Understanding emerging blockchain identity management systems

January 28 2020

Credit: CC0 Public Domain

Traditional identity management has typically involved the storing of user credentials (e.g., passwords) by organizations and third parties, which often results in concerns over interoperability, security, and

privacy. However, a possible solution has emerged through the use of blockchain technology to create novel identity management approaches with built-in control and consent mechanisms. This can potentially transform data governance and ownership models by enabling users to control their data and share select personal information, while helping businesses streamline operations by relying on verified user information without having to maintain the infrastructure themselves.

NIST announces the publication of the NIST Cybersecurity White Paper "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems (IDMS)," which provides an overview of the standards, building blocks, and system architectures that support emerging blockchain-based identity management systems and selective disclosure mechanisms. (A draft of this document was posted for public comment in July 2019.) The document considers the full spectrum of top-down versus bottom-up governance models for both identifier and credential management and addresses some of the risks and security concerns that may arise. The terminology, concepts, properties, and architectures introduced in this work can facilitate understanding and communications amongst business owners, software developers, cybersecurity professionals within an organization, and individuals who are or will be using such systems.

Provided by National Institute of Standards and Technology