Blockchain-based Identity Provisioning & Verification System (TRUST-DER)

Keshava Srinivas, Nithin Ram, Noora Alfayez, Pramod Illuri, Prerit Pathak, Vaanya Gupta

Sponsor: Mayank Malik (SLAC)
Advisor: Dr. Hanan Hibshi

ini — *Innovate in the Wild*

SLAC NATIONAL ACCELERATOR LABORATORY

Project Overview

Background and Motivation:

Currently, the method used to store identities of devices is imprinting a secret/identity information in a silicon chip such as an EEPROM (Electrically Erasable Programmable Read-only Memory) or SRAM (Static Random Access Memory). These identities are verified using hardware cryptographic operations like digital signatures and encryptions. The disadvantage in this method is that the manufacturing cost of imprinting secrets in these types of silicon is high. Moreover, The hardware required to implement Secure Hash Algorithms for digital signatures is expensive. This method also requires an additional protection mechanism to prevent invasive attacks, which would consume a lot of power.

Problem Goal:

The goal of this project is to develop software for an information theoretic approach that allows device identity to be verified by network participants. This approach aims to be decentralized, prevents a single point of failure, and can be as effective as imprinting an identity in silicon.

Why this approach?

The motivation behind a software-based decentralized verification system is that the identity of the devices can be verified while preserving privacy, meaning it does not need an additional protection mechanism. In doing so, the cost and power consumption of the devices are also reduced. An additional advantage of implementing this approach as a set of smart contracts on a blockchain-based network is, the code is shared and run on every single device, making it easier to scale reliably.

Solution

- A **decentralized blockchain based identity provisioning using hyperledger fabric & verification system** to prevent a single point of failure & be as effective as imprinting an identity in silicon.
- **Shamir Secret Sharing (SSS)** and encryption for identity sharding and verification

Advantages:

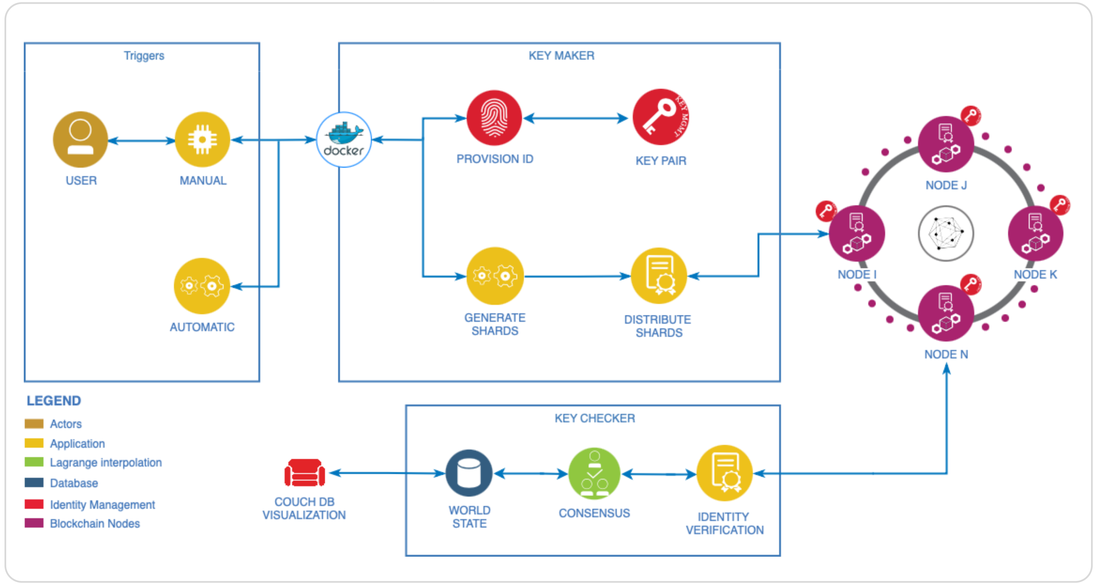
- Lower cost and power consumption
- Preserves privacy while verifying identities
- Easy management of the algorithmic logic for all nodes on the blockchain and Blockchain scalability

Results

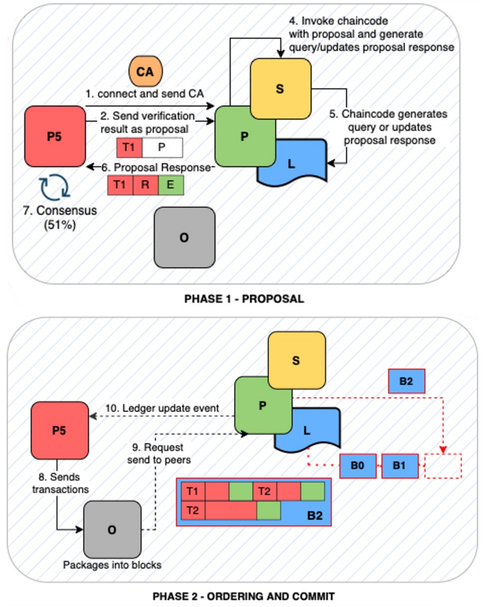
There are numerous advantages to shifting to a software-based identity verification. In our project, we demonstrated that it is possible to provision a device identity and authenticate it using subset of peer nodes on the blockchain network. There are still many opportunities to develop this further and have it ready for market-adoption.

Architecture

System Architecture

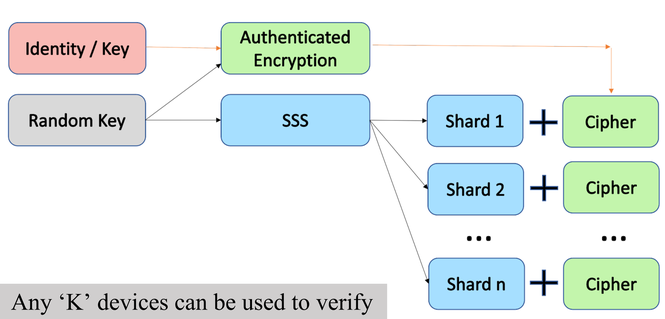


Blockchain Network

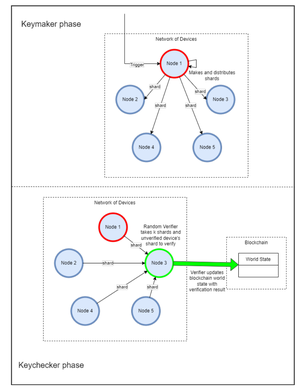


Identity Sharding & Verification

- The KeyMaker protocol uses Shamir Secret Sharing to distribute the shards of the random key, which is used to encrypt the actual identity of the device
- The encrypted identity is used as a cipher, which is appended to each of the shards
- Any shard Sx cannot be the subset of the key, and all shards S1, S2…Sn, when combined together, must not reveal the secret key
- Each device has visibility of only one shard



Any ‘K’ devices can be used to verify the identity of a devices where K is less than the total number of devices



Tools & Infrastructure

Code management: **Git**
Infrastructure: **Amazon web services (AWS), Hyperledger Fabric**
Programming Language: **Go, Python**

Future Work

- Increase scalability and optimize the approach
- Reduce the verification time and improve performance
- Improve false positive rate for the verification protocol

References

1. M. Malik, “Digital Identity Management,” YouTube, 16-Sep-2021. [Online]. Available: https://www.youtube.com/watch?v=9XgmZtdlSBQ&t=857s.
2. A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.
3. A. Shamsoshoara, “Overview of blakley's secret sharing scheme,” arXiv.org, 09-Jan-2019. [Online]. Available: https://arxiv.org/abs/1901.02802.
4. https://aws.amazon.com/blockchain/what-is-hyperledger-fabric/
5. https://docs.aws.amazon.com/blockchain-templates/latest/developerguide/blockchain-templates-hyperledger.html