CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

# PASS+ toward a Safe, Secure and Resilient Cyber Environment

Author: Geordy Vincent
Faculty Advisor: Dr. Zhixiong Chen(Mercy College), Dr. Deming Chen(UIUC)

## Homeland Security Challenge

Trustworthiness is important for the Cyber Infrastructure to build a safe, secure, resilient cyber environment. Recent attacks such as SolarWinds, Kaseya, and Codecov have shown the fragility of software supply chain, and the profitability it has for the attackers. The challenge we propose is a multi-party multi-level cryptographic token system known as Portfolio Artifact Service System (PASS). PASS allows a subject known as a holder to tokenize their portfolio artifacts such as diplomas, badges, knowledge, skills, and to store them in a decentralized verifiable data registry. This ensures trust between holders and their use applications. As an example, an applicant can present his/her PAs to a potential employer, and the employer could trust the presented claims without needing to manually check.

## PASS+ Objectives

The objectives of project is to build a trust environment in a 3D (Web3) Internet

1. Use ontology to structure portfolio artifacts (PAs) systematically
2. Develop JSON-LD schema to realize the PA structures
3. Design a decision expert system and develop machine learning models to build an engine to assess skill competency
4. Create portfolio artifacts (PAs) that are digitally signed, approved, or assessed by the assessment engine
5. Store these PAs in a decentralized blocks using Blockchain technology
6. Design and develop a platform that connects holders, certifiers or issuers, and end applications
7. Design and develop smart contracts that could create and retrieve PAs
8. Explore and design a consensus protocol, proof of me (PoM), to build secure and high performance blockchain

## Acknowledgements

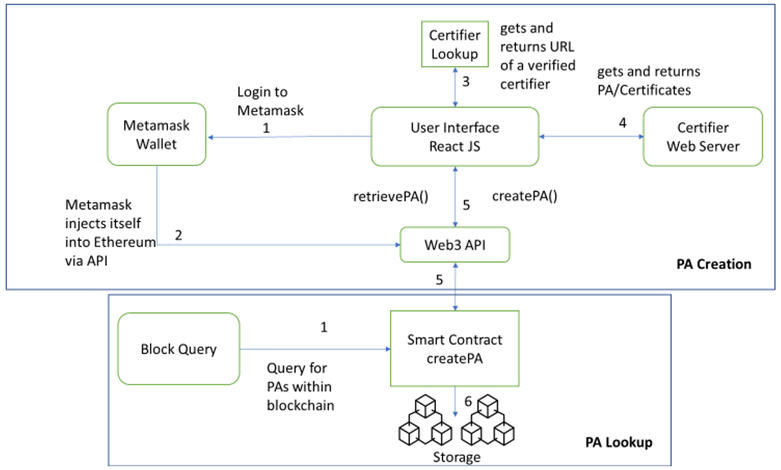
This research was performed under an appointment to the U.S. Department of Homeland Security (DHS) Science & Technology (S&T) Directorate Office of University Programs Summer Research Team Program for Minority Serving Institutions, administered by the Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS. ORISE is managed by ORAU under DOE contract number DE-SC0014664. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DHS, DOE or ORAU/ORISE..

## Methodology

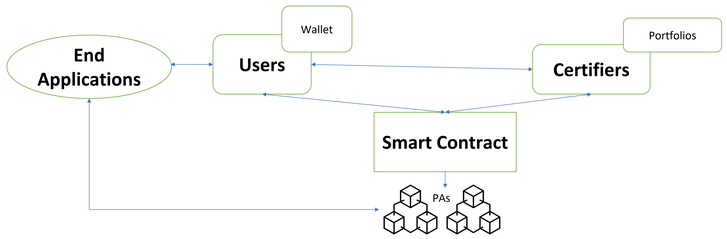
My focus in the project is on item 4-7 from PASS+ objectives

1. Use Truffle as the development environment to create and deploy Smart Contracts
2. Use Ganache to create a localized Ethereum Blockchain network to test Smart Contracts
3. Develop Smart Contract using Solidity Programming language
4. Use React Javascript Library to create the User Interface for the application
5. Use Web3.js API to connect the front-end to the Ethereum client
6. Use MetaMask Wallet to connect the user to the Ethereum network and also validate transactions
7. Use IPFS as the decentralized data storage for the application
8. Use Express to create Certification servers
9. Use Ganache Block Explorer to query blocks

### Workflow Diagram

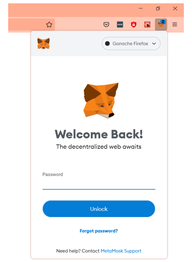



### Actor Diagram

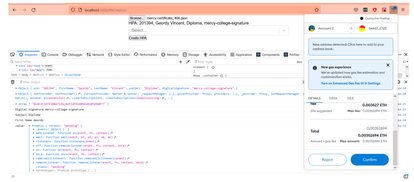



## Use Case Demo: PA Creation/ Retrieval

1. Login to metamask

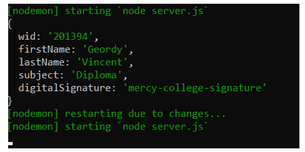



3. Upload the Certificate, and submit the certificate into the ethereum blockchain. Users must sign/confirm their transaction with Metamask for validity.



2. Request Diploma Certification from Mercy College and receive PA.

4. Lookup PA associated with an account from the front-end application





**Conclusion**: We established the technical feasibility of the project by showcasing a workflow and implementing a demonstrable use case scenario.

ILLINOIS