Table of Contents

Blockchain Key Management Position Statement

About Us

Blocko is a startup providing a bitcoin-based enterprise blockchain development platform. Our customers include JB Bank of Korea, one of the first banks in the world to provide blockchain-based authentication system to their customers. They are utilizing Open Keychain, an open standard promoted by Blocko to build PKIs on bitcoin blockchain fabric. Problem Statement

A secure blockchain application requires secure ways to manage user private keys. For fixed use cases such as Bitcoin or Ethereum asset transfer, users can utilize existing wallet software to manage their assets. However, for more general use cases for web applications utilizing blockchain, things get complicated.

The existing solution is to build propriety private key management apps for different blockchain services.

However, since each key management app requires different authentication scheme, despite the fact that many blockchain applications are able to utilize the same private key format, the approach results in fragmented experience for users and raised investment in time and resources for the service providers.

The lack of standard mechanisms to manage user private keys is one of the major hindrance to the widespread adoption of blockchain.

Requirements

Consolidated Key Management

Different blockchain applications should be able to utilize centralized key management functionality on each device, instead of implementing different key management features embedded to each application.

Access to Biometric Sensors

For ease of use, users should be able to safely guard their private keys using biometric sensors such as fingerprint scanner or iris scanner.

Access to Native Security Features

Private keys should be encrypted and stored safely utilizing different mechanisms present in devices.

Integration with Web Applications

The key management scheme should provide integration schemes on different environments such as custom URL on iOS or intent on android.

Blockchain Authenticators

FIDO UAF, an already established and popularized authentication scheme (https://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120) utilizes public key cryptography and require users to manage private keys on user devices, much like blockchain applications.

FIDO UAF authenticators provide an excellent design to create, register, use, and manage user private keys under PKI systems (https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-authnr-cmds-v1.0-ps-20141208.html.) Since FIDO UAF authenticators exist as separate native applications on mobile devices or as an embedded functionality provided by the OS, they provide access to integral native security features such as biometric sensors and secure elements.

The same design can be applied to blockchain applications to build a safe standard to manage blockchain private keys and facilitate applications.

Blockchain authenticators can provide such functionalities for blockchain web applications on mobile and desktop environment.

Unlike FIDO authenticators built for the sole purpose of challenge-response authentication, blockchain authenticators should be able to provide a much richer mode of operations by signing multitude of transactions generated by web applications.

Issues

Key Recovery

Since blockchain private keys provide not only ways for users to authenticate themselves, but manage important assets tied to the public key, there should be ways for users to backup and restore those as well.

Standard procedures to safely provision user identities for security and recovery must be established and existing bitcoin technologies such as BIP39 could be a good starting point (https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki.)