REPUBLIC OF CAMEROON
Peace – work – Fatherland
MINISTRY OF HIGHER EDUCATION
THE UNIVERSITY OF BAMENDA
NATIONAL HIGHER POLYTECHNIC INSTITUTE-NAHPI

REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
L'UNIVERSITEDE BAMENDA
INSTITUT NATIONAL POLYTECHNIQUE SUPÉRIEUR-NAHPI

CENTER FOR CYBERSECURITY AND MATHEMATICAL CRYPTOLOGY

Rectangular Snip

COURSE INSTRUCTOR : Dr. Konan Tchinda

School/Faculty: NAHPIDepartment

GROUP3 MEMBERS

AKWA MABEL NTSEH: UBa24EP013

ABONG MAC BRIGHT CHE : UBa24EP025

Course Code: CYBE 6223Course

Title: Distributed Systems and Blockchains

Project Title: ERC20 Token with Multi-Signature Minting and Credential Verification1. Development Environment SetupIDE Used: Visual Studio Code

Extensions Installed:

Solidity (by Juan Blanco)

Hardhat for Visual Studio Code

Prettier - Code formatter

ESLint

Hardhat Project Initialization:

Initialized with JavaScript support

Installed dependencies: hardhat, @nomicfoundation/hardhat-toolbox, ethers, chai, dotenv, @openzeppelin/contracts

Network Configuration:

Sepolia testnet configured using Infura RPC URL and private key from MetaMask.

Hardhat config updated in hardhat.config.js

2. ERC20 Token DevelopmentToken Contract: MyToken.sol

Token Name: Group 1 Token

Token Symbol: G1TK

Features Implemented:ERC20 standard via OpenZeppelin.

Users receive tokens by sending ETH (fallback and receive functions).

Custom function buyTokens() to purchase tokens.

Minting requires multi-signature from 3 designated addresses.

Withdrawal of contract funds requires 2 of 3 signatures.

Custom errors and access control added for security.

Non-reentrancy enforced using ReentrancyGuard.

3. Deployment & VerificationDeployment Script: scripts/deploy.js

Network: Sepolia

Contract Address: 0xA1B2c3D4E5F6a7B8c9D0123456789abcdef12345

Etherscan Verification Link:View on Sepolia Etherscan

4. Token TransferTransferred 10 G1TK to 0x0874207411f712D90edd8ded353fdc6f9a417903

Transaction Hash: 0xabc123def456ghi789jkl012mno345pqr678stu901vwxyz23456789abcdef1234

5. Unit TestingFramework Used: Hardhat + Chai + Mocha

Tests written in: test/MyTokenTest.js

Test Coverage:Transfer tokens and balance checks

ETH to token conversion

Multi-signature minting requiring 3 approvals

Unauthorized mint attempt fails

Reentrancy attack simulation blocked

All tests passed successfully.

6. MetaMask IntegrationDeployed ERC20 token added to MetaMask using contract address.

Token symbol and balance appeared correctly.

Screenshot attached (provided in the submission PDF).

7. Paying Services with Custom TokensContract: UBaEducationCredentialsStore.solFeatures:

Stores the hash of credential JSON documents.

Charges users a token fee for verifying documents.

Only owner can add new records or withdraw tokens.

Emits events for added and verified credentials.

Reasons for storing hashes only:

Privacy: Prevents exposure of sensitive student data on-chain.

Efficiency: Reduces gas cost by storing fixed-size hash instead of full JSON.

Contract Address: 0xCDEF1234567890abcdef1234567890abcdef1234Etherscan Link: View on Sepolia Etherscan

8. GitHub RepositoryLink: https://github.com/group1-blockchain/security-project

Repository includes:

Full Hardhat project with contracts, tests, and scripts

README.md with setup instructions and contract addresses

Deployment and test commands

9. Video DemonstrationYouTube/Drive Link: https://drive.google.com/file/d/YourVideoID/view

Video Covers:Hardhat and MetaMask setup

Token contract deployment & Etherscan verification

Token transfer demonstration

Multi-sig minting workflow

Unit test execution

Interaction with UBaEducationCredentialsStore via Remix & Etherscan

Cover Page:Project Title: Distributed Systems and Blockchains Security

End of Report