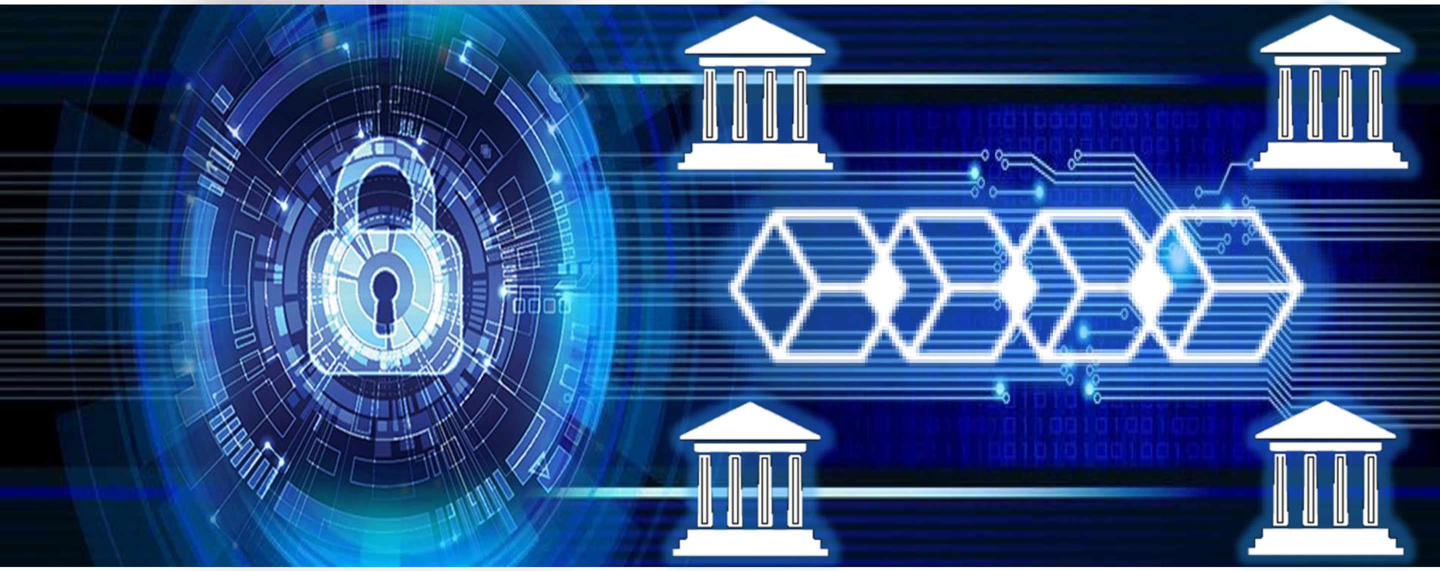
WHITE PAPER

WISeKey solutions as an answer to Blockchain Security concerns



- Bikramaditya Singhal
Practice Head- Blockchain, WISeKey India

WISekey
THE WORLD INTERNET SECURITY COMPANY
Swiss Cutting-Edge eSecurity Technology

© WISeKey India Pvt. Ltd. All rights reserved.

Abstract

Blockchain has been a strategic initiative for almost all kinds of businesses across industry sectors and the use cases that top the list come from Banking and Financial sectors. Many banks and financial institutions have successfully completed pilot programs using Blockchain. So, now is the time to really implement and realize the business value of these Blockchain use cases. However, "security" is still a biggest concern for all.

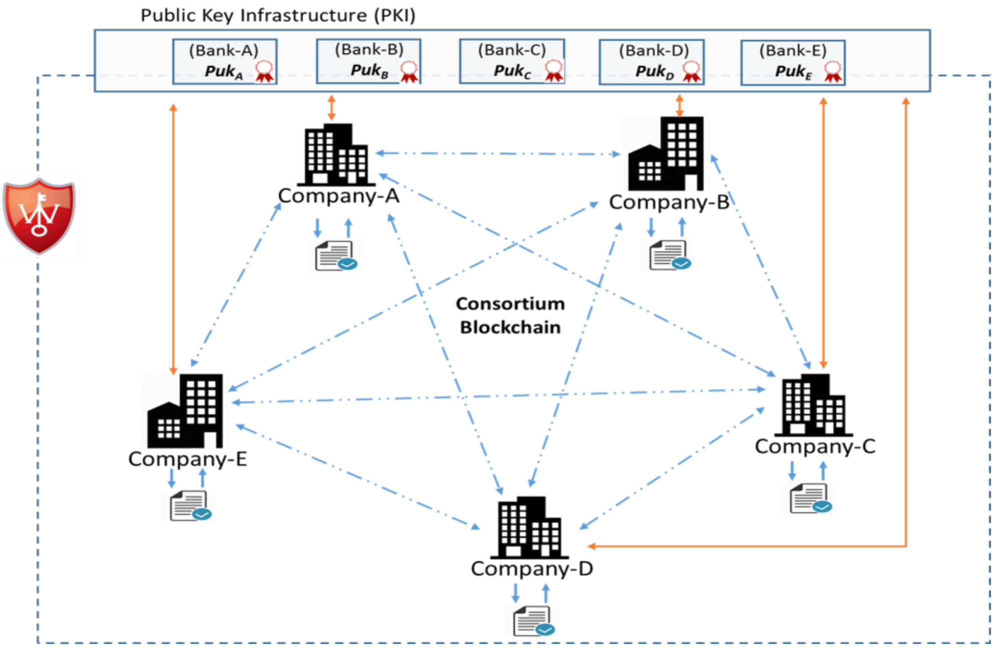
Developing a Proof of Concept using libraries of Java, Python or other languages for cryptographic elements is good to start with, but to take the use case to production, the cryptographic primitives should ideally be given the most priority and should be from a trusted and known source. Though some of the core cryptographic elements are available out of the box such as generating the private/public key pairs, there are many other areas where proper security components are needed, such as PKI based certificate solutions, customizable certificate authority to generate different types of certificates, or integrating external components with Blockchain that requires specialized Root of Trust based solutions.

WISeKey PKI Solution for Blockchain

WISeKey Public Key Infrastructure (PKI) solution for Blockchain can enable management of Public keys in a secured and efficient way, generation of Digital Certificates and their management, Authentication, Secure Signing, Document Signing and as well provide various other security based functionalities. Such a managed PKI solution can be centralized to introduce governance in a Blockchain solution and it can also be decentralized.

Example Use Case: Banks forming a consortium for a common KYC platform or any other interbank settlement, WISeKey Managed PKI solution can be a great fit that can address the security challenges by functioning as a trusted CA.

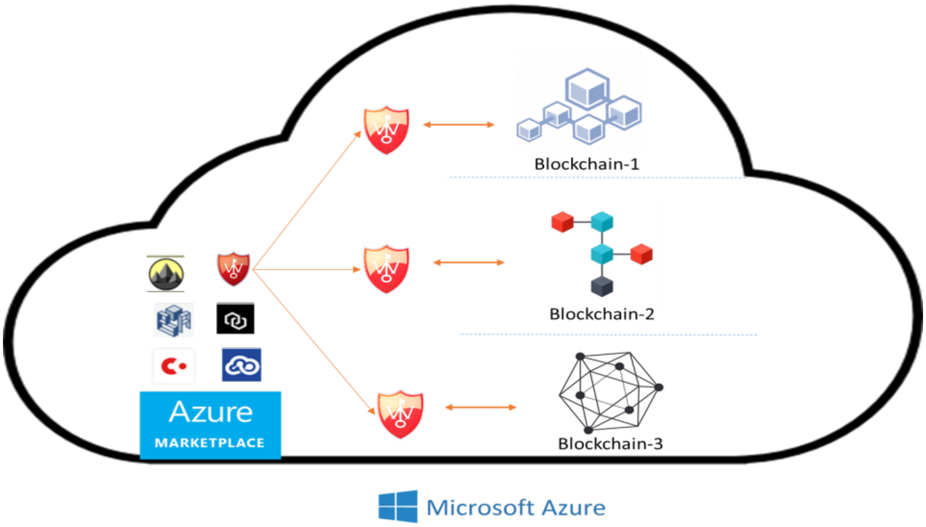
A generic representation of WISeKey PKI Solution for Blockchain at a high level:



WISeCA on Azure- A Certificate Authority Service for Blockchain

WISeCA, the WiseKey Certificate Authority can be an App in the Azure Market Place that can notonly provide an automated Managed PKI solution, but also allows the users to make customizations that can addresses their specific use case. The following is a list of possible offerings from WISeCA:

- Authenticate the participants (users or objects alike) of specific Blockchain use cases
- Generate Public/Private key pairs with the choice of algorithm such as RSA, Elliptic-Curve (ECC), Diffie-Hellman etc.
- Provide secured signing capability
- Provision temporary and permanent certificates
- Manage the certificate life cycle
- Provision wallets (wallet service) for the users to effectively use the Keys and Certificates
- Integrate with the AD service of Microsoft



WISeCA for Core Blockchain Solutions

For the Blockchain solutions that are being built ground up, and not on the Blockchain platforms such as Ethereum or Hyperledger, WISeCA can not only provide the managed PKI based solutions and wallet solutions, but also equip with basic cryptographic primitives such as Private/Public Key pair generations with the choice of algorithms, Hashing with the choice of Hashing mechanism and many more. It can also help provision the wallet services for the users and objects.

Apart from these, WISeKey solutions can integrate the IoT and other smart devices to Blockchain in a secured fashion with its state of the art Root of Trust, accelerated Crypto, Transactions with Secure Element based smart cards etc.

© WISeKey India Pvt. Ltd. All rights reserved.