DESIGNING A RESPONSIBLE UNIVERSAL LEARNING AND EMPLOYMENT RECORD ECOSYSTEM

Youngjin Yoo, PhD
Faculty Director, xLab
Elizabeth M. and William C. Treuhaft Professor in Entrepreneurship
Professor of Information Systems, Department of Design & Innovation
The Weatherhead School of Management, Case Western Reserve University

Erman Ayday, PhD
Associate Professor of Computer Science
Case School of Engineering, Case Western Reserve University

Natalie Smolenski, PhD
Strategic Advisor
Hyland Software

This work was supported by Walmart. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of Walmart.

CASE WESTERN RESERVE UNIVERSITY EST. 1826

xLab RE-IMAGINING DIGITAL FUTURES FOR EVERYONE @ WEATHERHEAD SCHOOL OF MANAGEMENT

SUPPORTED BY Walmart

CONTENT

EXECUTIVE SUMMARY

In today's rapidly transforming economy, finding qualified employees with necessary skills and credentials has become a major challenge for many organizations. The Covid-19 pandemic has only exacerbated the labor shortage problem, putting pressure on organizations to upskill their existing workforces, while individuals are seeking non-traditional venues to gain new skills and training to secure high-paying jobs. However, a major hurdle in accomplishing these goals is the antiquated ways in which educational institutions and employers provide records for education, training, and employment. What is needed is a universal Learning and Employment Record (LER) ecosystem that is distributed, interoperable, and open, allowing individuals to collect, store, own, and share self-verifying credentials that are issued and accepted by participating organizations. This requires platforms to provide privacy protection, verifiability, data portability, and scalability at the same time.

Our Approach

To address this challenge, xLab at Case Western Reserve University (CWRU) conducted extensive research on the current credentialing ecosystem. We conducted a literature review and deep dive into the history of labor markets, decentralized technology, Web3, and digital data privacy and ownership. We then conducted 54 interviews with various stakeholders and technical experts, including employers, employees, policy makers, non-profit organizations, training organizations, and technology providers. Finally, we conducted a two-day design workshop at Case Western Reserve University on January 13-14, 2023. Together with 34 participants, we further dived into the specific needs of the market and brainstormed ideas for implementing a new system on a nationwide scale. We developed four specific use cases to validate the design concept of our responsible LER ecosystem.

Our report demonstrates how the LER ecosystem can enhance hiring processes, increase access to opportunities, and reduce inequality through the use case scenarios we developed. We discuss challenges, opportunities, and recommendations for realizing this vision, contributing to ongoing efforts to transform the labor market.

Historical and Technical Contexts of LER Ecosystems

We contextualize our findings in the historical evolution of Labor Market and Web Technologies. At the dawn of the industrialization, Labor Market 1.0 was characterized by the emergence of large corporations and the institutionalization of labor unions. With the introduction of computers in organizations, rapid globalizations, and the increasing sophistication of financial markets, Labor Market 2.0 led to the standardization of knowledge workers, hallowing of middle management, and weakening of labor unions. As we enter the era of Labor Market 3.0, the labor market is undergoing a profound transformation driven by digital technology, the rise of digital platforms, artificial intelligence (AI), and the emerging Web 3.0 technologies. This new era presents both opportunities and challenges, requiring concerted efforts from policymakers, businesses, and individuals to ensure that it is efficient, equitable, and fair. By learning from the experiences of past labor markets and prioritizing the development of technology infrastructure that empowers individuals, we can pave the way for a more inclusive and resilient Labor Market 3.0.

The report also reviews the historical development of the Web, focusing on Web 1.0, Web 2.0, and the emerging Web 3.0. Web 1.0 was characterized by the birth of the World Wide Web, while Web 2.0 saw the rise of large internet platform companies and a backlash against data abuse, known as the "techlash." The report also discusses the debate surrounding platform responsibility and the regulation of user-generated content on social media platforms. We discuss the development of decentralized public key infrastructure (DPKI) and decentralized identity (DID) in the Web 3.0 era, aiming to address challenges related to censorship, surveillance, and information asymmetry. DID technology is poised to reconcile the demands of privacy and verifiability in managing personal data, shaping the future of Web 3.0 and the LER ecosystem.

Privacy Matters in LER Ecosystems

This section provides a summary of stakeholder interviews conducted with individuals involved in the LER space, including educators, employers, policymakers, tech providers, and researchers. Privacy is crucial for individual autonomy and fostering trust in the LER ecosystem. Interviews with stakeholders involved in the LER space revealed areas where the LER community can establish the trust needed as concerns remain regarding the current demand for LERs and skills-based hiring, with concerns about the ability to falsify information on resumes using LER technology and the potential loss of revenue for higher education institutions if self-sovereign credentials become more prevalent.

There is a need for a repository of credentials and learning outcomes to clarify what each credential means, and stakeholders advocate for a standardized process for turning learning into skills. The value assigned to skills is crucial to consider when thinking about common languages and standards. Privacy and data ownership are emphasized as key ethical considerations, and equitable, learner-centric design is highlighted as important, with a need to consider use cases beyond the traditional college-educated learner and worker. Policymakers and nonprofit participants stress the importance of exploring what is needed to support learners who have been disconnected from the current system to adequately address equity and inclusion.

Toward a Responsible LER Ecosystem based on Extended Comprehensive Trust Model (ECTM)

This report outlines the extension of the core trust triangle in the verifiable credential model to accommodate new requirements for a responsible LER ecosystem that respects individuals' data ownership and privacy rights. The trust triangle consists of issuers, holders, and verifiers, and the proposed extension focuses on interoperability, decentralized data storage and control, self-sovereign and derivative verifiable credentials, revocation and control, heterogeneous data sources, and extended chain of trust.

To ensure a universal responsible LER ecosystem that is secure and trustworthy, we propose the Extended Comprehensive Trust Model (ECTM). ECTM is a decentralized identity ecosystem designed to enable privacy-preserving, secure, and interoperable sharing of verifiable credentials. The ECTM comprises ten components, including a Decentralized Data Agent, a Decentralized Data Storage, Chain of Trust, Off-Chain Data Sharing, Interoperability Layer, Data Ingestion and Integration Layer, Data Transformation and Analysis, Data Source Verification Mechanism, Endorsement Mechanism, and Selective Disclosure of Endorsement.

To ensure responsible LER ecosystems, the ECTM proposes a set of design patterns ranging from a basic decentralized storage and agent to an advanced trust mechanism with endorsement and verification. The design patterns emphasize the privacy preservation, enabling users to maintain control over their data and its usage, facilitating a more flexible and privacy-preserving environment.

A responsible LER ecosystem based on ECTM architecture follows Agent-Centric approaches to privacy-preserving data sharing. The agent-centric approach (as opposed to container-centric approach) is recommended since it provides persistent control over data sharing and its use on behalf of the user. The agent-centric approach allows for interoperable sharing protocols and expressive consent for verifiable credential sharing while providing legal protection for data sources.

Finally, we propose incorporating three layers of verifiability that verify the identity of communicating agents, the data being shared, and the sharing transactions themselves. The report outlines specific use case scenarios, requirements, and a concrete

architectural vision for the extended trust model that empowers users to maintain full control over their data.

In conclusion, our report proposes a solution to address the challenges associated with the current educational and employment credentialing systems. The Learning and Employment Record (LER) ecosystem offers a decentralized, interoperable, and open system for individuals to collect, store, own, and share self-verifying credentials that are issued and accepted by participating organizations. The proposed responsible LER ecosystem is designed to promote privacy, verifiability, data portability, and scalability. By learning from past labor market experiences and prioritizing the development of technology infrastructure that empowers individuals, we can pave the way for a more inclusive and resilient Labor Market 3.0.

INTRODUCTION

The labor market is an engine of any economy and a nexus of society, connecting labor and capital; educational institutions and businesses; and human capital and machines. It is a place where individuals can earn income, develop their careers, and achieve their life goals. As the labor market continues to evolve in the face of rapid technological changes, it faces new challenges and opportunities, including addressing equity, diversity, and inclusion. The current labor market primarily relies on traditional credentials issued by formal education institutions and corporates. As a result, the market inadvertently promotes superficial measures of competence and perpetuates systemic biases, which disproportionately affect underrepresented groups. This approach overlooks the diverse range of specific skills and competencies that individuals possess, which are often more indicative of job performance and adaptability. Furthermore, by disproportionately valuing traditional educational and career milestones, the market marginalizes those who have acquired expertise through alternative pathways or face systemic barriers due to their gender, age, or race. As a consequence, the labor market fails to optimally allocate human resources, squandering talent and undermining economic productivity. This report aims to provide design principles and a vision for a responsible universal Learning and Employment Record (LER) ecosystem, leveraging emerging Web3 technologies, with the ultimate goal of transforming the labor market to make it more efficient and equitable.

The labor market refers to where workers and employers meet to exchange labor for wages, determining the price and quantity of labor demanded and supplied. A well-functioning labor market is essential for allocating the workforce efficiently, effectively, and equitably, enabling firms to hire skilled workers at the right price and providing workers with income to meet their needs and improve their living standards. However, the labor market has faced historical challenges and transformations, from ancient slavery and serfdom to the modern wage labor system. Today, the post-Covid, AI-infused, and de-globalized economy poses new challenges, including labor shortages, skills mismatches, and the need for greater equity, diversity, and inclusion.

Skill-based hiring practices have been proposed as a solution to these challenges, offering a better match between job requirements and candidate qualifications. However, conventional approaches to skill-based hiring face limitations, such as difficulty assessing candidates' skills and susceptibility to fraud. The emergence of Web3 decentralized technology offers new possibilities for designing an LER ecosystem that addresses some of these challenges.

In this context, xLab at Case Western Reserve University has conducted extensive research on data privacy and ownership in the context of emerging Web3 decentralized technology that underpins the emerging decentralized, verifiable LER ecosystems. Our aim is to develop design principles and a vision for a responsible universal LER ecosystem that respects individuals' rights to data privacy and ownership while considering other important design principles such as interoperability, scalability, and verifiability.

This report is organized as follows: First, we review the evolution of the labor market and the history of privacy and ownership debate in digital ecosystems. Next, we summarize our interviews with LER ecosystem stakeholders, examining their roles and interests. We then examine emerging technology standards and propose architectural and algorithmic approaches to realizing our vision of a responsible universal LER ecosystem. Through four use case scenarios, we demonstrate the potential efficiency, effectiveness, and equity of our proposed system in creating, generating, curating, storing, sharing, and verifying an individual's education and work history. Finally, we conclude with a discussion of challenges, opportunities, and recommendations.

By providing a comprehensive vision for a responsible universal LER ecosystem, this report contributes to ongoing efforts to transform the labor market, enhancing efficiency in the hiring process, increasing access to education and career opportunities, and reducing inequality.

EVOLUTION OF THE LABOR MARKET

Labor Market 1.0

The Industrial Revolution marked a turning point in human history, as it brought about a radical increase in productivity and transformed the nature of work. Prior to industrialization, economic activities were predominantly based on agriculture and small-scale artisanal production. However, the introduction of large-scale machines, new production techniques, and innovative transportation methods led to the rise of factories and the mass production of goods. This era, which we term Labor Market 1.0, was characterized by the emergence of large corporations, the institutionalization of labor unions, and a significant shift in the workforce.

One of the key aspects of Labor Market 1.0 was the industrialization of factories. As steam engines and mechanized production methods were adopted, traditional craftspeople and artisans found themselves displaced by new machines that could produce goods faster, more efficiently, and at a lower cost. This transition to mechanized production resulted in a shift from small-scale, decentralized workshops to large, centralized factories. Workers were now required to perform repetitive tasks on assembly lines, leading to a fundamental change in the nature of work and the skills needed for employment.

Scholars argue that the introduction of steam power, along with other key innovations such as the spinning jenny and the power loom, led to a rapid increase in productivity and economic growth during the Industrial Revolution[1] [2]. These advances allowed for the mass production of goods, which in turn increased the demand for labor in factories.

As workers moved from small-scale artisanal production to employment in large factories, the nature of work became increasingly standardized and impersonal. Workers were treated as interchangeable components within the machinery of the vertically integrated corporation, and their jobs often provided lifetime employment contracts. This led to the institutionalization of labor unions, as workers sought to protect their rights and improve working conditions.

The rise of large corporations during Labor Market 1.0 is well-documented by Alfred Chandler in his seminal work "The Visible Hand."[3] Chandler explains that the adoption of mechanized production methods and the creation of factory systems necessitated new organizational structures and management practices. As a result, large corporations emerged, characterized by vertical integration, centralized decision-making, and hierarchical management structures. These corporations were able to harness the power of economies of scale and scope to dominate their respective industries and shape the labor market.

1 Rosenberg, Nathan and Manuel Trajtenberg. "A General Purpose Technology at Work: The Corliss Steam Engine in the late 19th Century US." The Journal of Economic History 64, 1 (March 2004): 61-99.

2 Atack, Jeremy, Fred Bateman, and Robert Margo. "Steam Power, Establishment Size, and Labor Productivity Growth in Nineteenth Century American Manufacturing." Explorations in Economic History 45, 2 (April 2008): 185-98.

3 Chandler, A. D. 1977. The Visible Hand: The Managerial Revolution in American Business. Boston, MA: Harvard University Press.

Labor unions played a crucial role in shaping the labor market during this period. They provided a collective voice for workers, enabling them to negotiate better wages, working hours, and job security. The rise of labor unions also led to the establishment of labor laws and regulations, which further influenced the development of the labor market. The growth of unions was closely tied to the expansion of large corporations and the increasingly standardized nature of work in factories.

Labor Market 2.0

The second half of the 20th century saw the rise of computerization and automation, leading to another significant shift in the labor market. This era, known as Labor Market 2.0, was characterized by the introduction of computers, the development of global supply chains, the increasing sophistication of financial markets, and the emergence of a new class of professional management. The defining technology of this era was the "smart machine," as coined by Zuboff[4], which played a pivotal role in driving the changes in the labor market.

One of the defining features of Labor Market 2.0 was the introduction of computers, which began with mainframes and later evolved into personal computers. These technological advancements allowed for more efficient processing of data and information, leading to a radical increase in productivity. The work of Erik Brynjolfsson and his colleagues has documented the significant impact of these innovations on the economy, demonstrating that the adoption of information technology (IT) led to substantial productivity gains in various industries[5] [6]. These advances enabled organizations to streamline their operations, optimize their resource allocation, and capitalize on new opportunities in the increasingly interconnected and globalized business environment[7] [8].

As personal computers became more commonplace, they were increasingly interconnected through local area networks and eventually the global internet. This connectivity facilitated new ways of organizing work and collaboration, transforming the way businesses operated. The internet made it possible for firms to communicate and coordinate with one another at a much lower cost[9], enabling the development of complex global supply chain ecosystems. Companies such as Nike, Dell, and Cisco led the way in becoming globally networked firms, leveraging the digital infrastructure to locate their resources where it made the most economic sense[10] [11].

The emergence of global supply chains was closely tied to the process of globalization and modularization[12]. As firms sought to capitalize on the comparative advantages of different regions, they began to outsource parts of their operations across the globe. This strategy allowed businesses to reduce costs, access new markets, and tap into specialized knowledge and expertise. The formation of these global supply chains was supported by large-scale digital infrastructure, which facilitated the seamless flow of information and resources across borders.

During Labor Market 2.0, the financial markets also underwent significant changes, becoming more sophisticated and interconnected. The rise of professional management classes, including MBAs and consultants, played a crucial role in shaping the labor market during this period[13]. These highly skilled individuals brought specialized knowledge and expertise to organizations, helping them navigate the increasingly complex business landscape. This new class of highly mobile knowledge workers included consultants, lawyers, accountants, and technical experts in various fields. Their career trajectories often diverged from those of traditional employees, as they did not typically remain with a single company for an extended period.

4 Zuboff, S. 1988. In the Age of the Smart Machine: The Future of Work and Power. New York: Basic Books.

5 Hitt, L. M., and Brynjolfsson, E. 1996. "Productivity, Business Profitability, and Consumer Surplus: Three Different Measures of Information Technology Value," MIS Quarterly (20), pp. 121-142.

6 Aral, S., Brynjolfsson, E., Van Alstyne, M., and Alstyne, M. V. 2012. "Information, Technology, and Information Worker Productivity," Information Systems Research (23), pp. 849-867.

7 Sambamurthy, V., and Zmud, R. W. 2000. "Research Commentary: The Organizing Logic for an Enterprise's It Activities in the Digital Era--a Prognosis of Practice and a Call for Research," Information Systems Research (11:2), pp. 105-105.

8 Wheeler, B. C. 2003. "Nebic: A Dynamic Capabilities Theory for Assessing Net-Enablement," Information Systems Research (13), pp. 125-146.

9 Malone, T. W., Yates, J., and Benjamin, R. I. 1987. "Electronic Markets and Electronic Hierarchies: Effects of Information Technology on Market Structure and Corporate Strategies," Communications of the ACM (30), pp. 484-497.

10 Porter, M. E., and Millar, V. E. 1985. "How Information Gives You Competitive Advantage," Harvard Business Review (64), pp. 149-160.

11 Jarvenpaa, S. L., and Ives, B. 1994. "The Global Network Organization of the Future," Journal of Management Information Systems (10), pp. 25-57.

12 Baldwin, C. Y., and Clark, K. B. 1997. "Managing in the Age of Modularity," Harvard Business Review (75:5), pp. 84-93.

13 Drucker, P. F. 1988. "Coming of New Organizations," Harvard Business Review), pp. 45-53.

The widespread adoption of computers and automation had a profound impact on the demand for different types of labor[14]. Many low-skilled jobs were automated, leading to a decrease in demand for manual labor. At the same time, the need for skilled knowledge workers increased, as they were better equipped to leverage the capabilities of new technologies. This shift in demand contributed to the "hollowing" of the middle class and a decline in the influence of labor unions[15] [16]. As many firms outsourced their manufacturing operations and consolidated back-office functions, traditional middle-class jobs were replaced by more specialized roles.

In contrast to Labor Market 1.0, where labor work was standardized, Labor Market 2.0 saw the standardization of middle management work. This standardization allowed organizations to streamline their decision-making processes and improve their efficiency. New organizational structures and management practices emerged, enabling firms to respond more effectively to the rapidly changing business environment and better align their resources with their strategic objectives.

The demand for low-skilled manual labor decreased while the need for highly skilled knowledge workers grew. This shift contributed to the hollowing of the middle class and the weakening of labor unions. Additionally, the widespread adoption of computers and automation facilitated the rise of new organizational structures and management practices, enabling firms to respond more effectively to the rapidly changing business environment.

As the labor market continued to evolve, the transition from Labor Market 2.0 to subsequent phases required workers to adapt to new roles, skills, and technologies. The increasing interconnectivity and globalization of the economy, combined with the rapid advancements in technology, would continue to shape the landscape of work in ways that have far-reaching implications for individuals, organizations, and society as a whole. The lessons learned from the rise and development of Labor Market 2.0 would inform the approaches taken to address the challenges and opportunities presented by the next era of the labor market.

[14] Seo, H. J., Lee, Y. S., Hur, J. J., & Kim, J. K. (2012). The impact of information and communication technology on skilled labor and organization types. Information systems frontiers, 14, 445-455.
[15] Langley, P., and Leyshon, A. 2017. "Platform Capitalism: The Intermediation and Capitalization of Digital Economic Circulation," Finance and Society (3:1), pp. 11–31. (https://doi.org/10.2218/finsoc.v3i1.1936).
[16] Rahman, K. S., and Thelen, K. 2019. "The Rise of the Platform Business Model and the Transformation of Twenty-First-Century Capitalism," Politics & Society (47:2), pp. 177–204. (https://doi.org/10.1177/0032329219838932).

Labor Market 3.0

As we enter the era of Labor Market 3.0, the labor market is undergoing a profound transformation driven by digital technology, the rise of digital platforms, artificial intelligence (AI), and the emerging Web 3.0 technologies. In this new labor market, "generative machines" are introduced, which differ from previous generations' smart machines. These generative machines constantly learn, adapt, and have a degree of autonomy, marking a significant departure from the smart machines of the past. Additionally, demographic shifts, such as the influx of new generations and the retirement of baby boomers, as well as the impact of the COVID-19 pandemic, further contribute to the changes we are witnessing. This section will explore the key features and implications of Labor Market 3.0, aiming to provide a comprehensive analysis of this new era.

The growing presence of Millennials and Gen Z in the workforce is transforming the labor market landscape, with many individuals choosing or being forced to pursue careers outside of traditional organizations[17]. Labor Market 3.0 is characterized by increased automation and algorithmic management, an emphasis on skills, and a more fluid, decentralized workforce.

One of the main features of Labor Market 3.0 is the increasing automation of tasks previously performed by human workers. With the rapid development of AI and robotics, machines are now capable of performing cognitive and highly complex physical tasks, impacting not only low-skilled factory workers but also white-collar jobs[18] [19]. Furthermore, human workers are increasingly managed by algorithms, with AI integrated into standard work processes, constantly sensing and responding to changing environments and worker performance[20]. Thistrend is expected to continue, with the rise of organic machines that learn, adapt, and possess autonomy.

Another key feature of Labor Market 3.0 is the increasing importance of skills. In an era of automation, it is no longer sufficient for workers to possess degrees or specific backgrounds. Instead, they must demonstrate the skills and knowledge required for their tasks[21]. This shift necessitates continuous investment in education and training, as well as the provision of skill development opportunities by employers. Organizations are increasingly dropping education requirements in favor of verifiable skills, and there is growing interest in using AI for algorithmic hiring.

Labor Market 3.0 is also characterized by a more fluid, decentralized workforce. The rise of the gig economy and remote work has led many workers to opt for project-based work instead of traditional employment[22]. This trend is likely to continue as technological advances make it easier for workers to connect with employers and clients worldwide.

In contrast to the standardized labor work in Labor Market 1.0, middle management work has begun to be standardized in Labor Market 3.0. This shift highlights the need for adaptability and constant learning among workers to stay relevant in the ever-evolving labor market landscape.

As we navigate Labor Market 3.0, it is essential to consider how it will impact our lives. Will it be more efficient, effective, equitable, and fair? Will it offer greater opportunities for individuals to pursue their dreams and realize their full potential? Or will it subject human workers to increased monitoring and control by algorithms, eroding our dignity and agency?

A key lesson from the Web 2.0 era is the importance of owning and controlling our data and identity[23] [24] [25]. As we prepare for Labor Market 3.0, we must prioritize the development of technology infrastructure and architecture that allows individuals to own and

[17] https://www.businessinsider.com/gen-z-winning-great-resignation-changing-job-market-2022-6?r=US&IR=T
[18] Faraj, S., Pachidi, S., and Sayegh, K. 2018. "Working and Organizing in the Age of the Learning Algorithm," Information and Organization (28), pp. 62-70.
[19] Brynjolfsson, E., and McAfee, A. 2014. "The Second Machine Age," W. W. Norton & Company.
[20] Stark, D., and Pais, I. 2020. "Algorithmic Management in the Platform Economy," Sociologica (14:3), pp. 47-72.
[21] Lawler, E., & Ledford, G. (1992). A skill-based approach to human resource management. European Management Journal, 10(4), 383-391.
[22] Vallas, S., & Schor, J. B. (2020). What do platforms do? Understanding the gig economy. Annual Review of Sociology, 46, 273-294.
[23] Flyverbom, M. 2022. "Overlit: Digital Architectures of Visibility," Organization Theory (3:3), p. 26317877221090310. (https://doi.org/10.1177/26317877221090314).
[24] Gregory, R. W., Henfridsson, O., Kaganer, E., and Kyriakou, H. 2022. "Data Network Effects: Key Conditions, Shared Data, and the Data Value Duality," Academy of Management Review (47:1), pp. 189–192. (https://doi.org/10.5465/amr.2021.0111).
[25] Power, M. 2022. "Theorizing the Economy of Traces: From Audit Society to Surveillance Capitalism," Organization Theory (3:3), p. 26317877211052296. (https://doi.org/10.1177/26317877211052296).

control their learning and employment records[26]. This decentralized approach empowers workers to leverage the best models available to express their skills and competencies to prospective employers or clients.

Imagine a high school dropout who has been writing code for years with multiple GitHub repositories, using the trace data from GitHub to create verifiable credentials on programming skills and software engineering. Or consider an Uber driver with positive comments and ratings from customers, leveraging this information to create verifiable credentials for emotional intelligence and excellent customer service skills. Such a decentralized and verifiable data infrastructure would significantly reduce friction in the labor market, making it more efficient and responsive to the needs of both workers and employers.

However, the shift to Labor Market 3.0 is not without challenges. The rapid pace of change can lead to increased inequality, as those who are unable to keep up with the demands of the new labor market may be left behind. Furthermore, the increasing reliance on algorithms for management and decision-making raises concerns about fairness, bias, and the potential loss of human agency[27] [28].

To ensure that Labor Market 3.0 is both efficient and equitable, policymakers, businesses, and individuals must work together to address these challenges. This may involve investing in education and training programs to help workers develop the skills necessary for the new labor market, as well as implementing policies to ensure that algorithmic decision-making is transparent and fair.

As the COVID-19 pandemic demonstrated, the labor market is more vulnerable to external shocks than ever before. In the face of such uncertainty, it is crucial to build a resilient labor market that can adapt to change and provide opportunities for all workers.

In conclusion, Labor Market 3.0 is characterized by the rise of organic machines, increased automation and algorithmic management, a growing emphasis on skills, and a more fluid, decentralized workforce. This new era presents both opportunities and challenges, requiring concerted efforts from policymakers, businesses, and individuals to ensure that it is efficient, equitable, and fair. By learning from the experiences of past labor markets and prioritizing the development of technology infrastructure that empowers individuals, we can pave the way for a more inclusive and resilient Labor Market 3.0.

[26] Stark, D., and Pais, I. 2020. "Algorithmic Management in the Platform Economy," Sociologica (14:3), pp. 47–72. (https://doi.org/10.6092/issn.1971-8853/12221).
[27] Kellogg, K. C., Valentine, M. A., and Christin, A. 2020. "Algorithms at Work: The New Contested Terrain of Control," Academy of Management Annals (14:1), pp. 366–410. (https://doi.org/10.5465/annals.2018.0174).
[28] Curchod, C., Patriotta, G., Cohen, L., and Neysen, N. 2020. "Working for an Algorithm: Power Asymmetries and Agency in Online Work Settings," Administrative Science Quarterly (65:3), pp. 644–676. (https://doi.org/10.1177/0001839219867024).

HISTORY AND BACKGROUND OF PRIVACY

" Privacy is the power to selectively reveal oneself to the world. "

Eric Hughes
A Cypherpunk's Manifesto

Privacy: A Working Definition

At face value, the meaning of privacy seems self-evident. Upon closer consideration, however, there is significant disagreement about what it is and the extent to which it is valuable. For this reason, the authors of this report felt it appropriate to begin our discussion of privacy considerations in the Learning and Employment Record (LER) ecosystem with a basic definition of privacy and a discussion of why it matters for human beings and human societies.

In the words of cryptography pioneer Eric Hughes, "Privacy is the power to selectively reveal oneself to the world".[29] This definition of privacy makes clear that self-revelation is an empowered choice by a person in relation to another person or entity to whom he is or is not revealing himself. It also implies that the primary agent who reveals information about a person is–or should be–the person the information is about. In other words, for Hughes, in privacy-respecting social arrangements, the subject of data is the primary–and in some cases, sole–legitimate source of data about themselves (even if that data was authored by someone else).

Hughes's definition of privacy is not an outlier; the judicial and legislative branches of governments in the countries that led the information technology revolution during the 20th century have largely supported his view. In 1890, U.S. legal scholars Samuel Warren and Louis Brandeis postulated a "general common law right of privacy", which they defined as "the right to be let alone".[30] Since the article's publication, U.S. courts have relied on it in hundreds of cases to adjudicate various privacy issues.[31]

In 1965, the U.S. Supreme Court ruled in Griswold vs. Connecticut that the right to privacy, while not explicitly stated in the U.S. Constitution, can be inferred from the "penumbras" cast by the First, Third, Fourth, Fifth and Ninth Amendments.[32] In 1973, the Supreme Court case Roe v. Wade relied upon the inferred right to privacy and to due process (as described in the Fourteenth Amendment) to protect women's access to abortion.[33] Even the 2022 Supreme Court case, Dobbs vs. Jackson Women's Health Organization, which overturned Roe v. Wade's ruling that abortion is constitutionally protected, did not overturn its ruling about the implicit Constitutional right to privacy.[34]

In 1970, as the rise of networked computers was becoming more pronounced, the government of the United Kingdom appointed a "Committee on Privacy" (known as the Younger Committee) to determine whether new legislation was needed to protect the privacy of individuals. The Committee's 1972 report stated: "We have conceived of the right of privacy as having two main aspects. The first of these is freedom from intrusion upon oneself, one's home, family and relationships. The second is privacy of information, that is the right to determine for oneself how and to what extent information about oneself is communicated to others."[35] While the report did not find a right to privacy in English common law, it led to many new proposed laws to protect individuals from invasive information seeking. In 1998, the United Kingdom adopted the Human Rights Act, which incorporated into U.K. law rights enumerated in the European Convention on Human Rights. Article 8 states, "Everyone has the right to respect for his private and family life, his home and his correspondence."[36] While the Article immediately caveats this right with a list of exceptions, the general principle is confirmed in statute.

The above definitions of privacy indicate that privacy is not a thing but a mode of relating. In legal theory, the social dimensions of privacy have been elaborated within the theory of "constitutive privacy", or privacy as constitutive of social relations.[37] [38] [39] [40] It is through modes of relating that people are harmed or benefited, that rights are honored or breached, that intimacies are built and dismantled. Privacy can therefore be more precisely defined as the process of respecting the autonomy of the other with regard to disclosure about their self.

Importantly, privacy is a condition for a person's development into an autonomous, responsible contributor in human societies. As Ruth Gavison points out, individual moral autonomy is a prerequisite for a democratic society, and privacy creates the conditions for the development of that moral autonomy.[41] Therefore, in relatively healthy and free human societies, the fundamental–i.e. default–mode of relating is that of privacy.

Furthermore, within the mode of private relating, not knowing something about someone is the usual case. The vast majority of human beings are strangers to one another, and even those who do know one another have no need to know most things about those in their acquaintance. Unless some necessity for knowing something about someone arises, the relationship between people and organizations is generally one of not knowing. It is either necessity (intentionally) or contingency (unintentionally) that brings about the disclosure of information about another. Privacy describes a mode of relating that takes care that information is revealed only under necessity.

As a mode of relating, privacy is always–at least–a two-way street. In a private social relation, the subject of information discloses information about themselves only at will; whereas other subjects refrain from extracting information about that person or organization without their consent. Therefore, there is both a "not-making-visible" on the part of the self-disclosing subject and a "not-requesting-visibility" on the part of the recipient of the disclosure that constitutes privacy. This is what Canadian sociologist Erving Goffman referred to as "civil inattention", which is a form of "unfocused interaction" that affords others the "minimal courtesy" of recognizing their presence, but not otherwise attending or reacting to it in any way.[42] Civil inattention is not ignoring the other person, or pretending they are not there; rather, it is a kind of acknowledgement characterized by an aversion of the gaze in order to signal mutual respect and the absence of any problem between the parties.[43]

Civil inattention is reflexively practiced by most people who are both socially distant from one another and in physical proximity. The challenge posed by the digital world is that the same channels that have amplified individual speech and behavior have made it easier than ever for others to "stare" at others without being seen. The call for digital privacy is in many ways a call to restore the basic etiquettes of interpersonal relating that acknowledge how threatening the experience of being surveilled is and the importance of mitigating that threat.

However, in what we call investment-based social situations–where one party is making an investment of value in another, creating risk for themselves–verifying the truth of certain information about the counterparty to that transaction becomes necessary for self-protection.[44] Conversely, disclosure of information also creates risk. The more information is disclosed about the subject of that information, the riskier the transaction becomes for them. For this reason, investment-based social situations create risks for all parties involved and call for degrees

[29] Eric Hughes. "A Cypherpunk's Manifesto". Activism.net. 9 March, 1993. https://www.activism.net/cypherpunk/manifesto.html.

[30] Samuel D. Warren and Louis D. Brandeis. "The Right to Privacy". Harvard Law Review 4(5) (1890): 193-220.

[31] The Free Legal Dictionary. "Privacy." N.D. https://legal-dictionary.thefreedictionary.com/privacy.

[32] Cornell Law Institute. "Right to Privacy." N.D. https://www.law.cornell.edu/wex/right_to_privacy.

[33] "Roe v. Wade." Wikipedia. https://en.wikipedia.org/wiki/Roe_v._Wade#cite_note-FOOTNOTENowakRotunda2012%C2%A7 18.29(a)(i)-5.

[34] "Dobbs vs. Jackson Women's Health Organization." Wikipedia. https://en.wikipedia.org/wiki/Dobbs_v._Jackson_Women's_Health_Organization

[35] David Vincent. Privacy: A Short History. Cambridge, UK: Polity Press, 2016. p. 113.

[36] "Human Rights Act 1998." UK Public General Acts. https://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/7.

[37] John Dewey. "Liberalism and Civil Liberties". In Later Works, Vol. 11. Edited by Jo Ann Boydston. pp. 372-373 Southern Illinois University Press, 1987 (1936).

[38] Julie E. Cohen. "Examined Lives: Informational Privacy and the Subject as Object". Stanford Law Review 52 (2000): 1373-1438.

[39] Paul M. Schwartz. "Privacy and Democracy in Cyberspace". Vanderbilt Law Review 52 (1999): 1609-1702.

[40] Daniel Solove. "A Taxonomy of Privacy". University of Pennsylvania Law Review 154(3) (2014): 477-560.

[41] Ruth Gavison, "Privacy and the Limits of Law". Yale Law Journal 89(3) (1980): 421-471.

[42] Erving Goffman. Behaviour in Public Places. New York: The Free Press, 1963. pp. 83-88.

[43] Ibid.

[44] Natalie Smolenski. "Identity and Digital Self-Sovereignty: A New Paradigm for Sovereignty on the High Seas." Medium. Sep. 19, 2016. https://medium.com/learning-machine-blog/identity-and-digital-self-sovereignty-1f3faab7d9e3.

of disclosure and information security in proportion to that risk.

Stated otherwise, investment-based social situations create circumstances that function as exceptions to the default relational mode of not knowing: they create the conditions under which there is cause for one person or organization to request or even require information from another. Examples include:

1. An entity making a loan to another may require proof that the borrower has sufficient collateral to make whole the loan amount.

2. A parent giving a sick child over for treatment may require proof that the medical practitioner is in fact trained and experienced in the practice of medicine that they claim.

3. An employer may require proof that a prospective worker has the skills and qualifications needed for an open position.

4. A patient prescribed a medication may require proof of its safety and efficacy.

5. A pension fund investing capital in a hedge fund may require proof of its past performance as well as disclosures about the professional qualifications and history of its staff.

6. A car buyer may require proof of a car manufacturer's track record for safety and redress procedures within the legal jurisdiction in which they live.

Information disclosure is therefore both a critical element of risk management as well as a risk in itself. While certain kinds of information may be critical to establish the trust required for investment-based social transactions, that same information, when disclosed outside of the context of such a transaction, may critically damage the reputation, wealth, health, or other needs of a person or organization. The risk inherent in disclosure suggests that all forms of disclosure, no matter how big or small, should occur within the relational mode of privacy. Privacy, after all, does not mean not knowing something about someone, but rather knowing it with that person's consent, at an appropriate time, for appropriate reasons.

The meanings of the words "consent" and "appropriate" are of course highly contested. The point in this discussion is not that any human society should arrive at a final, closed meaning of these terms, but rather that the negotiation of consent, disclosure, and risk–*the practice of privacy*–is a delicately calibrated mode of relating that requires sensitivity and care. Even without a consensually agreed-upon definition of "sensitivity" and "care", human beings are attuned to when these qualities are low or absent in a relational encounter. The absence of care in the behavior of one party to an interaction is often an indicator that said party feels unthreatened by the potential negative social consequences of such an absence of care. This is a characteristic of actors who feel they possess power[45], and this feeling of power possession is not lost on those who interact with them. For example, most people have an intuitive sense that where there are significant discrepancies between the level of investment made by one party to a transaction and the level of informational disclosure that party requires of their counterparty (for example, requiring a social security number to enter a store), a large power asymmetry is likely present.

[45] Brian Resnick and National Journal. "How Power Corrupts the Mind". The Atlantic. 9 July, 2013. https://www.theatlantic.com/health/archive/2013/07/how-power-corrupts-the-mind/277638/.

Correcting Power Asymmetries in Disclosure

As a mode of relating that respects the autonomy of people to self-disclose, privacy requires a basic symmetry in how all parties to a transaction exercise their power vis-a-vis one another during the process of information disclosure. This behavioral power symmetry–which does not necessarily correspond to a symmetry of actual power, or capacity, between actors–results in a baseline mutuality that builds trust. This trust can be achieved even if the relationship is anonymous and terminates with the end of a single transaction.

By contrast, transactions whose participants leverage significant power asymmetries to extract information from other participants through coercion are not relating in the mode of privacy. Without baseline mutuality, information extraction can be considered a mode of social violence. While it is not the position of this report either that power asymmetries or even social violence are essentially good or bad, it is our view that persistent, indiscriminate, and unpredictable social violence destroys trust and the conditions for producing morally autonomous individuals that readily contribute to the healthy functioning of a free society.

Surveillance Capitalism

There is by now a copious academic and trade literature calling attention to the pervasive informational (i.e. power) asymmetries characterizing the internet economy, a phenomenon that has been labeled "surveillance capitalism".[46] This "system of surveillance" differs from traditional modes of surveillance not only in its unprecedented profitability, but in the degree of its persistence: what Andrew Guthrie Ferguson calls "the six A's of (1) automation, (2) acceleration, (3) accuracy, (4) accumulation, (5) aggregation, and (6) actualization".[47] Surveillance capitalism has profoundly shifted power in the direction of large organizational actors–corporations and governments–and away from individuals, who largely exercise day-to-day agency in light of the behavioral possibilities enabled and constrained by regulated and surveilled software platforms. This power imbalance shapes everything from consumer behavior to political engagement to the ways people engage in the organizations and communities they are a part of.

The distortions produced by today's knowledge economy for interpersonal relating are palpable. For one thing, it is increasingly difficult to ascertain the entity to whom disclosures of personal information are made. In other words, when people provide personal information in order to complete a purchase, apply for a job or a loan, check into a hospital, or cross a border, it is unclear exactly who is receiving, validating, and potentially sharing that information. Generally, the recipients of personal information (and they are usually multiple) are personalities of a higher order–collective persons–like government agencies, corporations, or other organizations. Some are known, while others remain secret. Regardless, the receipt, processing, and validation of personal information largely occurs away from the view of the subject of that information. This frustrates the relational logic of intimate disclosure in which the person sharing information about themselves has established a relationship of minimal required trust with their counterparty, and only some immediate necessity requires the disclosure of a reasonably corresponding type and amount of information to that counterparty specifically.

The advent and pervasiveness of digital networks has accelerated this asymmetric sharing of information.

[18] Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019.

[19] Andrew Guthrie Ferguson. "Persistent Surveillance". Alabama Law Review (forthcoming). (March 31, 2022). American University, WCL Research Paper 2022-10. https://ssrn.com/abstract=4071189.

Individuals are increasingly required to interact with and subject to known and sometimes unknown organizations (including government agencies) via the continuous disclosure of information about themselves, with no reciprocal disclosure of information by the entities receiving that information. Due to the rapid advance of information technologies, that personal information is immediately classified, stored, and aggregated, then used to produce both collective and highly targeted behavioral insights and predictions. Software can subsequently incentivize or modify these predicted behaviors as desired by the application's stakeholders.

While the rapidly-accelerating ability to process information has enabled vastly higher levels of efficiency, scalability, and speed in the processing of transactions, it has removed many of the social frictions that serve as checks on privacy violations when human beings relate directly. These social frictions are a necessary constituent of privacy. For this reason, although we agree with Daniel Solove that "privacy is the relief from a range of kinds of social friction",[48] we would add that it generates different kinds of social friction which are necessary for regulating mutuality in human relationships. The absence of these frictions creates the conditions for unchecked abuses of power by actors powerful enough to surveil and control without suffering any undesirable social consequences.

A Brief History of the Web

It is against this background of asymmetrical informational power that the technologies enabling the private issuance, sharing, and verification of digital claims–including LERs–are being developed. The "decentralized identity" movement, as it is referred to here (and of which LERs are one instantiation), represents a particular era in the evolution of the public internet.

There are many ways to periodize the history of the internet, which is a global, open network of networked computers. For our purposes here, however, we will focus on a condensed history of the World Wide Web, or the software used to discover, access, and share information on the internet. In the common vernacular, the terms "Web 1.0", "Web 2.0", and "Web 3.0" (and beyond) are frequently used to segment the history of the web. In what follows, we shall treat each of these stages in turn.

"Web 1.0" typically refers to the period roughly from the early 1990's to the early 2000's, characterized by the birth of the World Wide Web and its foundational protocols (HTTP and HTTPS; SSL; SMTP; PGP), languages (HTML; CSS; JavaScript), and standards (URIs/URLs). Web 1.0 was characterized by the first (static) web pages and web browsers, email, and real-time news. Because the web was still a vanguard technology during this period, its user base was relatively small; using it generally required some level of technical knowledge. The advent of SSL, a cryptographic protocol designed to encrypt data in transit over the web, ushered in the era of e-commerce by enabling secure financial transactions online. It was this commercial promise of the web that incentivized companies to develop simple, intuitive, and often "free" web applications that removed many of the previous barriers to using the internet, which exponentially grew the web's user base.

[48] Solove, "A Taxonomy of Privacy", p. 484.

Web 2.0 and Its Discontents

With the commercialization of the web came a burst of entrepreneurial activity and venture capital investment. This spurred the dawn of the "Web 2.0" era in the early 2000's, characterized by dynamic websites, user-generated content (including the social web), and mobile computing. Network effects incentivized the growth of the large internet platform companies known today as FAANG (Facebook, Amazon, Apple, Netflix, and Google). However, the consolidation of user bases enabled by network effects gave these preeminent platforms access to previously unimaginable amounts of user data. They quickly realized that this data could be used to create predictions about user behavior and to influence that behavior at scale. To put it bluntly, digital objects with durable structures about individuals became new currency[49]. A combination of subscription and especially advertising-basedrevenue models made these companies among the most profitable in human history.[50]

The very success of the Web 2.0 commercial model generated a backlash. In 2018, Tom Donohue, CEO of the US Chamber of Commerce, referred to this turning of sentiment against large internet companies as the "techlash", and use of the term quickly spread.[51] [52] In 2018, the world learned that Cambridge Analytica, a political advertiser, had accessed the data of 87 million Facebook users[53] and used that data to influence elections around the world, including the 2016 U.S. Presidential election and the 2016 U.K. "Brexit" referendum.[54] While some of that data collection occurred in violation of Facebook's terms of service,[55] the Federal Trade Commission slapped Facebook with a $5 billion fine for negligence with regard to securing user data.[56] In 2022, Facebook users won a class action lawsuit against the company, alleging similar negligence. Facebook's parent company, Meta, settled the lawsuit for a record $725 million.[57] Facebook also faced multiple enforcement actions in countries outside the United States.

[49] Alaimo, C., and Kallinikos, J. 2022. "Organizations Decentered: Data Objects, Technology and Knowledge," Organization Science (33:1), pp. 19-37.

[50] Yahoo! "15 Most Valuable Companies In History." 7 October, 2022. https://www.yahoo.com/video/15-most-valuable-companies-history-205700319.html.

[51] Mike Allen. "First look: 'Techlash' warning." Axios. 9 January, 2018. https://www.axios.com/2018/01/09/first-look-at-techlash-warning-1515534954.

[52] Darrell West. "Techlash continues to batter technology sector." Brookings. 2 April, 2021. https://www.brookings.edu/blog/techtank/2021/04/02/techlash-continues-to-batter-technology-sector/.

[53] "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users." The New York Times. 4 April, 2018. https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.

[54] The Guardian. "The Cambridge Analytica Files." https://www.theguardian.com/news/series/cambridge-analytica-files.

[55] Kurt Wagner. "Here's how Facebook allowed Cambridge Analytica to get data for 50 million users." Recode. 17 March, 2018. https://web.archive.org/web/20180328004259/https://www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

[56] David McCabe. "Facebook shareholders breathe sigh of relief on $5 billion FTC fine." Axios. 15 July, 2019. https://www.axios.com/2019/07/15/facebook-shareholders-breathe-sigh-of-relief-on-5-billion-ftc-fine.

[57] Joel Rosenblatt. "Facebook parent Meta pays record $725 million to settle Cambridge Analytica scandal." Fortune. 23 Dec., 2022. https://fortune.com/2022/12/23/facebook-parent-meta-pays-record-725-million-to-settle-cambridge-analytica-scandal/.

But the Cambridge Analytica scandal was only the tip of the techlash. In rapid succession, Google was fined over $7 billion in two separate antitrust actions brought by the European Commission.[58] [59] In 2022, Google's parent company, Alphabet, paid a nearly $400 million settlement to 40 U.S. states over location-tracking practices in the largest multi-state privacy pact in U.S. history.[60] [61] Also in 2022, Epic Games, maker of the wildly popular Fortnight game, was ordered to pay a $520 million fine by the FTC for illegally collecting the personal information of children under 13 and tricking players into making unintentional in-game purchases using so-called "dark patterns".[62] [63] But it isn't only consumer software companies that have felt the techlash. A 2022 class action lawsuit still moving through the courts as of this writing alleges that Oracle, a paragon of enterprise database software, harmonizes on- and offline data into detailed profiles of billions of people and that it collects and sells that data largely without user consent.[64] [65] It is likely that additional legal actions against the data broker industry will be taken if the United States adopts federal privacy legislation; currently, digital privacy laws are largely the purview of U.S. states.

Web 2.0 companies drew the scrutiny of lawmakers not only for surveillance and deceptive monetization practices, but for their responses to violent and politically inflammatory rhetoric. After Twitter banned then-U. S. President Donald Trump and 70,000 other accounts from its platform in January 2021 for allegedly inciting violence,[66] a new kind of techlash arose from those opposed to the arbitration of speech by social media companies. Over the coming year, state legislators in 34 U.S. States introduced more than 100 bills that would regulate how social media companies treat user-generated content.[67] Some of those bills forbid social media companies from censoring user speech, while others require companies to provide easily-accessible ways for users to report hate speech and misinformation.

[58] Sara Fischer. "EU hammers Google with record $5 billion fine over Android." Axios. 18 July, 2018. https://www.axios.com/2018/07/18/google-record-5-billion-antitrust-fine-eu-android.

[59] Jenni Reid. "Google loses appeal over EU antitrust ruling, but fine cut to $4.12 billion." CNBC. 14 Sep. 2022. https://www.cnbc.com/2022/09/14/eu-court-backs-antitrust-ruling-against-google-but-reduces-fine.html.

[60] Rosenblatt, "Facebook parent Meta", 2022.

[61] Erik Larsen. "Google to Pay $391 Million Over 'Crafty' Location Tracking." Bloomberg. 14 November, 2022. https://www.bloomberg.com/news/articles/2022-11-14/google-to-pay-391-5-million-to-states-over-location-tracking

[62] Sarah E. Needleman, Aaron Tilley, and Brent Kendall. "Epic Games, Maker of 'Fortnite,' to Pay $520 Million to Resolve FTC Allegations." The Wall Street Journal. 19 December, 2022. https://www.wsj.com/articles/epic-games-maker-of-fortnite-to-pay-520-million-to-resolve-ftc-allegations-11671456744.

[63] Katie Deighton. "Subscription Companies Rethink Irksome Cancelation Practices." The Wall Street Journal. 1 December, 2021. https://www.wsj.com/articles/subscription-companies-rethink-irksome-cancelation-practices-11638370800?mod=article_inline.

[64] Bob Sullivan. "'Data Broker' Oracle Enables Privacy End-Arounds, Lawsuit Alleges." Secure World. 28 August, 2022. https://www.secureworld.io/industry-news/data-broker-oracle-privacy-lawsuit.

[65] Natasha Lomas. "Oracle's 'surveillance machine' targeted in US privacy class action." TechCrunch. 22 August, 2022. https://techcrunch.com/2022/08/22/oracle-us-privacy-class-action/.

[66] Twitter Inc. "Permanent suspension of @realDonaldTrump." Twitter Blog. 8 January, 2021. https://blog.twitter.com/en_us/topics/company/2020/suspension.

[67] Rebecca Kern. "Push to rein in social media sweeps the states." Politico. 1 July, 2022. https://www.politico.com/news/2022/07/01/social-media-sweeps-the-states-00043229.

Only three of these bills have passed into law as of the writing of this report–in Texas, Florida, and New York. The Texas and Florida laws, which prohibit social media companies from censoring speech, have been challenged as unconstitutional by the technology industry for restricting the First Amendment right of companies to determine what they publish. The Florida law was ruled largely unconstitutional by the 11th U.S. Circuit Court of Appeals, while the Texas law was upheld by the 5th U.S. Circuit Court of Appeals.[68] The State of Florida and technology industry groups have appealed both rulings, respectively, to the Supreme Court, which has expressed initial interest in reviewing one or both cases.[69]

The issue of platform responsibility (or lack thereof) for user speech is profoundly significant for determining the contours of both free speech and the internet economy in the 21st-century United States. To date, there has been widespread agreement that Section 230 of the 1996 Communications Decency Act, which protects software companies from being held legally liable for content on their platforms that is generated by third parties, was instrumental in the growth of Web 2.0.[70] But if the technology industry succeeds in opposing the recent anti-censorship laws by arguing that technology companies are publishers with first amendment rights, it may undermine the very Section 230 protections that have insulated the industry from liability for user-generated content. This dilemma reflects an unsustainable tension at the heart of Web 2.0: if companies want to "own", monetize, and control all of the data produced on their platforms, they may place themselves in the same position of editorial liability as the traditional media companies they have disrupted.

While government enforcement actions against technology companies were painful, perhaps the clearest evidence of a techlash was the turning of public attitudes against those companies–even if their de facto monopolies over many routine, day-to-day activities prevented many people from leaving their platforms. The percentage of Americans who believe that technology companies have a largely positive impact on the United States has been steadily declining since its peak in 2015.[71] However, this decline mirrors a broader, secular decline of public trust in most social institutions–corporations, banks, and government.[72] [73] Because both corporations and government are increasingly mistrusted, many Americans also believe that increased regulation of technology companies is not the most effective way of stemming their abuses.[74]

[68] Jesus Vidales. "Texas social media 'censorship' law goes into effect after federal court lifts block." Texas Tribune. 16 September, 2022. https://www.texastribune.org/2022/09/16/texas-social-media-law/.

[69] Brian Fung. "Tech groups ask Supreme Court to rule on hot-button Texas social media law." CNN. 15 December, 2022. https://www.cnn.com/2022/12/15/tech/tech-groups-supreme-court-texas-social-media-law/index.html.

[70] Electronic Frontier Foundation. "Section 230 of the Communications Decency Act." https://www.eff.org/issues/cda230.

[71] Carroll Doherty and Jocelyn Kiley. "Americans have become much less positive about tech companies' impact on the U.S." Pew Research Center. 29 July, 2019. https://www.pewresearch.org/fact-tank/2019/07/29/americans-have-become-much-less-positive-about-tech-companies-impact-on-the-u-s/.

[72] Amina Dunn and Andy Cerda. "Anti-corporate sentiment in U.S. is now widespread in both parties." Pew Research Center. 17 November, 2022. https://www.pewresearch.org/fact-tank/2022/11/17/anti-corporate-sentiment-in-u-s-is-now-widespread-in-both-parties/.

[73] Pew Research Center. "Public Trust in Government: 1958-2022." 6 June, 2022. https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022/.

[74] Emily A. Vogels. "Support for more regulation of tech companies has declined in U.S., especially among Republicans." Pew Research Center. 13 May, 2022. https://www.pewresearch.org/fact-tank/2022/05/13/support-for-more-regulation-of-tech-companies-has-declined-in-u-s-especially-among-republicans/.

Beyond Web 2.0: DPKI

What is now called "Web 3.0" arose to solve the problems of censorship, surveillance, behavioral control, and informational asymmetry presented by Web 2.0 platforms–without relying on government regulation. The broad aim animating this latest stage in evolution of the web is to shift the balance of power online back in the direction of the individual by building technologies whose bottom-up adoption momentum cannot be stopped. The architects of the new web achieve this mainly by decentralizing the implementation of public key cryptography infrastructure (PKI)–the security innovation that enabled private online transacting (including e-commerce) via, among other things, the PGP, SSL, and TLS protocols.

Today, public key cryptography enables virtually all kinds of security operations online–from user authentication and access management to verifying the integrity of websites, digital signatures, and documents. Although PKI is highly secure, it is usually employed on behalf of users by service providers, rather than by users themselves. This introduces the possibility that those service providers can both access and provide access to private communications and transactions–even without the end user's awareness. For example, it has been the stated aim and routine practice of U.S. law enforcement and intelligence agencies to pressure commercial internet companies to grant them "exceptional access" to user data by bypassing their products' encryption schemes.[75] When such demands are made on companies, they are often accompanied by gag orders that prevent the company from disclosing that such access has been requested or granted.[76] Companies themselves may also be incentivized to monetize user data by decrypting that data for themselves but not for others. For these reasons, it is not clear to the public which encryption standards and services are truly secure and which are compromised.

Decentralized public key infrastructure–or DPKI–emerged within a small group of cryptographers and computer scientists known colloquially as "cypherpunks". This group informally coalesced in the early 1990's, attracting technologists who anticipated that shared interests between public and private sectors would incentivize the creation of a surveillance-based online economy. In the cypherpunks' view, the only way to preserve any sphere of individual privacy and liberty in such a political economy was through universal access to advanced cryptography. The group went about building open cryptography standards like PGP, or "Pretty Good Privacy", that could be used by anyone to encrypt their communications online. This resulted in prolonged contestation between some cypherpunks and the U.S. law enforcement and national intelligence apparatus, which classified encryption as a controlled munition and sought to prevent its use by anyone except U.S. and allied state actors.[77]

By the early 21st century, however, the economic power of the internet had become so apparent–accounting for roughly a quarter of annual GDP growth in advanced economies[78]–that government agencies quieted (though did not abandon) their attempts to suppress the widespread use of encryption. Nevertheless, the centralization of cryptographic key custody and distribution in the hands of both state and corporate actors left individuals vulnerable to having their communications compromised and their transactions surveilled and censored.

[75] Craig Jarvis. Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. Boca Raton, FL: CRC Press, 2021.

[76] Ibid.

[77] Craig Jarvis. Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. Boca Raton, FL: CRC Press, 2021.

[78] James Manyika and Charles Roxburgh. "The great transformer: The impact of the Internet on economic growth and prosperity." McKinsey Global Institute. October 2011. https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/the%20great%20transformer/mgi_impact_of_internet_on_economic_growth.pdf.

Surveillance and censorship power most worried cypherpunks in two domains: speech and money, or financial transactions. They saw the freedom to speak and the freedom to transact as cornerstones of a free society. Accordingly, some members and allies of this group had worked for decades to develop an internet-native form of money that could be used by individuals holding their own cryptographic keys, without relying on third-party intermediaries like banks, non-bank financial institutions, and government agencies. At last, in 2008, a pseudonymous member of the cypherpunks mailing list, Satoshi Nakamoto, published a white paper outlining the characteristics of a peer-to-peer electronic cash system called Bitcoin.[79]

Bitcoin seemed to present, for the first time, a working implementation of digital money that did not rely on any centralized third party to implement and use. As both a network (Bitcoin) and a currency native to that network (bitcoin), the software developed by Nakamoto presented both the framework for a new global payments system and its first implementation. The reader is invited to consult the Bitcoin white paper for an overview of the network's design principles and architecture.[80] In short, however, the protocol was designed to facilitate censorship-resistant transacting with absolutely scarce digital money. In this way, bitcoin has automated some of the functions of central banks by enabling both the issuance of money and monetary policy to be exercised by a global community of adversarial network participants.[81] The protocol is prohibitively difficult to modify, which results in a conservatism that has kept its foundational characteristics largely intact since its introduction.

Bitcoin inspired the many blockchain protocols tailored to primary use cases other than digital currency. We will mention two of them here: Ethereum and Hyperledger. Ethereum, developed by Vitalik Buterin and launched in 2015, sought to create a Turing-complete blockchain that could be used to encode decentralized applications (DApps) directly on-chain. While Bitcoin's scripting language supports simple, smart contracts – self-executing agreements with the terms directly written into code, Ethereum enables the anchoring of more complex smart contracts at the blockchain layer. Hyperledger, established by the Linux Foundation in 2015, is an umbrella project comprising several open-source blockchain frameworks and tools tailored for enterprise use. Unlike public blockchains like Bitcoin and Ethereum, Hyperledger is a toolkit for developing private and permissioned blockchains, where participants are known and pre-vetted. Hyperledger Fabric, one of the most popular frameworks within the Hyperledger ecosystem, was developed by IBM and Digital Asset, a company that builds custom blockchains for financial institutions[82].

[79] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". 31 October, 2008. https://bitcoin.org/bitcoin.pdf.

[80] Ibid.

[81] The Satoshi Papers. https://www.satoshipapers.org/.

[82] Anna Irrera. "Blockchain startup Digital Asset raises $40 million." Reuters. October 16, 2017. https://www.reuters.com/article/us-digital-asset-funding/blockchain-startup-digital-asset-raises-40-million-idUSKBN1CL22G.

From Money to Identity

Bitcoin serves as an independent verification infrastructure for the World Wide Web. By automating the financial process of final settlement, it has replicated globally a service that until now has only been provided by central banks (for example, the U.S. Federal Reserve's FedWire service[83]). The resilience, security, and stability of bitcoin's settlement function have given rise to Layer-2 and Layer-3 protocols that enable dramatic scalability of the network's transacting capacity. The most widely-used of these is the Lightning Network, which enables the creation of peer-to-peer payment channels that settle to the bitcoin blockchain.[84] The number of potential Lightning channels scales organically with the number of the network's users and the liquidity they provide, resulting in virtually unlimited transaction capacity.[85] Lightning transactions occur instantaneously and at virtually no cost because they do not rely on node consensus, users amortize base chain transaction fees, and Lightning Node routing fees are extremely low.[86] The result is a Visa- and Mastercard-like payment processing network with greater speed, lower cost, and higher throughput than the incumbents.

Lightning can also be used as a payment rail for currencies other than bitcoin. Some companies, like Strike, achieve this by converting any fiat currency into bitcoin, sending it via the Lightning Network, and then converting it into the recipient's desired currency upon receipt.[87] Other companies, like Lightning Labs, have built dedicated protocols (i.e. Taro) for minting any kind of currency using the Lightning Network.[88] These token transactions all eventually settle to the bitcoin blockchain, taking advantage of its decentralized, transparent, and politically neutral global ledger. This reiterates that Bitcoin is first and foremost a protocol and a network; the bitcoin digital currency native to that protocol is the first major use case for that network.

With the advent of the Lightning Network, Bitcoin is clearly establishing itself as the world's most socially and politically independent way to verify financial transactions, without sacrificing the speed or low costs of legacy financial rails. Bitcoin's success verifying financial transactions also makes it ideally suited for verifying other digital claims–data and information about anyone or anything. When digital claims are "anchored" to the Bitcoin blockchain, they leverage the network's function as a single source of truth to provide a high level of confidence for claims made online.

The challenge, however, is doing this in a privacy-preserving way. Since Bitcoin is a public, permissionless ledger, visible to and usable by all, that means, among other things, not encoding any personally-identifiable data on-chain. This is the challenge taken up by what we call the "decentralized identity" (DID) movement.[89] At times this movement has been referred to as the "self-sovereign identity" (SSI) movement,[90] although this has led some to erroneously surmise that the movement rejects, or seeks to minimize, the role of authoritative issuers of claims. While the term "self-sovereign identity" has value, in this report we will use the term "decentralized identity" in order to avoid wading into that debate. However, it is important to recognize the shared genealogy of both terms.

[83] The Federal Reserve. "Fedwire® Funds Service." https://www.frbservices.org/financial-services/wires.

[84] Lyn Alden. "A Look at the Lightning Network." LynAlden.com. August 2022. https://www.lynalden.com/lightning-network/.

[85] Ibid.

[86] Camomile Shumba. "The lightning network is driving the current burst of mainstream adoption in bitcoin — here's how it's speeding up transaction times and cutting fees." Business Insider. 14 August, 2021. https://markets.businessinsider.com/news/currencies/the-lightning-network-is-driving-mainstream-bitcoin-adoption-2021-8.

[87] Jack Mallers. "Announcing Strike Global." Medium. 6 January, 2021. https://jimmymow.medium.com/announcing-strike-global-2392b908f611.

[88] Michael Levin. "Hello Taro: Building the (Tap)Root of the World's Financial Network with Bitcoin." Lightning Labs. 28 September, 2022. https://lightning.engineering/posts/2022-9-28-taro-launch/.

[89] At times this movement has been referred to

[90] U.S. Chamber of Commerce Foundation. "Applying Self-Sovereign Principles to Interoperable Learning Records." June 2020. https://www.uschamberfoundation.org/sites/default/files/media-uploads/Applying%20SSI%20Principles%20to%20ILRs%20Report.pdf.

The origins of the DID movement extend to informal meetups of technical standards groups including the Internet Identity Workshop (IIW),[91] Rebooting Web of Trust (RWoT),[92] and the World Wide Web Consortium (W3C).[93] A vibrant ecosystem of early-stage technology startups, established technology companies, educational institutions, nonprofits, independent subject-matter experts, and industry consortia[94] has contributed to the elaboration of technical standards for DID.[95 96] These include Verifiable Credentials (VCs),[97] Decentralized Identifiers (DIDs),[98] and Decentralized Web Nodes (DWNs)[99] standards.

At root, DID is part of the broader post-Web 2.0 drive to reconcile the needs for both privacy and verifiability in the issuance, storage, sharing, and verification of personal data. Another important motivating factor behind the development of DID is the need for greater resilience of personal data–the ability of the end user to easily access and validate data about themselves even if the organization or individual who originally attested to that data and/or the technology provider they used to make the attestation are no longer functional. Greater data resilience would alleviate the significant human capital losses that occur during processes of migration, natural disasters, and economic and political unrest.

The earliest applications of DID have unsurprisingly appeared in the education and government sectors. This is because organizations within these spheres act as issuers of digital records that must be verified with the highest level of confidence while remaining under the control and discretion of the people they are about. Academic diplomas, transcripts, and professional licenses have been among the first use cases for decentralized digital identity implementations.[100 101 102] Multiple governments have also required and roadmapped the issuance of vital records using DID standards. [103 104]

[91] The Internet Identity Workshop. https://internetidentityworkshop.com/.

[92] Rebooting Web of Trust. https://www.weboftrust.info/.

[93] W3C. https://www.w3.org/.

[94] Decentralized Identity Foundation. https://identity.foundation/.

[95] "Texas Work Group on Blockchain Matters Report." 14 November, 2022. https://portal.bcwg.texas.gov/General-Documents/Texas-Work-Group-on-Blockchain-Matters-Report/wbtp-2m5k.

[96] Natalie Smolenski. "Blockchain for Education: A New Credentialing Ecosystem." OECD Digital Education Outlook 2021. pp. 211-252. https://read.oecd-ilibrary.org/education/oecd-digital-education-outlook-2021_589b283f-en#page211.

[97] W3C. "Verifiable Credentials Data Model v1.1." https://www.w3.org/TR/vc-data-model/.

[98] W3C. "Decentralized Identifiers (DIDs) v1.0." https://w3c.github.io/did-core/.

[99] Decentralized Identity Foundation. "Secure Data Storage Working Group. aka: SDS WG." https://identity.foundation/working-groups/secure-data-storage.html.

[100] U.S. Chamber of Commerce Foundation, "Applying Self-Sovereign Principles", 2020.

[101] Smolenski, "Blockchain for Education", 2021.

[102] Jobs for the Future Foundation. "Building a Skills-Based Talent Marketplace: Verifiable Credentials Wallets for Learning and Employment." April 2022. https://info.jff.org/hubfs/Digital%20Wallet%20Market%20Scan/Market-Scan-Digital-Wallet-040122-vF.pdf.

[103] California S.B. 786, "An act to amend Section 103526.5 of the Health and Safety Code, relating to blockchain technology," https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220SB786#93ENR.

[104] European Blockchain Infrastructure (EBSI). https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home.

It was not long before employers began to take notice of how emerging DID standards can facilitate the discovery and hiring of talent–and by extension increase equity and access to meaningful employment. In 2018, the U.S. Chamber of Commerce and the Lumina Foundation founded the T3 Innovation Network, a consortium of organizations across industry, government, education, and nonprofit sectors working to "to explore emerging Web 3.0 technologies in an increasingly open and decentralized public-private data ecosystem."[105] Over 500 stakeholders currently partake in the Network.[106] The aim of T3 is to harmonize technology standards used to record formal and informal learning in order to make talent more easily discoverable by employers in the United States. In the process, T3 hopes to both advance upward socioeconomic mobility and resolve the labor shortage that cost American businesses an estimated $738 billion in revenue during 2021 alone.[107]

Central to the transmission and verification of data about individual characteristics and qualifications is the learner record itself. T3 has defined the term "Learning and Employment Record" (LER) as "a comprehensive digital record of skills, competencies, and achievements learned in school, on the job, through volunteer experiences, or in the military. LERs go by many names and are also referred to as an interoperable learning record (ILR)."[108] T3 runs a comprehensive resource hub that provides information about the technology standards used in the implementation of LERs.[109] Although LERs don't require DID-based approaches to implement, T3 does include W3C Verifiable Credentials as a recommended standard.[110] A significant and growing number of LER pilots and production implementations have occurred throughout the world, many of them explicitly employing DID standards.[111] [112]

As DID technology continues to evolve, its ability to better reconcile the seemingly competing requirements of privacy and verifiability will likely make it a widely-used set of standards and paradigms for managing personal data.

[105] U.S. Chamber of Commerce Foundation. "T3 Innovation Network." 2018. https://www.uschamberfoundation.org/sites/default/files/CEW_T3_OnePager_September2018.pdf.

[106] T3 Innovation Network. "Modernizing the data and technology that power the talent marketplace." 2021. https://www.uschamberfoundation.org/sites/default/files/T3%20Network_OnePager_2021.pdf.

[107] Federal Reserve Bank of Atlanta. "Are Labor Shortages Slowing the Recovery? A View from the CFO Survey." 14 July, 2021. https://www.atlantafed.org/blogs/macroblog/2021/07/14/are-labor-shortages-slowing-the-recovery--view-from-cfo-survey.

[108] T3 Innovation Network. "LER Features and Orientation." https://lerhub.org/s/curators/ilr-utilities/zH53fdwb8G87X75Fe.

[109] T3 Innovation Network. "LER Hub." https://lerhub.org/g/bqCgme2fQxDbgJ6D7.

[110] T3 Innovation Network. "Verifiable Credentials (VC)." https://lerhub.org/s/curators/m7rgf7r2tCwM3CwsQ/sxAGAguomKdrosfLk.

[111] Smolenski, "Blockchain in Education", 2021.

[112] T3 Innovation Network. "Pilots Community: Pilots Directory." https://lerhub.org/s/curators/specs-0/ZT3McEDpgKayCXyqc-0.

REVIEW OF STAKEHOLDER INTERVIEWS

With this background, we conducted interviews of different stakeholders and reviewed existing technologies in the LER space. In this section, we summarize the key findings from the stakeholder interviews.

Overview of Stakeholder Interviews

We conducted interviews via Zoom with 54 stakeholders involved in the LER space, including various educators, university employees, employers, policymakers, non-profit organizations, researchers, tech providers, and tech experts. Participants took part in 60-minute interviews from July through November 2022. Several themes emerged in the interviews which can be grouped into three categories listed here: current demand and incentives for LERs; design and implementation; and ethical and equitable considerations. Each theme has a series of sub themes that will be further explored in this section.

Demand and Incentives for LER Ecosystem and Skills-Based Hiring

Current Demand

In terms of the demand for an LER ecosystem, responses from employers, researchers, and stakeholders in education seem to be mixed. A handful of employers, for example, argued that theoretically, LERs and skills-based hiring would be useful. However, it does not seem like many companies are asking for this solution right now. Skills-based hiring is not top of mind in most cases, so these issues are not current priorities for employers.

Researchers and data providers added that employer readiness to change hiring practices should be assessed. Some companies are not yet ready nor willing to change their hiring practices for many reasons. One reason may be that there is still a reliance on traditional degrees and qualifications rather than skills alone.

Annelies Goger, economic geographer and Fellow at Brookings Metro related that, "With a tight labor market, [companies] become more willing and they start looking at skills-based hiring more. But if you actually look at who they are hiring, you probably still see a lot of reliance on the pedigree. There is a lot more need for understanding the sort of HR incentives that make them go back to the degree, time and time again, instead of being willing to take a bet on a person that doesn't fit that typical profile." Some stakeholders in education argue that there is an increase in skills-based hiring among HR leaders, and if they have not already implemented skills-based hiring, they are at least interested in doing so. However, the problem then becomes how to move beyond interest and shift to implementation. Participants generally agreed that the demand was not quite there yet for skills-based hiring, while acknowledging that we are moving in this direction.

Employers may not be using skill-based hiring just yet, but the technology for LERs is being developed regardless. The technology is actually outpacing the policy for and use of LERs. This could lead to using funding and signing contracts with providers who are not really providing what will best support learners and workers. Amanda Winters, Program Director for the National Governors Association, stated that to combat this,

"We need to arm [states] with the questions and the information and the insight to be able to make sure they secure the right types of partners and vendors."

Incentives and Disincentives

Reflecting on the incentives and disincentives for adopting an LER ecosystem highlights the fact that each industry is motivated differently when it comes to skills-based hiring. For example, in the world of higher education, the use of self-sovereign credentials could mean that institutions lose revenue generated by issuing credentials like diplomas and transcripts. This revenue is often very important for university fees and budgets.

Amy Hammett is the Case Western Reserve University Registrar and Director of Student Information Systems. Hammett noted that

"We need to be prepared for when that income is no longer available. It is definitely on the minds of folks, as is the income that is derived from verification of degrees."

The loss of this revenue could be a limiting factor in the adoption of this system. Discussing alternatives to this business model will be critical to maintaining the functionality of higher education.

Several participants explained that one of the disincentives of adopting an LER is that people are confused about what an LER means, as well as what claims credentials are making. There are many debates about defining skills and what qualifies as a credential. Several stakeholders brought up how to define skills and make them relevant to a certain job or employer. While these are important conversations, they mean little if employers are not interested in adopting this approach. Before LERs can be truly useful, there must be changes in hiring practices.

Jason Tyszko is vice president for Education and Workforce for the Chamber of Commerce Foundation. He noted that until these "transactions become more mainstream, they are not going to change." Policymakers and folks in government agree, saying that until there is more widespread adoption, many will not abandon the system we have now. Researchers asserted that we need a better understanding of HR incentives and how to overcome risks of accepting those without degrees or those who may not fit the exact profile for a certain job.

There were also concerns about the ability to falsify information on resumes using LER technology. In response to these concerns, Sean Gallagher, Executive Professor of Educational Policy at Northeastern University, said that he does not think this is a major problem for employers. While he acknowledges that some falsification and credential fraud can occur, when he has asked HR leaders, they report that they take steps to verify credentials and that "If you are going to take the step to fake a credential, when that gets found out, there are going to be huge repercussions. It is something that has a binary outcome."

For Deb Everhart, Chief Strategy Officer at Credential Engine,

"It boils down to reducing the time and cost to hire and improving the quality of the hire."

Everhart explained that making it easier for people to match with jobs means you will get more matches, and those matches may be with people that you may not have been able to find before. "It really is a win-win-win, but it is driven by business value," she added.

Main Reservations and Concerns

While many acknowledge that skills-based hiring and LERs would supplement the hiring and credentialing, some still have reservations about the logistics. Several stakeholders voiced that their institutions are hesitant to experiment with new initiatives and pilot programs because they are not staffed nor budgeted to do so.

For example, Rob Groot from National Student Clearinghouse noted that "there's a lot of schools that are basically taking a waiting position because they can't afford to do something wrong and then have to redo it. They're basically waiting for everything to happen so they can then say, okay, I am going to jump on board now." Some institutions have experimented already with some success, but many are counting on institutions with more resources to engage and resolve issues in the system.

Nonprofits are also taking waiting positions until things have stabilized. Right now, experimenting with LERs and new credentialing systems is a tall order with limited return on investment. Participants at nonprofits also mentioned that money is a barrier. If grant money were available to make infrastructure changes, that could make experimentation seem more appealing to some institutions.

Employers have their own set of concerns which are echoed by several tech providers and researchers. Ethan Karp, CEO of MAGNET, made the point that

"There's no evidence that skills-based hiring has allowed a company to expand their recruitment tunnel in a comprehensive way. It helps modify it or refine it, but there are no substantial changes yet."

Karp even points out that there have been many unsuccessful LER pilots. This has been supported by other stakeholders, including Bledi Taska, Chief Economist at Lightcast. Taska added that you can interpolate that skills-based hiring will benefit society from other findings, but at this point there is no conclusive data. Taska went on to say that

"To some level, there is a belief in general [that skills-based hiring will work]. There is also the belief that there is something big happening behind that. We might not be confident around it, but we do know that that's the next thing. And we need to be ahead of the curve because if we're not then we are going to be stagnant."

Most acknowledge that skills-based hiring would theoretically allow people without formal education and training experience to get jobs, but this assumes that the current labor market is being overly picky, which may not be the case. Karp noted that this can be industry and level specific, so an entry level position compared to a more advanced position would respond to skills-based hiring in a different way. Most interviewees acknowledged that there is a general belief that skills-based hiring might work, which for some is reason enough to continue their efforts.

Design and Implementation

Lack of Infrastructure to Support LERs

It is obvious that the current infrastructure is not set up to accommodate LERs. The main problem with this is that if employers cannot accept and digest LER data, then there is no way to progress in the LER space. There are a series of changes that need to occur in order to make this happen, including shifting hiring practices, changing policies, and adapting technology. Most participants were still unsure what exactly is needed at this point, but it is clear that policy and data need to be ready for technology in order for the technology to function properly.

Winters stated that

"Certainly the technology is exciting, but technology platforms are only as good as the data we put into it. There has to be a dual emphasis on things like transfer and portability."

This would make it so that a credential has meaning across systems, as opposed to losing all functionality once one system does not accept it. Robert McGough, Chief Analytics Officer for the State of Arkansas, echoed these sentiments saying that they are "trying to get ahead of this with governance to where the technologies are interoperable, but a consumer has the choice to use multiple of these LER enabled technologies."

It is imperative that the technology starts and remains both interoperable and free to use. One stakeholder in education acknowledged that we are heading in the direction of LERs, but there are many unknowns. For example, one of the unknowns is how to convert current credentials into forms that are compatible with other systems. All efforts need to be made to make the process as simple and understandable as possible so it can be adopted easily. Mark McConahay, Senior Consultant and LER Coordinator at AACRAO, says that we need to

"push the easy button so that people can participate. And in essence, that means we need a conversion utility that basically says, give me anything you have got for a record… and we will convert it into the appropriate digital standard."

Common Language and Taxonomy

It has also been widely acknowledged that there is no common taxonomic system to use across domains, with the current system being very fragmented. As previously mentioned, the lack of willing participants in early stages has complicated efforts to come up with a clear standard. Some have posited that there may be no way to streamline standards for all industries, which further adds to the confusion. While some stakeholders advocated for a single standard for all industries, others suggested no standards and instead wanted to focus on AI. Some fall somewhere in the middle and believe that a single standard is an oversimplification. The answer, they argue, lies somewhere between the two where it is standards-based but AI-supported.

One tech provider pointed out that "digital credentials are on the rise, but they are not being leveraged by employers. If they are, they seem to lack useful information." Another tech provider explained that there is a need for specific credentials that align with the outcomes desired by employers. Nonprofit stakeholders built on these claims, adding that standardization is important when translating experiences into skills. They argue that it is ideal to have a standardized process for turning learning into skills so that there is less confusion for everyone.

As far as defining skills and competencies, there are issues with "semantic interoperability," as it was referred to by McConahay. Many companies don't have the same skills and competencies because they may be in vastly different industries. As a result, there are no agreed-upon standards for the skills learners should acquire that are attractive to employers. Stakeholders argue that we need a repository of credentials and learning outcomes because there is currently no frame of reference for skills or credentials. Policymakers note that there is a need for more competency data in order to clarify what each credential means.

According to Gallagher, data seem to support that most companies are interested in technical skills rather than soft skills. Soft skills can be difficult to measure, given that they often exist on a spectrum. Individuals also vary in proficiency with skills and competencies, ranging from novice to expert, for example, which is also hard to conceptualize. While skills are more dimensional, Gallagher says credentials are more of a "binary checkbox", meaning you either have the credential or you do not. This helps provide a framework to shape how we talk about credentials, skills, and what we want them to represent.

Tech providers have pointed out that digital credentials are on the rise, but they are not being leveraged by employers. If they are, they seem to lack useful information. One tech provider explained that there is a need for specific credentials that align with the outcomes desired by employers. Nonprofit stakeholders build on these claims by saying that standardization is important when translating experiences into skills.

Assessing Skills

A majority of participants expressed that skills are not represented well on a traditional transcript. It is also hard to translate experiences into skills which complicates the process of assessing them. One participant explained that it is important to examine the curriculum of institutions, programs, and other training opportunities that may lead to issuing a credential. This involves asking what people need to know how to do to succeed in the workforce. Examining the structure and design of a program in addition to the skills requested by employers can help future programs decide how to best support learners.

Interestingly, when exploring how one employer assesses skills, they explained that competencies are not always indicative of behaviors. As a result, in-person conversations with candidates and new hires have more impact than reviewing their information and pointing out where they can improve. Candidates who provide information on their resumes tend to be asked to demonstrate what they know when they get an interview. Google famously stated that they only need four interviews to determine a good hire,[113] and much tech has adopted something similar. However, one must be skeptical about the efficacy of such short interviews (4 x 60 mins) is enough to truly judge someone's skills. One participant involved in the hiring process at a local company explained that "Behavioral-based interviews are really the only way to determine the behavior of somebody. Tell me about a time when you disagreed with a colleague on an outcome and how did you handle it?" They argue that these types of questions better demonstrate competency when a person can show it in action rather than claiming to have it.

When it comes to writing resumes, some skills may need further elaboration than a few words can provide. Learners may need to explain what they mean when they say they are good communicators or know how to use Excel. Jake Hirsh-Allen, Head of Workforce Development at LinkedIn, said this prompts questions about what each "skill" means. For example, "If it is communication, what specifically does that involve? Writing, short writing or long writing? Is it public speaking, or is it speaking in small groups? Once you can get down to that level of granularity, I think it helps people elucidate their own skills in a much more granular, and not objective, but at least concrete manner."

This also applies to traditional college degrees in general. Simply knowing an individual has a bachelor's degree does not convey what was imparted in the classroom or through experiences that do not make it on a transcript. Rob Groot from National Student Clearinghouse explains this by saying, "If you have a bachelor's in economics, you might be somebody who has studied macroeconomics or you might be somebody who has studied accounting or bookkeeping. Those are completely different skills. There might only be a 20% overlap between those skills." One of the challenges we have to face is translating the contents of a learning experience into skills. This extends far beyond traditional degrees and also includes other extracurricular activities that people may be involved in. There are many skills that can be gleaned from participation in things like clubs, churches, sports teams, committees, and other activities that may not traditionally be considered.

Hirsch-Allen pointed out that other life experiences, like being a parent or a refugee, are not typically described as a job, but people can acquire many valuable skills from them. Hirsch-Allen continued that "If you're a parent of five children, you are doing project management every day. You have figured out time allocation every day. You can delegate. These are skills that people are looking for. A refugee with a family of three crossing a border is demonstrating language skills, resilience and perseverance…But because our society doesn't describe that as a job, nobody ever assigns any skills to it."
Another avenue to consider involves individuals who are already in the workforce with years of experience under their belt. New learning and credentials are easily

[113] https://rework.withgoogle.com/blog/google-rule-of-four/

issued, but what about everything people have done already? Jason Tyszko and the T3 Innovation Network have been exploring this with the creation of Experience You, a new initiative to "meet the workforce where they are at today, where there has been a ton of learning and work experience." Prior learning experiences are valuable, especially for individuals who are trying to re-enter the workforce after a period of time, so finding a way to translate that experience into skills is part of the ideal.

Value of Credentials

Another important theme addressed by multiple participants relates to the value of a credential. With the cost and quality of validating credentials becoming a particular challenge, reevaluating the value of credentials will be important to save time and money. A few participants in the nonprofit sector agreed, noting that there are many unanswered questions related to the quality of digital badges. Questions arise surrounding the purpose of each badge, what information it provides, and what the direct benefit is to the individual who earns it. One participant added that it is fairly easy to create new credentials or badges, but one should consider the practicality, relevance, and usefulness of a credential before creating it.

Even though soft skills may not be as easy to measure, they still carry weight in this space. Bledi Taska, Chief Economist at Lightcast, addressed soft skills, saying that "I can teach you technical skills. What I cannot teach you to be is a team player. I think the biggest challenge is not on the technical skills, which most of those micro-credentials are offering, but is actually on the softer skills - cultural fit, teamwork, go-getness." This gets at the assessment of skills as well as the value of particular skills or credentials over others, which naturally varies across disciplines and types of jobs. The value we assign to skills is important to consider when thinking about common languages and standards.

Another employer described using attitude and aptitude tests that are verified by an employer to measure job readiness. For example, if an employee has a good attitude and consistently shows up to work, this information might be more valuable than competencies provided in skills-based hiring. The argument according to this participant is that sometimes being willing to learn and showing up to work may go farther than skills. However, this may vary based on industry and job level, where higher job levels may require more industry-specific knowledge compared to an entry-level job where you can learn as you go.

Equity and Ethical Considerations

Privacy and Ownership

When asked about privacy and data ownership, the majority of participants believe that in order to maximize the potential of an LER, a user must own their data or at least co-own it. Several policymakers and tech providers highlighted self-sovereignty as a key component of this ecosystem. One such person was Nick Moore, the Education Policy Advisor and Coordinator for the Alabama Governor's Office of Education, Workforce, and Transformation. Moore said that "Self-sovereignty is key. And before we got into digital credentials and LERs it almost seemed farcical to have to remind people that you can't take away somebody's learning…Now that question has been opened back up." Moore added that there are times when a credential like an occupational license may need to be taken away for ethical or legal reasons, like a law or medical degree. However, for someone that earns a credential to show mastery of competencies, Moore said "We have to make sure that people own their learning and that the wallet, the credential, is owned by the individual learner, not the credential provider."

Education and understanding one's rights have also emerged as key parts of preserving privacy and ownership. It is important to think about the level of understanding among those who will be using this system. In order for people to make informed decisions about what to do with their information, they should be told how everything works as accurately as possible.

However, some of these concepts are often abstract and difficult to conceptualize. Kerri Lemoie, Director of Technology at Digital Credentials Consortium, said that "We have a long way to go in implementing and also in understanding." Lemoie said that we have a long way to go in terms of making these concepts approachable for others. "Think about SSL certs. You look at our browser and you see the lock in the URL space, and a lot of people know what that means and a lot of people don't, but to some extent, as long as you tell them, 'Look for the green lock,'" Lemoie says that is a good start. This may be as far as it goes for some, but at least you can offer some kind of support to get them started. However, Lemoie also noted that "The standards need to exist so that things like that can be built on top of it."

In addition to knowing what parts of their data are stored, users should be able to understand where their data goes and who has access to it. Companies have created profiles that are proprietary with the employer, in the cloud, or on their systems, which may not always make it clear where a user's profile lives. For Sean Gallagher, this raises questions like "Where does the profile go? Do you have a right to access it? Can you access it? Can you take it with you?"

Deb Everhart from Credential Engine said that "It is not just how the data is generated and held and stored. Do I have access to my own data? Will it be there tomorrow? Are you going to go out of business? But that fundamental question of, why should I trust you? And if we don't have trust networks, then it all falls apart." The ability to trust and understand what a company is doing with data will be critical for users to decide both if and how they want to share their personal information.

Users should also be given the right to hide certain information that might create bias in the hiring process, such as their name or other personal identifiers. This is an attempt to have individuals evaluated based on skills and competencies rather than characteristics. Some have suggested that hiring portals should only display competencies to employers and once an individual is invited for an interview, then contact information and other identifiers may be released. Users should also have the option to choose which competencies they display or do not display at any given time.

Sarah Cacicio, former Senior Project Director at Digital Promise, highlighted this concept when talking to non-traditional learners and potential LER users. She found that many people, especially Black women, voice concerns about displaying their names and other history because they believe employers are "going to judge if [they] didn't go to work for five years because they were taking care of a family member." Many people shared thoughts about wanting the option to control what information they hide or display, and who they share it with.

Potential to Expand Opportunities

As mentioned in previous sections, there are doubts about the effectiveness of skills-based hiring and LER systems in creating more opportunities for workers and learners. Winters commented that "We don't have a lot of firm evidence that the move towards skills or the utilization of digital wallets is going to fulfill the promise of more equitable access and opportunity that we hope it will." Others shared similar sentiments, noting that there are many assumptions made about more equitable outcomes with LERs, but the question of equity remains largely unanswered.

There are currently many gaps in the LER space related to equity, especially around data, access, opportunity, and even quality of credentials. One researcher explained that while there are misconceptions about technology involved, there are also misconceptions in the technical community about equity and bias that are not well grounded in data.

However, just because skills are more visible does not mean that people will perceive them differently. Goger explains further, saying that "You can articulate all you want, but if people have preconceived ideas about the value of those things, it doesn't necessarily mean that they're going to change their hiring practices." For example, people may still value a college degree or a certain qualification over another. Goger notes that if you take the name of the pedigree off and simply compare skills, that may work, but the value we assign to certain credentials will still play a role in hiring practices. An attitudinal shift may be required in order to see desired changes when it comes to LERs and more equity in hiring.

Equitable, Learner-Centric Design

In order to design an ecosystem that considers more equitable and ethical factors, interviewees outlined several key ideas. Policymakers noted that an ecosystem should include structures that meet the needs of communities with the lowest capacity for resources. One nonprofit participant added that this technology is often designed for those in the tech field because they are the ones designing it.

Equitable designs mean making sure that people have access to technical assistance if they need it, ensuring that users know what to do when they have a question. It is imperative to consider all the use cases that an LER ecosystem would need to support. A nonprofit participant emphasized that these conversations should factor in social, racial, cultural, language, and other barriers users may face. If online hiring becomes more mainstream, it is important to consider who would be left out as a result. For example, switching to technology could put people further behind if they do not have reliable access to the internet or to a computer. If digital solutions are not accessible to those who need the most help, then they are further disadvantaged.

Throughout the interviews, the idea of a learner-centric approach was repeated. Nonprofit participants noted that the best advocate for someone's journey is that individual. As a result, several nonprofit organizations and researchers suggest a shift from advising and mentoring to putting learners in the driver's seat of their future. Specifically, one stakeholder emphasized a focus "that is really centering the adult learner and not the typical university student or the university student graduate. How do you center that student's needs and make sure that it is built from the beginning to have value for that person?"

Cacicio shows why it is important to design with the learner in mind. If we do not do this, Cacicio asks the following question, "How can you guarantee that [the learners are] going to 1) use it, 2) that it is going to be relevant to them, 3) that it is even being designed right, with them in mind?" The design must be relevant and accessible to the learner in order to be meaningful. Most people in this space tend to focus on college students, but a large portion of the labor force may have no experience with college. A few individuals emphasized a user-centered design focused on the adult learner or the non-traditional student. Unfortunately, efforts in this area have been fragmented and tend to be more tech-centric than learner-centric.
Another participant explained that if you do not design with the learner, they might not even use the technology. The design must be relevant and accessible to them in order to be meaningful. Most people in this space tend to focus on college kids, but a large portion of the labor force may have no experience with college. A few participants placed special emphasis on a user-centered design focused on the adult learner or the non-traditional student. Unfortunately, efforts in this area have been fragmented and tend to be more tech-centric than learner-centric.

Populations of Interest

This interview process has reinforced our assumptions that the design of an LER ecosystem needs to consider use cases beyond a college-educated traditional learner and worker. Several interviewees provided specific groups that need to be considered in the design including women of color, immigrants, refugees, former inmates, gig workers, blue collar workers, small to medium sized businesses, and those who are not online. Cacicio sees gig workers as an especially important population to keep in mind because "They could be former inmates, high school students, or people coming out of a training program. They tend to be working more than one job, pursuing learning and work at the same time. There's a lot of social stigma to doing gig work even though it is so prevalent."

Kym Lavigne-Hinkley is the Senior Manager for National Career Coaching Initiatives at Markle Foundation. She echoes these considerations, highlighting that "When we think about the different technology that's being created to improve the efficiencies of a variety of stakeholders for individuals, for training providers, for employers, are we considering all of the use cases that the system could potentially support?" Lavigne-Hinkley prompts us to consider who is left out of the equation and why.

According to a few policymakers and nonprofit participants, in order to adequately address equity and inclusion it is important to explore what is needed to support learners who have been disconnected from the current system. Several interviewees, including Lavigne-Hinkley, explained that "We are trying to think about barriers from start to finish for individuals and thinking about the connection from education to career."

TOWARD THE RESPONSIBLE LER ECOSYSTEMS

In this section, we provide a high-level sketch of a responsible LER ecosystem. By responsible LER ecosystem, we refer to an LER ecosystem where users can exercise agency over their data. It also means that the design of the ecosystem is fair to all participating stakeholders. By fairness, we mean the equitable distribution of opportunities, benefits, and resources among all stakeholders, irrespective of their background, race, gender, or socioeconomic status. Fairness ensures that the LER system is transparent, unbiased, and inclusive in its design, implementation, and operation, fostering a sense of trust and promoting participation from diverse individuals, employers, and educational institutions. By emphasizing fairness, the LER ecosystem can create an environment that supports equal access to education, employment, and professional development opportunities, ultimately contributing to social and economic well-being.

At the same time, we must recognize that privacy and data ownership is the only requirement that the LER ecosystem must meet, albeit an important one. We must consider other principles, such as interoperability, scalability, verifiability, transparency, and compliance.

To explore the design possibilities, we held a two-day workshop at Case Western Reserve University on January 13-14, 2023. The full list of the participants is listed in the Appendix. During the workshop, participants developed four different use case scenarios that illustrate different and challenging requirements of the responsible LER ecosystem.

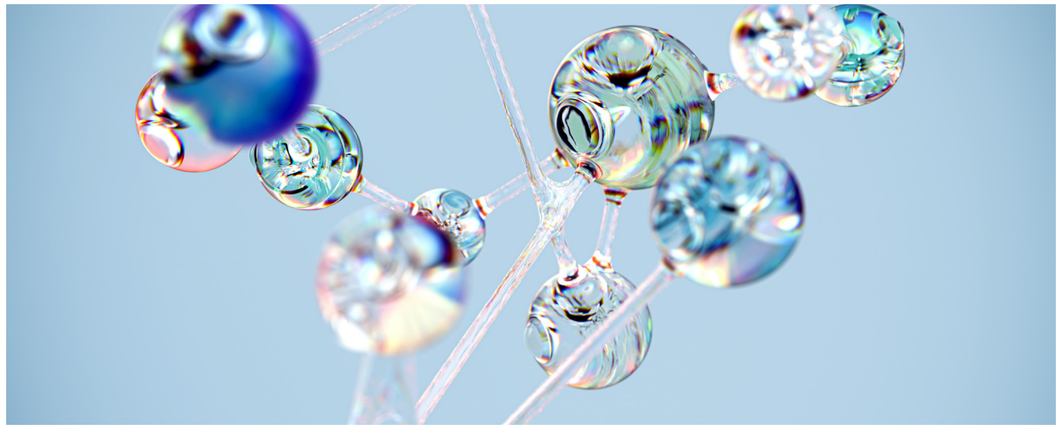
In what follows, we present the four use case scenarios. Then, we will extract different requirements and challenges related to privacy and data ownership from these four scenarios. Reviewing these requirements and challenges allows us to develop ways to extend the traditional trust triangle that underpins the distributed verifiable credential technology. From this analysis, we propose a responsible LER tech stack compatible with the existing LER tech stacks.

Trust Triangle Model

The core trust triangle in the verifiable credential model consists of issuers, holders, and verifiers. The concept of self-covereign identity (SSI) underpins the basic trust triangle model. SSI emerged from the word "self-sovereign," which refers to the authority controlled by the self rather than dependent on any power. This term describes the process as being in more control of an individual party, a shift in control based on the defined data standards and protocols. The self-sovereign provides a crucial solution where the control is shifted to an individual user based on the information that they might be sharing in public.

SSI focuses on privacy, security, ownership, authentication, and verifiability. SSI helps provide more equitable and better solutions to learners, workers, and employers. It will help create a more secure and verifiable ecosystem for learners and workers with the power to share relevant information and for employers to recognize and find the right candidate. The learner and worker will have more authority and control over the information that they might share, not resulting in more sharing or over-sharing.

Verifiable Credentials based on the defined standards and protocols are issued by the verifier to enable the authenticity and validity of the records. Digital Wallets, or data storage, where each agent will have access to act as individual data repositories. Data wallets enable sharing (publicly or privately) and accessibility with other individuals. All the individuals involved have ownership of the data and credentials. Decentralized identifiers (DIDs) for all the agents involved to establish individuality. Each identifier would enable the individual to verify the identity by cryptographic methods. Governance frameworks must be in place for the policies, structures, rules, and regulations. These protocols will incorporate technical, business, and legal frameworks to establish a



trust triangle.

The decentralized SSI model mainly focuses on issuing credentials that act as an interoperable method with other ecosystem participants. The LER ecosystem would comprise the listed participants, including Issuers, Holders, and Verifiers. It also includes Verifiable Data Registry as the backbone of the trust triangle.

- **Issuers:** These entities are responsible for creating and issuing verifiable credentials to individuals or organizations. In the context of education and labor markets, issuers could be educational institutions, certification bodies, or employers. Issuers utilize cryptographic techniques to sign the credentials, ensuring their authenticity and integrity. The issuers are responsible to maintain the proof of their issued credentials. Such proof can be centrally stored or maintained through distributed ledgers. Issuers include Schools, Universities, Employers, Training agencies, Government, and individuals.

- **Holders:** Individuals or organizations who receive and store verifiable credentials are known as holders. These parties are responsible for managing their credentials, deciding when to share them, and presenting them (or parts of them) to verifiers as needed. Holders typically use digital wallets to store and manage their credentials securely.

- **Verifiers:** Verifiers are entities that need to validate the authenticity and accuracy of a credential before relying on the information it contains. In the education and labor market context, verifiers could be prospective employers, universities, or government agencies. Verifiers use the issuer's public key to verify the credential's digital signature, ensuring that the credential has not been tampered with and originates from a trusted source.

- **Verifiable Data Registry:** A data registry is a decentralized, tamper-resistant storage system that plays a crucial role in the issuance, verification, and management of verifiable credentials. It facilitates the secure exchange and validation of data between the three primary entities involved in the trust triangle: issuers, holders, and verifiers. It serves as the backbone of the trust triangle model by providing a reliable and secure means for storing and retrieving critical information required for the issuance and verification of verifiable credentials. This information may include public keys for digital signatures, credential schemas, revocation registries, and other metadata needed to establish the authenticity and integrity of the credentials.

These three actors create a decentralized ecosystem in which trust is established through a combination of cryptography, distributed ledger technology, and standardized data formats. The trust triangle's primary goal is to ensure that verifiable credentials are authentic, tamper-proof, and issued by a legitimate source.

To design a responsible LER ecosystem that respects individual students' and employees' data ownership and privacy rights, we must extend the basic trust triangle to accommodate new requirements. Next, we will outline a set of specific use case scenarios and requirements, followed by a concrete architectural vision of an extended trust model that empowers users to maintain full control over their data.

Four Use Cases

Former Inmate

Daniel is a 55-year-old former inmate who recently went through a reentry program. Daniel has been out of the workforce for 15 years. He finished high school but did not attend college. Daniel previously worked as a construction worker and plans to continue this role temporarily. As Daniel gets older, he would like to find a job that does not involve as much manual labor, but he believes he is not qualified to do much else.

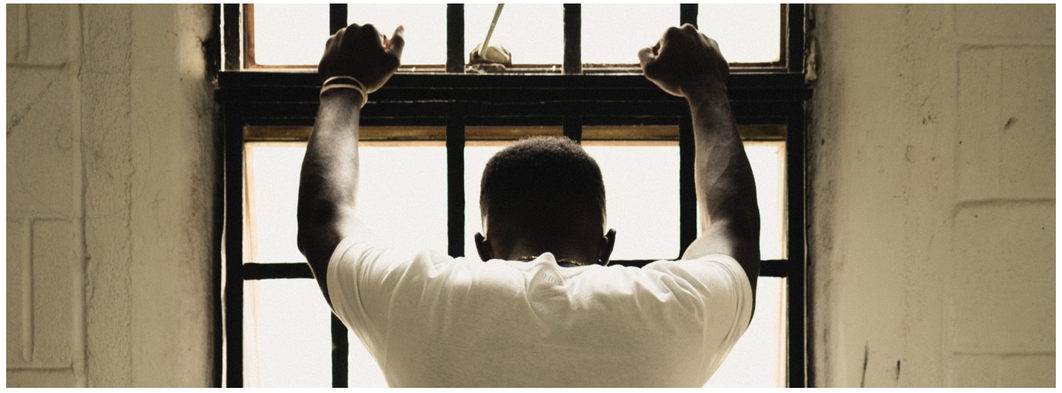
In this scenario, former inmate Daniel is nervous about experiencing discrimination based on the disclosure of his incarceration history. Now that Daniel is no longer incarcerated, he is looking for a way to support himself and move forward in his life as best he can.

Daniel completed a re-entry program at the conclusion of his incarceration which awarded him a certificate acknowledging his successful completion. One of the issues for Daniel is that this credential is associated with his prison time. Daniel may not want employers to see this part of his past unless absolutely necessary because it may harm his ability to get a job or even an interview for a job.

As a result of this potential discrimination, Daniel wants the option to hide his prison time on his LER. However, if he has a credential associated with a re-entry program, an employer would see that and automatically know that he was formerly incarcerated. What does it look like if Daniel tries to hide his history as an inmate while still reaping the benefits of the credential from his re-entry program?

To ensure a fair chance for Daniel in the labor market, we need a solution that allows Daniel to hide his name or other identifying information instead of his incarceration history as a way to mitigate bias. The solution also needs to hide the identity of the issuer so that the potential employer cannot infer his incarceration record from the identity of the issuer.

Since Daniel has been out of the workforce for the last 15 years, he might also struggle to be reacquainted with technology. This could pose challenges, particularly when it comes to creating his LER, knowing what his options are, and understanding how to market himself. Here it might be important to consider the ways that Daniel could receive support, perhaps in the form of advising or career coaching as a way to further support his ability to connect to opportunities.



High School Dropout

Charlie is a 17-year-old boy who recently dropped out of high school. Charlie has no plan to finish high school or attend college. In his free time, Charlie has been teaching himself how to code and taking a few free computer programming courses he found online. Charlie hopes to pursue a career in computer programming but has been told that his lack of degrees might hurt his chances of getting a job.

Charlie's scenario brings in the questions like – What are the reason(s) behind Charlie's decision to drop out of school? Is there something about the high school environment that does not work for him? Is it a financial reason? Is he confident his skills and proficiencies will be enough for a job? Acknowledging the social context of a high school dropout is important because it can influence what he does next. To take the discussion forward, it is assumed that Charlie is interested in finding a job and is in the job market.

Charlie is driven by other interests that may not be covered in high school. As a result, he may not want to spend his time there if he can focus his efforts elsewhere, such as on coding programs. If Charlie does not finish high school, his next step would be to determine what certifications or qualifications are going to be most useful to get a job. Charlie will need to have something in place of a traditional high school diploma that would appeal to employers.

In order to maximize his attractiveness as a candidate, Charlie could start by creating an online persona to showcase the existing skills that he has. This could be a combination of GitLab/Hub profiles or something similar. This allows him to see where he would best fit, how he can play to his strengths, and where to focus current developmental efforts. One challenge for Charlie will be learning how to express skills that jobs need, especially since it can change so drastically from one job to the next.

At this point, the role of a mentor or mentoring agency will come critical. The mentor/ agency can introduce him to a job of the least resistance, like gig work in the likes of Google SEO or some low-hanging fruit in UpWork etc. From there he could leverage his new portfolio of work and new digital personas along with social capital to aim for more aspirational positions like Analyst, Developer, Programmer etc. A coding bootcamp can also help in fast tracking this journey. The importance of creating the opportunity of the smallest increment possible can help Charlie from a financial perspective as well as personal motivational lines.

If the LER here can be made accessible to the mentoring agency, they could better understand Charlie's skills and help him to develop them. This can go beyond the certifications and online programs, or getting in his efforts outside the 'standard' that are not documented into the LER. Here, it is critical to deconstruct the skills in the programs or job roles Charlie has attended or can apply to. The extent to which LER can provide this clarity would aid someone of Charlie's capabilities and background. Ultimately, it would be ideal if an algorithm developed by a reputable institution or agency could issue verifiable credentials vouching for Charlie's technical competencies based on his records.

This scenario brings to light the questions of access to LER or the points of entry for someone like Charlie to be introduced to the system. Once introduced, the potential to use LER to validate his skills and be more visible in the job market is very significant. One could also look at the community support programs that reach out to school dropouts as a suggested point of entry. Programs like the cybersecurity professional certificate which has a well-developed framework, can be a right fit for Charlie to enter the workforce. Furthermore, an LER ecosystem that can provide algorithmic career advice, leveraging a knowledge graph, can help Charlie navigate the career space.

Stay-at-Home Mom

Alex is a 34-year-old woman who graduated from college with a bachelor's degree in business. Alex accumulated a string of professional experiences before giving birth to her son. Alex has been out of the workforce since her pregnancy 4 years ago. Despite not working for a few years, she has still developed soft skills like patience, resourcefulness, and time management. As her son gets closer to school age, she wants to pursue a new career in human resources. Alex is struggling to keep up with other competitive applicants and is not sure how to market her current skills and knowledge.

The case of a stay-at-home mom, Alex, is unique because Alex has been out of the workforce for some time, but she has been developing soft skills that come with raising a child and maintaining a home. One of the problems is that no one can verify Alex's claims, so they are self-assertions. What makes the self-assertions credible? Or even claims from someone she knows, validating her statements?

Alex might be able to link claims that then might be verified by someone else. This could be a piece of evidence from a person or from a digital object that she might link to. For example, perhaps she took on a leadership role at the parents' advisory board at her son's school, and there is a video of her speaking at a school board meeting. Alex could use artifacts to add evidence to her claims. Alex would need to identify and justify the claims she is talking about, and providing evidence to associate with her claims could help strengthen her profile.

It would be beneficial for Alex to stay involved in activities even as a stay-at-home mom that could later help her make self-assertions or add to her list of skills and competencies. Being involved in her child's school would help her continue to build skills and add to her knowledge base, even if it is not a formal job. By participating in the community or activities outside of being a stay-at-home mom, Alex sets herself up for success because people at these organizations or involved in the community could certify things that she has been doing during her time "at home." However, it is important to recognize that not everyone has access to these kinds of resources and opportunities outside of the home.

Another issue Alex might face is the fact that many employers might see the gap on her resume and automatically screen out her application. Employers often do not like to see gaps that go on for a few years, which is the case for Alex since she gave birth and was out of the workforce. One solution to this could be presenting the duration of her time in a particular position rather than the chronology of experiences.

For example, instead of saying that she was employed between 2016 to 2019, she might instead say that she was employed for 3 years. When anyone takes time off from work, including stay at home parents like Alex, it likely means that skills are not up to date. Is it possible to create a program that can bring the unemployed up to date in terms of skills?

In examining these use cases it is important to acknowledge the role of social capital. Many people are able to find jobs because of connections to others, which is evidenced by the success of networks like LinkedIn. As a result, it can be very hard to get a job without that social support network. LERs are a tool that we can use to evolve and help us with this, but it does not solve all of our problems.

Small Manufacturing Company

James is the president of a small manufacturing firm in Ohio. He is seeking to hire a machinist to operate a computer numerical control (CNC) machine. James has been comparing two candidates, one with technical experience with CNC machines, but references say he was often late to work or did not show up. The other candidate's references supported his work ethic and good attitude but noted that the candidate lacked technical skills. James is debating whether to hire the candidate who already has technical experience but a poor work ethic or the one with strong soft skills that he could potentially train and keep on staff longer.

James is facing limited resources as an owner of a small manufacturing company. This makes it difficult to have dedicated HR personnel to handle the hiring procedure for a machinist who is proficient in using CNC machines. The company does not have enough recruiters or a sophisticated HR system to effectively review many applications.

The procedure can be made simpler with the help of an effective LER system, which can quickly examine structured online application forms and individual resumes and present possible matches to the employer. A pre-review by LER can still save time, even for larger businesses with adequate HR personnel. LER can also suggest potential applicants from its database who are a good fit for the position but may not have been aware of the opportunity.

Using LERs to decide which candidate to hire would be useful and potentially make the process easier. However, it could also create more challenges because these decisions often require human expertise and intervention to make the final choice. Assessing if a person has a good work ethic can be difficult especially if this individual is joining the professional workforce for the first time. It may be hard to provide data on their work ethic unless they have other experiences that could provide verification. For example, if this individual went to high school or college, registrars in those educational institutions may have information of the student's attendance which could validate their consistency and work ethic. Thus, there is an opportunity in the LER space for Registrar Apprenticeship.

After employment, LERs also track any skill and experience updates of users. This helps employers evaluate employees' performance over time and provides convincing evidence while considering the promotion of employees. On the employees' side, LERs can suggest beneficial online training and workshops that may help build up experiences in the employee's current position. If they want to switch career paths, an LER also recommends close-match positions based on their skill sets and lists all the skills that need to be learned for their preferred job.

In this scenario, it is important to consider what the benefits are for the employer and the employee. The employee can potentially be upskilled and provided with training in some cases. The employer can retain more workers that they train and hire more employees who are attracted to the job because of additional training offerings. However, unless the employer is ready to recognize these soft skills and can offer training, it is likely not going to happen. The question would be: For credentialing, will the employers have any incentives in providing credentials to employees?

Due to their narrower reach than other companies that might draw more qualified candidates, HRs at medium-sized manufacturing companies will have a difficult time locating qualified candidates. The HR department of this organization may have to think about upskilling any available candidate to fill the role if there aren't many interested applicants. Finding talent and keeping staff will be this company's two biggest hiring concerns.

LER can be a helpful tool for workers to advance in their jobs. It is not just limited to showing their prior experience; it may also present chances for skill development and career advancement. The LER includes information on comparable career paths and suggestions for training programs that can assist staff members in gaining new skills and knowledge. This enables people to actively seek out new employment prospects and take charge of their own professional development. This can then result in better job performance, greater job satisfaction, and more opportunities for growth both inside the company and on the job market. Employees can stay ahead of the curve and continuously advance their skills and experience by using LER as a career advancement tool.

Design Requirements for The Responsible LER Ecosystem

To develop responsible LER ecosystems that meet the requirements of the four use cases, we identify a set of key design requirements. We begin with key stakeholders of the responsible LER ecosystem. Then, we identify a set of specific requirements and specific use case cases for each of those requirements. We propose three layers of verifiability to specifically support these requirements.

Key stakeholders in a responsible LER ecosystem include employers, employees, educational institutions, governments, and other key stakeholders, such as industry associations and professional organizations. Each of these stakeholders has their own key interests in the LER ecosystem:

1. Employees: Employees are interested in controlling their own information and deciding who has access to it, as well as in having a secure and transparent system for managing and sharing information about their qualifications and experience. This helps to promote job mobility and career advancement, and to ensure that employees have control over their own personal and professional information.

2. Employers: Employers are interested in having access to accurate and up-to-date information about the qualifications and experience of job candidates, in order to make informed hiring decisions. They also have an interestin maintaining the privacy and security of their own information, as well as the information of their employees.

3. Educational institutions: Educational institutions are interested in having a system for managing and sharing information about the academic achievements of their students, and in ensuring that this information is accurate and up-to-date. This helps to support the development of informed and effective educational policies and programs, and to promote the recognition of academic achievement across different educational institutions and settings.

4. Governments: Governments are interested in using the LER ecosystem as a tool for tracking and managing information about the qualifications and experience of their citizens, in order to support the development of effective and efficient labor markets. This helps to support informed policy making, and to promote the development of effective and efficient labor markets that benefit both employers and employees.

5. Industry associations and professional organizations: Industry associations and professional organizations are interested in using the LER ecosystem as a tool for tracking and managing information about the qualifications and experience of their members, in order to support the development of effective and efficient labor markets within their respective industries and professions. This helps to promote the recognition of professional achievement and to support the development of informed and effective industry and professional policies and programs.

To meet the needs of these stakeholders for the responsible LER ecosystem, we need the following set of requirements.

1. **Interoperability and Flexibility:** The ecosystem must support seamless integration and communication among diverse credentialing systems constituted by multiple trust triangles, allowing users to share credentials across platforms without being locked into a single standard.

   Use Case: A student with credentials from multiple institutions needs to share them with a prospective employer. They should be able to selectively disclose information from each credential, regardless of the issuing institutions' standards.

2. **Decentralized Data Storage and Control:** A decentralized data storage must be managed by a data agent representing the user to ensure user's control over data. This agent should establish off-chain peer-to-peer communication channels using a DIDcomm protocol which offers native support for selective disclosure and credential management.

   Use Case: An employee wants to share their credential with a prospective employer without disclosing their entire credential history. The decentralized data agent allows selective sharing in a verifiable way (i.e., the shared partial credential can still be verified through the issuer) without exposing unrelated information.

3. **Self-Sovereign and Derivative Verifiable Credentials:** Users should be able to create their own verifiable credentials using existing credentials or raw digital trace data, with the original source verifiable through a chain of trust.

   Use Case: A professional combines their academic degree with their work experience to create a new credential, using the original credentials as evidence while maintaining a verifiable chain of trust.

4. **Revocation and Control:** Users should be able to revoke shared credentials. This dynamic access control allows users to maintain ownership of their data even after sharing it with others. Similarly, an issue should be able to provide time-sensitive credentials that expire after a certain amount of time.

   Use Case: A job applicant shares their credentials with a company but later withdraws their application. They can revoke the shared credentials, ensuring the company no longer has access to their data.

5. **Heterogeneous Data Sources:** The ecosystem should support various data sources, enabling users to collect and curate diverse trace data that demonstrates their competencies and skills.

   Use Case: A software engineer showcases their problem-solving skills and teamwork ability, in addition to their programming expertise, by collecting trace data from online coding platforms, project management tools, and feedback from colleagues.

6. **Extended Chain of Trust:** Users should be able to share verifiable credentials without disclosing private information or the identity of the issuer. Instead, the verifier trusts the credential based on the endorsement of another disclosed institution.

   Use Case: A former inmate with a coding credential from a re-integration agency prefers not to disclose the issuer's identity. Instead, they demonstrate that the issuer is certified by the state government, which can be disclosed.

Three Layers of Verifiability

To ensure a secure and trustworthy responsible LER ecosystem, we propose the incorporation of three layers of verifiability. These layers are designed to verify the identity of communicating agents, the data being shared, and the sharing transactions themselves. In this section, we will discuss each layer of verifiability, their significance in the extended trust triangle, and the considerations for implementing them in a privacy-preserving manner.

1. **Verifiability of Identity:** The first layer of verifiability focuses on verifying the identity of agents (e.g., holder, issuer, and verifier) involved in peer-to-peer communication using DIDComm. To achieve this, both agents must be registered on the same foundation registry within the responsible LER ecosystem. This shared registry ensures that communication is only established between verified agents, fostering a secure and reliable exchange of information.

2. **Verifiability of Data:** The second layer of verifiability concerns the data itself. Issuers can use different W3C-compliant blockchains to issue verifiable credentials. Each credential should include specific information about the blockchain used, allowing the receiving agent (i.e., verifier) to verify the content. Since the DIDComm protocol wraps this information, it does not need to be aware of the individual verifiable credential protocol. This layer ensures that the data being shared is authentic and trustworthy.

3. **Verifiability of Transactions:** The third layer of verifiability involves recording sharing transactions in a distributed registry. This layer entails registering the hash value of each transaction in the registry. However, this practice can create privacy threats, as it may expose sensitive information about users and their sharing activities. For instance, if a particular transaction of a user (holder) is linked to the real identity of the user, all previous transactions of the users can be deanonymized. Therefore, it is advisable to avoid including this layer of verification unless absolutely necessary.

Considerations for Implementing the Three Layers of Verifiability include:

- **Privacy Preservation:** When implementing the layers of verifiability, it is essential to consider the privacy implications for users. As mentioned earlier, the third layer of verifiability can pose privacy threats and should be avoided unless requried. The other layers should be designed and implemented with privacy-preserving measures in mind, ensuring users' data and identities remain protected.

- **Interoperability:** To facilitate seamless communication and data sharing among various agents, the layers of verifiability should support interoperability. This can be achieved by adopting standardized protocols, such as DIDComm, and ensuring that all agents are registered on the same foundation registry.

- **Flexibility and Adaptability:** The responsible LER ecosystem should be designed to accommodate different verifiable credential protocols and blockchain technologies. This flexibility allows for the integration of various data sources and credentials, catering to the diverse needs of users, issuers, and verifiers.

Incorporating three layers of verifiability in the responsible LER ecosystem is essential to ensure the security, trustworthiness, and reliability of data sharing and communication. By verifying the identity of agents, the authenticity of data, and selectively employing sharing transaction verification, the ecosystem promotes a secure and privacy-preserving environment for all parties involved.

Architectural Vision for the Extended Comprehensive Trust Model (ECTM)

Based on our research, we propose an architectural vision for the extended comprehensive trust model as the foundation of the universal responsible LER ecosystem. The ECTM includes the following components:

1. **Decentralized Data Agent:** Represents the user, managing their credentials, establishing secure off-chain communication channels, providing selective, yet verifiable, disclosure, and creating and managing self-sovereign and derivative credentials.

2. **Decentralized Data Storage:** A secure, private storage system under the user's control, ensuring data ownership and privacy.

3. **Chain of Trust:** A mechanism to verify the original sources of self-sovereign and derivative credentials, ensuring their authenticity and integrity.

4. **Off-Chain Data Sharing:** A system for sharing verifiable credentials without tracking, preserving privacy while maintaining verifiability.

5. **Interoperability Layer:** A set of protocols and standards that facilitate communication and integration among diverse credentialing systems.

6. **Data Ingestion and Integration Layer:** Facilitates the collection and integration of diverse trace data from various sources to create a holistic view of users' competencies and skills.

7. **Data Transformation and Analysis:** Tools and algorithms to process, analyze, and extract insights from heterogeneous data sources, enabling users to create comprehensive self-sovereign and derivative credentials.

8. **Data Source Verification Mechanism:** A mechanism to verify the authenticity and reliability of trace data sources, ensuring the trustworthiness of credentials created using such data.

9. **Endorsement Mechanism:** A system that allows issuers to be endorsed by other institutions, enabling users to share verifiable credentials with an extended chain of trust without disclosing the issuer's identity.

10. **Selective Disclosure of Verification:** The decentralized data agent should enable users to selectively disclose verifiable credentials without revealing the issuer's identity or the user's private information.

11. **Decentralized Reputation System:** A decentralized reputation-based trust system to evaluate and manage the trustworthiness of issuers, verifiers, and credential holders mechanism to verify the authenticity of endorsements, ensuring the disclosed institution endorsing the issuer is trustworthy and reliable. It has the following components:

    a. **Reputation Scoring:** Develop a scoring mechanism that assigns reputation scores to issuers, verifiers, and credential holders based on their activities and interactions within the ecosystem. The scoring system should be transparent and take into account factors such as the number of credentials issued, verified, endorsed, and revoked.

    b. **Reputation History:** Maintain a history of each entity's reputation scores over time, allowing users to track changes in reputation and identify trends. This history can be stored in a decentralized manner, ensuring data integrity and transparency.

    c. **Endorsements:** Allow entities to endorse one another, further enhancing the reputation system. Endorsements from reputable organizations can significantly impact an entity's reputation score, making the trust network more reliable and robust.

    d. **Reputation Auditing:** Implement auditing mechanisms that periodically evaluate the reputation system's accuracy and fairness. These audits can be performed by independent third parties or through a decentralized consensus process.

    e. **Reputation-based Trust Decisions:** Enable users to make trust decisions based on the reputation scores of the entities involved. Users can set their own reputation score thresholds for issuers, verifiers, and credential holders, ensuring they only interact with trustworthy entities.

    f. **Dispute Resolution:** Establish a dispute resolution mechanism for situations where an entity's reputation score is challenged or questioned. This process should be transparent, unbiased, and involve multiple parties to ensure fairness.

Design Patterns of Responsible LER Ecosystem based on ECTM Architecture

In this section, we provide a set of design patterns (DP) for responsible LER ecosystems, starting with the simplest pattern toward progressively more complex ones.

DP1: Basic Decentralized Storage and Agent

As shown in Figure 1, in this simple design pattern, each user has a single data wallet, a decentralized data store, and a decentralized data agent. The data agent manages the decentralized identity, verifiable credentials, and the decentralized data store, which stores the credentials. The agent can establish secure off-chain communication channels using DIDComm protocol. This pattern offers single-platform native credential management with a single trust network.

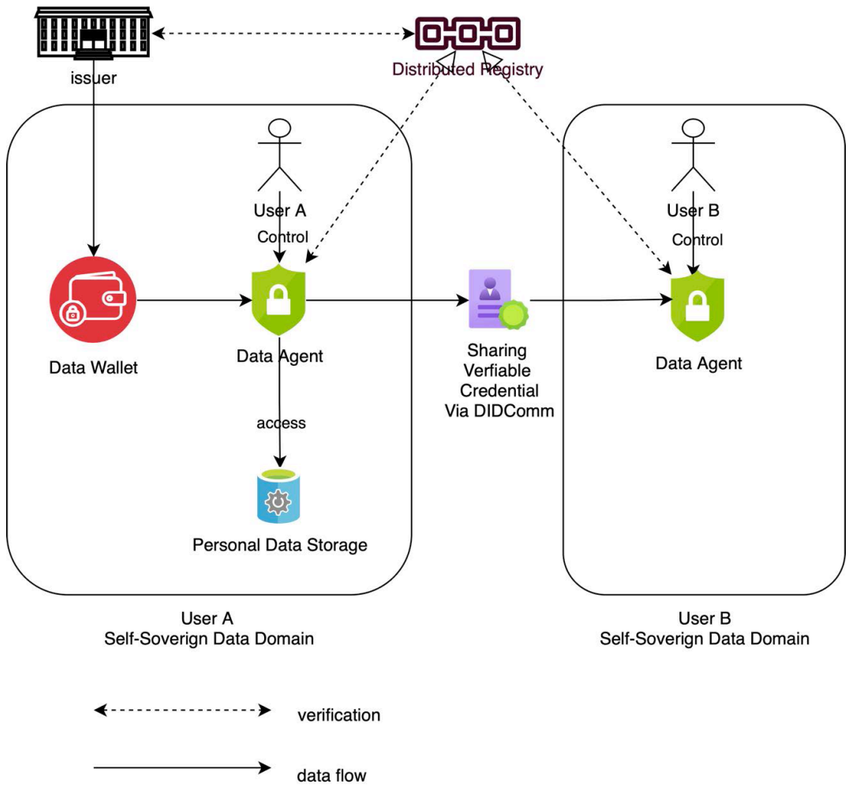


Figure 1. Design Pattern 1 of ECTM

DP1a: Basic Decentralized Storage and Agent with Centralized Service Providers

In this variant of DP1, in addition to individual users who own and control their verifiable credentials through data agents, there are service providers with a centralized architecture as shown in Figure 2. Each service provider has its own agent who negotiates with users' data agents to receive users' credentials via off-chain communications.

The agent of the service provider interacts with a single trust network natively. This design pattern is beneficial when centralized service providers, such as employers using centralized enterprise HR systems or government agents collecting employment or skill data, must interact with the decentralized identity ecosystem. It allows these service providers to leverage existing infrastructure while participating in the self-sovereign identity space.

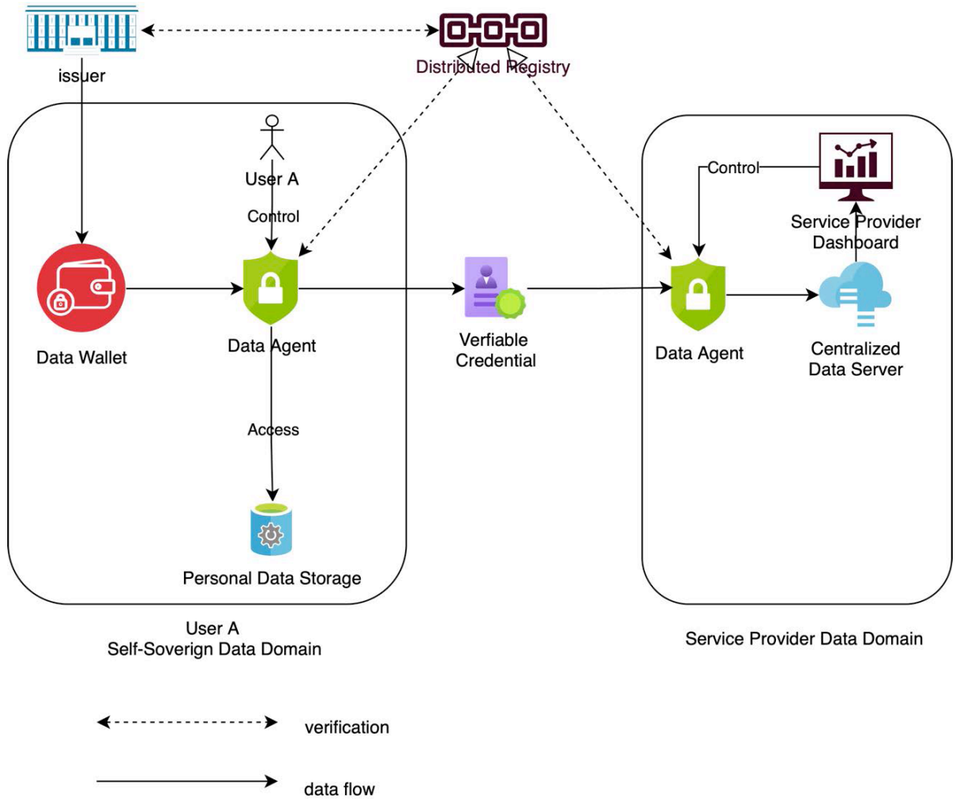


Figure 2. Design Pattern 1A of ECTM

DP2: Interoperable Heterogeneous Trust Systems

Building upon the basic decentralized storage and data agent, this design pattern as shown in Figure 3 introduces an interoperability layer. This layer consists of protocols and standards that facilitate seamless communication and integration among diverse trust networks, allowing users to share credentials across platforms without being locked into a single standard. In this design pattern, all user agents are under the same distributed registry. However, the user agents can interact with multiple data wallets belonging to different trust networks through an interoperability layer. This layer extracts signifiers of the particular trust network and generates extended verifiable credentials that embed the original verifiable credentials. Through the DIDComm protocol, data agents can ensure that the original verifiable credentials have not been tampered with since their issuance. Upon receipt, the receiving agent can decouple the original verifiable credentials from the extended verifiable credentials to perform verification of the original credentials. The interoperability layer can be established using Verifiable Credential API (VC-API), Credential Handler API (CHAPI), or OpenID Credentials (OIDC).

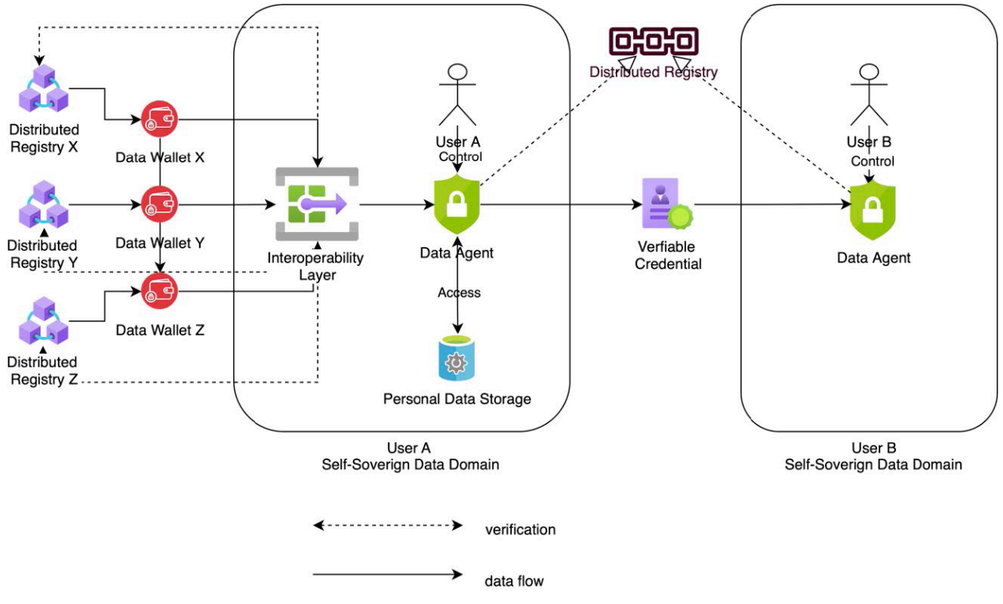


Figure 3. Design Pattern 2 of ECTM

DP2a: Interoperable Heterogeneous Trust Systems with Centralized Service Providers

This is a variant of DP2. In this design pattern, as shown in Figure 4, in addition to a data agent with an interoperability layer that allows it to control multiple data wallets, there are service providers with a centralized architecture. The agents of service providers will include an interoperability layer to enable interaction with heterogeneous trust networks.

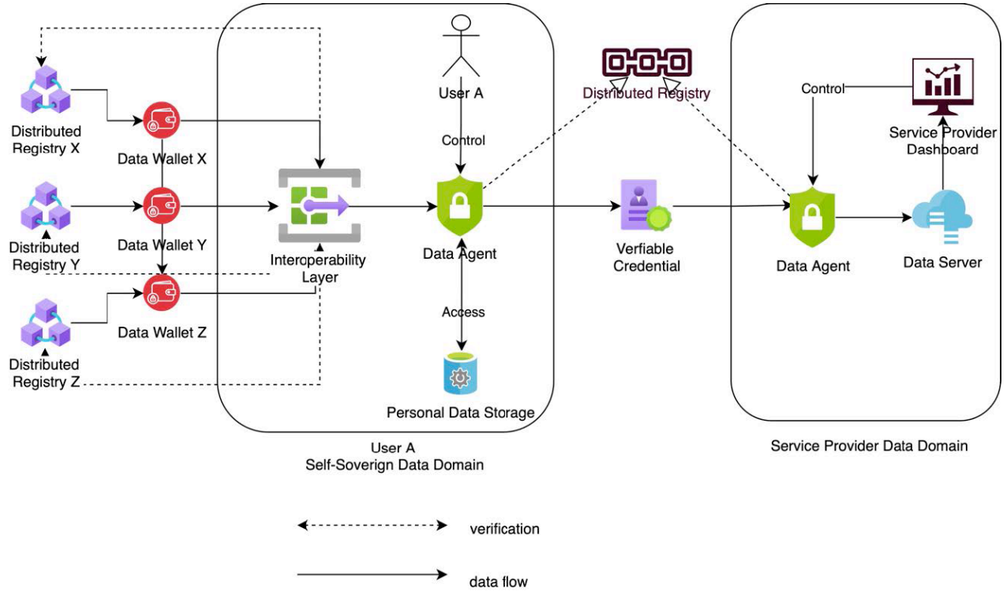


Figure 4. Design Pattern 2A of ECTM

DP3: Multisource Data Ingestion and Integration

This design pattern (shown in Figure 5) extends DP2 by adding a data ingestion and integration layer from multiple data sources. This layer facilitates the collection and integration of diverse trace data from various sources, enabling users to create comprehensive self-sovereign and derivative credentials that showcase their competencies and skills. In this use case scenario, a user may have trace data from an online education streaming service and different eBook platforms. Upon completion of the courses and reading several eBooks, the user's agent can issue verifiable credentials based on the completion of the courses and books. In this design pattern, the agent of a user controls three additional layers: the data ingestion and integration layer, the data source verification layer, and the data analysis and transformation layer. The data ingestion and integration layer allows the user agent to interface with various sources of user trace data on behalf of the users. The data source verification mechanism layer ensures that the trace data from the source has not been tampered with, providing an additional layer of verification for the self-sovereign credentials. Finally, the data transformation and analysis layer contains models provided by the third-parties to process the trace data, generating deviative verifiable credentials from the multiple trace data by the user agent. In this design pattern, third-party models are provided by trusted government agencies, education institutions, or other reputable organizations. These entities can inspect user-generated data from various sources and provide independent verifiable credentials on behalf of the users. These third-party models issue verifiable credentials and derivative credentials based on the user trace data and other verifiable credentials that the user stored in the distributed data store.

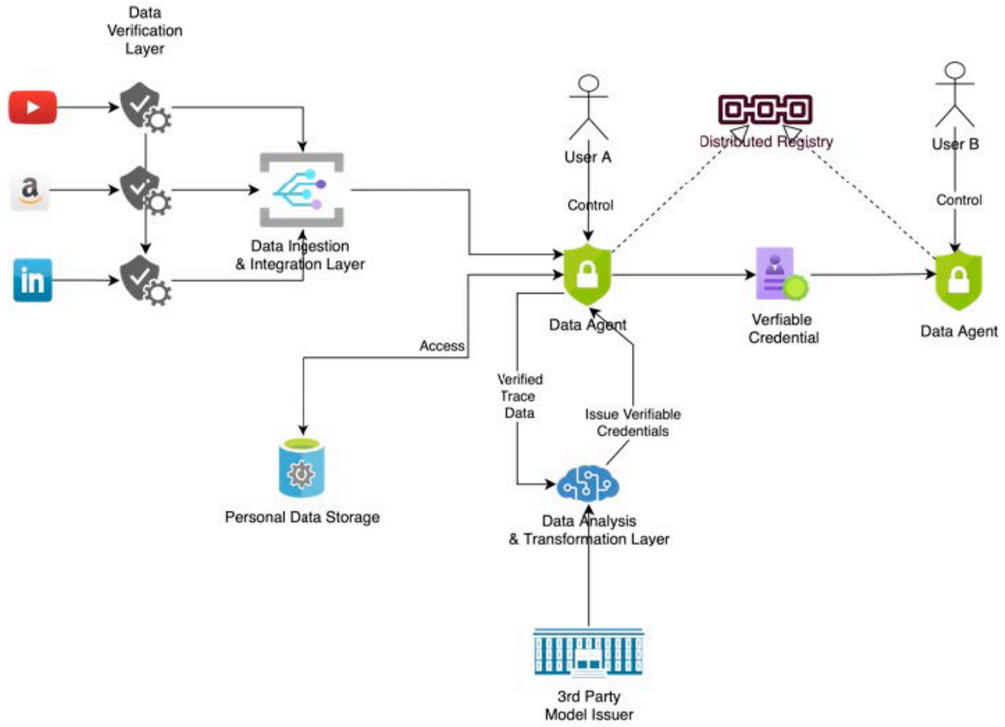


Figure 5. Design Pattern 3 of ECTM

DP4: Advanced Trust Mechanisms with Endorsement and Verification

In this complex design pattern as shown in Figure 6, we introduce advanced trust mechanisms, including chain of trust through endorsement mechanisms and selective disclosure. The chain of trust verifies the original sources of verifiable credentials issued by anonymous issuer, ensuring their authenticity and integrity. When users present verifiable credentials without the identity of the issuer, the user agent establishes a chain of trust by verifying that the anonymous issuer is endorsed by a third-party, such as a government agency, education institution, or other reputable organization, whose reputation and identity are established. The endorsement mechanism allows issuers to be endorsed by other institutions, enabling users to share verifiable credentials with an extended chain of trust without disclosing the issuer's identity. Additionally, the decentralized data agent should enable users to selectively disclose credentials without revealing the full information, providing maximum privacy control. In this case, the user agent can provide a trust response to a verifier's challenge, showcasing the source endorsement without revealing the full credential details. The selective disclosure can be strengthened by showing multiple sources of endorsement and credentials that provide affirmative responses to trust challenges.

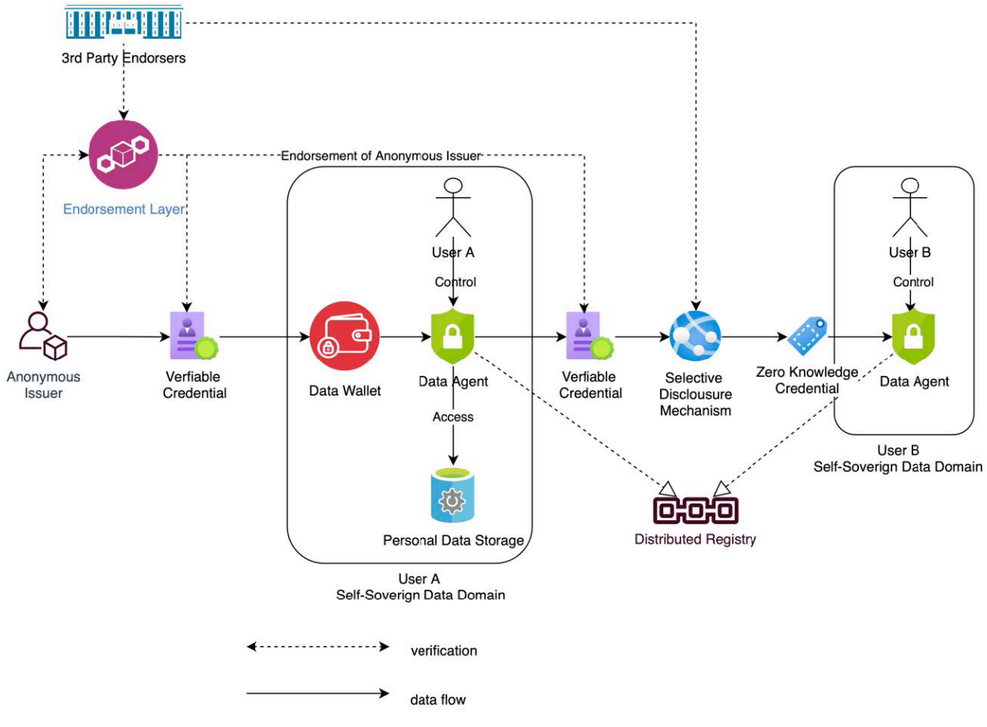


Figure 6. Design Pattern 4 of ECTM

DP5: Reputation-Based Responsible LER Ecosystem

In this design pattern as shown in Figure 7, we introduce a reputation-based trust system to evaluate and manage the trustworthiness of issuers, verifiers, and credential holders. The reputation system can be based on various factors, such as the history of issued credentials, successful verifications, and endorsements from other reputable organizations. By incorporating a reputation system, users can better assess the trustworthiness of the entities involved in the decentralized identity ecosystem.

The implementation of a reputation-based responsible LER system would require an additional distributed reputation ecosystem, which is beyond the scope of this report. However, a decentralized reputation ecosystem can be created using distributed ledger technology to ensure transparency, tamper-resistance, and fairness. Such an ecosystem would consist of: Decentralized Reputation Database, Decentralized Reputation Scoring Engine, Decentralized Endorsement Registry, Decentralized Reputation Auditing Component, and Decentralized Dispute Resolution Mechanisms.

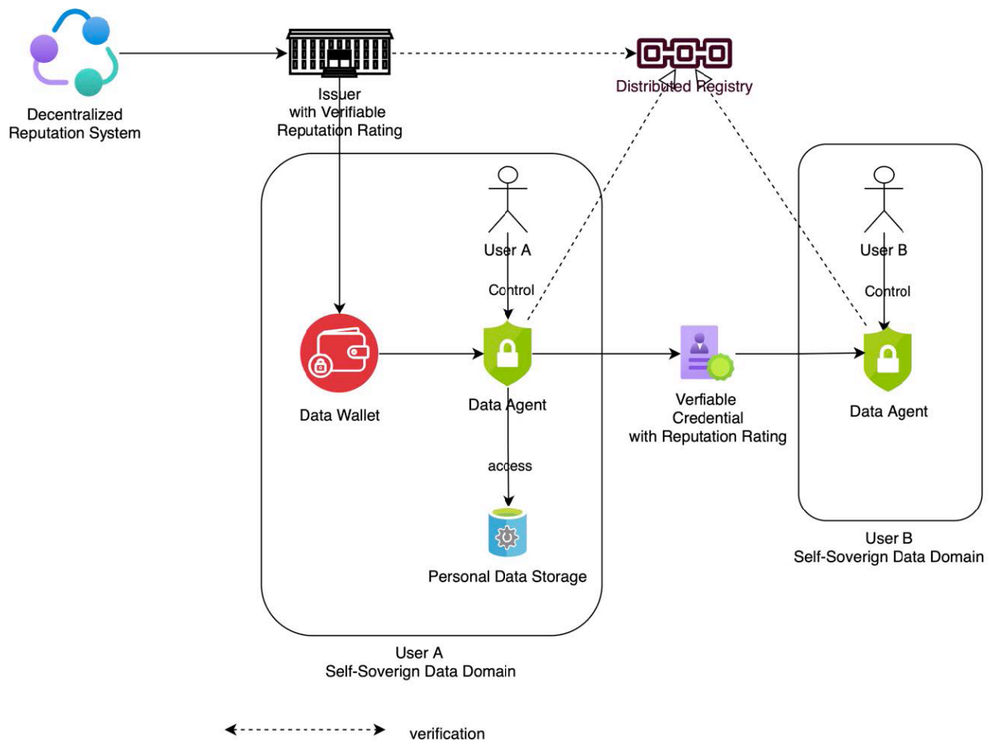


Figure 7. Design Pattern 5 of ECTM

Legal Considerations in Designing ECTM for Responsible LER Ecosystems

In this section of the report, we will discuss the legal aspects of data ownership and privacy control in the context of a responsible LER ecosystem. We will examine two approaches: the container-centric approach, which focuses on creating a legally owned and controlled container for users' digital data, and the agent-centric approach, which employs an agent to provide persistent control over data sharing and usage on behalf of the user. We will elaborate on the benefits and implications of adopting the agent-centric approach in the extended trust triangle.

Container-Centric vs. Agent-Centric Approach

Container-Centric Approach: This approach entails creating a legally owned and controlled "container" for users' digital data. By establishing legal contracts as part of the access control, the container-centric approach ensures legal ownership of digital data. However, this method may be more rigid and restrictive, potentially limiting users' control over their data.

Agent-Centric Approach: In this approach, an agent provides persistent control over data sharing and its use on behalf of the user. The agent ensures data use rights through peer-to-peer DIDComm-based data sharing and revocation. Since the agent is agnostic to specific protocols of individual verifiable credentials being shared, it offers an interoperable sharing protocol. This approach allows users to maintain greater control over their data and its usage, facilitating a more flexible and privacy-preserving environment.

Advantages of the Agent-Centric Approach

Interoperable Sharing Protocol: In the agent-centric approach, the sending and receiving agents can share data off-chain through a common protocol, promoting interoperability among various verifiable credential standards. This allows users to share their credentials seamlessly with different verifiers and issuers without being locked into a single standard.

Legal Protection for Data Sources: Service providers, such as Facebook, can share user trace data without fearing that third parties may exploit the data they provided. Users will only share derivative data in the form of self-asserted verifiable credentials, created from the raw data. As a result, service providers maintain control over their proprietary data, while enabling users to create self-sovereign credentials.

Expressive Consent for Verifiable Credential Sharing: Data sources that directly share verifiable credentials with users
do not face legal issues, as their intent is to grant users the verifiable credentials with an explicit consent for them to share with third parties. This ensures that users can legally share their credentials while respecting the rights of the data sources.

Legal Considerations for Implementing the Agent-Centric Approach

Defining the Rights and Responsibilities of Agents: To ensure the legal validity of the agent-centric approach, it is necessary to define the rights and responsibilities of the agents involved. This includes outlining the scope of the agent's authority, the degree of control they can exercise over data sharing and usage, and the legal implications of their actions.

Ensuring Compliance with Data Protection Regulations: The agent-centric approach must comply with relevant data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA) in the United States. Compliance measures may include implementing appropriate data security measures, obtaining user consent for data processing, and providing mechanisms for users to exercise their data rights.

Addressing Liability Issues: Legal issues related to liability must be addressed in the agent-centric approach, particularly in cases where agents might be held responsible for actions or decisions made on behalf of the user. Establishing clear liability guidelines and limitations can help mitigate potential legal risks.

Incorporating the agent-centric approach into the responsible LER ecosystem offers several advantages, including interoperable sharing protocols, legal protection for data sources, and expressive consent for verifiable credential sharing. By adopting this approach, users can maintain greater control over their data and its usage, while ensuring legal compliance and protection of all parties involved.

However, implementing the agent-centric approach also requires addressing several legal considerations, such as defining the rights and responsibilities of agents, ensuring compliance with data protection regulations, and addressing liability issues. Stakeholders must collaborate to establish clear guidelines and protocols that uphold users' rights and comply with relevant legal frameworks.

The agent-centric approach, as part of the extended trust triangle, supports a more inclusive, secure, and trustworthy digital landscape for all parties involved in the education and labor markets. By empowering users to maintain control over their data, this approach fosters a responsible LER ecosystem that respects individual data ownership and privacy rights while promoting data interoperability and flexibility. Through collaboration and adherence to legal guidelines, stakeholders can successfully implement the agent-centric approach to create a more equitable and transparent digital environment in the education and labor markets.

CONCLUSION

We are at a pivotal juncture in history. The global labor market, continuously shaped and reshaped by historical forces, faces the dawn of a new era. With the swift pace of digital technology development and the consequential shifts in work demands and structures, we are presented with a pressing need for a robust system that can keep pace with these changes. The age of digitalization, coupled with the rising need for specific skills and competencies aligning with the future of work, necessitates an innovative rethinking of our current labor market infrastructure. Our response to these challenges comes in the form of a universal responsible LER ecosystem.

Underpinned by the Extended Comprehensive Trust Model, the proposed LER ecosystem forms a solid foundation for data ownership and privacy. This model emphasizes the power of individuals, granting them full control over their personal data. As an innovative approach to verifying credentials, this model operates on a decentralized, privacy-focused basis, using technology to ensure data integrity and verifiability. It is a solution tailored to the evolving needs of the labor market, a significant stride toward accommodating a digitally-driven economy.

In this context, the LER ecosystem is key to three algorithmic aspects integral to the future labor market: algorithmic credentialing, algorithmic matching, and algorithmic allocation. The incorporation of these algorithmic mechanisms can substantially enhance labor market efficiency, augmenting the effectiveness of job matching and skill allocation, and encouraging greater equity. Through this integration, the LER ecosystem evolves to respond to both present and future needs, creating a dynamic and adaptive labor market.

Algorithmic credentialing democratizes the accreditation process, eliminating barriers and acknowledging a wider range of skills and competencies. Algorithmic matching refines the efficiency and accuracy of job placements, aligning individuals with opportunities that best reflect their unique skill sets. Algorithmic allocation optimizes resource usage within organizations, ensuring effective task distribution.

However, to successfully implement this ecosystem, active collaboration and participation from all stakeholders are essential, including policymakers, employers, educational institutions, and the technology community. As such, we present the following recommendations:

For Policymakers: Actively encourage and support initiatives focused on developing and standardizing the LER ecosystem. Promote data privacy, ensure information integrity, and guarantee equal access to opportunities for all. Furthermore, formulate policies incentivizing employers and educational institutions to restore the ownership of LER records to users.

For Employers: Adopt the LER system and leverage the insights it offers about prospective employees. Utilize the enhanced ability to verify credentials and identify skills that align with organizational needs. In acknowledging that an effective LER system can not only improve equity but also efficiency and effectiveness of existing employees, employers should actively integrate LER into their enterprise systems.

For Educational Institutions: Embrace the LER ecosystem as the new standard for verifying and issuing credentials, providing students with ownership of their data and a comprehensive record of their learning journey to enhance their employability.

For the Technology Community: Persistently innovate and enhance the LER ecosystem's technological capabilities, ensuring the system remains secure, reliable, and user-friendly. A particular area of opportunity lies in enhancing interoperability between not only different LER solutions, but also with existing enterprise solutions.

In essence, the LER ecosystem represents much more than a mere technological innovation; it marks a significant shift in our perception of education, skills, and employment. As we navigate this crossroad of change, we find ourselves with the unique opportunity to shape the future labor market into a more efficient, effective, and equitable entity. The challenge we face is undeniably substantial, yet with a committed spirit of collaboration, we can establish a responsible LER ecosystem that is beneficial for all parties involved.

Appendix A: Participants to the Interviews

NAME	ORGANIZATION	TITLE
Mark Leuba	1EdTech	Vice President, Product Management
Mark McConahay	AACRAO	Senior Consultant and LER Coordinator
Annelies Goger	Brookings	Economic Geographer; David M. Rubenstein Fellow, Metropolitan Policy Program
Amber Garrison Duncan	C-BEN (Competency Based Education Network)	Executive Vice President
Jason Tyszko	Chamber of Commerce Foundation; T3	VP of Center for Education and Workforce
Deb Everhart	Credential Engine	Chief Strategy Officer
Amy Hammett	CWRU SIS & Services	Registrar and Director
Daniel Buchner	Decentralized Identity at Block	Head of Decentralized Identity
Pam Frugoli	Department of Labor	Workforce Analyst
Kerri Lemoie	Digital Credentials Consortium, MIT Open Learning	Director of Technology
Sarah Cacicio	Digital Promise	Senior Project Director (Former)
Christina Luke Luna	Digital Promise	Chief Learning Officer for Pathways and Credentials
Kelly Page	Digital Promise	Director of Learning and Employment Innovations
Rachel Scherer	Gates Foundation	Senior Program Officer, Data Innovation
Erin Spring	Goodyear Tire & Rubber Company	Senior Director, Material Science
Monika Bose-Samanta	Goodyear Tire & Rubber Company	Human Resources Director, Global Technology
Glenda Lembicz	Hyland Software	Manager, Research and Development Education
Sarah Dukes	Hyland Software, Hyland HR	Senior Manager of Mobile Talent Acquisition
Kaliya Young	Identity Woman	Independent Consultant and Subject-Matter Expert
Oras Al-Kubaisi	Job Description AI	Founder
Sharon Leu	Jobs for the Future	Executive In Residence, JFFLabs
Bledi Taska	Lightcast	Chief Economist
Jake Hirsch-Allen	LinkedIn	Head of Workforce Development
Ethan Karp	MAGNET / Manufacturing Extension Partnership	CEO
Kym Lavigne Hinkley	Markle Foundation	Senior Manager for Career Coaching
Ankur Patel	Microsoft	Partner Product Manager
Gillian Walsh	MIT Media Lab	Program/Project Coordinator
Philipp Schmidt	MIT Media Lab	Director of Digital Learning and Collaboration
Amanda Winters	National Governors Association	Program Director
Corey Dixon	National Governors Association	Consulting Director
Nick Moore	National Governors Association Alabama	Director of the Office of Education, Workforce, and Transformation
Robert McGough	National Governors Association Arkansas	Chief Analytics Officer for the State of Arkansas
Rob Groot	National Student Clearinghouse	Managing Director for Learner Mobility
Zhewei Gregory	National Student Clearinghouse	Managing Director for Research Development and Philanthropy
Sean Gallagher	Northeastern University	Founder and Executive Director of Center for the Future of Higher Education and Talent Strategy at Northeastern University; Executive Professor of Educational Policy
Laura A Guilliam	Progressive	Research and Development Consultant
Dan Quigg	Public Insight	CEO
Ian Davidson	Smart Resume/iDatafy	Chief Growth Officer
Phillip Long	T3 Innovation Network, RHz Consulting LLC	LER Network Facilitator; Founder RHz Consulting LLC
Adam Snyder	Talan Products	COO
Jacob Duritsky	Team NEO	VP of Strategy and Research
Julie Szeltner	Team NEO	Director of Talent Engagement
Rebecca Busacca	Territorium	VP Business Development

Justin Coppedge	Texas 2036	Senior VP of Strategy and Operations
Dan Toliver	TodaQ	Co-Founder
Hassan Khan	TodaQ	Co-Founder
Karyl Fowler	Transmute	Co-Founder and CEO
Orie Steele	Transmute	Co-Founder and CTO
Kate Giovacchini	Trusted Learner Network, Arizona State University	Co-Executive Director of Engineering Core
Stephen Barley	UC Santa Barbara/Stanford	Distinguished Professor Emeritus of Technology Management (UCSB); Professor Emeritus of Management Science and Engineering (Stanford)
Etan Bernstein	Velocity Network Foundation	Co-Founder of Velocity Career Labs; Head of Ecosystem of Velocity Network Foundation
Jen Vanek	World Education	Director of Digital Learning and Research

Appendix B: Workshop Participants

NAME	ORGANIZATION	TITLE
Amanda Winters	National Governors Association	Program Director
Amy Hammett	CWRU	Director of Student Information Systems & Services
Carlier Myers	CWRU	Associate Registrar
Anu Yadavalli	We Can Code It	Director
Bob Sopko	LaunchNet	Executive Director
Charles McElroy	Cleveland State University	Assistant Professor Information Systems,
Corey Dixon	National Governors Association	Consulting Director of Skills and Credentials,
David Baumgartner	E-du Proof UG	COO
Deborah Everhart	Credential Engine	Chief Strategy Officer
Etan Bernstein	Velocity Network	Co-Founder and Head of Ecosystem
Naomi Szekeres	Velocity Network	Head of Global Education Ecosystem Strategy
George Westerman	MIT Sloan School of Management	Senior Lecturer
Jamaal Hill	CWRU	Project Manager, Siegal Lifelong Learning
Jason Tyszko	US Chamber of Commerce Foundation	Vice President, Center for Education and Workforce
Julie Szeltner	Team NEO	Director of Talent Engagement
Lucy Yang	Identity Woman	Managing Partner
Kate Klonowski	CWRU	Director of Local Government and Community Relations
Kerstin Rempe	E-du Proof	
Mark Dangelo	CWRU	Associate Director of Client Engagement, xLab
Mark McConahay	AACRAO	Sr. Consultant and CLR/LER Coordinator
Mike Glavin	Vice President, Talent Solutions	Greater Cleveland Partnership

Phillip Long	T3 Innovation Network	LER Network Facilitator
Prasanna Parasurama	NYU Stern School of Business	PhD Student
Rob Groot	National Student Clearinghouse	Director of Product Management in Education Services
Shiyan Yang	Stevens Institute of Technology	PhD Student
Youngjin Yoo	CWRU	Prof, Design and Innovation
Erman Ayday	CWRU	Assistant Professor of Computer and Data Science
Shubham Semwal	CWRU	MBA student
Grace DiPierro	CWRU	Student
Vasudeva Lenkala	CWRU	Student
Wenbiao Li	CWRU	Student
Benjamin Mucha	CWRU	Student
Fatih Ahmet Gurbuz	CWRU	Student
Ryan Tatton	CWRU	Student