Chapter 7
Moving Toward Self-Sovereign Identity:
How the Evolution of Blockchain Impacts Identity Management in Clinical Trials

Rama K. Rao
Bloqcube Inc., USA

Prem K. Narang
Bloqcube Inc., USA

ABSTRACT

Self-sovereign identity (SSID) is a digital solution intended to ameliorate the drawbacks associated with existing digital identification management approaches. This chapter begins with an overview of identity management systems. It explores the essential elements of SSID, including verifiable credentials, distributed ledger technology (DLT), and privacy engineering protocols, and highlights research initiatives, governmental projects, and regulatory frameworks that leverage evolving technologies to improve data integrity, efficiency, and security. The authors survey key challenges and advantages associated with SSID, establishing a taxonomy of the SSID model and a summary of privacy engineering techniques that work in concert with SSID, including zero knowledge proofs (ZKPs) and bring your own identity (BYOI) systems. The authors highlight several innovators in the SSID ecosystem that are contributing to the growth and maturity of this model.

DOI: 10.4018/978-1-7998-8966-3.ch007

INTRODUCTION

How can data be shared without jeopardizing the data owner, even in a worst-case scenario? How can data owners' identity be protected by individuals themselves, rather than by a central authority whose decisions the individual cannot control? Self-sovereign, electronic, trustworthy identification systems promise a possible answer. SSID implementation could prevent rightful identities from being misused or rejected for many people, in a variety of settings.

Here is a recent example that demonstrates the dangers inherent to our current digital identity management infrastructure: as western countries left Afghanistan in the summer of 2021, digital ID technology created to document Afghan nationals in a centralized system fell into the hands of the Taliban. In an article subtitled: "digital ID systems are powerful development tools providing a legal entity for millions, but their misuse can be deadly" Emry Schoemaker wrote for *The Guardian* that the Taliban had declared their intention to use this US technology to hunt down Afghans who had collaborated with the international coalition (Schoemaker, 2021). As of the writing of this chapter, the Taliban have access to, and control over, digital identification systems and technology, including e-Tazkira, a biometric identity card used by the Afghanistan National Statistics and Information Authority. Schoemaker writes that this is "yet another wakeup call illustrating the risks that new digital technologies, managed centrally, can pose when they end up in the wrong hands" (Schoemaker, 2021).

The solution cannot be to remove digital identity systems altogether. As is evident from today's world, an identification of some sort is needed wherever you go and whatever you do. In the world of the internet and web commerce, digital identity is necessary to seek services, provide services, or engage with entertainment, government, and healthcare systems alike. Digital identity ensures efficient and effective delivery of service.

Much of the innovation and leadership to find a solution to these risks, along with other issues associated with digital identity, has originated in the healthcare industry. Healthcare workers always grapple with the competing demands of highly sensitive identifiable information and the necessity of urgent delivery of service. According to a World Bank report on *The Role of Digital Identification for Healthcare (2018)*:

Providers need to know a patient's identity to access relevant medical and treatment histories and ensure that they are giving consistent and appropriate care. Patients also need documentation to prove enrollment in insurance programs or other safety nets that cover medical expenses. IHealth insurers need to be able to identify patients to ensure that those for whom claims are submitted are actually insured and to facilitate the adjudication of claims based on the patient's history. IA secure, inclusive, and