Paper Title:

VCTP: A Verifiable Credential-based Trust Propagation Protocol for Personal Issuers in Self-Sovereign Identity Platforms

Paper Link:

https://doi.org/10.1109/DAPPS57946.2023.00023

1 Summary

1.1 Motivation

- The paper suggests a trust propagation protocol for self-sovereign identity platforms that relies on verifiable credentials and focuses on personal issuers, aiming to enhance the verification process.
- The paper tried to provide a trust mechanism to individual issuers who are not part of the SSI solutions. Through this approach they will be able to issue credentials that can be verified in the business context.
- The paper hypothesizes that the proposed protocol can enhance the security, privacy and usability of SSI platforms by leveraging policy-based sanitizable signatures and voting mechanisms.

1.2 Contribution

- The paper introduces a new type of verifiable credentials that embeds an update policy section to specify the rules and conditions for credential updates by designated updaters.
- The paper designs and implements a set of cryptographic algorithms that can update the policy through a signature scheme that can also be sanitized. This will allow to make updates to the existing credential without making it invalid
- The paper conducts an in depth assessment of the security aspects of the proposed protocol and argues how it defends against several probable attack scenarios.

1.3 Methodology

- The paper first identifies the problem of trust management for personal issuers in SSI platforms, and reviews the existing literature on SSI, issuer trust, blockchain and cryptography.

- The paper then proposes a novel solution that combines the concepts of verifiable credentials, policy-based sanitizable signatures, chameleon hash functions, attribute-based encryption and voting processes to achieve trust propagation and verification for personal issuers.
- The paper implements the proposed solution using Python and deploys it on a blockchain-based SSI platform with smart contracts written in Solidity.
- The paper evaluates the proposed solution by conducting system load tests and security analysis to measure the performance and robustness of the protocol.

1.4 Conclusion

The paper concludes that the proposed protocol is a feasible and effective way to add trust to individual issuers in Self Sovereign Identity platforms, and to enable them to issue verifiable credentials in various business scenarios.

2 Limitations

2.1 First Limitation

The paper does not provide a quantitative or comparative analysis of the trust level or reputation of the personal issuers, which could be useful to measure the effectiveness of the protocol and compare it with other trust management schemes.

2.2 Second Limitation

The paper assumes that the L1 issuers are trusted by the governance authority and the verifiers, and that they can define the update policy and access attributes for the credential template. However, this may introduce a single point of failure or compromise in the protocol, if the L1 issuers are malicious or dishonest.

3 Synthesis

The paper opens up potential applications and future scopes for the protocol, such as extending it to other domains (e.g., education, finance, social media), integrating it with other trust management models (e.g., reputation, endorsement, feedback), and improving it with other cryptographic schemes (e.g., zero-knowledge proofs, homomorphic encryption).