OSAKA METROPOLITAN UNIVERSITY

GRADUATE SCHOOL OF INFORMATICS

Explore all Researches

A Privacy-Preserving Selectively Disclosed eKYC System Using Merkle Tree and Zero-Knowledge Proofs

Istiaque Ahmed[1], Tadashi Nakano[1], Kentaroh Toyoda[2], Thi Hong Tran[1]; [1]Graduated School of Informatics, Osaka Metropolitan University; [2]AIFT, Singapore, and Keio University, Japan

I. Background

Blockchain-based eKYC is capable of single authentication and sharing data among multiple organizations using Blockchain.

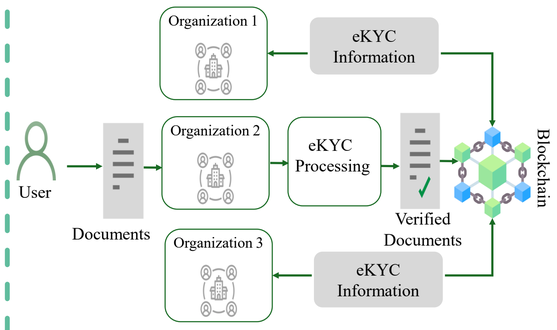

Fig. 1 Blockchain-based eKYC

SSI model for issuing Verifiable Credentials, the Holder keeps the credentials and submits them to the verifier.

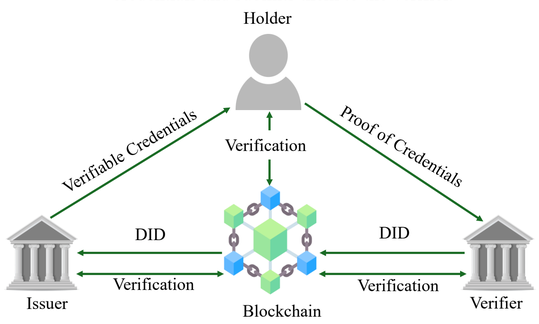

Fig. 2 Blockchain-based SSI

II. Current Problems

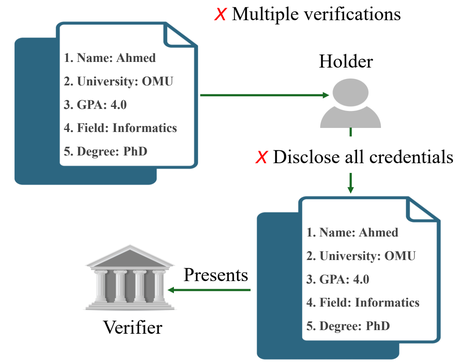

Fig. 3 Disclosing All Information

III. Preliminary Ideas

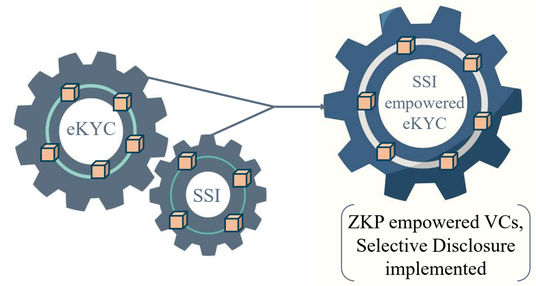

Fig. 4 eKYC and SSI Integration

IV. System Overview

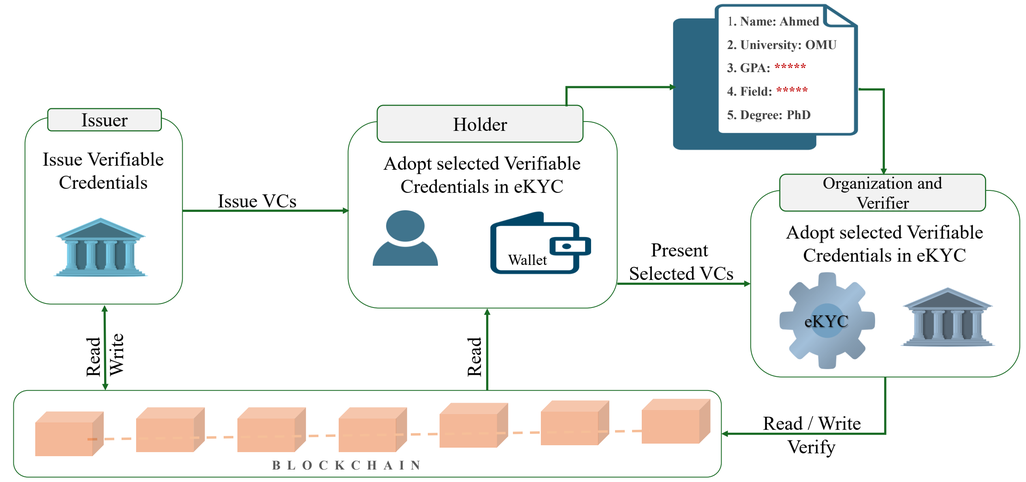

Fig. 5 SSI empowered eKYC

V. ZKP Implications

Fig. 6 Zero Trust VC

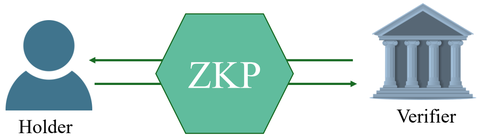

Fig. 7 Present Zero Trust VC for Verification

In this Proof of Concept (PoC), we successfully implemented eKYC and zk-SNARKs. SSI is a well-established approach, but it is still not included in this PoC. Implementing selective disclosure using zk-SNARKs requires more computational cost to achieve higher privacy.

VI. zk-SNARKs Implementation

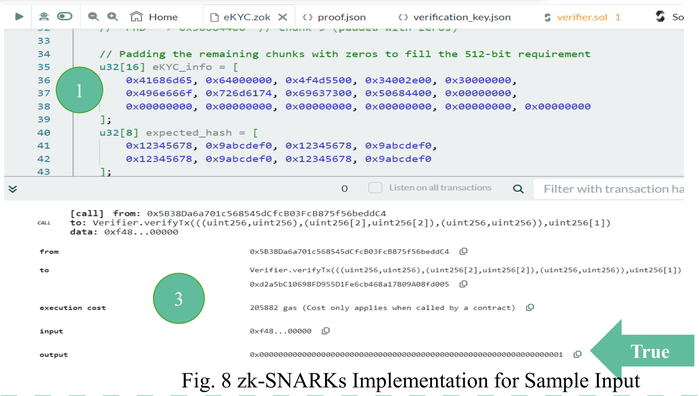

Fig. 8 zk-SNARKs Implementation for Sample Input

```
// Hash the user's eKYC information (preimage)
u32[8] computed_hash = sha256(eKYC_info[0..8], eKYC_info[8..16]);
// Verify that the computed hash matches the expected hash
bool isValid = computed_hash == expected_hash;
// Return whether the proof is valid
return isValid;
```

Approach of zk-SNARKs:

- ✓ Convert eKYC data into ASCII and pack into 16 chunks of 32-bit int (512 bits).
- ✓ Compute expected hash
- ✓ SHA-256 h= SHA-256(eKYC[0-7], eKYC[8-15],)
- ✓ isValid = computed_hash = = expected_hash;

During this fellowship period 3 of articles have been published in top **5%** to **10%** journals including **IEEE** and others. More 2 articles are under review in top tire **IEEE** journals. I have been participated conferences too.

Some selected articles:

- A Systematic Review on Blockchain-Enabled eKYC: Leveraging SSI and DID for Secure and Efficient Identity Verification; **IEEE IoT Journal**
- Efficient Verifiable Credential Aggregation with Blockchain Anchoring and ZK-SNARKs; **IEEE Access**

For research collaboration:
isti.ru.cse@gmail.com