CYBERBAHN
Training and Advisory Services

Record Educational Certificates on Blockchain for Authentication and digital verification (Implementation of Proof-of-Concept)

www.cyberbahntas.com

Digital Blockchain Certificates POC – What we are trying to solve..

- Academic credentialing fraud is a reality; methods include counterfeiting and through the complicity of an institution's authorities or staff.
- Need a straightforward process to verify the authenticity and genuineness of certificates.
- Manually submitting certificates/documents in paper records to various authorities increases chance of misusing the paper records by third person.
- Potentials for breach of privacy and personal security as no control on who is allowed to access the certificates.
- Centralized document storage not a solution as it is difficult to synchronize issuer, receiver and viewer entities together to authenticate the documents and centralized storage may be a single point of failure.
- A cryptographic hash function shall be applied on document and result may be stored on public blockchain in a transaction signed by private key of issuer institution which ensures the validity of documents.
- Blockchain with distributed storage like IPFS allows the document to be stored locally and shared with requester after proper validation.

For whom?

- This POC is for ICB: International Consortium for Blockchain.
- ICB accredits training providers (known as REPs – Registered Educational Partners) for blockchain-related courses.
- The REPs can then train people on the accredited Courses and ICB issues certificates on successful course completion.
- This POC deals with storing the details of the generated certificates on the blockchain and retrieving it upon request.

Digital Blockchain Certificates POC– Solution Overview

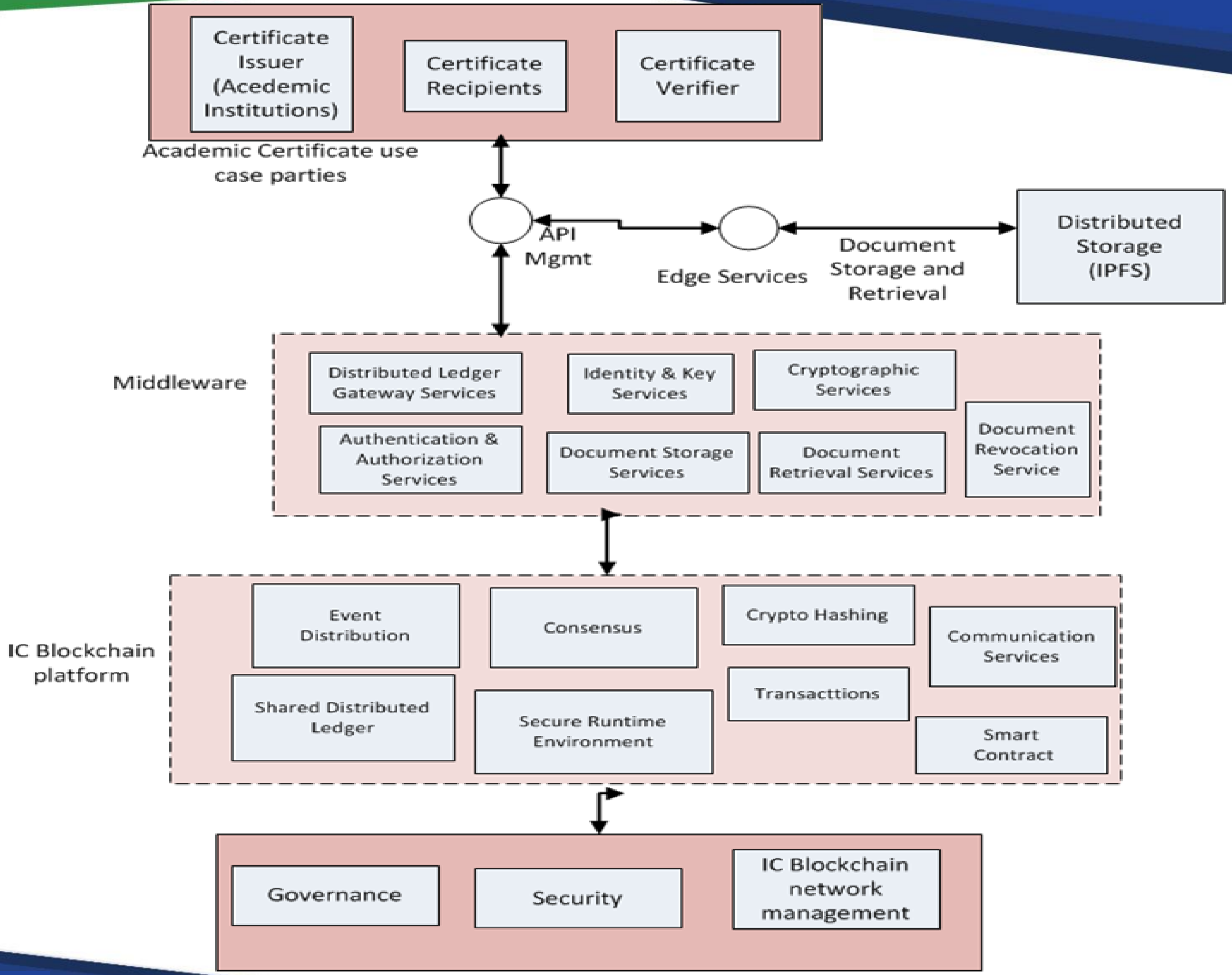
Our Digital Blockchain certificates POC based on Ethereum Platform consists of following components:

- **Certificate Issuer program** - The certificate issuer (ICB) issues blockchain certificates by creating a transaction from issuing institution to the recipient on the ethereum blockchain that includes the hash of the certificate itself. The blockchain may not be running locally on the machine of certificate issuer and may use REST web service API to lookup and broadcast transactions.
- **Certificate Verifier program** - The blockchain certificate contains the issuer information. The certificate verifier program provides mechanism to check certificate integrity and authenticity. The blockchain certificate also contains the Issuer revocation list to check if certificate has not been revoked by the Issuer or user and is not expired.
- **Certificate Viewer** - The cert-viewer project is a php/angularjs webapp to display and verify blockchain certificates after they have been issued and to allow learners to request a certificate and generate their own ethereum identity needed for the certificate creation process.

Digital Blockchain Certificates POC– Solution Overview…

- **API Management** - The API calls between issuer, requester, user and blockchain platform are made using secure REST web service calls. These API calls are made as wrappers to web3.js API calls which invoke smart contract functions related to Digital Blockchain certificates (issue certificates, request certificate, verify certificate and share certificate and transaction history.)
- **IPFS (distributed storage)** - The certificates stored on blockchain has associated registry smart contract with data structure that links to the document path URL (documents stored on IPFS) The requester after proper authentication and security verification will access the document URL and retrieve the document for access.
- **Messaging framework** - The messaging framework based middleware will be used to send request and response between requester and user and the actual document exchange.

Digital Blockchain Certificates POC– Solution Architecture


Certificate Issuer (Acedemic Institutions)
Certificate Recipients
Certificate Verifier
Academic Certificate use case parties
API Mgmt
Edge Services
Document Storage and Retrieval
Distributed Storage (IPFS)
Middleware
Distributed Ledger Gateway Services
Identity & Key Services
Cryptographic Services
Authentication & Authorization Services
Document Storage Services
Document Retrieval Services
Document Revocation Service
IC Blockchain platform
Event Distribution
Consensus
Crypto Hashing
Communication Services
Shared Distributed Ledger
Secure Runtime Environment
Transacttions
Smart Contract
Governance
Security
IC Blockchain network management

Digital Blockchain Certificates POC – Solution Overview

Our Blockchain based certification is designed to be:

- Secure in Access, Transmission and Distributed Storage of documents owned by document owners.
- Based on Modular components.
- Smart contracts with fine grained ownership checking rules to secure transactions.
- Smart transactions. Example:
  - when a issuer issues certificate– it updates transactions with certificate hash and generate receipt.
  - when a document requester requests a certificate – validates certificate, sends request to document owner, receive document along with signed digital certificate by issuing authority.
- Distributed Storage Architecture using IPFS , document owner can decide with whom to share documents.
- Ethereum Blockchain distributed transaction ledger to provide information on members identity and roles, certificate transaction history (issue, validation, revocation etc.)
- Authentication mechanism to validate the requestor using public/private key pair based credentialing.

Digital Blockchain Certificates POC– Technologies Used

The technology stack used in developing this POC is:

- Ethereum Blockchain (ethereum ropsten network)
- PHP/Angularjs for webApp development
- Solidity smart contracts
- IPFS distributed file storage
- RabbitMq /whisper – messaging framework
- PHP MVC for development of model view controller
- PHP laravel for RESTful web service framework
- PKI and digital certificates (X.509 digital certificates)

Digital Blockchain Certificates POC– Results

As a result of successful POC , our team would be able to

- Setup Ethereum Blockchain to store transactions about the digital certificates issued by academic institution and verified by requester.
- Shared distributed transaction ledger allows proof of existence of digital certificates issued by academic institutions and verified by the requester. Users can access and store documents on their IPFS storage and exchange documents with requesters.
- WebApps and (in future mobile apps) to interact with digital certificate smart contracts deployed in blockchain.
- Future Scope of work to extend POC use cases e.g.
  - Android and iOS mobile apps to store and validate the digital certificates.
  - Development of real time notifications to notify the requests made by various document requester and document exchanged by users.

Thank You

CYBERBAHN

Training and Advisory Services

www.cyberbahntas.com