

If I'm using the service I want to use, then I will share my information in order to be able to use that service. But like I said I don't screw around sharing everything on online or on social media or uploading anything. I'm not reckless... I do browse through it and see what I'm sharing but usually it's like your name, your age, or something. If you want to know my age, sure...When the information [being shared] is specific, I look at what the information is, and besides reporting needs, [it's] usually nothing big. Then it's about, let's say cookies or some kind of data phishing. Then I prefer to go with the minimum of sharing, if there is an option (P13).

The user's comment about not being "reckless" in sharing information online was something echoed by many participants. Though information sharing may be required to achieve the user's goal with a particular service, almost all users explicitly attempted to assess and mitigate what they felt were inherent risks while maximizing rewards. They did so by engaging in an explicit process of assessment of what information was being collected, and how it was being used and shared, and then implementing behaviors that minimize the perceived risk. Another user summed up the comments of many users, describing MYPDx as "complicated but trustworthy" (P3). Speaking further about this description, the user said:

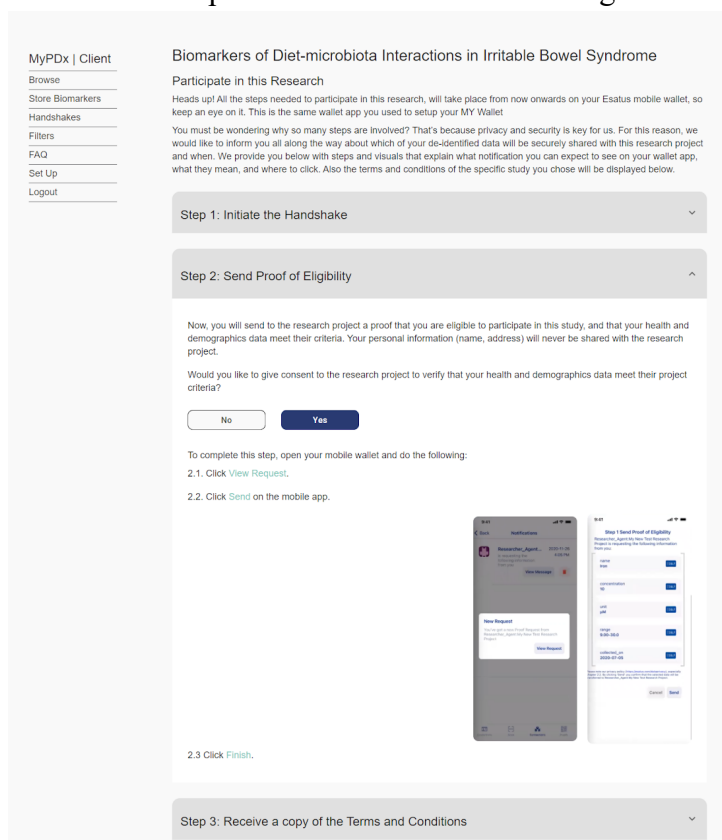
And after that you you're putting a lot of faith in the fact that you're telling me it's not malware and you're not hacking me... There's no way for me to look to see where it's being stored, demonstrate that you're not stealing it, right? You've got to take a leap of faith... Every time you give somebody your email address it's a leap of faith...It's just in general online, right? You might sign up for Hotmail or you know they give you an address, but what are they doing in return? Whether it's Gmail or any of those guys. You are giving up something (P3).

Like many of the users interviewed, this user explicitly notes that their assessment of the system as “trustworthy but complicated” is based on features and indicators that mitigate risk. This assessment is also based on the information on the platform, which communicates how the system is being used. However, they note that there is no way for them to know with certainty how the system will use the information, regardless of what the system may tell them. There is no way for them to “look to see where it's being stored”, to see what is being done with their information. Therefore, the user’s assessment of trustworthiness is not a statement of certainty about the system, rather the user speaks about trust as a “leap of faith” that they will receive sufficient benefit for “giving up something”. The user perceives inherent known and unknown risks to using the system. This structure of assessment was observed in the majority of users, in which risk is either limited, mitigated, or accepted based on the benefits of using the system or the reward received. Once an assessment has been made, the user makes a ‘leap of faith’, where they may still face consequences from using the service, but accepts this risk due to their goals, or the reward presented.

### 4.9.3 Reward

A majority of users spoke about reward or “benefits” as being a relevant aspect to their assessment of the system. The reward presented by the system was cited as a way of either motivating their data sharing or as a tangential benefit of data sharing, in the context of usability issues and general risk with using the system. The nature of the “reward” of using the system was almost always connected explicitly to the way the system offered monetary compensation to users for the contribution of their data, rather than the quality of their experience, as reward it characterized in the UES-SF. This divergence is discussed further in the Discussion section.

Some users were more explicit than others about needing to be compensated: “Once you



**Figure 6 - Sign Up for Research Study**

go in there, 100 bucks to like share information and not have to do anything? Yeah, that’s pretty good (P15).” In other cases, the reward was seen as a benefit to having already shared the

information with the testing company by sharing a blood sample: “It's a pretty easy reward for all you're doing. All you're doing is giving permission for researchers to use your data, you know? Once you've got the information it's there to be utilized. If somebody wants to pay me for it, great (P17).” For some users, the role of reward was even more explicit when talking about sharing their biomarker information. In the case of one user who had indicated they trusted the system: “That's why I said, you know, repeatedly, that I wouldn't do this without any incentives, right? Just for fun? I wouldn't do it (P13).” This user, in particular, cited usability issues as a problem with the system as a reason why they would need to be further motivated to use the system.

In a minority of cases, participants spoke to how the benefit to society or individuals currently affected by diseases without treatment regimens was seen as a “benefit” or “kickback” for users. As one user said, “There's definitely that little kickback that helps, but you know from a community perspective, how are we going to fight all these illnesses that we have? We need people to volunteer to share data or share their experiences, right? (P7).” In these minority of cases, monetary compensation was not mentioned at all, with the social good of sharing information seeming to take the place of reward as a motivation for signing up for a study to share their information (see Fig. 6). For example, one user stated:

I like the idea, just like doing this, you know? Being able to help with research for things are [sic] going to make things better, hopefully...whether it's a medication or some sort of a program that can help, you know, deal with different health issues. That type of a thing.... I just I like the idea of, you know, the altruistic aspect of it right, helping society to better [understand] something. So those are the benefits to me (P20).

However, even though compensation wasn't mentioned by the user, the social benefit of their information was also understood as a benefit of using the system, rather than strictly speaking as a way in which the experience of using the system was inherently rewarding. We can see from these examples that the picture of how the system presented rewards was understood by users as distinct from whether their experience of using the system itself was rewarding. These social rewards, like the monetary rewards, were discussed in reference to the perceived risks of using the system. The evaluation of what constituted a risk and reward was explicitly connected by users with past experiences with technology, perceptions of security online, attitudes towards different kinds of actors that might be able to access the information, and their own value systems.

#### **4.9.4 Engagement as Learning Process**

Echoing the literature on engagement, A theme that emerged from the interviews was the role of engagement both as a process and a product relevant to users' assessments of the system's trustworthiness. A majority of users indicated that they learned through engaging with the system, either explicitly or implicitly. As one user stated: "It was kind of like connecting the dots a little bit...wasn't as clear the first time, but second or third time we were kind of repeating the things [and] it did get a lot easier (P3)." A good example of the process of learning in this system comes from one user who explicitly spoke about their confusion concerning how what they were being asked to do connected with the usability testing session: "It was very obvious what I needed to do with the directions that were provided. But I guess like, overall, the sort of purpose of it, you know, clicking on entering these codes... Yeah, that's confusing (P1)." Later in the same session, the user spoke to their process of learning: "It took me a bit of time to realize that when I click "yes" on the screen here [on the computer] that it sort of sends a request to my app [on my phone]. That

wasn't quite intuitive<sup>2</sup> (P1)” (See Fig. 4). Still later in the same session, the same user was able to speak clearly to the conceptual model of the system, and used it as a rationale for their assessment of the system’s trustworthiness when asked about the potential for the system to be ‘hacked’: “I think given there’s such like, strong linkage, for lack of a better term, between what's on the web, and you know, how permissions are provided, or the data is shared through the app (P1).” In this example the user clearly spoke to a process of learning how the system worked, through using the mobile wallet app to send information with the help of the web browser. They then applied that knowledge to speak to their assessment of the trustworthiness of the system. It is also worth noting that the user here is actively speaking about how the system mitigates what they see as potential risks. Users also gained a sense of confidence in the purpose and outcome of what they were being asked to do with the system. As P1 (quoted above) said: “Well, I literally saw what happens in what order so now I’m comfortable with it. I see what happened... there's no surprises.” The confidence expressed by P1 presents an example of the process of learning mirrored by the majority of participants, where they moved from confusion to confidence through learning by engaging with the system. Echoing the literature on engagement, other users mentioned that the ability to experiment with and “play” with the system was essential to their comfort with the system:

I found it really helpful...my only concern was that you know I could play with this all day long...I was going to mention that at one point: please don't tell me that there's ever a time

---

<sup>2</sup> For example, in Fig 4, we can see a screen shot of the process of contributing biomarker data to a researcher’s study. On this page, users needed to read the information, click the “Yes” button to send credentials to the researchers that would verify their eligibility for the study using zero-knowledge proofs. Once they clicked “Yes”, a notification appeared on their smartphone wallet app, indicating that the credentials had been received and approved. This process then required users to look back and forth across their two devices, something this user was unfamiliar with.

constraint on...your ability to you know be in the system. Because I think that would frustrate people...if it's something that you know they can [do] on their own time, get familiar with and get comfortable with and navigate through...familiarize themselves with it, I think it's going to go like gangbusters (P6).

This user speaks clearly to how their ability to experiment with different parts of the system helped them to “familiarize” and “get comfortable with” the system. This kind of deep structure use is understood as a part of engagement within the literature. While this user was the only user to speak of “play” as part of their process of learning, the comments about how using the system helped them to form an image of how the system works echo the majority of participants. As demonstrated above, for a majority of users, engagement was the process by which they learned about the structures of the system that were relevant to their assessments of the trustworthiness of the system.

To a certain extent this finding is intuitive, as users were asked to complete tasks with a system they had never seen before without other sources of information than what the system presented. Further, the relationship between engagement and learning has been explored in eLearning settings with reference to how specific populations and designs influence learning (O'Brien & Toms, 2008, O'Brien, 2016b, Vail et al, 2015). The relationship between engagement and learning has also been explored within the field of cognitive psychology (Weibe & Sharek, 2016). For example, Cognitive Load Theory posits that a primary goal of information processing is the “activation and modification of existing schemas for learning” (Weibe & Sharek, 2016, p.58), and that attention is limited and selective, such that “While the learner has made the higher-level decision to engage in a learning task, the design of the learning environment will heavily influence what specifically is attended to over the arc of a learning session” (Weibe & Sharek,

2016, p.58). The specifics of this process and its relationship to the design of this system however are beyond the scope of these findings and this research.

#### **4.9.5 Experience of Engagement as Information for Assessment**

Within the interviews, users cited their experience of how well the system engaged them as a primary source of information for their assessment of the system's trustworthiness. Following the literature on engagement, this theme broadly aligns with the understanding of engagement as a product of user experience.

For a majority of users, relevant information was derived from users' experiences with different features that engaged them in a relevant way to their users' assessment of trustworthiness. For example, many users cited their perceptions of MYPDx's usability, specifically, experiences of interactivity and feedback, as a reason the system was secure. For these users, the metaphor of having experienced "steps" or "checkpoints" was used as a rationale for the system's security. As one user said:

The way that it's been set up to keep things like quite safe...going to your phone and then [information] being sent to [it] and, like you kind of make these calls and there's a lot of checkpoints. I think that really helps and making it feel like a safe tool (P2).

For this user, the experience of feedback (or perhaps friction) gave them a sense of control over the system and therefore over their information. The "steps" also gave users a clearer sense of the technical architecture of the overall system, through helping develop a conceptual model. For example, the user quoted above spoke to how they felt their data was being minimized through the

technical architecture of the system: “I think, especially because of all of the steps that I’ve had to go through it's like okay, yeah, they really are getting this one bit (P2).” The ability of this user to identify that their data was being minimized by design speaks to the way in which users’ experiences of the system’s usability, mediated through the interface, became an important source of information for users about the goals and structure of the system as a whole. It is also worth noting here that this sense of security, that researchers are “getting this one bit” of the users’ information, comes not from any knowledge of blockchain technology or zero knowledge proofs, but rather from information gained from their experience of engagement with the interface of the system.

Many users were observed to use how they were engaged by the system as a source of information for their assessments of trustworthiness. For example, one user commented about how MYPDx was “definitely trustworthy. Just the sheer amount of times [I was asked for] verification and QR codes, I felt that whatever was happening in the background or even like presently in the front. It was overly secure... (P14).” In this quote the user identifies how the modality of the system in requiring verification from both the web and mobile phone helped their sense of overall ‘safety’ of the system. Like the user quoted above, they spoke to how their impression of the back end of the system was explicitly formed by their experience of the system through the design of the front end of the system, without reference to any other understanding of the technology. However, rather than speaking to how the process of sending information made them feel secure, they note that they felt the system required their “active participation”, and therefore they had a greater amount of control over their data. The same user further spoke to the role of “participation” in their sense of trust later in their interview:

I do like having to actively participate in actually saying ‘yes’, and [the system] kind of stopping you before you proceed on to the next step, just to kind of show you... in essence that it's trustworthy and then you kind of have control of where you're going with it (P14).

This connection between the feedback and interactivity users experienced through the novel modality of the system and a sense of control can be noted in other comments made by users about their experience. It should be noted that a minority of users made explicit connections to the deeper goals of the system or their understandings of the architecture. However, it is also worth noting that when users did speak to a deep understanding of the system, it was primarily discussed with reference to the most interactive part of the system (sending information) as in the example above. Some users with a particularly strong conceptual model were even more explicit about how their experience of the modality was central to their understanding of the system as trustworthy:

I mean, there's a lot of permissions in the sense that, like, I'm having to scan QR codes that only I would have access to. So that's nice to know. And two factor authentication along with like, again, there's different levels. At first, you're just checking your eligibility, and there's an entire process that goes through you. Nobody else can do that. Because yeah, I can imagine it'd be hard to access, I reckon....I think, what's great about it, in terms of sort of data and what I sort of decide to share given that there's so many steps, [is that] I can stop at any step and say, ‘okay, you know what, I don't think it's a good idea for me,’ that I'm going to stop here and not move forward. I can just drop that there, and it's fine. Um, and I think because, again, it doesn't, you know, the data doesn't get sent with one click. So I think that allows for more control over what you decide to share. And at some level, I

mean, if for some, you know, for some people, if it's a big deal for them to be sharing their data, like, they're really getting the chance to think about it while they're going through these steps, I think, right? So at some level, just being more sort of conscious of their actions, you kind of have to pay attention. You can't just do it off hand. You know, it's not a single absent-minded click that gives that info away. And, yeah, I think it's the steps primarily, in my perspective (P1).

Within this exchange the user spoke to how the “permissions” within the system were a key reason why they trusted the system and connected those “permissions” with the experience of scanning QR codes to authorize information being sent. The user demonstrated a strong conceptual model of the system, noting that only the user themselves can send their information. They then identified that their experience of the modality was the reason why they felt that information could not just be sent accidentally with an ‘absent-minded click’. Citing their experience of the feedback and interactivity of the system, the user connected their experience of engagement with having greater control of their information and with information being sent intentionally with full consent, directly connecting their experience to the goals of the overall system. More than this, this user was able to correctly understand some of the design decisions and goals of the architecture from the perspective of the overall security of user’s information. Specifically, we can see that the user speaks obliquely to how privacy by design (“I can stop at any step”) and the principle of minimization (“it's not a single absent-minded click that gives that info away”) are embedded in MYPDx as a design artifact solely through their experience with the front end of the system.

Throughout these examples then, we can see that users relied upon their experience of engagement with the system as a source of information as to how the system mitigated risk. This

took the form primarily of observations of users about the system's perceived usability, specifically feedback, interactivity, and friction. Other aspects of user engagement from the literature were relevant to users' assessments of trustworthiness, including reward and aesthetic appeal. This will be explored in the next section.

Returning to RQ1, we can build upon the strong positive correlation between trust and user engagement with the following: trust was understood by users to be meaningfully related to risk, such that the system had to either mitigate risk and/ or present rewards to be trusted. Users spoke to a common understanding of risk, namely that their biological information would be accessed by an unauthorized actor. Sharing information online, and specifically sharing biological information online were understood to be fundamentally a risky behavior by almost all users. Users were also receptive to rewards offered for using the system and taking that risk, using them to justify using the system in instances where they felt the system was insufficiently trustworthy. In every interview, users were observed to engage in an explicit process of assessing MYPDx's trustworthiness based in their understanding of the risks of using the system, how MYPDx mitigated those risks, and how MYPDx presented rewards that incentivized use. A common picture of the relationship between engagement and trust emerged, whereby engagement was both a process by which users learned relevant information about the system, and a source of information for the overall assessment of trustworthiness. Building off the quantitative findings, a majority of users' experience of MYPDx's perceived usability, as a factor of engagement, was cited by users as a reason for their assessment of the system as trustworthy.

#### **4.10 The influence of the design of SSI systems on user trust and user engagement**

With a broad set of results that answer what the nature of the relationship between trust and engagement was in this SSI system, this section outlines qualitative results relevant to answering RQ2 and RQ3, namely:

*RQ2: What elements of the design of SSI systems influence user trust in the system?*

*RQ3: What elements of the design of SSI systems influence user engagement?*

Within the MIS literature on trust, trust of users in a technology is understood to focus on an object. The object can be the organization providing the service (Gefen et al., 2008), or, in the case of the theory of trust in a specific technology, it can be “a specific technology (a human-created artifact with a limited range of capabilities that lacks volition (i.e., will) and moral agency)” (McKnight et al., 2011, p.5). Answering RQ2 and RQ3 requires a focus on the object of SSI systems, such that relevant aspects of their design can be differentiated and analyzed for their potential influence on user trust and user engagement. Within endeavoring to provide an answer to these questions, we therefore first must answer a larger question, namely: how did users understand MYPDx as a potential object of trust? This section begins with an overview of the way users conceived of MYPDx as an object of trust, and then explores specific elements of the design of the system that were influential on user trust and engagement. This includes how users understood the ‘technology’ in relation to their pre-existing or emerging conceptual model(s), how the social layer of the system was relevant to trust, how information operated both as a tool for and object of assessment, and, finally, which elements of the design of MYPDx were relevant to users’

assessments of trustworthiness (which turned out to be the novel modality of MYPDx, the information architecture, organizational assurances, and visual indicators).

#### **4.10.1 ‘Technology’ as Conceptual Model**

In keeping with McKnight et al.’s work (2011) most users relied on their understanding about the capabilities of the technology they interacted with as a basis for their trust in the system. However, this understanding was not related to an understanding of the solution architecture used to implement the MYPDx platform or the ‘technology’ per se. As a general point, we can begin by noting that a majority of users did not speak about, or indicated they were explicitly unaware of, the presence of blockchain technology within the system. While some users spoke about the relevance of blockchain to their trust assessments, these comments were made only after the interview and surveys were completed and users received an explanation from the interviewer about the general role of blockchain in the system as part of the protocol used in this research. Therefore, these assertions have been excluded from this analysis.

Instead, all of the users’ interviewed indicated that their assessments of the technological layer of the system were based on their perception of how MYPDx worked, understood by means of interacting with the system, the information conveyed to them through the system, as well as their own past experiences with technology. As one user said “At first, you’re just checking your eligibility, and there’s an entire process that you go through. Nobody else can do that... I can imagine it’d be hard to access (P1).” In this example the user demonstrates a conceptual model of the system that allows them to understand how the system preserves security and enables greater confidence in the ability of the system to keep them safe (Norman, 2013). For the purposes of this assessment, it is irrelevant that the reason “no-one else can do that” is because only individuals

with access to a private key through the user's wallet can exchange data. To the extent that the user understands the security features of the system within their conceptual model, those beliefs become part of their assessment of the system's trustworthiness.

This meant that, in instances where the system was insufficiently clear on why the users were asked to undertake certain actions, the users had no way of troubleshooting or correcting their understanding, leading to confusion. As one user said:

And not really knowing anything about how it's stored, but just knowing that it's already there, and then I'm going on to that server sending it to an app and then from the app sending it to a researcher, I think there's just a disconnect in my mind as to why that's necessary (P1).

McKnight et al. (2011) note that one of the relevant items for their model of trust was what they called situational normality, or the assurance that a new system would work based on experience with other similar systems. However, in the case of MYPDx as a novel blockchain-based SSI system for sharing biomarker information, there simply is no similar system with which the users in this study have interacted. When asked, most users compared MYPDx to either a government website or to two-factor authentication systems they had used. Neither system gives much context for the particular technology at play, though the latter seemed to have helped to inform users' conceptual model. This means that, in examples like the one above in which the structure of the technology is unclear to the user, users had no past experience with blockchain systems that could help them understand, troubleshoot, or revise their understanding, thus, the perceived "disconnect" in the above quote.

Another indicator of how users' conceptual models were distinct from the actual system came from conversations within the interviewees about security. A majority of users spoke to their understanding of how the perceived security of the system was sufficient, or insufficient, for the system to be seen as secure. However, users' understandings of 'security' in the context of this novel technology varied widely based on their experience with technology. For example, one user was particularly focused on the level of security involved in signing into MYPDx: "I think someone could hack...into this information...I'm saying if the signing in isn't as secure as it could be, someone could get into someone's account information (P3)." This user later indicated they had experience with cybersecurity training through their work. Given this background, they felt that only using a username password combination to log into the MYPDx website was insufficiently secure. While this may be a relevant consideration for the system, it is worth noting from this example that, because the user was unaware of the role of blockchain in the system, assessments of the technology were based upon their understanding of what 'secure' systems looked like from past experience.

A majority of users spoke about whether or not the technology, as they understood it, would be able to mitigate risk, based on their experience with other, non-blockchain based systems. Speaking about the process of authorizing information transfer using their phone, one user said: "I felt that...it would be very difficult for somebody to break into and...imitate me (P12)." This user also indicated that they were unaware that blockchain was involved in the system. When the user spoke to the ability of someone to "break into" the system then, it is unlikely that they are referring to common threat vectors within blockchain systems that involve imitating identities, such as a Sybil attack (Zhang & Lee, 2019). Rather, this user was making the more intuitive assessment that it would be difficult for a bad actor to replicate the same process they had just gone through,

without access to their phone, login credentials for their computer, MYPDx, and their blockchain wallet.

In conclusion then, while almost all users spoke about the role of the technology in enabling their assessment of the system's trustworthiness, all users spoke about their understanding of the conceptual model of the system, rather than anything objective about their understanding of the technical architecture of the system. This finding can be understood to differ from the theoretical foundation used in this work (i.e., McKnight et al., 2011). This differentiation is considered in the Discussion section ([Section 5.7](#)), however, for the purpose of understanding the findings of this work, I will briefly summarize the argument here. I argue we can profitably clarify the definition of 'technology' in this work to formalize some of the unclear aspects from McKnight et al.'s (2011) theory, in keeping with their theoretical orientation, by redefining technology as 'the user's conceptual model'. I argue that this redefinition resituates the focus of the theory within a design thinking context better suited for deriving actionable insights about users' interactions with the system. The reliability, functionality, and helpfulness beliefs about a specific technology that underlie McKnight et al.'s work can then be understood to refer to this modified definition of 'technology.' To whatever extent the beliefs of users in the functionality, reliability, and helpfulness of the technology are present, we can understand them to be referring to the user's conceptual model of the technology, rather than the specific technical stack and architecture enabling the user's experience.

#### **4.10.2 Social layer as relevant to assessment**

While all users spoke about the technology underlying the system as being relevant to their assessment of the trustworthiness of the system, most users also spoke about the role of the social

aspects of the system as being relevant to their assessment of the trustworthiness of the system. Given that the characterization of risk in this system was focused around bad or unknown actors accessing sensitive information without permission, it stands to reason that users were concerned about which social actors had access to their information. As one user said: “P9: I’m apprehensive just about...because it's not just you it's also like who you're sharing the data with and what they’re doing with it. And so in trusting you I’m also trusting potentially all those other people.” In this quote the user speaks to a general sentiment that the motivations of other actors within the platform were relevant to users’ assessment of the overall trustworthiness of the system. A majority of users wanted to know more about the other social actors that were on the platform and looked for information that indicated what permissions different agents had. However, even in cases where users had a strong understanding of which other actors were able to access what information through the system, they were still concerned about those actors’ motivations:

At that point it's not really... it's no longer about like personal safety because I trust that the [system] is working, and they would only get what I wanted them to receive. But the issue is that I don’t really know enough about them and what they're going to be doing with the data (P2).

In this case the user indicates a concern both with what information the other actors can receive, and with what other actors are able to do with their data within the system, as well as what their motives or goals with that data may be. Within users’ assessment of MYPDx, as a system for sharing information with researchers, the risk of using the system was frequently connected to the motives and backgrounds of social actors that could be given access to their biomarker

information, and whether the system placed restrictions on their actions. In general, users were more likely to indicate they felt comfortable with universities, not-for profits, or government, based on what they felt were profit-focused motivations that could negatively impact them. For example, some users expressed concern about whether life insurance agencies would have access to their biomarker information: “the hesitation would be ...say, for example, [the researchers] use [my information] and companies had... access to [my] info and it [was] used against you say when you're applying for life insurance or something like that (P20).” Other users wanted to know more about what kind of actors would be able to sign up to the research job board: “on the kind of doctor side of things, is there, like an application process, for... universities or whatever to sign up, or could anyone technically sign up? (P8).” This user was particularly concerned with what kind of organizations could sign up to receive biomarker information and wanted more information about how the studies on the platform were vetted.

Both for vetting and establishing an accountability process, MYPDx incorporates an independent Research Ethics Board (REB) review within the system to review and approve the available studies on the platform. A minority of users, when they were made aware of the REB, spoke to how the presence of the REB gave them a sense of security. As one user stated, they trusted the system in part because “there is some board you could follow up with to say ‘hey, did they play within the boundaries?’, right? (P5).” In this case the idea that there was some social recourse for the user should the actors in question act suspiciously helped to enable the user’s assessment of the system being trustworthy. Overall, diverging from the work of McKnight et al., (2011) a majority of users spoke to some aspect of the social layer of the system, understood as the relevant social actors with which users were interacting, their motivations, and the abilities and restrictions they have within the system, as being relevant to their assessment of the trustworthiness

of the system. Users used their conceptual model of the system as a basis for understanding how the system enabled or restricted the access of different users to different information they shared with the system. The implications of this divergence are explored in the Discussion section ([see Section 5.7](#)).

#### **4.10.3 Information as Tool and Object of Trust**

A majority of users indicated that how their information was being treated was a factor in their trust assessments. It is important here to note that the concept of information functioned in two distinct ways within the users' assessment of the system: as a basis for decision making, and as an object of trust. As one user said: "I think it's trustworthy because it clearly identifies how that information is collected, how that information is shared and how it's used (P18)." We can see here how the user identified trust as being based both on how the system shared and used their information, and how MYPDx "clearly identifies" the way the system was managing that information. Users also spoke about how the way information was managed, and how MYPDx communicated about how it managed risk helped them to trust the system even when they weren't entirely unsure about what technology was involved with the system:

Because it has all this information about like the privacy and the REB certificates and all of that, then that makes me feel like 'okay, well, they're giving me lots of information about what they're doing with my data and how they're like, you know, doing these studies,' so, like I guess the confidence in that information that's being presented, makes me feel like I can just like trust whatever weird backend stuff is happening (P8).

The user here identified the REB certification process, and the information about how the system communicated about its privacy preserving measures as being an indicator of the overall clarity and transparency of the system, enabling a sense of safety. The user indicated that the way information was used in the system was at least partly the basis for their trust in the system in situations where they were uncertain about whether the technology itself was reliable, or functional.

A majority of users looked for information about the information management protocols of the system, i.e., how their information was shared, used, structured, managed, accessed, or stored. This may be attributable to a self-selection bias within the pool of participants, some of whom indicated they were currently students in health-related fields. However, far more participants actively assessed the informational layer of the system ( $n=17$ ) than those who indicated they were currently students in health ( $n=5$ ). Regardless, users clearly articulated nuanced questions about the way information was managed. This is discussed further in the limitations section ([see Section 5.9](#)). Users spoke clearly to questions about retention and destruction: “and how's it destroyed? Fine. Okay, this is when it's kept until... what does destruction entail?...Is it that like, ‘it's kept until this day?’ Does that mean that I won't see it on my phone anymore? (P1).”

Other users asked questions about what sharing information entailed, specifying concerns about control: “I want to know what I'm sharing, and then what control I have over that (P9).” Other users asked questions about the structure of the information, and how it related to the technological layer of the system.

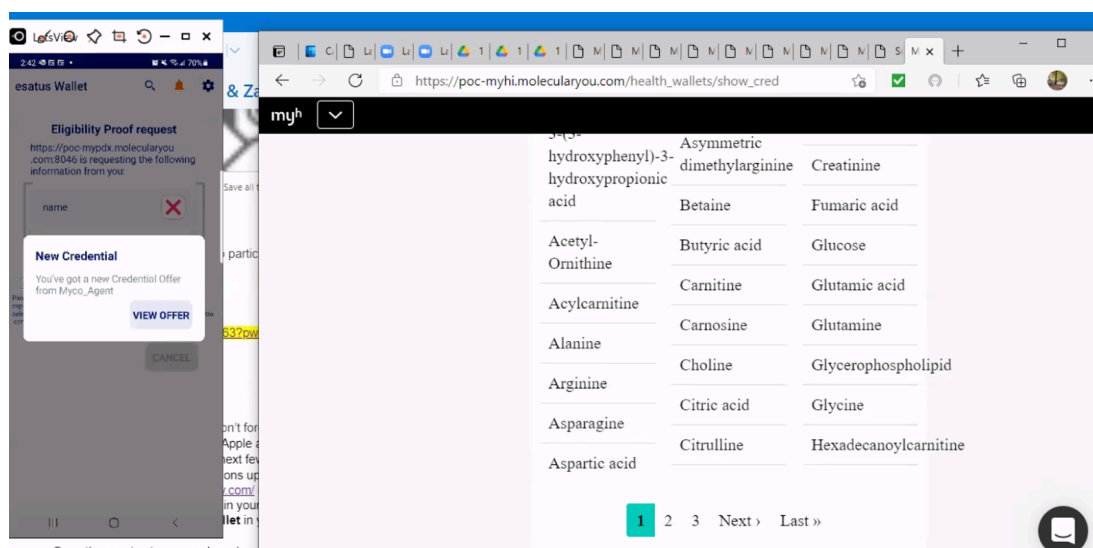
Because I don't really know like... I'm just looking through the app right now and I don't see much information [about] the app. I think it's the unknown that's creating the uncertainty and with regards to the browser. I haven't really reviewed to learn a bit more about the organization and the platform, so in that sense lack of information is giving me some uncertainty (P18).

Here we can see information being used as a tool for assessment, and for sensemaking about the system. The user spoke to a process of using the information presented on the app to make sense of how their information is being structured between the phone and the browser. Because there was insufficient information on the app to make sense of the technology involved, the uncertainty the user had transferred to the browser, as another technological feature of this uncertain system. We can also note how the user speaks to their parallel assessment of the social layer of the system in the context of that uncertainty about the technology, i.e., in relation to having insufficient information. In this aspect of the system, they also have insufficient information and so are left feeling “uncertain” about the system. From these examples, we can see that they used their perception of information as a basis for their assessment of the system as being trustworthy in addition to as an object in which to place their trust as a means of sharing their information.

To return to the question asked at the outset of this section, we can answer that the object of trust for users in this system was MYPDx, understood as a system with relevant technological, social, and informational layers. It was not the case that users placed their trust solely in specific aspects of the system’s functionality as might be suggested by McKnight et al.’s (2011) theory of trust in a specific technology. Rather, various levels of the system were relevant to different users’ assessment of the how the system mitigated risk in order to be perceived as trustworthy.

#### 4.10.4 Relevant Design Elements for Assessment

While the previous section outlined how users understood MYPDx, the level of abstraction of users' comments was at the level of the system as an object (or actant). Users also spoke to specific elements of the front-end design of the system that were most relevant to their trust assessment. These elements consisted of specific design elements (e.g. buttons) structures (e.g. information

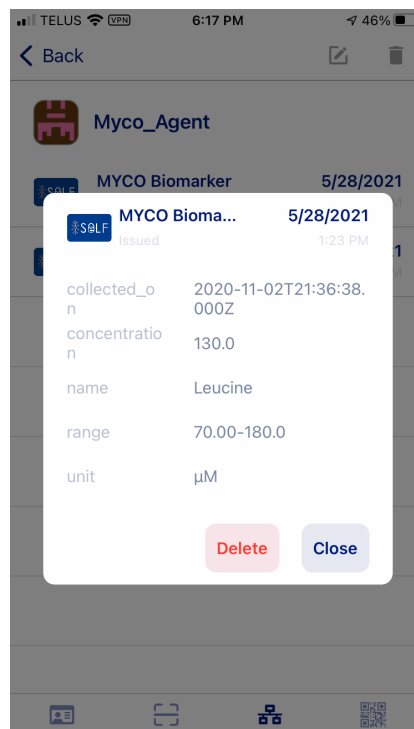


**Figure 7 - Adding Biomarkers to blockchain wallet app**

architecture) and features (e.g. sending information via mobile wallet) that presented users with information relevant to their trustworthiness assessment. Building on previous sections, this information was gained through the process of engaging with the system and took the form of either users' experience of engagement or information explicitly conveyed to users (e.g. how to send information to researchers). This section explores the specific design elements, structures, and features from MYPDx that were most relevant to the majority of user's assessment of the system's trustworthiness in service to answering RQ2 and RQ3. As mentioned above, the process of sending information to researchers through MYPDx represented a novel modality of usage for the majority of users. This process required users to utilize both their smartphone and computer to

scan QR codes on their computer screen with their wallet app. In Figure 7, the window on the left of the screen shows the participants' mirrored smartphone screen, displaying the eSatus wallet App. The user has just been asked to add a biomarker from the platform to their wallet by clicking on the name of the biomarker. The eSatus wallet app has just received a credential from the platform. The window on the right displays the MYPDx platform in an internet browser, which is currently browsing biomarkers to send in this study. In the next image, we can see a message the user received when adding a biomarker to their wallets in order to share those biomarkers with researchers. (See Fig. 8). This system represented a novel modality for users, involving using a smartphone to create visible changes in both their wallet app and web browser.

#### 4.10.4.1 Modality



**Figure 8 - Biomarker Credential Confirmation**

A majority of users indicated that the process of sharing information positively influenced their perception of the system as trustworthy. While some found the movement between phone and

computer confusing, which lowered trust, the majority used the experience of engaging with this new method of sharing information as a basis for their assessments of the system as secure and trustworthy. As was discussed above, this process explicitly created an experience that engaged users by giving them a sense of control over their data through feedback and indicators. From a system perspective, it was one of the main points at which the UX and technical stack of the system overlapped in a way that actively demonstrated the technical architecture and backend design choices to users. This experience of using the system helped many users to develop their conceptual models of the system and make an assessment of the relevant risk. As one user said:

There's such like, a strong linkage, for lack of a better term between what's on the web, and you know, how permissions are provided, or the data is shared through the app. I just imagine it being like a wall. So every QR code you have to scan is like a wall, that you have to go through, that you only have the key for if you have your phone and your app, and you've got that sorted. So that's, that's nice to know. And then, yeah, I think the steps are probably the biggest piece... in terms of making [the system] feel trustworthy (P1).

In this instance the modality of MYPDx was a key factor for the development of this user's conceptual model and sense of the security of the whole system. In experiencing the interactivity and feedback from the system, this user puts forward their own design metaphor to explain their understanding of how the architecture of the system makes it secure, namely that each QR code is like a wall only users can get through. The user specified that this experience formed part of their assessment of the system as trustworthy; however, recalling the bimodal distribution of the perceived usability factor from the UES-SF, for some users the modality of MYPDx was confusing

rather than informative. Some users were unsure of where to go: “I was getting more fixated on answering all the questions on the phone and then thinking well why do I need to go back to the laptop? (P6)”. In these instances, users felt that the modality was disorienting, and found insufficient guidance on the screen they were looking at. Other users felt that as they already trusted the system, the modality was unimportant for their trust and was instead inconvenient:

I mean that, because it is a lot of steps, like, I would say, like if it was shortened a little bit... Like there's a lot going on in like scanning the QR code accepting this clicking this accepting this clicking this... I think...when you're ready to just share the information you don't need as much like when you're ready to go you're good, you know? (P11).

Here as well we can see the conception of trust outlined above in which users trust the system once, after their assessment of it, and no longer need assurances of the system's security. This implies that the modality, while understood by the user as a feature that increases security or autonomy, is not felt to be relevant when they no longer need assurances or evidence of how the system mitigates risk. Indeed, some users who trusted the system indicated similar sentiments of the process being inconvenient, or indicated a preference for more convenience, at the expense of security. As such, users' experience of the modality of the system can be understood as an important source of information for their assessment, positive or negative, of the system.

#### **4.10.4.2 Information Architecture**

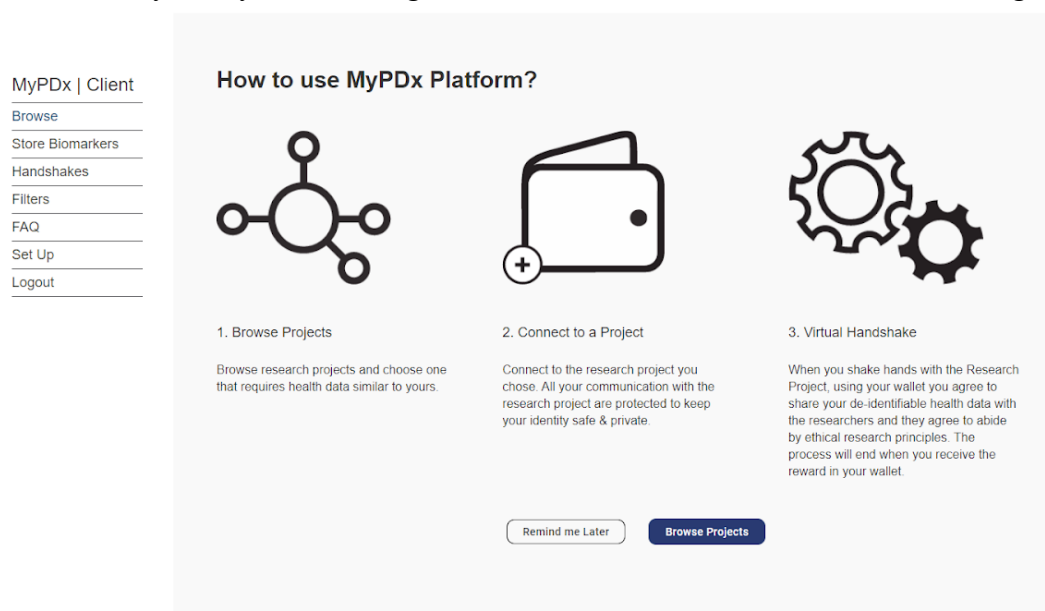
Rosenfeld et al., (2015, p11) describe the design discipline of information architecture as “a systematic, comprehensive, holistic approach to structuring information in a way that makes it

easy to find and understand—regardless of the context, channel, or medium the user employs to access it”. They define information architecture as “the structural design of shared information environments” and “the synthesis of organization, labeling, search, and navigation systems within digital, physical, and cross-channel ecosystems” (Rosenfeld et al., 2015, p. 13). When speaking about the information architecture (IA) of a system, we refer to how a system attempts to make what information users need from or about the system findable, and to make the conceptual model of the system itself understandable. As such information architecture can be understood as being better or worse relative to this goal and is often improved upon iteratively within the product lifecycle (Rosenfeld et al., 2015).

A majority of users spoke about how they relied upon the information architecture of the system to navigate in a new modality. One user was particularly explicit about how the structure of the system helped him navigate:

I would say that I’m pretty good at glancing and trying to find a button that I think would work rather than actually reading through it... there wasn't anything that really jumped out in terms of like bolding or quotation marks or navigation pictures, but it was well enough laid out that I could pull and extract what the actual button was, because it was very similar if not exact. Matching word to word... You can make the headers, more appealing.... researchers [are] obviously going to [need to use] pretty dense text [in posting about their research study], but at least you got markers and headers that will draw you to give you a pretty quick indication of what it's about, what each segment’s about (P14).

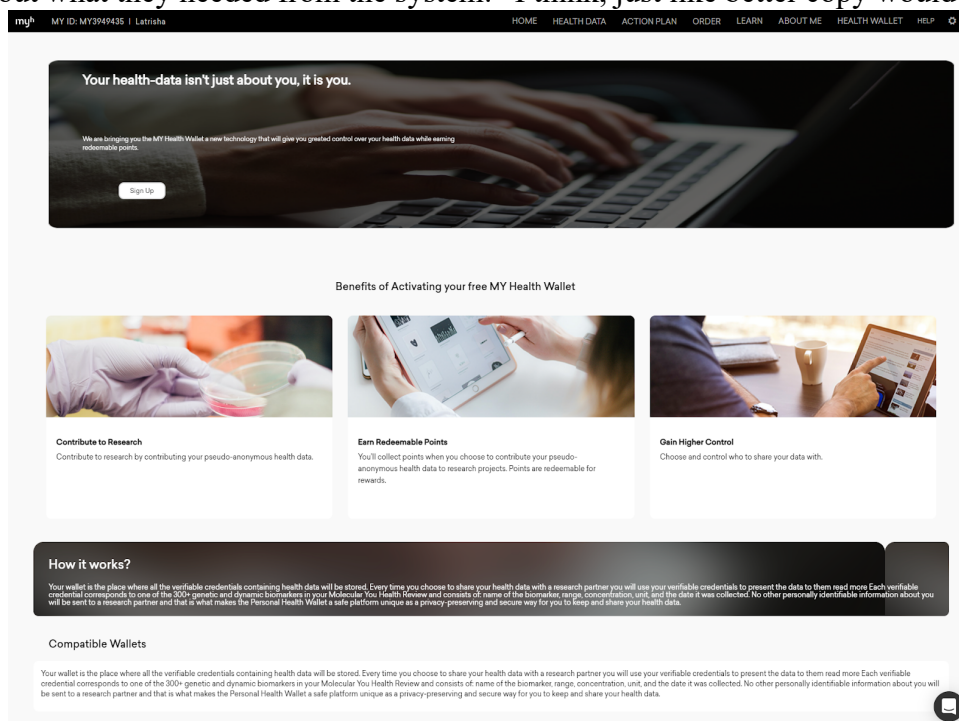
This user spoke about how their practices when browsing a website involve moving efficiently through a website based on familiar indicators and text (i.e., the information architecture). Despite the system relying on text to give guidance, they were able to navigate based on the signifiers presented by the buttons on the website. They also noted that despite the presence of unfamiliar information architecture structures, the structure was sufficient for them to be able to use the system coherently. They then distinguished the information relevant to their navigation to the



**Figure 9 - MYPDx Browse Page**

information relevant to their operation of the system, saying that while the content may need to be “dense”, the headers and other tools users use to navigate could be clearer, more understandable, and less ambiguous. This distinction made by the user exemplifies the two ways in which users were observed to make use of the information provided on MYPDx: as a way to navigate through the system, and to make decisions about the trustworthiness of the system as a whole. Because users relied upon text to troubleshoot when they were lost and used the directions and explanations to form their conceptual models through looking for information about how information is used, shared, managed, and stored, the clarity of information became crucial. Some users were quite

blunt about what they needed from the system: “I think, just like better copy would make it easier



**Figure 10 - MYPDx Page - MYHI**

[to navigate] (P16)”. A strong majority of users expressed concern with whether the text they were reading was understandable and consistent. In instances where users noticed inconsistencies or errors in the text shown, it sometimes led users to doubt the system because, in the words of one user: “that just was inconsistent and so then I’m like ‘Oh, maybe they’re not actually doing what they’re saying’(P9).” The text-based information given by the system was seen as authoritative by users, and a key part of their process of learning. As such, in instances where the text had spelling or grammatical errors, or appeared to contradict other information on the platform, users’ spoke about how it negatively affected their ability to be certain the system was authoritative and correct, and therefore to trust the system.

The need for information to be correct and complete was particularly important, as a majority of users looked to the text content to make decisions about whether it was trustworthy. As one user said:

[They give] you plenty of info on how they use the [biomarker information], how it may potentially be used, what they do with it, that you know they don't share it with anybody, so I think they give a lot of detail there that would make me feel comfortable using [MYPDx] (P20).

This user spoke of how they found information about how their biomarker information was used, managed, and shared, and that this information was relevant to their assessment of the system. As the system conveyed the vast majority of relevant information for users through text, this is somewhat unsurprising. This text-based information was used to generate knowledge about the



**Figure 11 - Esatus Wallet Proof Request**

system by users, informed their trust assessment, and gave them a greater sense of control over the system. In general, users were interested in receiving enough information, with some users indicating that more information was better than less, as a rule. As one user said, “[the FAQ’s] on the website, I do think that what was there was good, I think it's good to have I mean, in my opinion, I think it's good to have more information than not because it just makes it seem more trustworthy (P2).” It’s worth noting here that the user did not extensively use the FAQ section of the system. Instead, just the presence of information to satisfy any question the user might have was seen as important to helping build their sense of the goals and attributes of the system, and the user’s sense of its trustworthiness.

However, even though users looked for and valued detailed information that could answer their questions, the use of specialized language (such as the names of the biomarkers users could share within the system) made some users feel confused and overwhelmed (see Fig. 7 above). This was particularly the case with users who had difficulty understanding other aspects of the system, such as the modality. As one user said:

[Speaking about moving between phone and browser to send information] And once I did something where do I, what am I going back to? and not even that. And again, the, the names! Titles, right?... it's easy to go... 'I'm going to Twitter', 'I'm going to Instagram', but 'MYPDx?' 'MYHI?'...or whatever it is. There's just too many convoluted terms. I think I guess right and so and just that again just focusing on that just a little bit more complicated in the sense that it sounds like they weren't consistent but also just like the words. I didn't know what the heck any of these things mean (P17).

This user articulates how their frustration and confusion about the terms and titles of the different parts of the system made them feel confused about the system as a whole. Both the kind of specialized language used and the consistency of that language are noted as issues by the user, but also the information architecture itself. In this case, the information architecture wasn't sufficient to enable the user to make sense of what they were being asked to do. To a certain extent scientific terminology is unavoidable in a health data sharing platform like MYPDx, but this user spoke to feeling lost before speaking about the terms, indicating that the confusion around terminology was compounded with a more fundamental confusion about the conceptual model, goals, or design of the system.

Given the importance users placed on text and the information architecture of the website, it is logical then that the part of MYPDx the most users felt confused or uncertain about was the integrated mobile app. Because the eSatus wallet app used did not enable MYPDx developers to edit the text or presentation of the wallet, the design and messaging users received through the app were seen as incongruent with the rest of the platform. Specifically, the confirmation messages that users received on the wallet app presented machine readable identifiers for the credentials and other actors sending and receiving information through their own wallets. For example, in Fig. 11, the app uses a URL (rather than a name) under "Eligibility Proof Request" to identify a researcher asking for proof of the users' eligibility in their study. This led many users to be confused by and suspicious of the wallet app, even when they indicated they trusted the overall system. We can understand this in reference to the examples above around how users perceived discrepancies in language. As one user said, "I'm just looking through the app right now and I don't see much information about the app. I think it's the unknown that's creating the uncertainty with regards to the browser (P18)." Another user articulated a similar comment about starting with a URL:

[even] knowing that it's Molecular You or whatever like trusted [organization] it would still just give me an uneasy feeling my stomach because it just reminds me of like downloading something you're not supposed to on the Internet, or something like that (P16).

We can see in this example the importance this user places in the language in the system to help them assess what is normal and how to navigate. Language was spoken about by almost all users as part of the process of sensemaking within an unfamiliar system. They also related what they're seeing to their experience to assess how the system is trustworthy. Users clearly placed importance on language, specifically the clarity and understandability of content and the information architecture of the system, as a basis for their trust assessments.

#### **4.10.4.3 Organizational Assurances**

A majority of users looked for assurances about the social actors on the platform, such as for indicators of authority, authenticity, and oversight. This finding builds on the analysis of how users understood and assessed the social layer of the system as part of assessing its trustworthiness. Users did not inherently trust the legitimacy or future conduct of actors just because they were on the platform or were from a specific university or company. Instead, users looked for information about organizations and actors on the platform to gauge their trustworthiness, and to see what actions they were permitted or constrained in taking with the information they were sharing. This often took the form of users asking explicitly what assertions there were that actors were acting ethically or were otherwise legitimate. For example, one user said, “the ethics board certificates

need to be there, and probably the proof as well to verify the company (P7).” Some users explicitly asked for logos or badges from participating companies or universities, which conveyed authority and a sense that the research being conducted was official, or sanctioned:

As long as it had the local logo of who was conducting the research, when I was actually choosing it, that would be enough for me to go about my day without worrying... I guess it gives you like a sense of the counterparty. You can see who's actually conducting the research to get to see... if you had a bad experience with say some pharmaceutical company, like ‘yeah, no, I'm out I don't want to deal with you’ (P14).

In this quote the user specified that a logo helped to give them a sense of the other actors on the platform, to give users a chance to connect other reputational information about the actor, including their past experiences with the company. Indeed, other users asked specifically for links to websites or other ways of assessing actors from third-party sources: “I do believe that would be kind of essential, and you know, important to include... whether it's the label and there's a link that you can click on it takes you to the site that's approved the research... something like that would be helpful as well (P3).” In this case the user quoted specifically is looking for a third-party site that verifies the validity of the research outside of the platform, seeing this as helpful for them to triangulate the authenticity of the research. Ultimately this information functions as an assurance for the user about the intentions and validity of the social actors on the platform.

In this vein, users also looked for relevant indicators about the governance of the system, specifically about the REB that approved research on the platform. For most users, the REB was seen as a way for users to hold actors accountable: “there is some board you could follow up with

to say hey, did they play within the boundaries (P5).” For some users, the REB was important to their trust assessment: “I would feel comfortable sharing my data with those researchers, knowing the rigour that [researchers] would have had to go through to get their project onto this platform (P4).” Here the REB was seen as ensuring the quality and standards of the research being conducted on the platform and thereby ensuring that user’s information was used ethically.

Users were observed to place the burden of proof on whether social actors were trustworthy firmly on the platform, asking detailed and focused questions about specific aspects of the oversight provided. For example, users asked for further clarification about what principles the REB was following: “I would want to know more like, for example, it says ‘Oh, they agree to abide by ethical research principles’, [...] what standards is that? who's standard is that? (P8)”. Other users asked questions about the authenticity of the REB itself: “You know, I would like to be convinced that it's an authentic board and that it has credibility because all I saw was three words. (P12)”. Overall, however, the presence of the board itself and the verification that the projects and actors on the platform had ethics certification was seen as giving users a greater sense of trust in the way their information would be used and shared. As one user said:

Because it has all this information about like the privacy and the [REB] certificates and all of that, then that makes me feel like okay well, they’re giving me lots of information about what they're doing with my data and how they're like you know reading these studies so. Like I guess the confidence in in that information that's being presented, makes me feel like I can just like trust whatever weird backend stuff is happening (P8).

Here the user speaks clearly to how both the presence of the REB, and the presence of detailed information about the REB, research, and projects were foundational to their sense of trust. Notably the user mentions that they don't need to understand the technical aspects of the system to trust that the system is safe if they feel that there's both enough information and assurances of authority and authenticity to guarantee MYPDx mitigates any risks of using the system. This further builds on the assertion from above that knowing whether or not blockchain technology was involved in the system, or anything 'technical' about the system, was not a prerequisite for users' assessments of its trustworthiness. Put another way, the system's "weird backend stuff" was something to be mitigated as a risk for this user, rather than a source of trust.

#### **4.10.4.4 Visual indicators**

Finally, many users spoke to the value of visual indicators and ways of conveying information. This should be understood within the context of the system, which was primarily textual. Users, including P5, spoke to how the few images that were used to convey information were particularly helpful, especially the screen captures of the application displayed on the browser to show users what to expect when completing an action (See Fig.12). For example, "they had like the little icons of what you should be seeing and all that type of things go along, and so I think those are really helpful to take a look and go okay yeah that's what I have this is what I'm doing so (P13)." However, many more users spoke to how they felt communicating information visually was important and was missing within the system. Some users spoke to the need for a video explainer of the overall system:

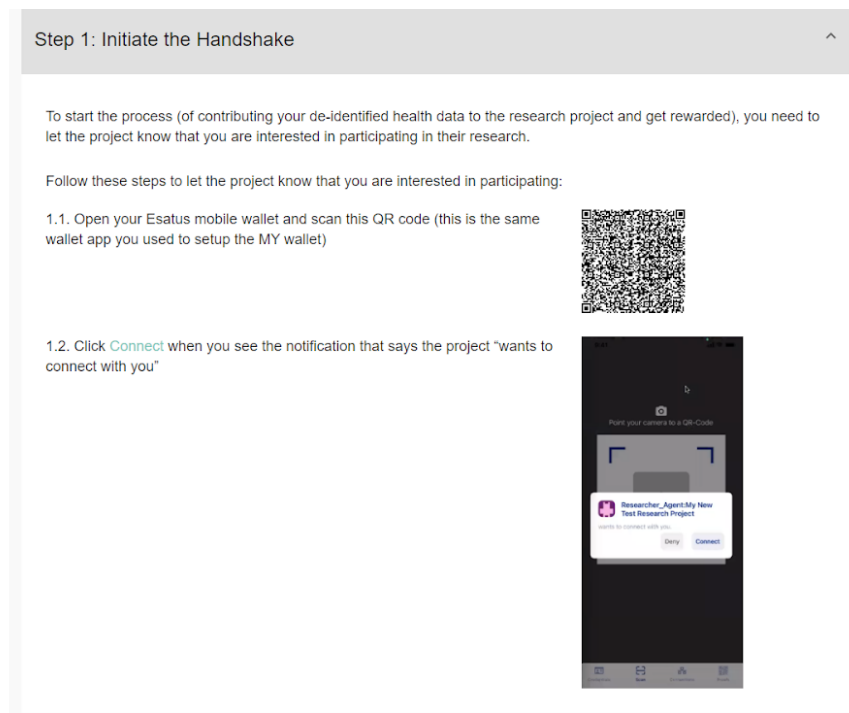
I think as a user there almost needs to be like a simple one or two or three minutes or even a couple one-minute videos at the beginning of YouTube videos about what it's about...I would say the videos give a little bit of variety, to understand right over just reading text sure, and a lot of people don't read well (P7).

Echoing the sentiment in this quote, some users also spoke to how having multiple modes of communicating information, through images, text, or videos, would be helpful for users with diverse information needs and literacy. For these users, visual indicators were a way both of conveying information succinctly and efficiently, but also of helping new users to navigate an unfamiliar system. However, while visual indicators were mentioned by a minority of users, they were not the primary reason the majority of users cited as a reason for their sense of the system's trustworthiness.

#### **4.11 System Elements Supporting Trust and Engagement**

With the findings explored, this section outlines the findings and provides preliminary answers to RQ2 and RQ3. There was a positive and strong correlation between users' perceptions of the system's trustworthiness and their experiences of engagement. From the analysis, users were observed to undertake a process of assessing the system to determine if it was trustworthy. The system was determined to be trustworthy to the extent that it mitigated risks and/or presented rewards that compensated for inherent risks perceived with using the system. Risk for the users interviewed was understood as the potential for the information they were sharing to be accessed or used by bad or unknown actors, resulting in personal negative consequences. Users' assessment of risk was informed by past experiences with technology, organizations, and experiences with

data breaches or being “hacked”. Users gained information they needed to make an assessment through a process of learning through their experience of engaging with the system.



**Figure 12 - Notification examples**

This process of learning involved users gathering information both from the system and their experience of engagement with the system. This information was then used to inform their assessment. Contrary to the literature, the object of their trust assessment was not the ‘technology’ itself or the ‘vendor’ of that technology. Instead, the system as an object of trust was understood to have social, technical, and informational layers by users. Users assessed one or more layers of the system that they felt were relevant to how the system mitigated risks and presented rewards. Within the assessments of users, information was used both as a tool to determine trustworthiness and an object of dependence for trust.

Users spoke about basing their assessment of the system upon how MYPDx communicated about how their information was used, shared, managed, structured, and/or handled and stored. They also spoke to their assessment of the system being based on their experience of engaging

with MYPDx, specifically the perceived usability, reward, aesthetic appeal, and helpfulness of the system. Users gained this information through different aspects of the front-end design of MYPDx, namely the information architecture of the system, the content displayed on the system, the experience of the novel modality used by the system, indicators of authority and authenticity, and explicit asks for consent from the system. Based on information gained from these elements of the design, users spoke to making an assessment about how trustworthy the system, which was based on users' assessment of potential risk relative to their goal of using the system, and how the system presented reward or mitigated risks.

This research asks the following questions of the specific trust (RQ2) and engagement (RQ3) components of the design of SSI systems like MYPDx:

*RQ2: What elements of the design of SSI systems influence user trust in the system?*

*RQ3: What elements of the design of SSI systems influence user engagement?*

Based on the analysis, we can answer RQ2 as follows: through learning about the system by engaging with it, user trust in the system was influenced by the modality, textual content, information architecture, indicators of authority and organizational assurances of the system. Information explicitly conveyed by the system in the form of text, and information derived from users' experience of engagement, primarily from the novel modality of the system, informed their assessments of how the system mitigated risks and presented relevant rewards. Users felt the system was trustworthy when it either was perceived to mitigate risk or offer sufficient rewards to compensate users for the risk inherent in sharing information. In terms of RQ3, user engagement was influenced primarily by the modality of the system, which presented users with feedback

interactively and through control across devices. In addition, the information architecture and visual indicators of the system were relevant to the engagement of users, with users looking for additional visual indicators and ability to navigate the website.

## Chapter 5: Discussion

The purpose of this multi method usability study was to conduct exploratory research with the goal of describing an understudied phenomenon to generate implications for the design of blockchain-based SSI systems. The questions asked by this research were:

*RQ1: What is the relationship between trust and user engagement in SSI systems?*

*RQ2: What elements of the design of SSI systems influence user trust in the system?*

*RQ3: What elements of the design of SSI systems influence user engagement?*

This chapter includes a discussion of major findings as related to the literature on trust in blockchain technology, trust in technology from the MIS field, the literature on engagement from the Information Science field, and literature on design from the Human Computer Interaction field and the emerging area of blockchain studies. This chapter discusses implications that may be valuable to blockchain researchers, designers, and academics interested in the relationship between trust and engagement in user's experiences of technology. This chapter also delivers design implications to inform the design of future systems. It concludes with a discussion of the limitations of this research and avenues for future research.

### 5.12 The Relationship between Trust and Engagement

*RQ1: What is the relationship between trust and user engagement in SSI systems?*

We can begin to answer this question by noting a few things about how users conceived of trust in the SSI system under examination in this study. Firstly, in keeping with the MIS and blockchain literature, trust was understood by users to be fundamentally related to a risk of some kind, arising in situations where achieving some aim is reliant on another person or object (McKnight et al., 2011, Lemieux, 2022). As such, users' conception of risk became important to their conceptions of trust, whatever their relationship to engagement. The specific 'risk' in question was understood by users as the potential for the information that users were asked to share to be accessed or used by malicious or unknown actors, resulting in harmful personal consequences. While not explored in depth in this work the analysis indicates that users' understandings of risk were informed by past experiences with technology, organizations, and experiences with being 'hacked', among other sources. The analysis also indicates that users' perceptions of relative risk were influenced by the perceived motivations, incentives, and credibility of the actors with which they were being asked to share their personal information. Based on this understanding of risk, a majority of users were more interested in sharing their information with projects posted by government, non-profit organizations, or universities than by corporations, as additional risk was understood to be associated with sharing that information with organizations that had a clear profit motive. Rewards in the system for users who shared their data with other projects were thought of as a counterweight to the perceived risk of the system by users who felt the system was not sufficiently reliable. For some users, the potential social benefit of helping advance research, or helping to cure currently incurable diseases, was a motivation for sharing information. However, this was only a motivation for a minority of users.

The quantitative analysis demonstrates a strong positive correlation between user assessments of trustworthiness and user engagement in this SSI system, whereby users whose

experience of the system was characterized by engagement were also likely to see the system as trustworthy. The qualitative analysis was then used to understand the phenomenon. Users' sense of 'trust' in the system was observed to take the form of an assessment of trustworthiness, whereby the system was assessed as having whatever attributes users felt were necessary to mitigate risk. Based on the analysis, we can describe the phenomena of users deciding whether to trust this new system in the following way: users felt the system was trustworthy to the extent that it's perceived attributes mitigated relevant risks and/or presented rewards relative to the perceived attributes of the system based on a process of learning based in engagement with this new type of system.

The qualitative analysis indicates that engagement was related to trust in two ways: as a tool for gaining information relevant to the users' trust assessment of the system, and as an output relevant to the user's trust assessment. It is important to note that participants in this research were presented with not just a new system, but a novel application of an unknown technology, and the system under study involved sharing highly personal and sensitive information. In addition, that technology relied on a novel modality (scanning QR codes on a platform using a wallet app). It was observed that users engaged with MYPDx as a mode of learning, sensemaking, and generating a conceptual model of the system, which informed their assessment of the system's trustworthiness. The analysis supports the idea that users also based their assessment of the system in part on their experience of engagement, specifically their experience of perceived usability, reward, and aesthetic appeal within the system. Further, several of the quantitative engagement factors were shown to be positively correlated with an assessment of trustworthiness by users. Out of the engagement factors, perceived usability was most strongly and positively correlated with an assessment of trustworthiness by users. From the qualitative analysis, it was observed that experiences of interactivity, control, and feedback were cited by all users within their experience

of the usability of the system as a reason for their assessment (positive or negative) of the system's trustworthiness. In most cases, users' experience of feedback, interactivity, and control helped to develop their conceptual model of the system, and what safeguards were present to protect their information. However, in the cases where users were confused by MYPDx, the perceived lack of usability of the system was cited as a reason for their lack of trust in the system.

Reward was positively correlated with trust. Users also spoke about how the system presented 'rewards', either monetary or social, for using the system. However, we should make a distinction here between the system presenting rewards ('rewards for using the system') and a users' experience of using the system as being 'rewarding'. The former is a way in which the system incentivizes usage, and emerged as relevant to users from the qualitative analysis, whereas the latter is a quality of the experience of users which was measured quantitatively by the UES-SF. As such we need to be careful to not misinterpret the comments of users as being about the capacity of the system to present rewards as users speaking about their perception of their experience being rewarding. What we can conclude from the qualitative analysis is that the ability of the system to offer rewards was understood by a majority of users to be relevant to their assessment of whether to risk placing trust in the system. The correlation of users' experience of the system as rewarding and users' assessment of trustworthiness then should be understood as a separate finding.

However, it should be asked whether the interviews, which were conducted before the administration of the UES-SF, influence the way users rated their engagement? These questions are meant to capture an aspect of the experience of users' engagement with a system, as is discussed within the literature on their creation, refinement, and usage (O'Brien, 2016a, O'Brien, 2016b, O'Brien et al., 2020) Within the UES-SF, (and the survey administered in this study)

“Reward” pertained to the use of the application as worthwhile and whether the experience was rewarding and interesting (O’Brien et al., 2018)

It is worth remembering here that the reward factor, as part of the four factors within the UES-SF was refined from a six-factor model. This model included Felt Involvement and Novelty as factors, which upon analysis were refined into the reward factor (O’Brien et al., 2018). As such the items in the UES and UES-SF have been designed (and proven) to measure the way in which user’s experiences are novel, spur curiosity, or are worthwhile. We can also note that the reliability analysis conducted for the reward factor with the survey data gave a rho value that was positive and moderate to strong, indicating the reward items are functioning as intended in this context. We can see, then, that the focus of these items, and indeed the factor of ‘reward’ within the UES is unrelated to ways in which the system present rewards. A system that presents explicit rewards may be worthwhile, rewarding, or novel to users, but this is not the focus of the UES-SF or the analysis of how engaging users found the system in this study.

Within the findings of this study, it is more accurate to say that the presence of explicit rewards was important to user’s assessment of whether to risk placing trust in the system, and that there was some relationship between their experience being rewarding and the system being trusted. The latter was not seen to be supported in the qualitative analysis. While the ability of the system to offer rewards may be in some way related to the way the experience of the system was rewarding, this will need to be further explored in subsequent work. This distinction is further discussed in the Limitations section.

Finally, while not as strongly correlated as the other factors, Aesthetic Appeal correlated with trust. However, from the quantitative analysis it was observed that the aesthetics of the system as a prototype were associated by users with secure, spartan, government websites, which were

seen to be secure. The observed relationship between engagement and trust then can be understood to be constitutive. Engagement can be theorized as a way in which users gather information on which to base their trust assessment. It is therefore a part of that assessment, such that the quality of the way the system engages users may have an effect on the perception of the system's trustworthiness. Further work will need to be conducted to prove this connection to be more than correlative, as well as the valence and strength of the engagement factors with user trust.

### **5.13 The Relationship between Design and Trust**

*RQ2: What elements of the design of SSI systems influence user trust in the system?*

User perceptions of trustworthiness were observed to be influenced by two different levels of abstraction of the design of SSI systems. As mentioned before, the object of the users' trust assessment was not the attributes of technology, nor the 'vendor' of that technology, but rather elements of the social, technical, and informational layers of the system taken together. These three subsystems, plus an additional governance subsystem, have been shown through this analysis to be variously relevant to the trust assessment of the users interviewed, with all users speaking to their assessment with reference to one or more layers. Within the three layers, users based their assessment of the system upon information explicitly conveyed by the system about how their information was to be used, shared, managed, structured, and/or stored. They also relied on information about the motivations, incentives, and capabilities of social actors within the system. Finally, they relied upon their own conceptual model of the system they were interacting with to help them understand how the technology mitigated relevant risks. Therefore, we can understand the system-level design decisions as represented to users through the user interface to be influential

on users' assessment of trustworthiness, though quality and character of the specific relationship will need to be explored in future work.

Users gained information relevant to their assessment of trustworthiness through different aspects of the design of the system, namely the information architecture of the system, the content displayed in the system interface, the experience of the novel modality used by the system, indicators of authority and authenticity, and explicit asks for consent. Representation of the information architecture was a centrally important aspect of the UI design within this system for users, with a majority speaking to the importance of IA in this unfamiliar digital context as a way of enabling sensemaking. This observation is broadly in keeping with McKnight et al.'s (2011) work on trust, which identifies what they call "situational normality", or "familiar structures" within a new technology as being relevant to the trust assessments of users (though they do not offer more about what this entails other than referring to similar "features" of other technologies) (McKnight et al., 2011). While there may be a temptation to uncritically treat 'IA' as what the concept of 'situational normality' denotes, this is likely stretching the theory of trust in a specific technology too far to be considered valid. However, the analysis shows that we can think of IA as a kind of relevant 'structure' to users' assessment of trustworthiness within an unknown and novel technology. The analysis shows that in unfamiliar contexts for users an SSI system's IA may help users to 'wayfind' as part of the sensemaking process, and ultimately to learn in a way that is related to their trust assessment. It is worth noting that the IA of the system also gave users a sense of control through being able to correctly predict how the system would operate, which was particularly relevant as they learned to use the novel modality present in this system. In terms of the specific (primarily textual) information conveyed, the analysis indicates that users were looking for the information to be clear, understandable, and non-technical. Some users were

concerned about specialized and incomprehensible health sciences language, which underscored users' need for the right information to inform their decisions. The importance of IA to trust is further reinforced by the observation that when the IA was unclear, or inconsistent, this generated in users a sense of insecurity, uncertainty, or a lack of safety in using this system relative to the potential risks involved with sharing their information.

The other element of the design that was shown through the analysis to be relevant to users' trust were indicators of authority, authenticity, and oversight. Specifically, users looked for logos, badges, links to third party websites, or other ways of triangulating the information about the involvement, motivations, and incentives of actors on the platforms. In general, the data shows that users wanted to know 1) if the involvement of potentially trusted actors was legitimate and 2) to find out more information about their involvement. Users then looked for information about what information the actors would be able to access and what kind of oversight was in place to ensure the actors complied with the stated restrictions. The results indicate that users were interested in the REB certification included in the MYPDx platform as a key method of assurance about the oversight and quality of actors on the platform. Based on information gained from the three layers of the system's architecture, and these aspects of the UI and UX design, the analysis indicates users made an assessment of how trustworthy the system was, based on the potential risk relative to their goal of using the system and how the system presented reward or mitigated risks.

As such we can answer RQ2 by noting that there were both relevant system-level design choices and design elements that were relevant to users' assessment of the system's trustworthiness. These elements were relevant to users' trust assessment by helping to convey information to users about what were perceived to be relevant aspects of the system that helped to mitigate risk. Importantly, information here was understood both as explicit information conveyed

to users through the system, and information users gained through their experience of engaging with the system.

#### **5.14 The Relationship between Engagement and Design**

*RQ3: What elements of the design of SSI systems influence user engagement?*

User's experience of engagement with the system broadly followed the picture outlined in the literature whereby the factors of perceived usability, focused attention, aesthetic appeal, and reward influenced their engagement. In keeping with the literature, users' experience of engagement was primarily influenced by aspects of the system that gave them a sense of control, feedback, and interactivity, presented rewards, or presented relevant aesthetics. Within the system the specific element of the design was the novel modality users engaged with in order to share their personal information. This process explicitly created an experience that engaged users by giving them a sense of control over their data through feedback and indicators. From a system perspective, it was one of the main points at which the UX and technical stack of the system overlapped in a way that actively involved the user in the process of sharing information. As such, it became a key site for users to learn about the system in a way that strengthened their conceptual model and understanding of the technological layer of the system architecture. The other engagement factor most present in the quantitative analysis was reward. However, the difference between the way reward emerged from the qualitative analysis and the factor of reward measured by the UES-SF makes it hard to infer anything other than that users' experience of the system being rewarding was significant to their overall experience of engagement within this system.

What exactly users found rewarding about using the system will need to be explored in future work.

Other aspects of engagement were notably absent here. Specifically, the factor of Focused Attention from the UES was weakly correlated with trust and was not a significant feature of the qualitative analysis. This may be attributable to methodological issues with think aloud protocols, an issue discussed further in the Limitations section below. Finally, the aesthetics of the system were minimally relevant to users experience of engagement, and weakly correlated with trust. People looked to the few visual indicators there were to gain a sense of how the system worked. This should be understood within the context of the system, which was primarily textual. Users spoke to the helpfulness of the few images that were used to convey information. Some users also spoke about how the “lack” of aesthetics, or more specifically the visual similarity of the prototype to government websites, led them to associate the system with a higher sense of security. However, this was not a significant or consistent phenomenon across study participants. Nevertheless, it points to the potential that more ‘aesthetic’ designs might not necessarily correlate with higher assessments of trustworthiness by systems users in the context of health information sharing.

### **5.15 Design Implications**

It is a common practice within HCI scholarship to derive design implications as a way of making insights from research actionable for future designers. The primary audience for the recommendations below is designers and researchers exploring how to develop new and trustworthy technologies within the area of health-related blockchain systems more generally (with the caveat that the relationship between the findings of this research and other blockchain systems has yet to be empirically demonstrated). Design principles often take the form of short

descriptions, sometimes approaching aphorisms in structure (Fogg et al., 2003). However, some researchers have critiqued design implications as an output of design research as being unable to be assessed for their quality or speaking to different levels of the design process which may be insufficiently generative for future work (Dourish, 2006, Fallman, 2007). Recent work has attempted to correct this by establishing a participant derived taxonomy of design implications to enable a greater ability for researchers to speak to what the characteristics of design implications are and how they can be evaluated (Sas et al., 2014). The design implications presented in this work are constructed with this nascent taxonomy in mind, with an eye to presenting high quality, generative design implications for future work. Specifically, they aim to offer meta-abstractions, or “suggestions for interpreting more abstract technology goals captured by sensitizing concepts” (Sas et al., 2014, p.1974), and socially oriented design concepts, understood as “a preferred form of generalized design knowledge for moving beyond the situatedness of requirements. Described in user-oriented language, they capture abstract ‘design knowledge’ that is relevant both to the socio-technical context of the users and system” (Sas et al., 2014, p.1974). These implications were derived with consideration given to key dimensions for evaluating the quality of design implications, namely validity, generalizability, capacity to be generative for designers, capacity to be inspiring for designers, and actionability (Sas et al., 2014, p.1977-1979).

#### **1. The user’s conceptual model of the entire system is essential to trust**

When it comes to trusting a new system, users look to learn about a new system to see whether it is trustworthy. Explicitly supporting the development of a conceptual model through both the information conveyed to users and the experience provided to users may help users make better sense of this new type of system.

## **2. Designing for engagement may support trust**

While causation has yet to be proven, there is a strong correlation between users' assessments of the trustworthiness of a system and their engagement with a system. This means that designing for engagement may entail designing for trust. The ability of a new system to convince users that it is trustworthy relies on its ability to show users relevant features that mitigate risk and present sufficient reward. Engagement is an important source of information for users. In addition, treating engagement as a design outcome may also lead to an improved experience for users.

## **3. Balance information asymmetries**

When it comes to trusting a blockchain system, users are in an inherent information asymmetry with the system and other users. While users may have relevant design or technology metaphors to draw upon in interacting with a blockchain-based system, these metaphors may do more to confuse than inform. Therefore, a design goal should be to provide users with the information that they need to assess the system's trustworthiness.

## **4. Support learning through feedback**

Users may learn through a process of engaging with the system. The way users perceive the usability of the system and, specifically, experiences that give users a sense of feedback and control, help users to gain information about the space of permissible action for them and other users. This information is important for users' assessment of the system's trustworthiness. Design elements and sections should carefully consider where it may be appropriate to communicate key ideas about the system through feedback or even friction.

## **5. Focus on Information Architecture**

When encountering a new technology, or an unfamiliar modality, information architecture is a key place where users find information and use it to make sense of their new digital context. The end goal for users is to develop a conceptual, or mental model, of the unseen aspects of the system, such that they can make a reasonable assessment as to its trustworthiness. Focusing on creating a coherent, logical, and approachable means of representing a system's information architecture for users should be prioritized to help users develop a conceptual model within unfamiliar systems.

**6. Ensure that the system is helpful in an accessible, clear way**

Content, copy, and images are primary avenues for communication about an unknown type of system. Language should be clear, accessible, and informative without being overwhelming. Images should be integrated thoughtfully in places where they have the greatest explanatory power. Conducting content audits or testing language with lay users may be useful avenues for future designs.

**7. Give users ample organizational assurances**

Users are looking to learn more about the motives, incentives, and capabilities of other users they may interact with through a platform. Clearly speaking to the incentives, actions, restrictions, and oversight placed on other actors by the system may help users to assess whether other users are trustworthy. Logos, third party links, and other markers of authenticity that allow users to corroborate the information presented from other sources may also be relevant.

**8. Offer rewarding experiences.**

Reward is a relevant part of user's assessments of trustworthiness and can help motivate users to continue to use a system as part of their assessments of risk and rewards of system use.

Careful consideration of where and what kind of rewards and rewarding experiences are being presented to users should be a focus of future designs

## **5.16 Research Implications**

In this section, the relevance of the findings of this study for research and practice are discussed with reference to the relevant interdisciplinary literature reviewed. In particular, the findings of this research are relevant to researchers interested in user engagement, user trust, and the design of non-cryptocurrency, specifically SSI, focused blockchain systems.

### **5.16.1 Design of Blockchain Systems**

We can begin with looking at the research on the design of blockchain systems. The findings of this study contribute to work by Khairuddin et al. (2019) to further confirm that users have mental models of blockchain systems architecture that change with exposure to information and are sensitive to design choices. This research highlights how these mental models, understood here using Norman's (2013) definition of conceptual models, are central to users' assessment of the trustworthiness of systems. Within the intersection of research on blockchain systems and trust within HCI, understanding these mental models could be a primary area of exploration going forward, as well as seeking to explore how these mental models might change in different contexts with more detail.

In their typology of blockchain systems, Elsdén et al. (2018) concluded that there is a question of how to demonstrate the trust-preserving nature of blockchain systems to users (Elsden et al., 2018). However, the findings of this study demonstrate it is not sufficient to demonstrate *solely* how the technical layer of the system is “trust-preserving” to users as technical components

are not the only relevant factor to users' trust in blockchain systems. Rather, users may be looking at one (or a combination) of the informational, social, and technical layers of the system to find information that is relevant for their assessment of the trustworthiness of the system as a whole. Indeed, contrary to work by Eskandari et al. (2015) and Voskobochnikov et al., (2020 & 2021) confusion about how blockchains worked was not a deterrent to users understanding or wanting to use the system. Likely because both Eskandari et al. and Voskobochnikov et al.'s work focuses on wallets for managing cryptocurrency, there is an assumption in the work of both scholars that the trust of users is primarily located in the blockchain technology that enables cryptocurrencies like Bitcoin. What was important for trust, rather than an awareness of how the blockchain technology in MYPDx was implemented, was a robust conceptual model of the system, which was utilized to assess the system's technical, informational, and social design and operation in order to assess its trustworthiness. This highlights the need to deeply understand user trust in blockchain technology beyond the technical aspects of design, a finding consistent with Lemieux & Feng's concept of a blockchain as a socio-informational-technical system (Lemieux, 2022).

This research builds on the UX-focused work of Voskobochnikov et al. (2021) in a number of areas. Firstly, Voskobochnikov et al. in their research on non-custodial wallet apps have written that UI issues "present a unique case where user interface (UI) issues that would be harmless in many apps can have a disastrous impact on the UX and can lead to monetary losses" (Voskobochnikov et al., 2021, p.16). Based on the findings of this study, we can reasonably expand Voskobochnikov et al.'s findings to include other blockchain-based systems used to store and secure sensitive or valuable information. In fact, a UI issue leading to a user inadvertently sending genetic and other biomarker information to an actor that users do not trust may potentially be more consequential than sending a small amount of cryptocurrency. As such, usability issues are a

particular issue for all blockchain systems, especially those that are novel to users. Usability, clarity, and intelligibility are important not just for the user's experience of a system, but for the more fundamental processes of users gaining an understanding of the system structures relevant to their sense of trust.

This research also provides new insight into the relationship between UX and trust in Voskobochnikov's work (2021). Voskobochnikov et al.'s research demonstrates that "poor UX" leads users to lose trust in cryptocurrency wallet apps and to question the motives of designers and developers (Voskobochnikov et al., 2021). The results of this study build on Voskobochnikov et al.'s findings, corroborating that UX issues diminish the trust of users in a blockchain-based health information platform and asserting that 'good UX,' (understood as an engaging user experience) may lead users to place their trust in such systems. Specifically, this work adds to this literature through the finding that users' object of trust was not solely the technology or social layers (i.e., other social actors with whom they interact mediated through the blockchain system) but one or more of the social, technical, and informational layers of the system. Further, it places UX within a framework that enhances the intelligibility of the concept of how 'poor UX' may lead users to distrust systems. Because users' experience with a system informs their conceptual model of said system and their trust assessment, systems with 'poor UX' do not demonstrate to users how the system mitigates users' perceived risk, or can even demonstrate the opposite (i.e., that the system is riskier to use). Further, we can expand on what 'poor UX' might mean by citing a lack of tools that allow users to make sense of their new digital environment, including coherent information architecture, indicators of authority and authenticity, feedback, and control. It is worth noting here however that findings of this research are preliminary and further research would need to be conducted to prove the generalizability of these assertions.

This research also supports Zavolakina et al.'s (2020) finding that design elements play an important role in giving users information and context about blockchain systems. Elements of the front-end of design of blockchain systems have been observed here to provide users with an epistemic foundation for trust by giving users information about the space of permissible action the system enables. While this work does not rely upon the same trust supporting design element (TSDE) framework that Zavolakina et al. (2020) employ, it is likely that the elements outlined in the results section could be understood as kinds of TSDE's. Importantly, the elements specified by the Zavolakina et al.'s (2020) use case (a blockchain platform for sharing car information) were also noted as relevant by users in this research. Specifically, elements that give users a sense of organizational assurance (logos, descriptions of the restrictions on the actors, the REB), and elements that gave users information to better understand the system and the motivations of the parties involved (FAQ and informative text throughout) (Zavolakina et al., 2020). In general, the design principles surfaced by Zavolakina et al.'s research, that it was important to not 'black box' the technology in blockchain platforms and that systems must provide users with enough information to wayfind in a new environment without overloading them, are consistent with the findings of this research (Zavolakina et al., 2020). This research also supports Zavolakina et al.'s (2020) framing of the interface as the primary point of contact of the user to the blockchain platform and therefore crucial to user trust in such systems. This research contributes a more robust picture of how UX influences user trust through helping users to form trusting beliefs based on their assessment of a system's trustworthiness. It also clarifies the object of trust of users as the system and presents empirical evidence to support the view that social, informational, and technical layers of the system are relevant to users' trust in blockchain systems.

### 5.16.2 Trust

The findings of this study present important implications for the strand of technology-oriented user trust research exemplified by the theoretical framework of trust in a specific technology (McKnight et al., 2011, Meeßen, 2019). The findings of this study show that users' beliefs about the attributes of MYPDx were not solely based on the 'technology' in a positivist sense, but instead about the social, technical, and information layers of the system as understood by users. While it could be argued that this finding contradicts the theory of trust in a specific technology outlined by McKnight et al. (2011), I instead argue that these findings indicate a definitional move is more profitable. I argue that within the context of 'trusting beliefs in a specific technology', 'technology' can be meaningfully understood to mean each user's 'conceptual model' of the system. It will be shown that this definition more closely aligns with the findings of this study and is consistent with McKnight et al.'s (2011) theoretical background. Further, this movement enables McKnight et al.'s (2011) work to have additional explanatory power and clarity by situating the theory within a design context that can inform both future research and the design of future systems.

We can begin by noting that McKnight et al. (2011) define technology as "the IT software artifact, with whatever functionality is programmed into it" (McKnight et al., 2011, p.2). Users' beliefs about the technology are understood to focus on "the favorable attributes of a specific technology", namely its perceived functionality, reliability, and helpfulness relative to completing a goal the user has in mind (McKnight et al., 2011). It is worth noting that while McKnight et al. speak at length about users' trusting beliefs, as part of their development of a testable construct, they do not specify what they mean by the technology aside from mentioning 'features' (McKnight et al., 2011). For example, when speaking about structure that added to the system's helpfulness, they mention "the tutorials embedded in the software" (McKnight et al., 2011, p.14). McKnight et

al. (2011) frame their focus as differentiating literature on trust in a technology from what they argue are measures of trust developed from human agents, which have been applied wrongly to ‘IT artifacts’ (McKnight et al., 2011). At the time of publication of McKnight et al.’s (2011) foundational paper, there was a clear need within the MIS literature to develop a theoretical framework that focused on the role of technology as an object of trust. The majority of work in the field at the time instead focused on technology vendors (e.g. Microsoft) as the object of user trust rather than the technology they created (e.g. Excel). McKnight et al.’s work remains the dominant (and only) strands of work on trust to focus on technologies as an object of trust within the MIS field to date (Meeßen et al., 2019). This focus on the role of technology in influencing user trust motivated the selection of this theoretical orientation for this work. While McKnight et al. discuss technology as “a human-created artifact with a limited range of capabilities that lacks volition (i.e. will) and moral agency”, they do not go on to define the term technology within their work in a way that differentiates it from the larger system, or differentiates components within a system such as the interface, the design elements within the interface, the larger technical architecture, or the hardware used to enable the system (McKnight et al., 2011, p.5). These components are essential for understanding the relationship between the design of a system and the users’ trusting beliefs. Further, given that McKnight et al.’s work is preoccupied with the way in which technology influences trust (as opposed to human agents) this level of granularity is desirable both for informing future research into the specifics of how technology influences trust and the further development of trustworthy systems.

Thus far, the word ‘technology’ has been used uncritically, but it is important to refocus on what the term ‘technology’ meant for the users interviewed. As noted in the findings, users were observed to assess the technology with reference to their beliefs about how the system

functioned, based on their experience of engaging with the system. The majority of users' beliefs about MYPDx were shown to be based on their beliefs about one or more of the following areas: 1) their beliefs about the technical architecture that enabled their experience with the system; 2) other actors on the platform, such as the organizations with whom users would be sharing information; and 3) the way users perceived that their biomarker information was managed, used, stored, shared, and structured. While it might be asked whether the trust measures were operating as intended, through the reliability analysis conducted, the trust construct adopted from McKnight et al.'s (2011) work was shown to be functioning acceptably within this new context. Further, through interviews with users, many of them spoke of trusting the 'technology' itself. As one user said, MYPDx was "definitely trustworthy. Just the sheer amount of times [I was asked for] verification and QR codes, I felt that whatever was happening in the background or even like presently in the front. It was...overly secure (P14)." The same user also spoke to the role of social aspects of the system as being influential to their sense of trust:

It gives you like a sense of the counterparty. You can see who's actually conducting the research. if you had a bad experience with say some pharmaceutical company you could be 'like, yeah no I'm out, I don't want to deal with you and I don't want to provide any of my information to help you broaden your scope or anything' (P14).

From this quote, and the other findings above, we can see that the users in this study placed their trust in their understanding of how the technology worked based on specific structures (e.g., QR Codes) or experiences (e.g., being asked for verification); they didn't need to have any understanding of how the technology actually worked to trust it. They also assessed other aspects

of the system, such as the reputation of actors within the system, as part of determining whether MYPDx was trustworthy. These findings could be understood to fully contradict McKnight et al.'s (2011) theory. However, we can profitably understand these findings in the context of McKnight et al.'s (2011) theory by redefining technology as 'conceptual model'. Following Norman (2013) a conceptual model within a designed object "is an explanation, usually highly simplified, of how something works" (Norman, 2013, p. 25). As he writes, the conceptual model is distinct from the actual technological stack that underlies a system, though it may not appear that way to a user, who only interacts with the system's front end:

The conceptual model is of one, coherent image, whereas it may actually consist of parts, each located on different machines that could be almost anywhere in the world... The major clues to how things work come from their perceived structure—in particular from signifiers, affordances, constraints, and mappings. (p.25)

The system's conceptual model then is theorized as the way the designers of the system understand how their system can be used, and how they communicate that information to users through the structures they create (Norman, 2013). Users then are understood to have mental models<sup>3</sup> that inform their understandings about what to expect when using the system (Norman, 2013). Mental models are developed through the interactions of users with the technology (or object) in question, but ultimately are a series of beliefs; they are not the system itself or the conceptual model designers have when creating the system and communicating how to use it. Therefore, users'

mental models can and do change over time while interacting with a given system. In this study users mentioned their understanding of the conceptual model of the system, accurate or inaccurate, as a key reason for their positive or negative trust assessment of the system. It's also worth recalling here that a majority of users were unaware of the presence of blockchain technology within the system. As such when users spoke to their trust being based in the technology, they spoke to their conceptual model of the system rather than anything specific about the technology itself. Within the findings the 'technology' that formed part of the object of user trust, then, was more accurately 'users' understanding of the conceptual model of the system'. As these findings are based in the theoretical constructs and orientation of the theory of trust in a specific technology, these findings should spur us to consider whether this redefinition is relevant for the theory as a whole within the MIS literature.

Further, there are benefits to this redefinition for this theoretical strand. Firstly, the idea of a conceptual model is ubiquitous both within the psychology and cognitive science literature from which Norman initially imported the concept, and also in the last 30 years of UX and interface design work within the HCI field (Guarino et al., 2020, Markman, 2013, Norman, 2013, Carroll, 2003). Redefining 'technology' as 'conceptual model' therefore places McKnight's constructs in relationship with design methods that can lead to implications for future designs. Understanding, for example, that there is a relationship between the strength of a user's conceptual model and their sense of trust in an SSI system could be actionable information for a designer, leading them to improve their system's information architecture through a content edit and card sort, and then to run subsequent testing with users to assess the changes.

Secondly, understanding 'technology' within McKnight et al.'s theory also adds a level of clarity that has been shown to be missing regarding what specific aspects of the system are relevant

to the trust of users. While McKnight et al.' speak about the 'technology' or 'IT artifact', understanding user trust in 'technology' as 'user trust in a conceptual model of a technology' means that the parts of the technology that are relevant to user trust are the ones that are most impactful on their experience. While a causal argument could be made that the back end of the system enables the features that make systems something users think of as trustworthy, ultimately the main effect on users' experience comes from the interface that they experience and manipulate to operate the system. There are a multitude of important engineering problems that form the basis for the improvement of user experience, but ultimately a user's trust is not dependent on how a particular system manages hardware problems (for example, compute power over scale), but rather how a system supports users' experience of using and learning about the system. In fact, it's unclear analytically how users' trust *could* be based on anything other than the front-end they're interacting with when it is their sole point of contact with a system. In practice even professional software developers would be hard pressed to correctly identify the entire technical stack of a previously unknown technology solely through interacting with its user interface. Further, while software developers and other expert users might find relevant information for their assessment of trust in knowing more about the implementation of a particular system, lay users are unlikely to, and the population we are interested in is not necessarily expert users. Therefore, this redefinition not only better accounts for the findings of this study, but re-focuses McKnight et al.'s (2011) theory in a direction that clarifies what aspects of 'technology' are important, leading to new avenues for research and design.

Taking this different definition does represent a departure from the conceptual framework used by McKnight et al. (2011) that grounds this work. However, it can also be shown that this definition is consistent with the theoretical background of the theory. We can begin by noting that

in McKnight's work, the conception of trust in a specific technology is a primarily cognitive form of trust (McKnight et al., 2011). They argue that the beliefs about the functionality, reliability, and helpfulness of the technology, which form the foundation of the construct measures they subsequently test are based on "knowledge that users have cultivated by interacting with a technology in different contexts, gathering data on its available features, and noticing how it responds to different actions" (McKnight et al., 2011, p. 9). For example, the theory differentiates between initial and knowledge-based trust, which is gained through use of the system over time and an increased ability to predict how it can be used to achieve the user's goals (McKnight et al., 2011). They also note that the beliefs that the users form are "perceptual, rather than objective in nature" (McKnight et al., 2011, p. 6). In McKnight et al.'s theory then, the beliefs that users form do not have to have any objective validity, but rather can be based on attributes they believe the system to have, given their experience of the features, capabilities, and responsiveness of the system. It appears then that the object of trust in this theory need not be the technological stack in any strong ontological sense, but rather must be a belief that the user has about the system. In practice, this conception bears a striking similarity to the idea of a user's conceptual model, or a theory of how the system works based on the perceived structure of the system gained through interaction with the system (Norman, 2013). Within the idea of a conceptual model, there need not be a strong link between how the system is implemented and how users understand it. While layers of abstraction within the system, from electrical signal to frontend language, may be essential to the functioning of the system, in so far as they are invisible to how users understand and operate a system, they need not be relevant to the conceptual model. As such, this redefinition can be understood to be consistent with the findings of this study and broadly consistent with the theoretical outlook of McKnight et al.'s initial theory, while giving the theory additional clarity

and connecting it to generative design-based practices. Further work will need to be done to explore the relationship between the idea of the conceptual model (within the HCI literature), users' mental models, and users trusting beliefs (within the MIS literature). For example, whether 'users' beliefs' about the system are subsumed by their mental model, or meaningfully related to it. It may also be worth considering the goals and focus of McKnight's model of trust in a specific technology in light of these findings. In proposing this redefinition, this work argues for the need for additional conceptual clarity, both within this work and in work seeking to explore the interaction of users, trust, and interface.

Regarding the object of trust for users interacting with this blockchain system, the findings of this research provide (limited) empirical support for the view that the object of trust for users in blockchain systems is the technology alone; rather the object of trust should be understood as being a socio-information-technical system, with one or more of the layers being relevant to users' assessment of the system's trustworthiness. Users were observed to look for information about the system, the actors, and the way the system handled their information through explicit information on the website and their experiences of engagement. Users were also observed to undergo a process of learning through engagement, attempting to find the information that they needed to assess the trustworthiness of the system. This information often focused on how the system constrained or provided oversight for social actors, and how the system protected and enabled control over users' information. This aligns with emerging work by Lemieux, which argues that "to attempt to understand blockchain purely in terms of the computational technologies...is to miss the mark by focusing on the wrong abstraction layer" (Lemieux, 2022, p.8) The findings of this work also broadly support Lemieux's picture of risk as arising due to uncertainty based on an information asymmetry between trusting party and trusted party (Lemieux, 2022). Further users' conception of

risk as communicated by users in this study can be understood to be consistent with Lemieux's work. We can recall that users' picture of risk within MYPDx was focused on the possibility of information being accessed by unauthorized or malicious actors. While this is technically very unlikely within the structure of the private permissioned ledger used by MYPDx, users were not aware of the particular ledger used, and a majority had no real familiarity with blockchain systems. It's perhaps unsurprising, then, that users were observed to associate significant risks with using the system, and in instances where the information architecture or system in general was unclear, indicated this as a reason for not trusting this system. As Lemieux writes "When trusting parties lack knowledge of blockchain and distributed ledger systems, or when information is misleading or confusing, trusting parties are likely to perceive the risks of transacting as too high and thus are likely to avoid it" (Lemieux, 2022, p.45). This work also contributes the idea that reward may be a moderating force on users' trust assessment, where reward is also relevant to the experience of users.

Lemieux also outlines within their conception of user trust that users look to see how the system constrains and permits the actions of other users. As Lemieux writes "power and authority are algorithmically encoded into the ledger. They are endogenous; that is, they are achieved via the operation of the rule of code" (Lemieux, 2022 p.54). The findings of this study support this, as users were observed to look for information about how other actors were constrained and permitted to act within the system, and to use that as a basis for their assessment. Finally, this research supports the idea that the interface of a system, and specifically the design elements of a system are what Lemieux calls a 'filter', mediating the trust of users in the three layers of the system by presenting information relevant to their assessment of the risk of using a particular system as a

basis of interaction with other social actors, in the case of MYPDx for example, to exchange health information with researchers. As they write:

Thus, there are many filters through which information about the trustee must pass in the process of a trustor forming a belief that it is good, safe, or reasonable to trust, or conversely, mistrust. Once a decision is reached to trust or not trust, then further active gathering of information often ceases (Lemieux, 2022 p.36).

This work therefore provides limited empirical support for Lemieux’s theoretical framework. It also contributes the conception of the design of systems being relevant to the way in which users learn about the system through engagement, in order to assess a blockchain system’s trustworthiness.

### **5.16.3 User Engagement**

This work extends work by O’Brien et al. into a new context, demonstrating that the UES-SF can be applied to measure engagement factors for users of blockchain systems. As such, this work adds to the extensive number of studies that have employed the UES, speaking to the generalizability of this theory and tool.

In the literature, engagement is theorized as both a process and a product of the quality of user experience with a system (O’Brien, 2016a). Engagement is understood as when users “move beyond cursory use of a system and invest themselves in the interaction” (O’Brien & Toms, 2008). We can and should ask here: how do we know that the users in this study *engaged* with the system, rather than simply using it “cursorily?” To answer this, we can make a basic assertion, following

O'Brien and Toms, that engagement “operates on a continuum...it may be poor, average, or high” (O'Brien & Toms, 2008, p.948). Therefore, we can note generally that engagement can be a lens for analyzing any user's experience and can be generative even where there is little or no engagement. However, in this research the users surveyed had overall positive scores for the engagement items measured by the UES. This indicates the presence of aspects of the construct of engagement within the experience of individual users at significant levels for this analysis. In addition, we can note that the engagement construct measured by the UES was shown to be reliable, indicating that there is a latent trait being measured (Hattie, 1985). Thus, from the quantitative data we can assert that in this instance users experience of using the system can be characterized by engagement, and that the experience of engagement was significant enough to be relevant to the findings of this study and this analysis.

It is worth noting here that while engagement has been used to describe the structure and analyze the outputs of this study, the specific platform under examination was a prototype. As one user noted, this was a platform where the designers had not “got their fill” and was still multiple iterations away from being market ready. The platform was designed with the goal of testing the viability of key features of the system as part of an iterative design process towards the development of a minimum viable product. The prototype had limited visual elements, and primarily relied on text to convey information. As such, it is somewhat unsurprising that the design elements most relevant to engagement were the few that gave users the most feedback, presented information in delightful ways, or held users' attention. This is most telling in the lack of relevance of Focused Attention as a factor to users' experiences of engagement in the context of this study. While this will be explored further in the limitations section, the guided tasks given to users as part of the interview protocol may have interrupted users' immersion in the system, meaning that the

user behavior observed was not naturalistic. While this is not an issue for validity, as will be discussed, this may have detracted from users' focused attention while using MYPDx. As this factor would likely be relevant to users' experiences of engagement in a market-ready iteration of MYPDx, these findings should also be contextualized as relating to user engagement within a prototype version of this kind of system, rather than being construed as applicable to all SSI blockchain-based systems. While there are implications within these findings that may be generative, they have not been demonstrated to be generalizable.

Lastly, this work connects user trust to user engagement, and to the researcher's knowledge is the first study to do so using the process theory of user engagement, and the UES-SF. Future work could explore the relationships between these two areas, and the work of O'Brien et al. (2018) and McKnight et al. (2011) within the perceptions of users and the systems they use. Indeed, as outlined in the methods section, there are theoretical resonances that make this a useful connection. Both theories conceive of the phenomena they describe as being context specific to the system under examination and conceive of the phenomenon in cognitive, behavioral, and affective terms. It should be noted however that McKnight's 'trust' is primarily a cognitive phenomenon, where O'Brien and Tom's 'engagement' is understood to have affective, cognitive, and behavioral dimensions.

### **5.17 Limitations**

While the scope of this work has been ambitious, it is worth contextualizing the limitations so as to better understand the context in which the findings can be profitably interpreted and built upon. There is an initial methodological question regarding the effect of conducting qualitative data collection from interviews with users about a system *after* the users interact with the system. In

the context of user research, there are noted questions about whether self-report data effectively captures users' experience of engagement, as this data is necessarily a recalled and cognitively processed recollection of a past events (O'Brien et al., 2020). Faced with this problem, other work attempts to ask users questions about what they are thinking, feeling, and experiencing as part of a user testing methodology during the users' interactions with the system. However, there is a methodological counterargument that suggests that this approach can be invasive and interrupt the attention and experience of users, leading to poorer data from which to explore aspects of user experience within a given system (Kelly, 2009). This is particularly worrisome in regard to research on engagement, as attention is an engagement factor. In future research, a more integrated user testing methodology could be used, though it would need to be designed in a way that takes the noted issue into account.

Another limitation of the methodology is the influence of pre-assigned tasks. This research asked users to follow pre-assigned tasks to ensure consistency across participants as part of the usability testing. This research also treated the experience users had through interacting with the platform in the context of a usability protocol as representative of their natural engagement with the system outside of such conditions. In practice the freedom to engage with a system without preassigned tasks may have been a more representative, if less reliable, method of user interaction. In future work, a methodology could attempt to account for this by leaving users to explore the system for a set period of time without restrictions before being interviewed and attempt to improve the reliability of the results through a deductive method of qualitative analysis.

Regarding the recruitment of participants, a limitation of the recruitment process was the observation of a potential self-selection bias. While this research sought to recruit participants through both a web portal and with the help of a polling firm, there were some potential self-

selection issues within the samples. Specifically, while we attempted to achieve a diversity in education and occupational backgrounds, six participants indicated they were either biomedical researchers or had experience recruiting participants using health-research focused portals. This is likely attributable to self-selection in the participant pools of REACHBC. Anecdotal information from participants indicates that some participants had joined the portal to contribute to medical research based on their understanding of the lack of participants in their own work. This is not a serious issue for the validity of the results of this research, as the novelty of the system under examination ensures that no users would have interacted with a technology of this kind, or a modality of this kind, before in the context of sharing genetic and other biomarker information. Regardless, this could have been better mitigated by working with a specific sampling frame from the beginning that filtered participants by their familiarity with biomedical research, rather than just by their familiarity with the Canadian healthcare system.

While a variety of steps were taken to ensure the validity of the qualitative analysis, an additional and final step to ensure validity and reliability would have been to ensure intercoder reliability of the qualitative results through the creation of a codebook. This step was deemed to be unnecessary for the goals of the current research, as the current methodology triangulates the findings sufficiently. However, this choice ultimately limits the extent to which the findings of this research can be generalized. While the findings here largely align with the existing literature on trust and engagement, we would be much more able to ascertain the validity of the findings if a future multi-case study was conducted with the same constructs. It remains to be seen how and if this work can be generalized to other health-related blockchain-based SSI systems, other blockchain systems, or omic information sharing platforms in general. Indeed, we simply do not know from this research whether or not the findings are generalizable as the sample size is not

statistically significant (as is often the case with the HCI field for usability studies). Additionally, the methodology is focused on exploring an under researched phenomenon in a novel system, rather than operationalizing existing constructs.

Finally, another limitation is the questionable ecological validity of the findings. It is unclear how valid these findings would be in a real-world context, given both the artificial context of the study and the guided interaction that users had through the usability testing. As such, a primary focus of future work would be to begin exploring the applicability of these findings in more naturalistic settings, such as clinical sites.

### **5.18 Future Work**

This research establishes nascent design principles and theorizes the interaction between two types of relationships (trust and engagement) that users have with technology. Specifically, with a novel type of blockchain-based SSI system implemented within the area of research focused on patient-facing health information technologies. Within the literature, this is an emerging area, with only one study directly related to this topic and few relevant studies in the same area at the time of writing.

Regarding the findings themselves, given both the sample size and exploratory nature of this research, future work could be confirmatory rather than exploratory. Future work could focus on expanding these initial findings and exploring the nuances of the relationship between user engagement and trust in this context. The work in this area could begin by building upon the findings with an eye to establishing the generalizability, ecological validity, and relevance of the design implications discussed here. As part of this work, a methodology could leave users to explore the system for a set period without restrictions before being interviewed to improve the

reliability of the results through a deductive method of qualitative analysis developed from the findings of this study.

Future work could be aimed at replicating the methodology as a multi-case study, exploring whether the findings hold in different examples of the same type of technology, with the goal of establishing the replicability and external validity of these initial findings. This work could be conducted with the goal of synthesizing coherent operational definitions of the constructs explored within this context, should the findings here be shown to be sufficiently generalizable and externally valid. Once validity and generalizability have been better established, subsequent scholarship could build towards the development of a thorough nomological network and the development of scale measurement tools (such as those developed by O'Brien et al. (2018)) to be able to thoroughly measure the construct of trust as related to the construct of engagement within the context of blockchain systems. Being able to reliably measure this construct in diverse blockchain-focused contexts would be of great use to future designers and theorists in this emerging space.

Regardless of the development of a scale, attempting to explore the relationship between trust and engagement in future work would be particularly helpful to build a vein of literature in the area of designing user experiences in blockchain-based systems, given that the majority of academic work in this area focuses solely on cryptocurrency wallet apps as a use case. Future work in this area would begin by exploring the specific relationships between perceived usability, reliability, and functionality within similar blockchain-based systems as these concepts seem intuitively to be related, despite coming from separate theoretical backgrounds.

Another avenue of exploration would be to conduct subsequent user research within iterations of the same system, exploring the effect of different iterative prototypes on users' trust.

Future work could take a more explicit design research or design science approach and explore the impact of these design principles in iterations of competing design artifacts with groups of users. Such a method could also take a co-designing or community-based design approach, and work with the same group of users to explore what aspects of the system can be refined to better assert the trustworthiness of the system within the minds of users. Specifically, the structure of how users learn about a new technology within the context of assessing its trustworthiness could be further explored through subsequent prototypes. A possible goal could be generating a taxonomy of relevant TSDE's (e.g., FAQ's) that help to enhance users' perception of the trustworthiness of systems and create a 'library' or nascent design system to guide the work of future designers in this space.

Initially then, there is a need to establish the validity and generalizability of this work in a larger context, as the findings here are exploratory. Once a more confirmatory approach has been taken, this work has the potential to be generative in many directions.

## **5.19 Contributions**

This research offers several contributions that while limited in scope are potentially relevant to multiple fields and endeavours. First and foremost, this work expands on the blockchain literature by conducting (to the authors knowledge) the second usability study with users of a blockchain platform and the first study on the relationship between trust and engagement in blockchain systems. Importantly, it is also one of two studies at the date of publication that explore the design of non-crypto focused blockchain systems, and focuses on the effect of the front-end design, rather than the effect of the solution architecture, on trust. This work also contributes a design focused study to literature on the design of self-sovereign identity systems. This work also creates

theoretical connections between the relationship of engagement and trust in between the theoretical framework of McKnight et al. (2011) and O'Brien et al. (2018), and is (to this authors knowledge) the first research to explore this intersection. In addition, this work expands the application of the UES-SF and the process model of user engagement to a new domain (blockchain systems) further demonstrating its generalizability. This work also contributes limited empirical support for emerging work by Lemieux, though further work is needed to validate Lemieux's (2022) work on trust and blockchain technology, as this research focuses only on one aspect of the model, namely user trust. This work also expands on McKnight et al.'s (2011) theory of trust in a specific technology, proposing a redefinition that is theoretically relevant for generating design implications, and adding conceptual clarity to this theoretical strand within the MIS literature. Finally, this work contributes to the small body of work on the design of blockchain systems, building on work by Sas & Khairruddin (2015), Voskoboynikov et al. (2020), Eskandari et al. (2018), and Zavolagina et al. (2020) and presents design implications to guide future work by researchers and designers.

## Chapter 6: Conclusion

This research contributes design implications and an initial theoretical exploration of the relationship between trust and user engagement to the emerging area of the study of blockchain systems. In so doing, it argues for the importance of the design of systems, specifically the front-end design of systems, to user's perceptions of the technologies they use. Unlike the vision of Bitcoin users outlined by Satoshi Nakamoto (2008), users of current consumer facing blockchain technologies, seeking to take advantage of the benefits of this social technology, are not experts. Many may have never heard of blockchain technology before, much less understand how it works in a way to be able to verify their transactions on the ledger. This means that for many users, the most important information that will guide their decision to trust, and ultimately to use, a blockchain system is conveyed through their experience of the front-end of that system. Designing for engagement, then, emerges within this work as one way to create positive user experiences that have the potential to influence the way users assess the trustworthiness of new blockchain systems. As we've seen through the COVID-19 pandemic, omic sciences have been instrumental in delivering valuable lifesaving vaccines at an unprecedented pace and helping to limit the ravages of the virus on a global scale. Given the potential social benefits of omic-focused blockchain technologies like MYPDx, the design of engaging systems represents an area where a better user experience may help lead to a better world.

## References

- Abedi, M (2019, December 19). LifeLabs hack: What Canadians need to know about the health data breach. Global News. <https://globalnews.ca/news/6311853/lifelabs-data-hack-what-to-know/>
- Aboueid, S., Liu, R. H., Desta, B. N., Chaurasia, A., & Ebrahim, S (2019). The Use of Artificially Intelligent Self-Diagnosing Digital Platforms by the General Public: Scoping Review. *JMIR Medical Informatics*, 7(2), e13445. <https://doi.org/10.2196/13445>
- Ahluwalia, P., Ahluwalia, M., Vaibhav, K., Mondal, A., Sahajpal, N., Islam, S., Fulzele, S., Kota, V., Dhandapani, K., Baban, B., Rojiani, A. M., & Kolhe, R. (2020). Infections of the lung: A predictive, preventive and personalized perspective through the lens of evolution, the emergence of SARS-CoV-2 and its pathogenesis. *EPMA Journal*, 11(4), 581–601. <https://doi.org/10.1007/s13167-020-00230-1>
- Allen, C. (2016, April 25). The Path to Self-Sovereign Identity. Retrieved November 20, 2020, from <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
- Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, 23(1), 4–17. <https://doi.org/10.1016/j.intcom.2010.07.003>
- Bencharit, S (2012). Progresses and challenges of omics studies and their impacts in personalized medicine. *Journal of Pharmacogenomics and Pharmacoproteomics*, 3(1), e105.
- Bothos, E., Magoutas, B., Arnaoutaki, K., & Mentzas, G (2019). Leveraging Blockchain for Open Mobility-as-a-Service Ecosystems. *IEEE/WIC/ACM International Conference on Web Intelligence - Companion Volume*, 292–296. <https://doi.org/10.1145/3358695.3361844>

- Boren, T., & Ramey, J. (2000). Thinking aloud: Reconciling theory and practice. *IEEE Transactions on Professional Communication*, 43(3), 261–278.  
<https://doi.org/10.1109/47.867942>
- Carroll, J. M., Mack, R. L., & Kellogg, W. A. (1988). Chapter 3—Interface Metaphors and User Interface Design. In M. Helander (Ed.), *Handbook of Human-Computer Interaction* (pp. 67–85). North-Holland. <https://doi.org/10.1016/B978-0-444-70536-5.50008-7>
- Clark, L. A., & Watson, D. (2016). Constructing validity: Basic issues in objective scale development. In A. E. Kazdin (Ed.), *Methodological issues and strategies in clinical research* (pp. 187–203). American Psychological Association. <https://doi.org/10.1037/14805-012>
- Clark, V. L. P., & Ivankova, N. V. (2016). *Mixed Methods Research: A Guide to the Field*. SAGE Publications, Inc. <https://doi.org/10.4135/9781483398341>
- Clemmensen, T. (2021). Socio-Technical HCI Design in a Wider Context. In T. Clemmensen (Ed.), *Human Work Interaction Design: A Platform for Theory and Action* (pp. 267–280). Springer International Publishing. [https://doi.org/10.1007/978-3-030-71796-4\\_10](https://doi.org/10.1007/978-3-030-71796-4_10)
- Davis, F. D (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- Deleuze, G., & Guattari, F. (1988). *A thousand plateaus: Capitalism and schizophrenia*. Bloomsbury Publishing.
- Doherty, K., & Doherty, G (2018). Engagement in HCI: Conception, Theory and Measurement. *ACM Computing Surveys*, 51(5), 99:1–99:39. <https://doi.org/10.1145/3234149>
- Dourish, P. (2006). Implications for design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 541–550. <https://doi.org/10.1145/1124772.1124855>

- Elsden, C., Manohar, A., Briggs, J., Harding, M., Speed, C., & Vines, J (2018). Making Sense of Blockchain Applications: A Typology for HCI. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1–14. <https://doi.org/10.1145/3173574.3174032>
- Fallman, D (2007). Why Research-Oriented Design Isn't Design-Oriented Research: On the Tensions Between Design and Research in an Implicit Design Discipline. Knowledge, Technology, & Policy; New York, 20(3), 193–200.  
<http://dx.doi.org.ezproxy.library.ubc.ca/10.1007/s12130-007-9022-8>
- Fallman, D (2011). The new good: Exploring the potential of philosophy of technology to contribute to human-computer interaction. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1051–1060.  
<https://doi.org/10.1145/1978942.1979099>
- Fan, M., Shi, S., & Truong, K. N. (2020). Practices and Challenges of Using Think-Aloud Protocols in Industry: An International Survey. Journal of Usability Studies, 15(2).
- Fogg, B. J., Soohoo, C., Danielson, D. R., Marable, L., Stanford, J., & Tauber, E. R. (2003). How do users evaluate the credibility of Web sites? A study with over 2,500 participants. Proceedings of the 2003 Conference on Designing for User Experiences, 1–15.  
<https://doi.org/10.1145/997078.997097>
- Gefen, Karahanna, & Straub. (2003). Trust and TAM in Online Shopping: An Integrated Model. MIS Quarterly, 27(1), 51. <https://doi.org/10.2307/30036519>
- Gefen, D., Benbasat, I., & Pavlou, P. A. (2008). A Research Agenda for Trust in Online Environments. Journal of Management Information Systems, 24(4), 275–286.

- Gefen, D., & Reich, B. (2014). Why trustworthiness in an IT vendor is important even after the vendor left: IT is accepting the message and not just the messenger that is important. *Omega*, 44, 111–125. <https://doi.org/10.1016/j.omega.2013.11.002>
- Gebresilassie, S. K., Rafferty, J., Morrow, P., Chen, L., Abu-Tair, M., & Cui, Z (2020). Distributed, Secure, Self-Sovereign Identity for IoT Devices. 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 1–6. <https://doi.org/10.1109/WF-IoT48130.2020.9221144>
- Government of Canada, S. C. (2017, October 25). Ethnic Origin Reference Guide, Census of Population, 2016. <https://www12.statcan.gc.ca/census-recensement/2016/ref/guides/008/98-500-x2016008-eng.cfm>
- Guarino, N., Guizzardi, G., & Mylopoulos, J. (2020). On the Philosophical Foundations of Conceptual Models. In J. Huiskonen, Y. Kiyoki, & A. Dahanayake (Eds.), *Information Modelling and Knowledge Bases* (pp. 1–14).
- Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. *IEEE Access*, 6, 11676–11686. <https://doi.org/10.1109/ACCESS.2018.2801266>
- Haraway, D. J., & Wolfe, C. (2016). *Manifestly Haraway*. University of Minnesota Press. <https://doi.org/10.5749/minnesota/9780816650477.001.0001>
- Hattie, J. (1985). Methodology Review: Assessing Unidimensionality of Tests and Items. *Applied Psychological Measurement*, 9(2), 139–164. <https://doi.org/10.1177/014662168500900204>
- Hazenhals, M (2011). User Experience and Experience Design. Retrieved December 17, 2020, from <https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/user-experience-and-experience-design>
- Hardin, R (2002). *Trust and trustworthiness*. Russell Sage Foundation

- Huang, S., Chaudhary, K., & Garmire, L. X. (2017). More Is Better: Recent Progress in Multi-Omics Data Integration Methods. *Frontiers in Genetics*, 8.  
<https://www.frontiersin.org/article/10.3389/fgene.2017.00084>
- Hoffmann, H., & Söllner, M (2014). Incorporating behavioral trust theory into system development for ubiquitous applications. *Personal and ubiquitous computing*, 18(1), 117-128.
- Houtan, B., Hafid, A. S., & Makrakis, D (2020). A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare. *IEEE Access*, 8, 90478–90494.  
<https://doi.org/10.1109/ACCESS.2020.2994090>
- InterPARES. 2017. InterPARES Trust Terminology Project: Key Blockchain Terms and Definitions (2017). <http://arstweb.clayton.edu/interlex/blockchain/>
- ISO DIS 9241-210:2019 (2019). Ergonomics of human system interaction – Part 210: Human-centered design for interactive systems. International Organization for Standardization (ISO), Switzerland
- Jin, X.-L., Zhang, M., Zhou, Z., & Yu, X (2019). Application of a Blockchain Platform to Manage and Secure Personal Genomic Data: A Case Study of LifeCODE.ai in China. *Journal of Medical Internet Research*, 21(9), e13587. <https://doi.org/10.2196/13587>
- Karahalil, B. (2016). Overview of systems biology and omics technologies. *Current medicinal chemistry*, 23(37), 4221-4230
- Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *Journal of medical systems*, 42(8), 156.

- Kelly, D. (2009). *Methods for Evaluating Interactive Information Retrieval Systems with Users*. Now Publishers Inc.
- Khairuddin, I. E., Sas, C., Clinch, S., & Davies, N. (2016). Exploring Motivations for Bitcoin Technology Usage. Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, 2872–2878. <https://doi.org/10.1145/2851581.2892500>
- Khairuddin, I. E., Sas, C., & Speed, C. (2019). BlocKit: A Physical Kit for Materializing and Designing for Blockchain Infrastructure. Proceedings of the 2019 on Designing Interactive Systems Conference, 1449–1462. <https://doi.org/10.1145/3322276.3322370>
- Lankton, N., McKnight, D. H., Tripp, J., & Baylor University. (2015). Technology, Humanness, and Trust: Rethinking Trust in Technology. Journal of the Association for Information Systems, 16(10), 880–918. <https://doi.org/10.17705/1jais.00411>
- Latour, B. (2012). We Have Never Been Modern. Harvard University Press.
- Lazar, J., Feng, J. H., & Hochheiser, H. (2017). Research Methods in Human-Computer Interaction. Morgan Kaufmann.
- Lemieux, V. L (2016). Trusting records: Is Blockchain technology the answer? Records Management Journal, 26(2), 110–139. <https://doi.org/10.1108/RMJ-12-2015-0042>
- Lemieux, V. L. (2017, November). Blockchain and distributed ledgers as trusted recordkeeping systems. In Future technologies conference (FTC) (Vol. 2017).
- Lemieux, V. L., & Feng, C. (2021). Conclusion: Theorizing from Multidisciplinary Perspectives on the Design of Blockchain and Distributed Ledger Systems (Part 2). In V. L. Lemieux & C. Feng (Eds.), Building Decentralized Trust: Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers (pp. 129–163). Springer International Publishing. [https://doi.org/10.1007/978-3-030-54414-0\\_7](https://doi.org/10.1007/978-3-030-54414-0_7)

Lemieux, V. L., Hofman, D., Hamouda, H., Batista, D., Kaur, R., Pan, W., Costanzo, I., Regier, D., Pollard, S., Weymann, D., & Fraser, R. (2021). Having Our “Omic” Cake and Eating It Too?: Evaluating User Response to Using Blockchain Technology for Private and Secure Health Data Management and Sharing. *Frontiers in Blockchain*, 3.

<https://www.frontiersin.org/article/10.3389/fbloc.2020.558705>

Lemieux, Victoria L. *Searching for Trust: Blockchain Technology in an Age of Disinformation*. Cambridge University Press, 2022.

LifeLabs. (2021, November, 20). Retrieved November 23, 2021, from

<https://www.lifelabs.com/about-us/about-lifelabs/?myProvince=on>

Lin, E., & Lane, H.-Y. (2017). Machine learning and systems genomics approaches for multi-omics data. *Biomarker Research*, 5(1), 2. <https://doi.org/10.1186/s40364-017-0082-y>

Linxen, S., Sturm, C., Brühlmann, F., Cassau, V., Opwis, K., & Reinecke, K. (2021). How WEIRD is CHI? In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1–14). Association for Computing Machinery.

<https://doi.org/10.1145/3411764.3445488>

Lu, R., Zhao, X., Li, J., Niu, P., Yang, B., Wu, H., Wang, W., Song, H., Huang, B., Zhu, N., Bi, Y., Ma, X., Zhan, F., Wang, L., Hu, T., Zhou, H., Hu, Z., Zhou, W., Zhao, L., Tan, W.

(2020). Genomic characterization and epidemiology of 2019 novel coronavirus: Implications for virus origins and receptor binding. *The Lancet*, 395(10224), 565–574.

[https://doi.org/10.1016/S0140-6736\(20\)30251-8](https://doi.org/10.1016/S0140-6736(20)30251-8)

Markham, S. K. (2013). The Impact of Front-End Innovation Activities on Product Performance. *Journal of Product Innovation Management*, 30(S1), 77–92.

<https://doi.org/10.1111/jpim.12065>

- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3), 709–734.  
<https://doi.org/10.2307/258792>
- McCarthy, J., & Wright, P. (2004). Technology as experience. *Interactions*, 11(5), 42–43.  
<https://doi.org/10.1145/1015530.1015549>
- Meeßen, S., Thielsch, M., & Hertel, G. (2019). Trust in Management Information Systems (MIS) A Theoretical Model. *Zeitschrift Für Arbeits- Und Organisationspsychologie*, 64, 6–16.  
<https://doi.org/10.1026/0932-4089/a000306>
- 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.  
<https://doi.org/10.1016/j.cosrev.2018.10.002>
- Muthuramalingam, P., Jeyasri, R., Valliammai, A., Selvaraj, A., Karthika, C., Gowrishankar, S., Pandian, S. K., Ramesh, M., & Chen, J.-T. (2020). Global multi-omics and systems pharmacological strategy unravel the multi-targeted therapeutic potential of natural bioactive molecules against COVID-19: An in silico approach. *Genomics*, 112(6), 4486–4504.  
<https://doi.org/10.1016/j.ygeno.2020.08.003>
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.
- Nielsen, J., & Molich, R. (1990). Heuristic evaluation of user interfaces. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 249–256.  
<https://doi.org/10.1145/97243.97281>
- Norman, D (2013). *The Design of Everyday Things: Revised and Expanded Edition*. Basic Books. <http://ebookcentral.proquest.com/lib/ubc/detail.action?docID=1167019>

Norman, D. A (1999). Affordance, conventions, and design. *Interactions*, 6(3), 38–43.

<https://doi.org/10.1145/301153.301168>

O'Brien, H. L., & Toms, E. G (2008). What is user engagement? A conceptual framework for defining user engagement with technology. *Journal of the American Society for Information Science and Technology*, 59(6), 938–955. <https://doi.org/10.1002/asi.20801>

O'Brien, H. L., & Toms, E. G (2010). The development and evaluation of a survey to measure user engagement. *Journal of the American Society for Information Science and Technology*, 61(1), 50–69. <https://doi.org/10.1002/asi.21229>

O'Brien, H. L., & Toms, E. G (2013). Examining the generalizability of the User Engagement Scale (UES) in exploratory search. *Information Processing & Management*, 49(5), 1092–1107. <https://doi.org/10.1016/j.ipm.2012.08.005>

O'Brien, H (2016a). Theoretical Perspectives on User Engagement. In H. O'Brien & P. Cairns (Eds.), *Why Engagement Matters: Cross-Disciplinary Perspectives of User Engagement in Digital Media* (pp. 1–26). Springer International Publishing. [https://doi.org/10.1007/978-3-319-27446-1\\_1](https://doi.org/10.1007/978-3-319-27446-1_1)

O'Brien, H (2016b). Translating Theory into Methodological Practice. In H. O'Brien & P. Cairns (Eds.), *Why Engagement Matters: Cross-Disciplinary Perspectives of User Engagement in Digital Media* (pp. 27 - 52). Springer International Publishing. [https://doi.org/10.1007/978-3-319-27446-1\\_1](https://doi.org/10.1007/978-3-319-27446-1_1)

O'Brien, H. L., Cairns, P., & Hall, M (2018). A practical approach to measuring user engagement with the refined user engagement scale (UES) and new UES short form. *International Journal of Human-Computer Studies*, 112, 28–39. <https://doi.org/10.1016/j.ijhcs.2018.01.004>

- O'Brien, H. L., Morton, E., Kampen, A., Barnes, S. J., & Michalak, E. E (2020). Beyond clicks and downloads: A call for a more comprehensive approach to measuring mobile-health app engagement. *BJPsych Open*, 6(5), e86. <https://doi.org/10.1192/bjo.2020.72>
- O'Donoghue, O., Vazirani, A. A., Brindley, D., & Meinert, E (2019). Design Choices and Trade-Offs in Health Care Blockchain Implementations: Systematic Review. *Journal of Medical Internet Research*, 21(5), e12426. <https://doi.org/10.2196/12426>
- Omersel, J., & Karas Kuželički, N. (2020). Vaccinomics and Adversomics in the Era of Precision Medicine: A Review Based on HBV, MMR, HPV, and COVID-19 Vaccines. *Journal of Clinical Medicine*, 9(11), 3561. <https://doi.org/10.3390/jcm9113561>
- Patten, M. L., & Newhart, M. (2017). *Understanding Research Methods: An Overview of the Essentials* (10th ed.). Routledge. <https://doi.org/10.4324/9781315213033>
- Quiñones, D., & Rusu, C (2017). How to develop usability heuristics: A systematic literature review. *Computer Standards & Interfaces*, 53, 89–122. <https://doi.org/10.1016/j.csi.2017.03.009>
- Rosenfeld, L., Arango, J., & Morville, P. (2015). *Information architecture for the world wide web*. O'Reilly.
- Sas, C., Whittaker, S., Dow, S., Forlizzi, J., & Zimmerman, J. (2014). Generating implications for design through design research. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1971–1980. <https://doi.org/10.1145/2556288.2557357>
- Sas, C., & Khairuddin, I. E. (2015). Exploring Trust in Bitcoin Technology: A Framework for HCI Research. *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*, 338–342. <https://doi.org/10.1145/2838739.2838821>

- Sas, C., & Khairuddin, I. E (2017). Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 6499–6510. <https://doi.org/10.1145/3025453.3025886>
- Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2016). Grand challenges for HCI researchers. *Interactions*, 23(5), 24–25. <https://doi.org/10.1145/2977645>
- Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, 8(2). <https://doi.org/10.3390/healthcare8020133>
- Shin, D., & Hwang, Y (2020). The effects of security and traceability of blockchain on digital affordance. *Online Information Review*, 44(4), 913–932. <https://doi.org/10.1108/OIR-01-2019-0013>
- Singh, R., Singh, P. K., Kumar, R., Kabir, Md. T., Kamal, M. A., Rauf, A., Albadrani, G. M., Sayed, A. A., Mousa, S. A., Abdel-Daim, M. M., & Uddin, Md. S. (2021). Multi-Omics Approach in the Identification of Potential Therapeutic Biomolecule for COVID-19. *Frontiers in Pharmacology*, 12, 1062. <https://doi.org/10.3389/fphar.2021.652335>
- Söllner, M., Hoffmann, A., Hoffmann, H., & Leimeister, J. M. (2012). How to use behavioral research insights on trust for HCI system design. CHI '12 Extended Abstracts on Human Factors in Computing Systems, 1703–1708. <https://doi.org/10.1145/2212776.2223696>
- Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A., & Leimeister, J. M. (2014). Understanding the Formation of Trust. In K. David, K. Geihs, J. M. Leimeister, A. Roßnagel, L. Schmidt, G. Stumme, & A. Wacker (Eds.), *Socio-technical Design of*

Ubiquitous Computing Systems (pp. 39–58). Springer International Publishing.

[https://doi.org/10.1007/978-3-319-05044-7\\_3](https://doi.org/10.1007/978-3-319-05044-7_3)

Söllner, M., Benbasat, I., Gefen, D., Leimeister, J. M., Pavlou, P. A. (2016a). Trust. In Ashley Bush and Arun Rai (Eds.), MIS Quarterly Research Curations.

<https://doi.org/10.25300/10312016>

Söllner, M., Hoffmann, A., & Leimeister, J. M (2016b). Why different trust relationships matter for information systems users. *European Journal of Information Systems*, 25(3), 274–287.

<https://doi.org/10.1057/ejis.2015.17>

Staa, T.-P. van, Goldacre, B., Buchan, I., & Smeeth, L. (2016). Big health data: The need to earn public trust. *BMJ*, 354, i3636. <https://doi.org/10.1136/bmj.i3636>

Swan, M (2015). *Blockchain: Blueprint for a new economy*. Sebastopol, CA: O'Reilly Media.

Tarkkanen, K., & Harkke, V. (2019). Scope of usability tests in IS development. *AIS Transactions on Human-Computer Interaction*, 11(3), 136-156.

Thielsch, M. T., Meeßen, S. M., & Hertel, G. (2018). Trust and distrust in information systems at the workplace. *PeerJ*, 6, e5483. <https://doi.org/10.7717/peerj.5483>

Tobin, A., Reed, D., Windley, F. P. J., & Foundation, S (2017). *The Inevitable Rise of Self-Sovereign Identity*. 24.

Von Bertalanffy, L. (1950). An outline of general system theory. *British Journal for the Philosophy of science*.

Voskoboynikov, A., Obada-Obieh, B., Huang, Y., & Beznosov, K. (2020). Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users. In J. Bonneau & N. Heninger (Eds.), *Financial Cryptography and Data Security*

(pp. 595–614). Springer International Publishing. [https://doi.org/10.1007/978-3-030-51280-4\\_32](https://doi.org/10.1007/978-3-030-51280-4_32)

Voskoboynikov, A., Wiese, O., Koushki, M. M., Roth, V., & Beznosov, K. (2021). The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. 22.

Vail, A. K., Boyer, K. E., Wiebe, E. N., & Lester, J. C. (2015). The Mars and Venus Effect: The Influence of User Gender on the Effectiveness of Adaptive Task Support. In F. Ricci, K. Bontcheva, O. Conlan, & S. Lawless (Eds.), *User Modeling, Adaptation and Personalization* (pp. 265–276). Springer International Publishing. [https://doi.org/10.1007/978-3-319-20267-9\\_22](https://doi.org/10.1007/978-3-319-20267-9_22)

Vailati-Riboni, M., Palombo, V., & Loor, J. J (2017). What Are Omics Sciences? Periparturient Diseases of Dairy Cows: A Systems Biology Approach, 1–7. Springer International Publishing. [https://doi.org/10.1007/978-3-319-43033-1\\_1](https://doi.org/10.1007/978-3-319-43033-1_1)

Van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N (2019). Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. ArXiv:1904.12816 [Cs]. <http://arxiv.org/abs/1904.12816>

Venkatesh, V., & Bala, H (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, 39(2), 273–315. <https://doi.org/10.1111/j.1540-5915.2008.00192.x>

Watson, C., & Kharrufa, A. (2021). HCI - H is also for Hazard: Using HAZOP to Identify Undesirable Consequences in Socio-Technical Systems. *ACM SIGCAS Conference on Computing and Sustainable Societies*, 230–242. <https://doi.org/10.1145/3460112.3471959>

- Webster, P (2020). Canadian digital health data breaches: Time for reform. *The Lancet Digital Health*, 2(3), e113–e114. [https://doi.org/10.1016/S2589-7500\(20\)30030-3](https://doi.org/10.1016/S2589-7500(20)30030-3)
- Wiebe, E., & Sharek, D. (2016). ELearning. In H. O'Brien & P. Cairns (Eds.), *Why Engagement Matters: Cross-Disciplinary Perspectives of User Engagement in Digital Media* (pp. 53–79). Springer International Publishing. [https://doi.org/10.1007/978-3-319-27446-1\\_3](https://doi.org/10.1007/978-3-319-27446-1_3)
- Westbrook, L., & Saperstein, A. (2015). New Categories Are Not Enough: Rethinking the Measurement of Sex and Gender in Social Surveys. *Gender & Society*, 29(4), 534–560. <https://doi.org/10.1177/0891243215584758>
- Winner, L (1980). Do Artifacts Have Politics? *Daedalus*, 109(1), 121–136. JSTOR.
- World Health Organization. (2020a). Laboratory testing strategy recommendations for COVID-19: Interim guidance (pp. 1–5). <https://www.who.int/publications-detail-redirect/laboratory-testing-strategy-recommendations-for-covid-19-interim-guidance>
- World Health Organization. (2020b). COVID-19 Strategic Preparedness and Response (SPRP) Monitoring and Evaluation Framework (pp. 1–33). <https://www.who.int/publications-detail-redirect/draft-operational-planning-guidance-for-un-country-teams>
- Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 8(2), 44
- Zavolokina, L., Zani, N., & Schwabe, G. (2020). Designing for Trust in Blockchain Platforms. *IEEE Transactions on Engineering Management*, 1–15. <https://doi.org/10.1109/TEM.2020.3015359>
- Zhang, P., White, J., Schmidt, D. C., & Lenz, G (2017). Applying software patterns to address interoperability in blockchain-based healthcare apps. arXiv preprint arXiv:1706.03700.

Zhang, S., & Lee, J.-H. (2019). Double-Spending With a Sybil Attack in the Bitcoin Decentralized Network. *IEEE Transactions on Industrial Informatics*, 15(10), 5715–5722.  
<https://doi.org/10.1109/TII.2019.2921566>

## Appendices

### Appendix A: Consent Form and Pre-Survey

*The below comprises the consent form and Pre-Survey administered to participants through ReachBC and Insights West, respectively.*

UBC School of Information  
470 – 1961 East Mall  
Vancouver, BC Canada V6T 1Z1  
Tel 604 822 2404

#### **PARTICIPANT INFORMATION AND CONSENT FORM**

**Title:** Blockchain-based Consent Management for Personalized Medicine

**Principal Investigator:** Dr. Victoria Lemieux, PhD, Associate Professor and Blockchain@UBC Cluster lead

**Principal Investigator Disclosure Statement:** In addition to her faculty position at UBC, the Principal Investigator also serves as Chief Information Security Officer at Molecular You.

**Co-investigator:** Hoda Hamouda  
Doctoral Student Faculty of Library, Archival and Information Studies, UBC

#### **Project Funding Partners:**

Molecular You (<https://molecularyou.com/>)  
StonePaper.io (<https://stonepaper.io/#/>)  
Canada's Digital Technology Supercluster (<https://www.digitalsupercluster.ca/>)  
Mitacs (<https://www.mitacs.ca/en> )  
Graduate students enrolled in UBC's blockchain graduate training pathway receive additional funding from an NSERC CREATE grant.

#### **Purpose**

The purpose of this study is to research new technologies used to manage users' health data. These interviews are part of a larger study examining the application of blockchain technology for the management of consent and use of health data. This larger study – of which these interviews form a part – examines the environmental, ethical, economic, legal, and social issues raised by the use of blockchain technology for the management of personal health data. The interviews will be used to discuss with clients of Molecular You their views on this new technology that could be used to manage personal health data. The aim is to open a discussion

that inform Molecular You about ways to improve its services and to make necessary changes to improve its offering to its clients.

### **Study Procedure**

Your involvement will entail answering a pre and a post online survey using the platform Qualtrics and a usability test session with an interview of 2.5 hours. We present to you about Molecular You online services and the way individuals could share their health data reports generated by Molecular You, then we will present to you a new technology that could be used to manage and share personal health data reports and ask you for develop some tasks such as setting up a dummy account, browsing research posts, trying the website filters.

We will use Zoom as the platform for the usability test session. During the task execution we will request you to share your screen. We recommend that you log in using only the nickname sent to you on the recruitment email. You can turn off your camera during the whole session. You can stop sharing your screen and you can mute your microphone when not needed.

Foreseen outcomes of this research include: further development of novel technologies, a report, a journal articles, a presentation and a master's thesis. It is possible that data of this study will be re-analyzed for another research.

### **Project Outcomes:**

#### **Confidentiality**

All data from participants will be kept confidential so that your identity is protected in all publications and presentations that result from this work. Data will be pseudonymized - able to be connected to you only through a secret code, kept in a locked cabinet accessible only to our researchers - until such time as the study is completed. After the study is complete, the secret code will be destroyed and your data will be anonymous. If you permit us to do so, the interview will be audio recorded and later transcribed in order to ensure the accuracy of the research. Audio recordings will be destroyed after transcription. If you do not prefer that the interview is recorded, then we will take written notes. Results of your participation in the interview will be reported without referring to your identity.

#### **Data Retention**

Participants will not be identified by name in any report. Identifiable data and audio recordings will be stored securely. All documents containing the results of the interview will be identified only by code number and kept in a secure data repository. Digital documents are going to be stored on password protected computers. Information you will provide to us will be stored in Canada.

### **Potential Risks**

We do not think that the questions could harm you. There is no physical risks associated with your participation.

You could choose to terminate the interview or survey at any time and you do not have to answer any questions or perform any tasks that make you feel uncomfortable. You could also withdraw from the interview at any time.

### **Potential Benefits**

Potential benefits of participating in this interview are becoming informed and gaining general knowledge about a new technology that is being used to keep, manage, and share health data.

### **Contact for information about the study:**

If you have any questions or desire further information with respect to this study, you may contact:

Principal Investigator: Dr. Victoria Lemieux, PhD  
Associate Professor and Blockchain@UBC Cluster lead

### **Contact for concerns or complaints about the study:**

If you have any concerns or complaints about your rights as a research participant, and/or your experiences while participating in this study, contact the Research Participant Complaint Line in the UBC Office of Research Ethics at 604-822-8598 or if long distance e-mail to [RSIL@ors.ubc.ca](mailto:RSIL@ors.ubc.ca) or call toll free 1-877-822-8598.

### **Consent:**

Your participation in this study is entirely voluntary and you may refuse to participate or withdraw from the study at any time.

Ethics Certificate Number: H18-02127-A008

## **Pre- Survey**

Please fill in the below fields, and rate your agreement or disagreement with the following statements about your experience of using MYPDx.

- Age

<b>20 - 34</b>	<b>35 - 44</b>	<b>45 – 54</b>	<b>55 - 64</b>	<b>65 – 74</b>
----------------	----------------	----------------	----------------	----------------

- Sex\*

<b>M</b>	<b>F</b>	<b>Other (Please Specify)</b>
----------	----------	-----------------------------------

*\* Sex at birth refers to sex assigned at birth. Sex at birth is typically assigned based on a person's reproductive system and other physical characteristics. Sex may or may not have any relationship to an individual's gender identity and gender expression.*

- Population Group
  - a. **First Nations**
  - b. **Metis**
  - c. **Inuit**
  - d. **White**
  - e. **South Asian (e.g., Indian, Pakistani, Sri Lankan, etc.)**
  - f. **Chinese**
  - g. **Black**
  - h. **Filipino**
  - i. **Latin American**
  - j. **Arab**
  - k. **Southeast Asian (e.g., Vietnamese, Cambodian, Laotian, Thai, etc.)**
  - l. **West Asian (e.g., Iranian, Afghani, etc.)**
  - m. **Korean**
  - n. **Japanese**
  - o. **Other – specify**

*\* Population groups, as representative of “race” or “Ethnicity” within the Canadian Census was treated as inclusive, whereby Participants were allowed to select multiple population groups to represent combinations of ethnic heritage if they felt it appropriate.*

- Please indicate your level of education completed
  - 1. **Some High School**
  - 2. **High School**
  - 3. **Trade School**

4. **Some college**
5. **Undergraduate Degree**
6. **Master's Degree**
7. **PhD**

- Do you have any Pre-existing Health Conditions? (Pre-existing: A medical illness or injury that you have had before. A pre-existing condition is typically one for which you have received treatment or diagnosis)

Y	N
---	---

- Occupation

- a. **Student**
- b. **Skilled manual worker**
- c. **Employed position in a service job**
- d. **Self-employed/freelancer**
- e. **Unemployed or temporarily not working**
- f. **Retired or unable to work through illness**
- g. **Employed professional**
- h. **Other**
- i. **Prefer not to answer**

- Please indicate your agreement with the following statements

- a. My typical approach is to trust new technologies until they prove to me that I shouldn't trust them.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

- b. I usually trust a technology until it gives me a reason not to trust it.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

c. I generally give a technology the benefit of the doubt when I first use it.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

d. I have heard about blockchain technology (True/False)

e. (IF/ELSE) I think about blockchain technology positively.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

f. (IF/ELSE) I think about blockchain technology negatively.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

g. I have heard about Self Sovereign Identity technology (True/False)

15. (IF/ELSE) I think about Self Sovereign Identity technology positively.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

16. (IF/ELSE) I think about Self Sovereign Identity technology negatively.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

- I have shared my personal health information with these digital health services. (Check all that apply.)
  - a. My E-Health
  - b. Telus Bablyon
  - c. 23andMe
  - d. Ancestry.com
  - e. Thrive COVID Self-assessment Tool
  - f. Other, Please Specify

## Appendix B: Usability Test Protocol

### Recruitment

#### PRE-STUDY QUESTIONNAIRE

To attain maximum variation, we could reply to participants asking about their age, sex, background. Demographics.

### Reminders/Discussion for the Team

(√) When aspects are not clear to users in regards to why steps are layed out in this (e.g. handshake) How much we will tell the client about it? How much we will tell them about it versus how much we would like them to conclude and infer why things are laid out this way?

( ) Study the Usability test essential background material

#### Pre-session steps

( ) Send the demographics questionnaire email to participants and the consent

(√) Third party transcription token

( ) Esatus

( ) Try Let's view ourselves

( ) enable multiple screen sharing

### INTRODUCTION/ CONSENT

Say: "Hi, we are Hoda Hamouda, Danielle Batista, Henry Kan, and Zakir Suleman, and we are researchers from the University of British Columbia. We are working on a research project to develop a solution called MYPDx, which is a platform for secure health data sharing.

Brief intro to purpose of study:

"We are currently trying to test the usability of the platform, and would like to investigate how users will interact with the interface. In this study, we will ask you to share your computer and mobile phone screens later to document your interaction with the given interface as we provide you with some tasks."

Ask for consent to participating and to the consent form we have sent to them.

"So if we have your consent, we will start the recording"

REMINDERS to PARTICIPANTS in the Client Role

#### Check that they have:

- Connect phone/pc to a charger
- Make sure the user knows how to share their screen. Ask them to share their screen.
- Have you downloaded LetsView?
- LetsView demo Video
- <https://letsview.com/ios-app>

- [https://play.google.com/store/apps/details?id=com.apowersoft.letsview&hl=en\\_US&gl=US](https://play.google.com/store/apps/details?id=com.apowersoft.letsview&hl=en_US&gl=US)
- Get LetsView running on your computer.
- Have you downloaded and setup your Esatus wallet? Make sure you know your PIN.
- Esatus
- <https://apps.apple.com/ca/app/esatus-wallet/id1496769057>
- <https://play.google.com/store/search?q=esatus%20wallet>
- Walk users through Changing network from Sovrin to **BCGov test ledger**:
- Click on the settings cog
- Scroll down to change ledger
- Change to BCGOV test ledger
- Navigate to the Esatus Wallet.
- 

### **ACTION: Introduction to the e.Platform**

MYHI, or Molecular You's Health Intelligence is an online personalized health service. It allows users to buy a test kit, and send the kit back to a partner lab for analysis. After the package is analysed, clients have access to their biomarker health reports, and see more about their results compared to the average person, and gain insights on their healthy biomarkers, or biomarkers that might signify a health problem. MYHI offers extensive overviews for a client's health data, which addresses how each of their biomarkers are important for things like diet and fitness, and what implications they have on health and disease. WeThe team at Molecular You have 've been working on a new platform related to MYHI called MYPDx, which enables users to securely store and control their genetic biomarker information, and share it to help advance important research while receiving rewards.

Link

All biomarkers

Through this usability walkthrough, we are trying to test the functionalities of some of the MYHI and MYPDx platforms, and test the fluidity of the interface as you (the user) are prompted with a

series of tasks. We hope to gain insights throughout the session as to what can be improved, changed, or added to MYHI and MYPDx.

### **Question:**

Is there anything we can clarify for you before we get started?

When you're interacting with MYHI and MYPDx, we're going to ask you to think aloud as you're working on the tasks we give you. This means that while you're working, you talk out loud about what you're seeing, what's interesting to you, and what you want to do or click on in the system. We'll show you a quick example of what we mean here:

We will show you a quick demonstration

**Question:** Check in again and ask if they have any follow up questions

### **ACTION: Move to their screens**

**PROMPT:** Navigate to MYHI (send link): [https://poc-MYHI.molecularyou.com/clients/sign\\_in](https://poc-MYHI.molecularyou.com/clients/sign_in)

**PROMPT:** Use the correct credentials to log in

We know you're looking at this for the first time, but let's pretend that you've already set up an account with MYHI, and sent a test kit back to their lab for analysis. After a few weeks you have received your Health report. As a current user, you would be asked to provide some information about yourself so that they can better analyze your data.

**PROMPT:** Check the **ABOUT ME tab**. And take a look at the information that a user would be asked to fill in.

While you do so, we would like to kindly remind you to think aloud meaning to verbalize your thoughts.

**PROMPT:** Check under Health Data you will see > **ALL BIOMARKERS**. Could you click it? Take your time exploring this page.

**QUESTION:** Could you tell me what do you think is displayed on this page under the biomarkers list on the left?"

If user got it right, confirm it.

If user did not get it, explain it "these is a list of biomarkers, similar to the one you would get on your lab results from let's say a blood work. ... "

Today you logged in and found a new service promoted to you on MYHI, it's called the **HEALTH WALLET**. The tab for it is at the top, can you click on it?

### **Usability session**

We will ask you to perform some tasks on the **Health Wallet**.

We want to remind you that this is a prototype, and we're really looking for the things that we can change and improve. Please let us know anything that isn't clear or confusing to you, that indicates something we need to change.

User Flow #1: MYHI then MYPDx then MYHI (to store biomarkers) then MYPDx

## Tasks / MYHI

### Task: Explore MY Health Wallet Home page

You'll notice at the top bar, there's a tab that says Health Wallet

**PROMPT:** Go to the Health Wallet

**Question:** Could you read the body text, and tell us what you understand about this service?

### Task: Sign up for the My Health Wallet

myh MY ID: HOME HEALTH DATA ACTION PLAN ORDER LEARN ABOUT ME HEALTH WALLET HELP

#### Download the Esatus Wallet

Your wallet is the place where all the verifiable credentials containing health data will be stored. Every time you choose to share your health data with a research partner you will use your verifiable credentials to present the data to them. Each verifiable credential corresponds to one of the 300+ genetic and dynamic biomarkers in your Molecular You Health Review and consists of: name of the biomarker, range, concentration, unit, and the date it was collected. No other personally identifiable information about you will be sent to a research partner and that is what makes the Personal Health Wallet a safe platform unique as a privacy-preserving and secure way for you to keep and share your health data.

Download on the App Store | Get it on Google play

#### Configure Network Settings

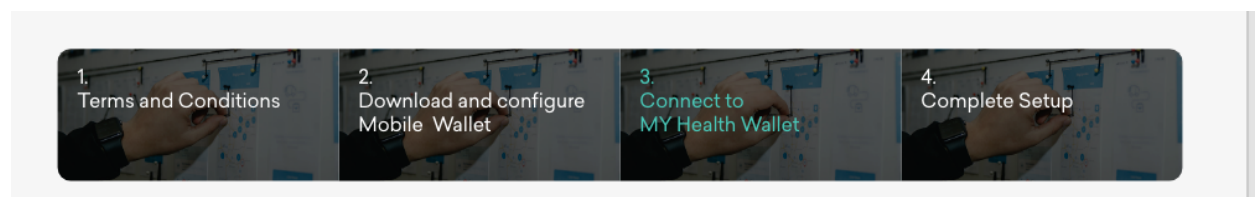
1. Open the MyPDx platform on your computer.
2. Download the Esatus wallet app on your mobile. (put the links to the compatible wallet apps).
3. Follow the app guidelines to set up your mobile wallet.
4. Prepare your network.
  - i. Open the settings menu on your wallet app.
  - ii. Change network from Sovrin to BCovrin Test

Next

[https://poc-myhi.molecularyou.com/health\\_wallets/connect\\_health\\_wallet](https://poc-myhi.molecularyou.com/health_wallets/connect_health_wallet)

[user have Downloaded the eSatus wallet page]

**REMINDER TO PARTICIPANTS:** As you move through the process to complete the task please remember to think out loud, verbalize your thoughts.



(reference screens: Flow 10)

[1. Terms and conditions] **Observe** if they'll read/ not the T&C

[2. Download the eSatus wallet] page

**Debugging questions (only if they are stuck):**

[Could you read the body text, and tell us what's unclear about it ?

Have you downloaded it? Do you recall the PIN?

Could you check your **network**?

If they've not, give them time to do so ]

Remind them to verbalize their thoughts.

### - [ 3. Connect to MY Health Wallet ] (reference screens)

Terms and conditions

Download and configure Mobile Wallet

Connect to MY Health Wallet

Complete Setup

Save and Continue Later Skip

Step 1

Open your **Esatus wallet app**

If you have not downloaded the app yet, please download it and follow the steps on this page.

Download on the App Store

GET IT ON Google play

If you are unable to connect, ensure your network settings are set up correctly.

Configure Network Settings

Open your Esatus mobile wallet

Prepare your network

Open the settings menu on your wallet app

Change network from Sovrin to BiCovinn Test

Next

Step 2

iii. Press **Connect** on your mobile wallet. [Learn more](#)

**Connect to Mobile Wallet**

This will create a secure connection between your mobile device, and MY Health Wallet.

**PROMPT:** Please read the text on the different steps starting from Step 2.

### **IF QR CODE DOESN'T WORK, ASK THEM TO MOVE BACK AND FORTH WITH CAMERA**

If the [learn more](#) or additional text contains the answer to a question they ask, read it to them or say: “We tried to clarify this here [point to them where the learn more is], could you let us know if it needs more clarification?”

[4. Setup Complete]

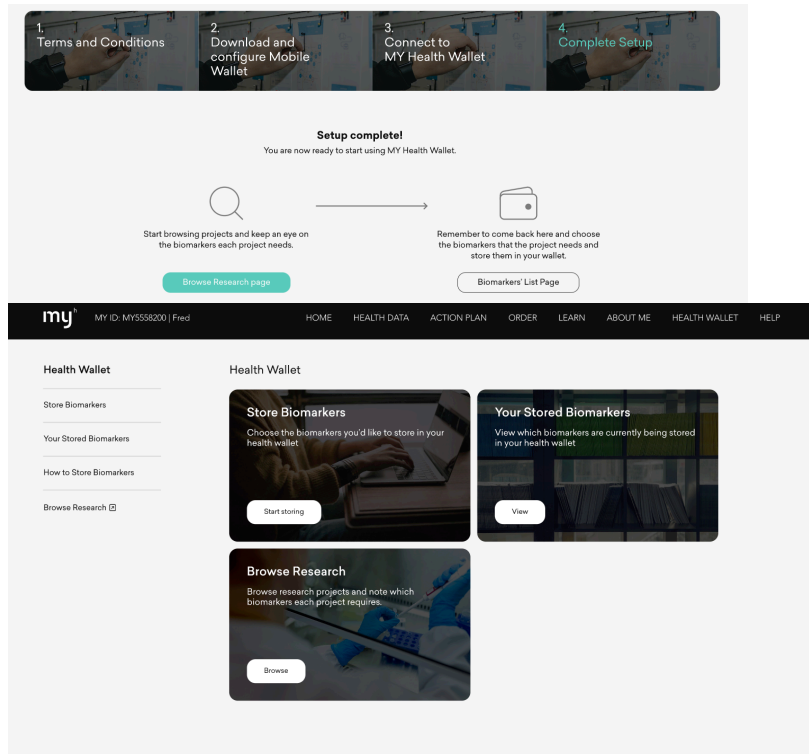
**Question: (If they have not made any comments, ask them):**

What questions might you have in mind about the steps you undertook?

**If not clear:** What’s unclear about it

**Question:** Where would you go at this point? [Browse Research Page or else]

**PROMPT:** Could you go back to the Health Wallet home screen?



### Task: Try to store **calcium** biomarker

[Store biomarkers]

Observe if they can follow the steps mentioned.

### Questions:

**What do you think about this page?**

**PROBE:** What do you think the relationship is between storing the biomarkers, and sharing them?

**PROBE:** What might be unclear about the process?

What questions might you have about this page?

**ACTION:** Ask participants to stay on this page for a moment.

### End of MYHI Questions:

**Question:** So far, what questions or comments do you have in mind in regards to the platform so far? As a reminder you've just:

Signed up for MYHI health wallet (through setting up a mobile agent))

Sent a biomarker credential to your mobile wallet (from MYHI)

Would you sign up for the MYHI health wallet? Y/ N.

**PROBE:** What encouraged you/ discouraged you? (KEEP THIS BRIEF)

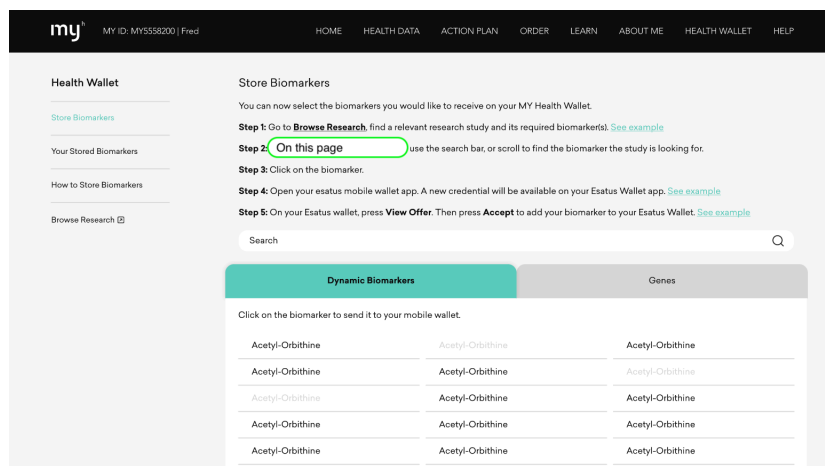
**BREAK:** So now that we've taken you through the MYHI platform, perhaps we can take a short 5 minute break before moving on.

## Tasks / MYPDx

### Question:

If I were to ask you to contribute your de-identified health data to a research project, how would you navigate to get there?

**PROMPT:** What would you click to get there?



**Reminder:** Act as you would normally act, if you are on this platform. Read the content of the pages that you'll visit, and verbalize your thoughts, as to what is unclear to you, where would you click to move from one page to the other, and why.

Login (possible)

At the browse page:

**PROMPT:** Take a quick skim through this page for a bit, and read the footer text about privacy.

We will come back to this page in a moment, let me just take you to the home page to get some background info about it.



**Start contributing your de-identified health data to research projects,  
to advance research, and earn rewards (if applicable)**

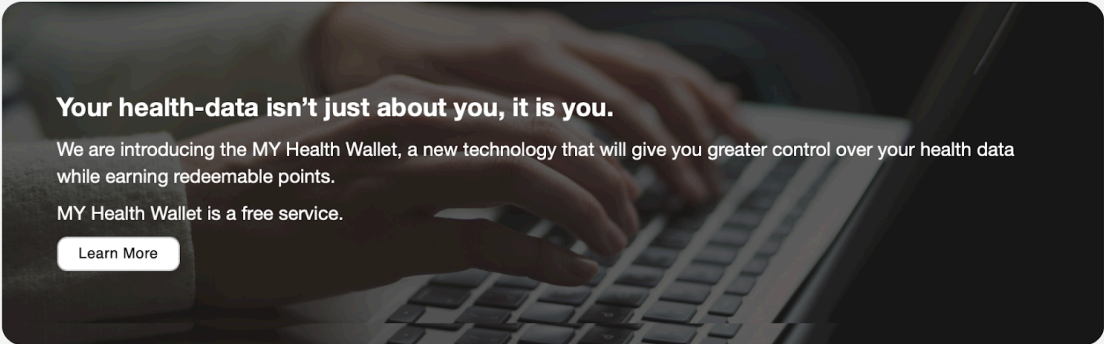
To check your eligibility for participating in a project, you'll need to first store the relevant biomarkers in your wallet. To get started, note the name of the specific biomarker(s) requested by the researchers in the project post below, then go to the [Store Biomarkers](#) page, and follow the steps.

Filter

**For example, you can track if a participant**

Conducted by: SPARC, March, 11, 2021	Reward : 100
You can search the exchange of data between you and a participant using the participants Unique ID. For example, you can	

MYPDx Home page






**Your health-data isn't just about you, it is you.**

We are introducing the MY Health Wallet, a new technology that will give you greater control over your health data while earning redeemable points.

MY Health Wallet is a free service.

[Learn More](#)

**Benefits of Activating your free MY Health Wallet**

 <p><b>Contribute to Research</b></p> <p>Advance important research by contributing your <u>de-identifiable health data</u> to research projects you are interested in.</p>	 <p><b>Earn Rewards (if applicable)</b></p> <p>You'll collect points when you choose to contribute your <u>de-identifiable health data</u> to research projects. Points are redeemable for rewards.</p>	 <p><b>Gain Higher Control</b></p> <p>If anyone tries to access your data you will get notified, and you will be the only one granting or revoking access to your de-identified health data.</p>
--	--	---

Task:

**PROMPT:** Could you explore the content of this page,

**Question:** what information might not be clear to you at this point ?

**FOLLOW UP:** So far, what pros and cons do you see to using this platform?

**If user expressed that something is not clear, and there is more info about it in other page they'll test:**

Inform them that's a good question, there is a page that elaborates a little more about this, when we get to it, I'll remind you of your question, and we'll look into whether or not it did not clarify this aspect.

**PROMPT:** We'd like to ask you to apply to a research project using this platform. Where would you go to do that?

**ACTION:** Have them stop on the Browse home page

**QUESTION:** From this page, can you explain how the process of applying works?

MyPDx | Client

Browse

Store Biomarkers

Handshakes


Filters

FAQ

Set Up


Logout

## How to use MY Wallet and collect rewards?




**1. Browse Projects**

Browse research projects and choose one that requires health data similar to yours.



**2. Connect to a Project**

Connect to the research project you chose. All your communication with the research project are protected to keep your identity safe & private.



**3. Virtual Handshake**

When you shake hands with the Research Project, using your wallet you agree to share your de-identifiable health data with the researchers and they agree to abide by ethical research principles. The process will end when you receive the reward in your wallet.

Remind Me Later

Browse Projects

### [Job board page]

**TASK:** Attempt to apply to one of the projects on this page and let us know which one you'll sign up with:

**MAKE SURE TO ASK PARTICIPANTS TO READ THROUGH THE PROJECT DETAILS.**

A. [Choosing a project]

- If user clicks on study that contains the biomarker in their wallet:

**Question:** Can I ask why you chose to participate in this study?

- Could you read the details of this research project? [Learn more/ click on the card]

- When they scan the posting we will mention:

**PROBE:** What do you think the Research verification section means?

If they get it right or wrong,

**ACTION:** Show them the REB certificate

“There is a preview available of the Research Verification [REB Self attested], in a real life situation would you be interested to see the verification that this project has? If yes, send them a link to REB PDF. “

**PROMPT:** “Could you try to apply to this research project? ”

B. [Checking their eligibility]

Note whether they have difficulty with this process.

**Question:** Do you have any questions at this point?

C. [Handshake]

**ACTION:** Stop participant on Handshake page.

**PROMPT:** Could you take a moment to look through all of the Header text?  
Check if they have questions about the header information.

**Question:** There are a number of steps, laid out on this page,  
Do you understand what you're being asked to do so far?

## For example, you can track if a participant

### Participate in this Research

Heads up! All the steps needed to participate in this research, will take place from now onwards on your Esatus mobile wallet, so keep an eye on it. This is the same wallet app you used to setup your MY Wallet

You must be wondering why so many steps are involved? That's because privacy and security is key for us. For this reason, we would like to inform you all along the way about which of your de-identified data will be securely shared with this research project and when. We provide you below with steps and visuals that explain what notification you can expect to see on your wallet app, what they mean, and where to click. Also the terms and conditions of the specific study you chose will be displayed below.

#### Step 1: Initiate the Handshake

**PROMPT:** please read through the information in the steps, and as you're going through each step, if there may be anything unclear at any point, please let us know. (Also, please remember to think aloud.)

## ONCE HANDSHAKE IS COMPLETE

### Question:

Do you have questions in mind in regards to the tasks you've just completed? Suggestions.

After 1:30 hour. (If we found out that they do not get to Flow 2, we will change the order so that ½ will test flow 1, and ½ will test flow 2.) SKIP IF PAST 1H45M into the session

**Flow #2: User is asked to Sign up for the second research project**, that does not require the biomarker in their wallets. The task ends when the user stores the correct biomarker and sees the first step in the handshake process.

**PROMPT:** Try to apply to the other project

**ACTION:** Note where in this process you have to intervene to give direction, and record how the participants are able to navigate on their own.

4:43



### Eligibility Proof request

<https://poc-mypdx.molecularyou.com:8046> is requesting the following information from you:

name	✗
concentration	✗

Please note our privacy policy (<https://esatus.com/dataprivacy>), especially chapter 2.2. By clicking 'Send' you confirm that the selected data will be transferred to <https://poc-mypdx.molecularyou.com:8046>.

Cancel

### If they see this error and are stuck:

**Question:** Why do you think you are not eligible for this study? (encourage them to try reasoning with themselves why that might be the case.)

**If they are still stuck:** Can you see any additional information on the screen that would be helpful? (“find out why”)

- If they are stuck after the “find out why”, lightly guide them.

When Directed to MYHI store biomarkers page: [Facilitator] [ User]

Observe if they recall/ know which biomarker to store? P1 [ ]

**PROMPT:** If [X] and they ask you, ask them “where do you think you could find this info?” P1 [ ]

**ACTION:** (If participants are lost)

**PROMPT:** Go to the project detail page on MYPDx and try to search for which biomarker the study needs. Did they find it P1 [ ]

**PROMPT:** If they could not find it, ask them to go back and read this info here.

To “Check your eligibility” for this project, you must have the **Glucose** biomarkers stored in your wallet. To store them, simply remember the name of these specific biomarker(s) displayed in the above table, then go to the [Store Biomarkers](#) page, and follow the steps.

> They will be taken to MYHI, Store Biomarkers Page

Observe is the user able to follow the steps on MYHI Store Biomarker page? P1 [ ]

Which step the user is stuck at? P1 [ ]

Did the user move back to MYPDx? P1 [ ]

Did they ask you for clarifications? P1 [ ]

The next steps the user should undertake on MYPDx:

> check their eligibility > Apply > Get to the Handshake page > Initiate the handshake.

Did the user recognize that the next step is to check their eligibility? P1 [ ]

### Paleolithic Diet and Exercise Study

Conducted by: University of California, San Francisco, Reward :  
March, 18, 2021

Because genetic evolutionary changes occur slowly in Homo sapiens, and because the traditional diet of Homo sapiens underwent dramatic changes within recent times, modern humans are better physiologically adapted to a diet similar to the one their hominid ancestors evolved on than to the diet typical of modern industrialized societies. The investigators developed a computational model to estimate the net acid load of diets from the nutrient composition of the diet's component ingredients, and suggest that the majority of these hominid diets yield a negative net acid load (that is, yield a net base load), in addition to being low in sodium chloride, high in potassium-containing fruits and vegetables, and low in saturated fats, with the majority of the non-animal-source calories coming from fruits and vegetables, not from acid-producing grains, separated fats and oils, starches and refined sugars. According to paleonutritionists, Homo sapiens' recent switch from their ancestral Paleolithic-type diet to the modern Western diet has contributed in a major way to so-called age-related diseases of civilization. The investigators hypothesize and will test whether: 1. consuming a high-potassium, low-sodium, net base-producing "Paleolithic-type" diet, even in the short term, has detectable beneficial effects on cardiovascular physiology, serum lipid profiles, insulin sensitivity, and exercise performance; and 2. their computational model predicts the measured negative net acid loads of a net base-producing "Paleolithic-type" diet, using steady-state values of renal net acid excretion as the measure of the diet net acid load (a.k.a., net endogenous acid production), which will be of value in constructing net-base producing diets for modern consumption. The long term complications of the combination of high blood pressure, high blood sugar and high fat and cholesterol levels, sometimes called the "metabolic syndrome", has been termed the number one medical problem in modern society today. If eating a "Paleolithic" diet helps improve these diseases, this would be the first step in both improving people's health as they get older as well as contributing to future national dietary guidelines for Americans.

Biomarker(s) needed: Glucose,

### Paleolithic Diet and Exercise Study

Research	Biomarkers	Range of Biomarkers	Reward
University of California	Glucose	4000 - 6000 $\mu$ m	

Please note your name, address, contact info, will **never** be shared with the study. All your data is de-identified

## Store Biomarkers

You can now select the biomarkers you would like to receive on your MY Health Wallet.

Step1: Go to **Browse Research**, find a relevant research study and its required biomarker(s). [See example](#)

Step2: On this page, use the search bar, or scroll to find the biomarker the study is looking for.

Step3: Click on the biomarker. [See example](#)

Step4: Open your esatus mobile wallet app. A new credential will be available on your Esatus wallet app. [See example](#)

Step5: On your Esatus wallet, press **View Offer**. Then press **Accept** to add your biomarker to your Esatus Wallet. [See example](#)

Q Search

Dynamic Biomarkers

Genes

Click on the biomarker to send it to your mobile wallet.

3-(3-hydroxyphenyl)-3-hydroxypropionic acid

Asymmetric dimethylarginine

Creatine

**The task ends when the user stores the correct biomarker and check their eligibility and sees the first step in the handshake process.**

SKIP IF PAST 1H45M in the session.

TASK: Setup your filters

TASK:

We will now ask you to visit the filter page.

**PROMPT:** Could you navigate to the filters and tell us:

Which ones are clear/ not?

And which one you are more likely to toggle?

Regarding the last filter, which option you'll

Please take a moment to read the information at the very bottom of the page, and don't (Note to the team there are two options that the user can't use on the filters page)

**Instruct NOT to save your options.**

[If the user saves it, guide them to how to clear their browsing history.]

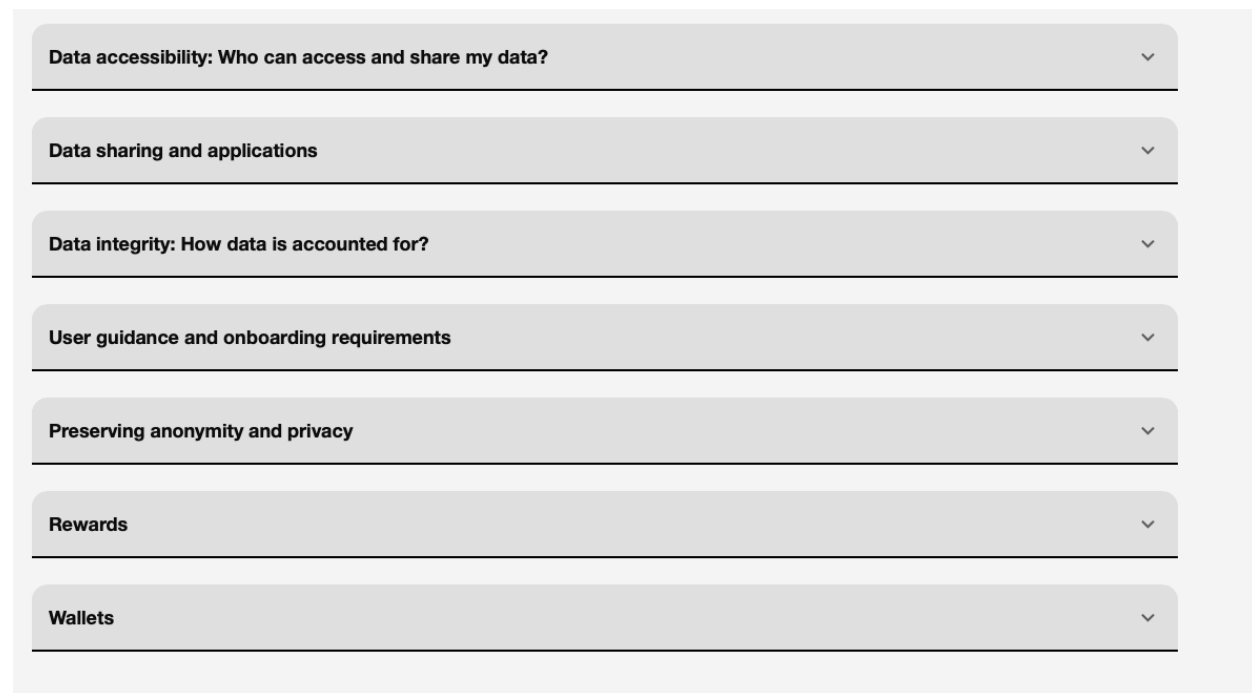
**TASK:** Explore the FAQ

**PROMPT:** Can you please navigate to the FAQ page? Can you explore this page and see if you can find answers to any of the questions you've had so far?

**QUESTION:** Which parts/categories of the FAQ were of interest to you?

**QUESTION:** Were you able to answer a question that you had about MYPDx from this page?

**QUESTION:** Was there information you looked for that you wished was there?



The image shows a screenshot of a FAQ page with seven expandable sections. Each section has a title and a downward-pointing chevron icon on the right. The sections are: 'Data accessibility: Who can access and share my data?', 'Data sharing and applications', 'Data integrity: How data is accounted for?', 'User guidance and onboarding requirements', 'Preserving anonymity and privacy', 'Rewards', and 'Wallets'. The sections are stacked vertically and separated by thin horizontal lines.

**Post Session Questions:**

**SEE INTERVIEW PROTOCOL**

Check if participants need a break after completing the survey, then move into context for discussion.

## **Context for further discussion**

You may be aware of advances in personalized medicine that allow medical researchers to use your genetic biomarkers, to give you personalized health recommendations. Genetic biomarkers are biological indicators that can be used to measure different states of your body, and can help give information about your current and future health. For example, there is a biomarker that gives researchers important information about your glucose levels, which can be really important for people who are diabetic.

There are many advances in medical science that rely on the sharing of individual health data. As an example, the current coronavirus vaccines were able to be developed quickly because of the

collaborative effort to share data about the virus. But there are also examples where hackers and other bad actors have tried to steal people's sensitive health information. For example, you might have heard about the LifeLabs hack that happened a couple of years ago where people's test results were exposed. That's why the team at Molecular You has been working on a new platform called MYPDx. MYPDx is a platform that provides for secure sharing of clients' health information for research and business purposes, while protecting the privacy and security of clients' personalized information and health data. The platform is built on blockchain technology, which is an immutable distributed database. The technology allows for users to choose which aspects of their health information they are willing to share with researchers, and control exactly what information researchers are able to see.

## **Final Questions**

How likely would you be to sign up for MYPDx?

How likely would you be to use MYHI?

**ACTION:** End Recording

## **REQUIREMENT\***

( ) A MYHI account (for the client)

( ) Process/ timeline for processing gift cards (for the client. researcher?)

## Appendix C: Interview Protocol

### Interview Protocol Questions

**Introduction:** We're going to go ahead and ask some questions about your experience now. You don't need to have the app or the platform up while we talk, but it might be useful as an aid. So to start with:

22. D  
Did you feel that MYPDx was trustworthy, or not trustworthy? (Open) *(reverse wording between interviews)*  
PROBE: For example, was the research being approved by an Ethics Board important?  
PROBE: Was approving each aspect of the information you were sharing important?

22. W  
What aspects of MYPDx made you feel more assured that the system was trustworthy? (Open)  
PROBE: Did you find the guidance and detailed instructions helpful?

22. W  
What aspects of MYPDx made you feel more assured that the system was not trustworthy? (Open)  
PROBE: Did you find the information to be overwhelming at any point?  
PROBE: Were you unclear on what the system was doing when you were including credentials?

**Prompt:** Thank you. We know it's been a long session; do you need to take a quick break? (Take a break as needed.) As a final step, we'd like you to fill out this survey about the system. You can find the link here: We'll turn off our microphones and video, but we'll be here if you have any questions.

(Once survey is completed) We want to thank you again for your time, and help improving this system. Someone from Insights West will be in touch with you shortly regarding the honorarium for this session, which you should be able to receive over email. This work is really important for us, and so we want to thank you for being willing to share your experience. Hopefully it will help us design another iteration of this system and enable users to have control over their health information.  
Thank you!

## Appendix D: Post Task Survey

Questions 1- 12 are 5-point Likert scale questions. This Survey was distributed to participants using Qualtrics Survey Software

Please rate your agreement or disagreement with the following statements about your experience of using MYPDx.

1. I lost myself in this experience.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

2. The time I spend using MYPDx just slipped away.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

3. I was absorbed in this experience.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

4. I felt frustrated while using MYPDx.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

5. MYPDx was attractive.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
------------------------------	-----------------	---	--------------	---------------------------

<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
6. MYPDx was aesthetically appealing.				
<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

7. MYPDx confusing to use.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

8. MYPDx was taxing.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

9. MYPDx appealed to my senses.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

10. Using MYPDx was worthwhile.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>		<b>4</b>	

3

5

11. My experience was rewarding.

**Strongly  
Disagree**

**Disagree**

**Neither  
Agree nor  
Disagree**

**Agree**

**Strongly  
Agree**

1

2

3

4

5

12. I felt interested in this experience.

**Strongly  
Disagree**

**Disagree**

**Neither  
Agree nor  
Disagree**

**Agree**

**Strongly  
Agree**

1

2

3

4

5

13. I would share my personal health information with MYPDx.

**Strongly  
Disagree**

**Disagree**

**Neither  
Agree nor  
Disagree**

**Agree**

**Strongly  
Agree**

1

2

3

4

5

14. I feel that MYPDx will ensure the privacy and security of my personal health information.

**Strongly  
Disagree**

**Disagree**

**Neither  
Agree nor  
Disagree**

**Agree**

**Strongly  
Agree**

1

2

3

4

5

15. I feel that MYPDx is a reliable platform.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

16. I felt MYPDx gave me the ability to do what I wanted to do.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

17. MYPDx gave me the features I need to share my personal health information securely.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

18. MYPDx supplies me with help when I need it

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

19. MYPDx provides competent guidance when I need it.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

20. When I interacted with MYPDx it reminded me most of \_\_\_\_\_ (Please indicate the type of system MYPDx most closely reminded you of.) (*OPEN*)

21. I am comfortable working with MYPDx, as an instance of the type of system I previously specified. *(Conditionally formatted to Q20)*

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

22. I am comfortable working with MYPDx, as an instance of the type of system I previously specified. *(Conditionally formatted to Q20)*

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

23. I feel very good about how things usually go when I use this type of system. *(Conditionally formatted to Q20)*

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

24. I felt okay using MYPDx because the research on the platform is approved by a Research Ethics Board.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

25. Clear communication about how I can exercise control over my health data makes it feel alright to use MYPDx.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

26. Knowing MYPDx is designed to preserve my privacy makes me feel safe using MYPDx.

<b>Strongly Disagree</b>	<b>Disagree</b>	<b>Neither Agree nor Disagree</b>	<b>Agree</b>	<b>Strongly Agree</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>