Secure Credential Sharing with Blockchains

Rahma Mukta [1], Hye-young Paik[1], Salil S. Kanhere [1], Qinghua Lu [2]
[1]University of New South Wales, Sydney [2]Data61, CSIRO

ABSTRACT

The digitized credentials with cryptographic signature facilitate secure sharing. However, sharing credential data electronically could raise privacy concerns. For the digital credentials to be widely accepted, (i) securely verifying the participants and credentials to increase trust, and (ii) a control to selectively disclose the content of the credentials to increase privacy are important. Our research focuses on designing a blockchain-based, decentralised credential and identity management system that allows secure creation and sharing of credentials equipped with selective disclosure solutions based on attribute-based signatures.

KEYWORDS

Blockchain, SSI (Self Sovereign Identity), smart contract, credential, selective disclosure, DApp

1 INTRODUCTION & RESEARCH PROBLEM

Credentials are privacy sensitive, but requires frequent sharing. A digitized credential can reduce the cost and increase security and integrity. The management and use of conventional digital credentials require a centralized database (single point of failure) for verification purpose. Furthermore, fraudulent activities and lack of unified standards are barriers to global acceptance. A blockchain can solve these challenges by recording and sharing data in a temper-proof manner.

Researchers have proposed architectures using blockchain in educational ecosystem [1]. However, they paid less attention to managing user identities and privacy. Recipients require all their credentials to be associated with an identity that is accepted globally. Also, only sharing the necessary set of information would improve privacy. Grather et al [2] have developed a prototype for credential management which considered selected credential sharing. But an attribute-level selective sharing, where certain attribute of the credential can be redacted, is still not supported. Our proposed solution extends the previous works of credential sharing with self-sovereign identity (SSI)[3] and attribute level selective disclosure. We also embedded accessible time period on the shared credentials.

2 PROPOSED SYSTEM

2.1 Selective Disclosure

We use Attribute-based signature (ABS) [4] for the attribute-level selective disclosure. Using ABS, the signature acts as an attestation to attributes of the student credential that marks the signed attributes owned by the student. During verification, the verifier can validate the signature by issuer's public key.

2.2 Workflow Overview

Each certificate issuer and recipient is uniquely represented by blockchain account and associated decentralized identifier (DID) [5](step1). DIDs are stored on registry contract. Recipient sends

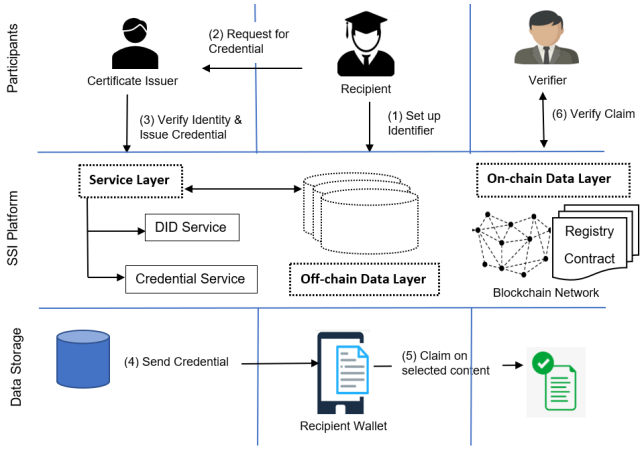

Figure 1: Proposed Credential Sharing Architecture

credential request to issuer(step2). After identity verification, issuer fetches relevant data from his off-chain repository to create the credential and signs the credential with signing key, generated at the service layer for ABS(step3). Credential is stored on issuer local storage, while hash of the credential and signature is stored on chain. Issuer sends the link of signed credential to recipient(step4). Recipient generates his claim(step5) with required subset of attributes. A Jason Web Token (JWT) is generated by the platform with accessible time period. Both the claim and token are sent to the verifier. Verifier verifies it via *verification* from credential services(step6). Verification module first decodes the JWT. If access period is valid, the module receives verification key of ABS from service layer. This verification key is then used to verify the authenticity and integrity of shared attributes and corresponding issuer signature. The implementation is in progress. We plan to implement a decentralized application (DApp) for the system and an user interface through mobile application to mark the potential practicality of the infrastructure.

REFERENCES

[1] Ali Alammary, Samah Alhazmi, Marwah Almasri, and Saira Gillani. 2019. Blockchain-Based Applications in Education: A Systematic Review. *Applied Sciences* 9, 12 (Jun 2019), 2400. https://doi.org/10.3390/app9122400
[2] Wolfgang Gräther, Sabine Kolvenbach, Rudolf Ruland, Julian Schütte, Christof Torres, and Florian Wendland. 2018. Blockchain for Education: Lifelong Learning Passport. *Proceedings of 1st ERCIM Blockchain Workshop 2018* 2, 10 (2018).
[3] Yue Liu, Qinghua Lu, Hye-Young Paik, Xiwei Xu, Shiping Chen, and Liming Zhu. 2020. Design-Pattern-as-a-Service for Blockchain-based Self-Sovereign Identity. arXiv:2005.01346 [cs.SE]
[4] Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. 2008. Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance. http://eprint.iacr.org/2008/328 rosulek@uiuc.edu 14089 received 29 Jul 2008.
[5] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, and Markus Sabadello. 2020. Decentralized Identifiers (DIDs) v1.0; Core architecture, data model, and representations. https://w3c.github.io/did-core/ Accessed: 18-05-2020.