

Know Your Customer (KYC) on Blockchain

Contents

1.Business Context.....	2
1.1 Context	2
1.1.1 KYC Policies	2
1.1.2 Objectives of KYC.....	2
2.Problem Statement.....	3
3.Challenges in KYC Process	3
4.Applicability of Blockchain as a Solution	4
5.Blockchain Benefits.....	4
6.Blockchain Solution Approach	5
6.1 Platform Evaluation Specs	5
6.2 KYC Business Flow	6
6.3 KYC Functional Flow	6
6.4 Logical Architecture	7
6.5 Deployment Architeture	8
6.6 Blockchain Solution Components.....	9
7.Solution Features	10
8.Conclusion	12

1. Business Context

1.1 Context

- As per the Anti money laundering and terror financing guidelines issued by various regulatory agencies worldwide, banks are required to put in place a comprehensive policy framework covering KYC standards and AML Measures
- KYC means “Know Your Customer”. It is a process by which banks obtain information about the identity and address of the customers
- This process helps to ensure that banks services are not misused
- The KYC procedure is to be completed by the banks while opening accounts
- Banks are also required to periodically update their customers’ KYC details

1.1.1 KYC Policies

Banks should frame their KYC policies incorporating the following four key elements:

- a. Customer Acceptance Policy
- b. Customer Identification Procedures
- c. Customer Profilings
- d. Risk Management
- e. Reporting

1.1.2 Objectives of KYC

- a. To prevent banks from being used, by unscrupulous or criminal elements for their criminal activities including money laundering.
- b. To minimize frauds and risks and protect banks reputation.
- c. To avoid opening of accounts with fictitious name and address.
- d. To weed out bad customers and protect good ones.

The increasing cost of regulatory compliance is among every banker's top concerns, having to comply with regulations such as Anti-Money Laundering (AML) and Know Your Customer (KYC). KYC and AML frameworks require banks to verify client identities. This process has various manual steps, involves many different institutions and is often duplicated among departments and other banks for one and the same customers.

Document validation and verification play a vital role in the KYC process. There has been an upsurge in the number of KYC registries because of initiatives by private entities such as the Society for Worldwide Interbank

Financial Telecommunication (SWIFT) and banking consortiums, as well as government bodies. These registries act as centralized repositories that store all documents and information related to KYC compliance.

Every bank and financial institution has to perform the KYC process individually, and upload the validated information and documents to the central registry that stores digitized data tagged to a unique identification number for each customer. By using this reference number, banks can access the stored data to perform due diligence whenever customers request for a new service within the same banking relationship, or from another bank.

2. Problem Statement

- a. For any account opening, loan processing etc, the customer is required to submit their KYC Documents in original attested by lawyer/notary. The reliance on paper documentation is cumbersome, resource intensive and expensive
- b. For KYC and AML requirements, customers have to repeat the same process and provide the same information to every financial institution.
- c. AML is a process that is common across the financial industry but today's solutions are build at individual institution level rather than at industry level
- d. Many financial institutions struggle to maintain an up-to-date database for AML checks. In reality, this data is not proprietary yet is maintained separately by each financial institution.

3. Challenges in KYC Process

- a. **Customer data related**
High volume, diverse, imprecise, decentralized, redundant and non-standardized. Problems related to confidentiality of client and financial data
- b. **Document Management**
Paper driven processes, lack of imaging and electronic content management, inadequate automation techniques
- c. **Workflow processing systems**
Non-automated approval processes, inefficient incident tracking techniques and lack of defined SLAs leading to long lead times for account opening
- d. **High operational cost**
Non-standardized processes, lack of proper training to processors, inadequate documentation, lack of multi-skilled processors, inadequate effort forecasting techniques, insufficient automation, leading to higher operational cost
- e. **Process management**
Decentralized and scattered processes, lack of well defined SLAs
- f. **Regulatory compliance**

KYC, AML – Tracking and implementation of changing regulations. Lack of adequate domain knowledge with processors

The use of Distributed Ledger Technology (Blockchain technology) can help to address most of the aforementioned challenges and ensure seamless exchange of documents and information between banks and external agencies.

4. Applicability of Blockchain as a Solution

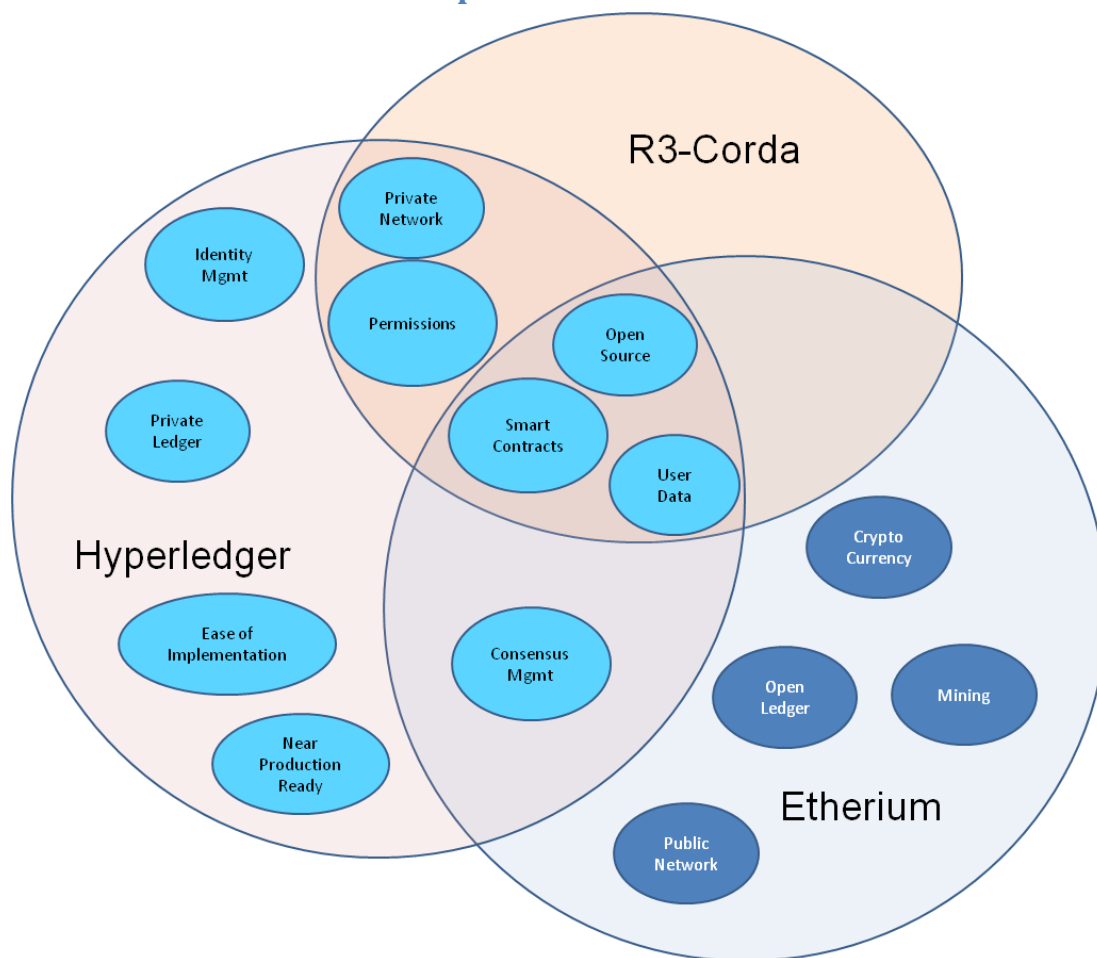
To solve this problem, we need a shared database into which all of the KYC records are written, with each record accompanied by a timestamp and proof of origin. The standard solution would be to create a trusted intermediary, whose role is to collect and store the KYC records centrally. But blockchains offer a different approach, giving the organizations a way to jointly manage this archive, while preventing individual participants (or small groups thereof) from corrupting it. The trust factor is built in by the blockchain thus eliminating the need for a centralized intermediary.

5. Blockchain Benefits

- a. **Reduced Operational Cost:** Blockchain technology could foster a standard KYC and AML data request across the industry, while allowing banks to share such information among departments and with other banks.
- b. **Enhanced customer experience:** Customers could be required to verify their identity in person the first time they engage with any of the blockchain's member institutions. Subsequently, they would be able to sign KYC and AML requests with their digital private signature.
- c. **Reduced Operational Cost:** This would potentially reduce the need for KYC and AML vetting and associated compliance costs every time a customer engages in a new product with another bank department or joins a new bank, while the cryptography can ensure data security
- d. **Increased security:** Increased security through near real-time distribution of updated KYC documentation, verified digital identities, and the opportunity to share, in near real-time, fraudulent transaction details
- e. **Increased transparency:** Increased transparency for regulators as both the immutability of the blockchain, and the opportunity for regulators to have nodes on Blockchain networks, support the ability to get a full, transparent audit trail of all transactions

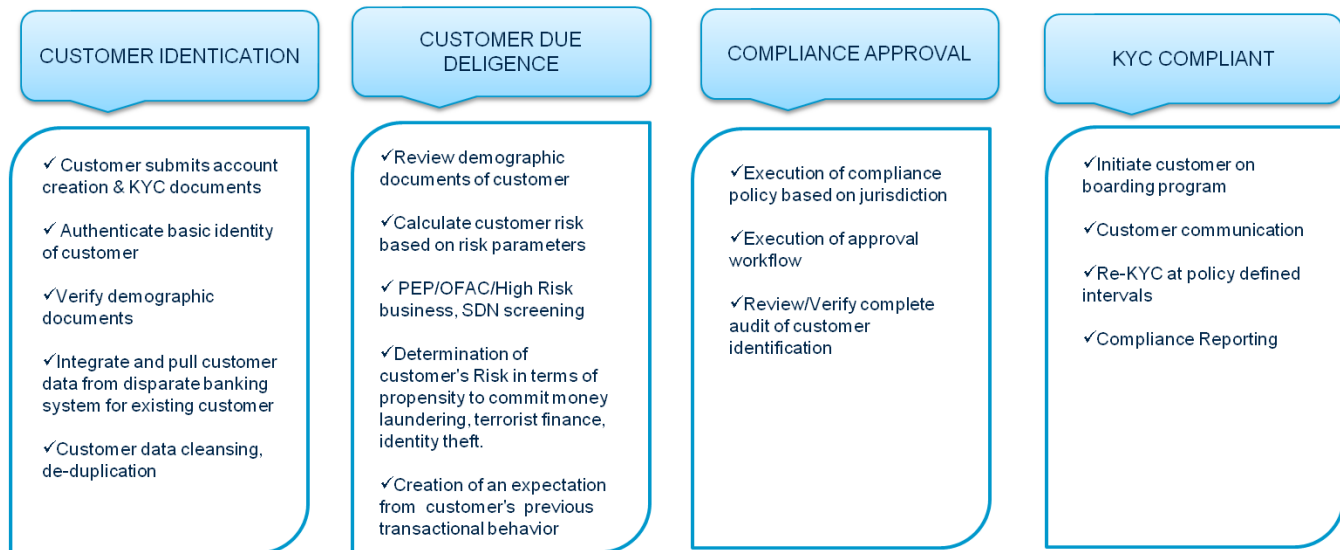
6. Blockchain Solution Approach

6.1 Platform Evaluation Specs



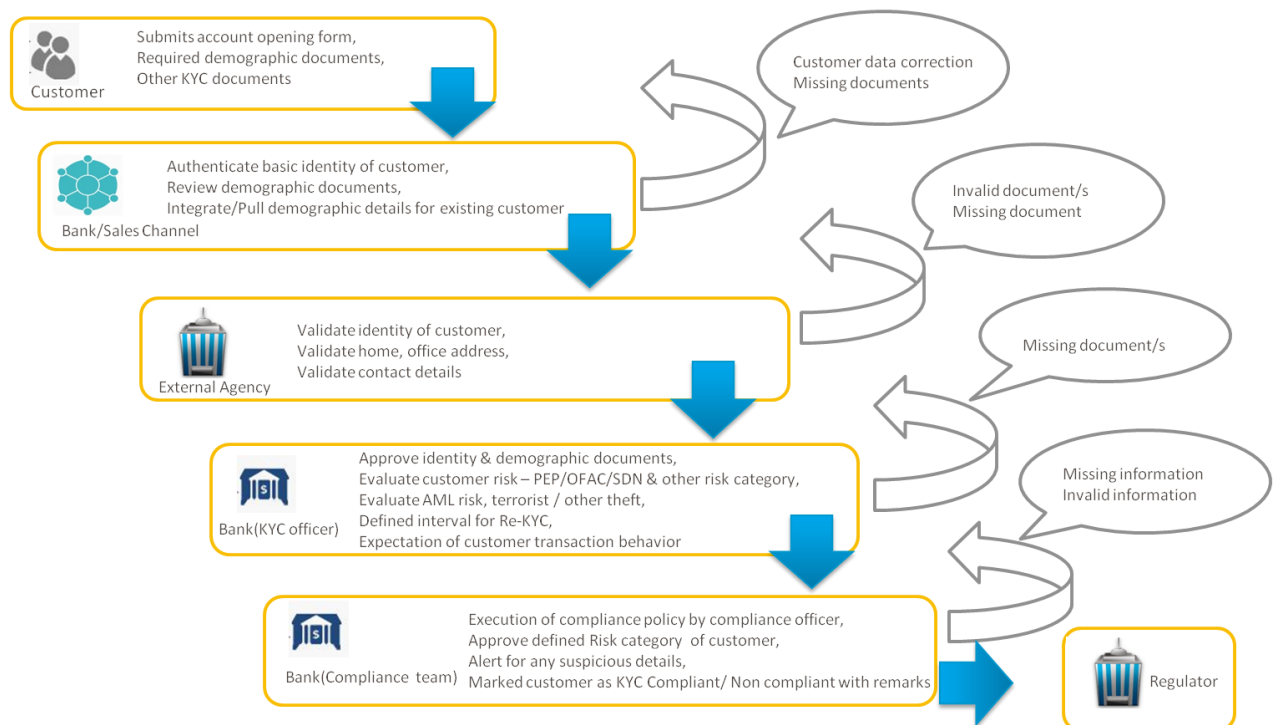
Suggested Option: IBM Hyperledger Fabric is suggested

6.2 KYC Business Flow

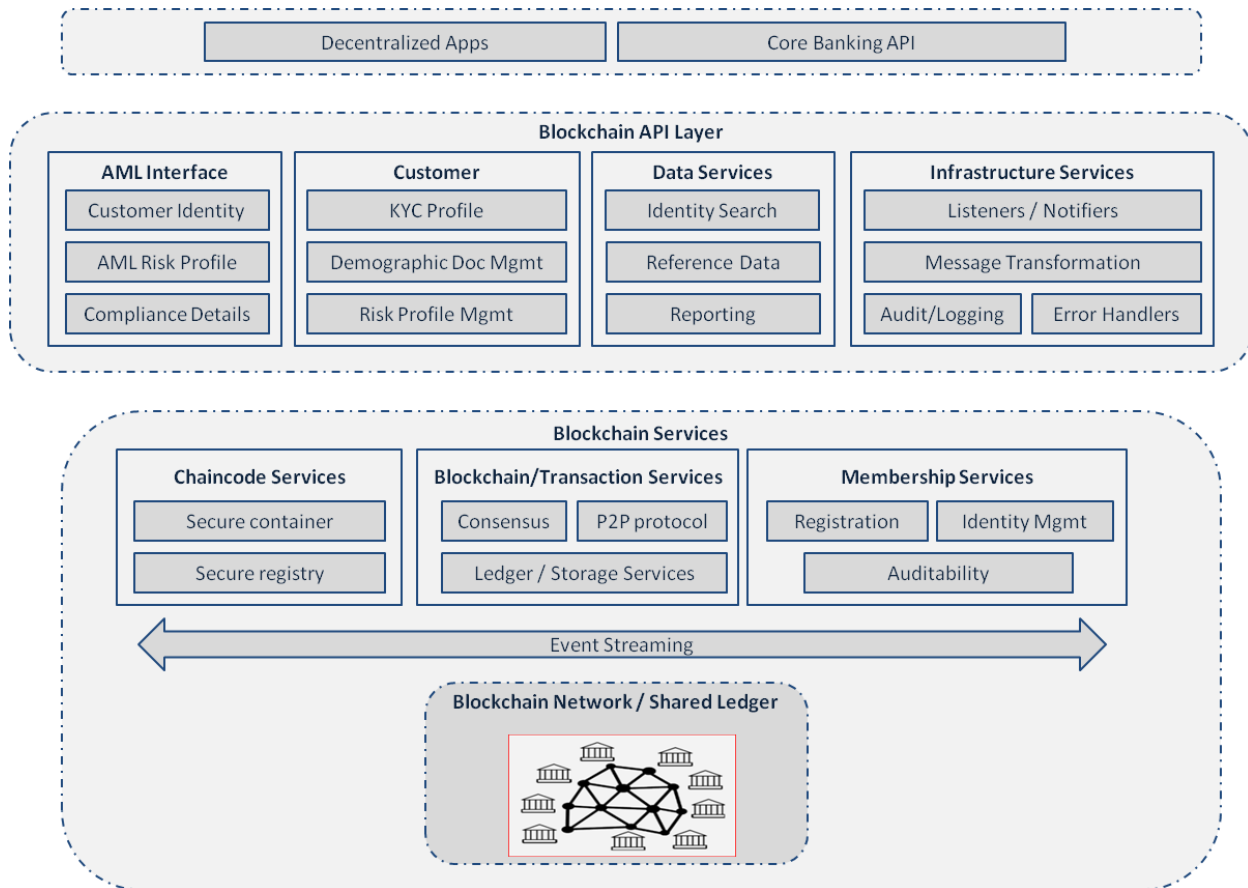


6.3 KYC Functional Flow

Functional Flow



6.4 Logical Architecture

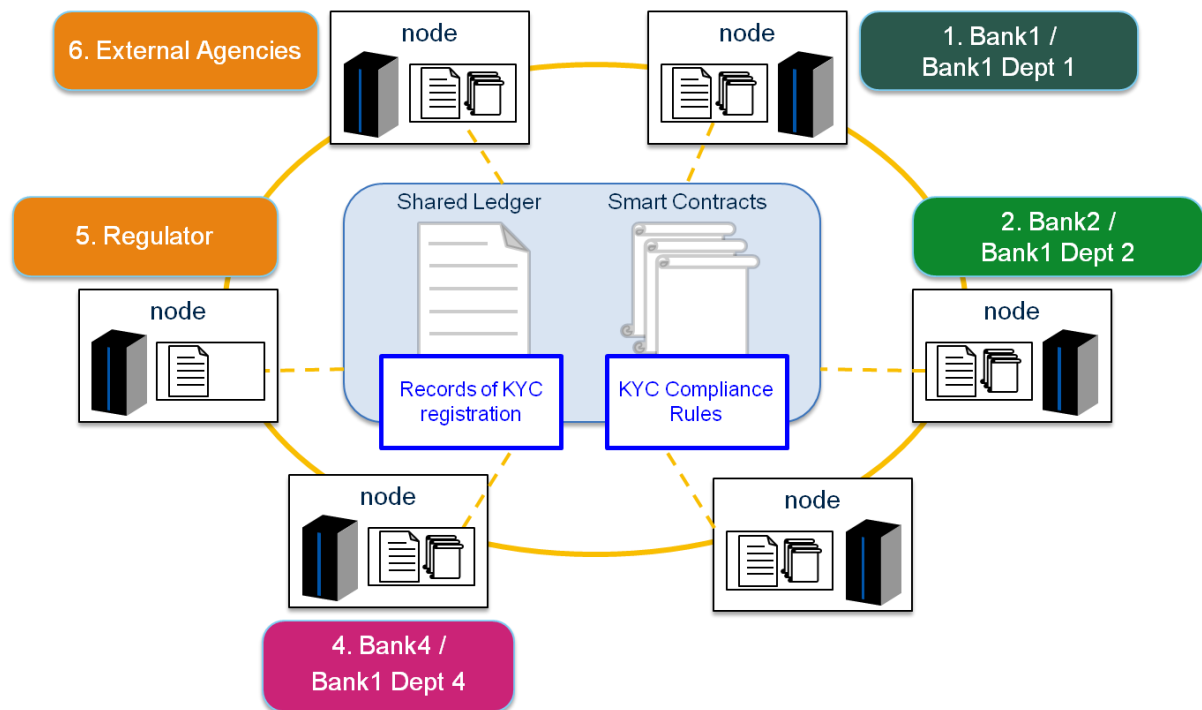


6.5 Deployment Architecture

This model requires consensus among participating banks on the validation process in order to maintain the trust and integrity of the system. Here, one bank plays the role of the originating bank and performs initial KYC verification for a customer. When the customer approaches another bank to open an account or request some banking services, the approached bank acts as a requesting bank and queries the ledger to check the KYC status of the customer. The requesting bank can request the originating bank to share the documents available, and the blockchain platform ensures secure transfer of documents between the two banks. With this model, banks can enhance process efficiency, standardize KYC processes, and perform customer validations in near real-time.

Regulator can act as a supervisory node and every transaction on blockchain has to be approved by this node. External agencies will refer information on ledger and perform validation checks. Validation checks performed by external agencies won't be part of blockchain network but after successful validation external agencies will update the KYC status on shared ledger.

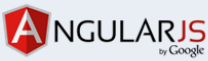












Below is the sample deployment architecture involving 4 banks:



Workflow Steps:-

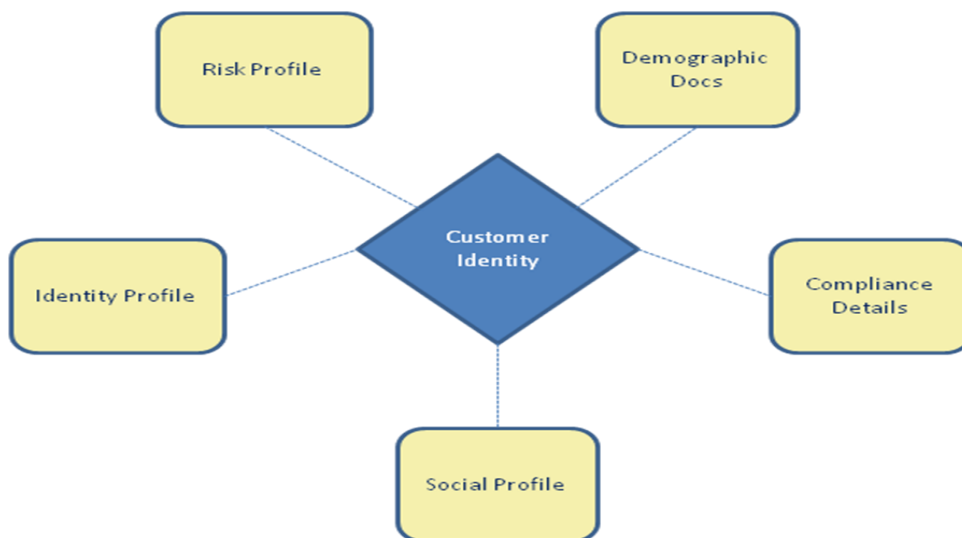
- Blockchain network that simulated 4 banks along with Regulator (regulated clearing authority) and external agencies responsible for validation checks.
- Customer fills up details and uploads KYC documents while opening a account with bank
- KYC related documents will get stored on shared ledger (blockchain network) and marks status as "Pending Validation".

- External agencies then look up the customer information submitted by the bank, and perform requisite validation checks. Validation checks performed by external agencies won't be part of blockchain network. On successful validation, the customer information on the ledger is updated and the status is changed to 'KYC compliant and validated'.
- Every transaction on blockchain network should be approved by Regulator node (regulated clearing authority).

Technology Stack				
User Interface	API	Blockchain Network	Smart Contract	Deployment
 ANGULARJS <small>by Google</small>	 spring	 HYPERLEDGER		 docker
 Bootstrap	 node	 Apache CouchDB	 java	 VAGRANT
	 java	 levelDB		

6.6 Blockchain Solution Components

Ledger Data Model (Conceptual): The KYC transactional data can be stored in the **struct** type in Hyperledger table. The database will be noSQL database.



Smart Contract:

The Smart Contract will have the business logic for the various KYC checks. Some of the check can be placed outside of the Smart Contract (will be detailed out in the solutioning phase). E.g

- Minimum required data fields for KYC
- Identity validation (calling out to external/federal agencies)
- Create Risk profile (call out to existing banking applications)
- Provide customer KYC Status (call in from the existing banking application)
- Generate alerts when the customer's KYC profile gets not compliant (these alerts can be listened in existing banking applications for further processing)

7. Solution Features

- Smart programmable contract to automate the process of Identity verification
- Ability to interact with External / Federal / Identity management systems
- Ability to change the smart contract based on the change in the regulatory needs
- Ability to add new financial institutions onto the solution platform
- Ability to onboard existing KYC profiles on blockchain platform
- Ability to provide external subscriptions to the smaller institutions to leverage KYC platform
- Ability to use customizable business rules build customer profiling
- AML processes for transaction monitoring and Suspicion detection which resides on core banking can interact with the external interfaces provided by blockchain solution to assist providing customer risk and other profiles
- Blockchain Ledger can be utilized to store the AML profiled results and summaries to be reported to the regulatory and legal agencies

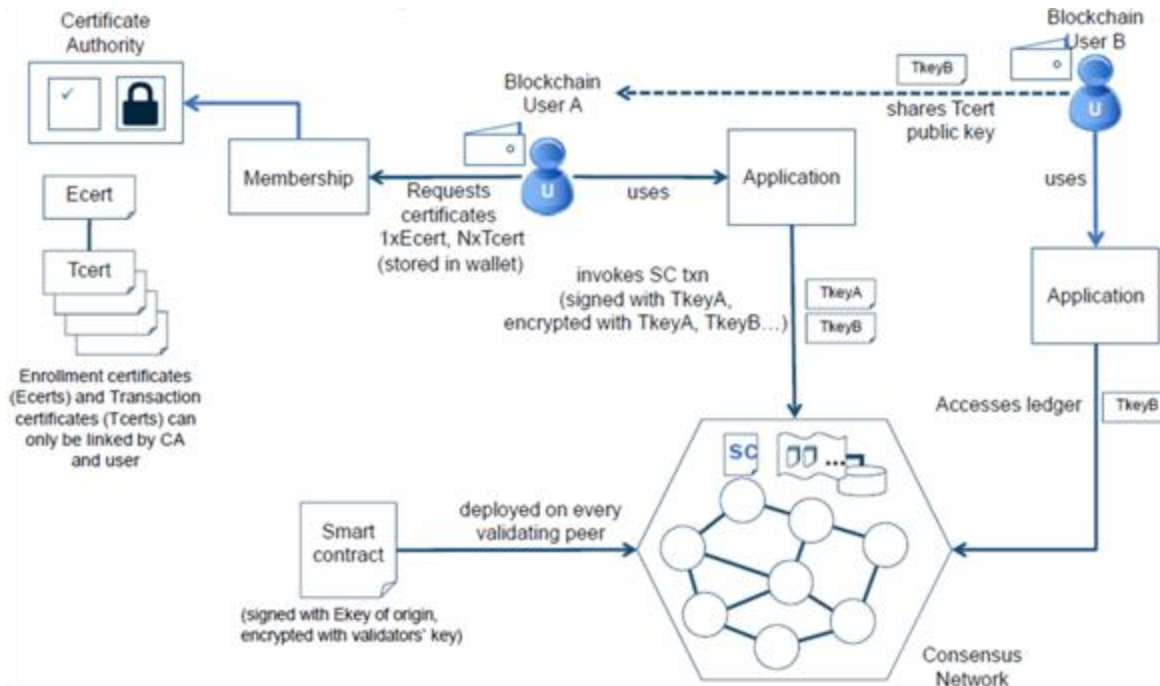
Hyperledger Fabric Platform Features:

- Permissioned shared Ledger with Need to know basis data sharing
- Identity Membership provider to manage members and permissions
- Separate Membership and Transaction certificates to members for security
- Chaincode (smart contracts) to endorse and validate the transactions on the shared ledger
- Enterprise grade and modern technology support like Rest / APIs with Docker containers.

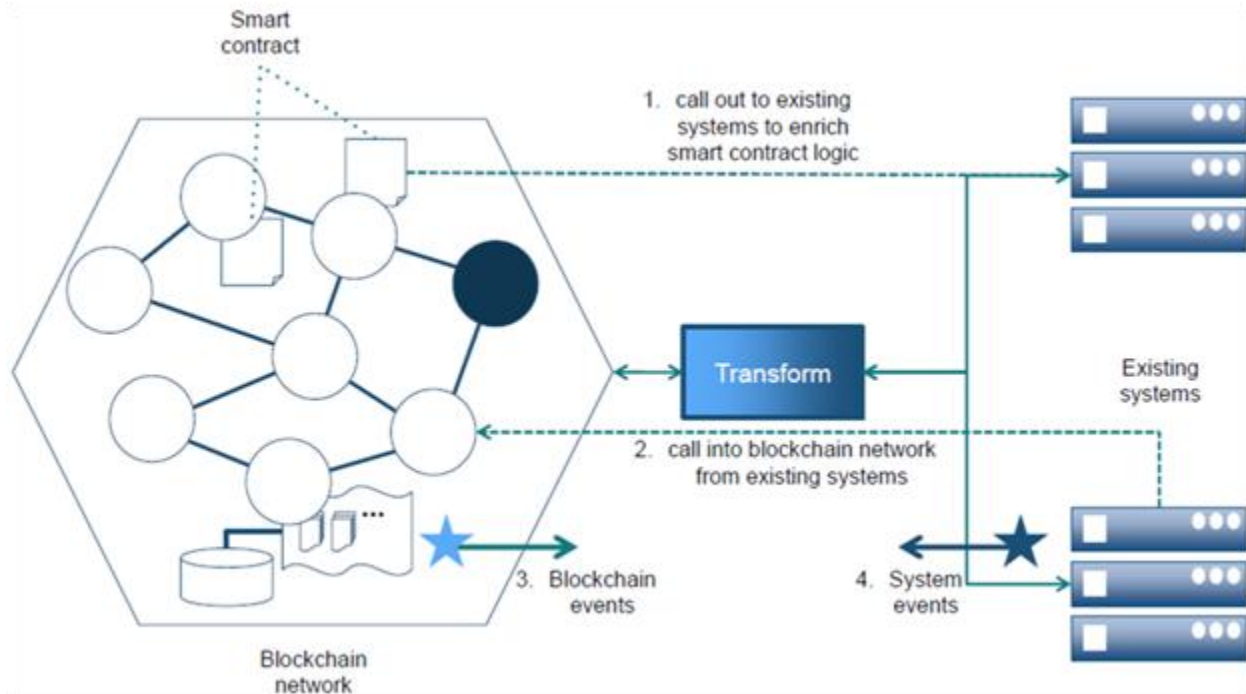
Permissioned Ledger Access:

1. User registers on the network. In return the membersrvsvc will create 1 Enrollment Certificate and n Transaction certificates

2. Blockchain Developer User creates a Smart Contract (SC) and *deploys* it by signing with his Enrollment Certificate. The SC is deployed on every VP
3. Blockchain User A *invokes* SC using his Transaction Certificate
4. Blockchain User B (Auditor) *queries* SC using Blockchain User A's Transaction Certificate (keys)



Blockchain Integration with existing applications:



8. Conclusion

A blockchain-based solution offers a unique set of advantages over the current crop of technology solutions, given its immutable ledger that can be replicated across different nodes and use of cryptography to convert information to hash codes for secure distribution over peer-to-peer network. These features enable seamless and secure exchange of information between different trusted entities. KYC is an apt candidate for the use of blockchain technology, as it results in significant reduction in of the time, cost, and effort involved in KYC validation.