Cryptography (BITS F463)

Term Project

Weightage: 15%

Centralized UPI Payment Gateway with Blockchain, SHA 256, LightWeight Cryptography, and Quantum Cryptography

1. Introduction

The exponential growth in digital transactions has revolutionized the financial landscape, significantly reducing the reliance on physical cash. With the widespread adoption of **Unified Payment Interface (UPI)** systems, users can conduct seamless and instant financial transactions. However, this increased convenience brings about major security challenges. Ensuring data privacy, safeguarding against fraudulent activities, and maintaining accurate transaction logs are critical requirements for any UPI payment gateway.

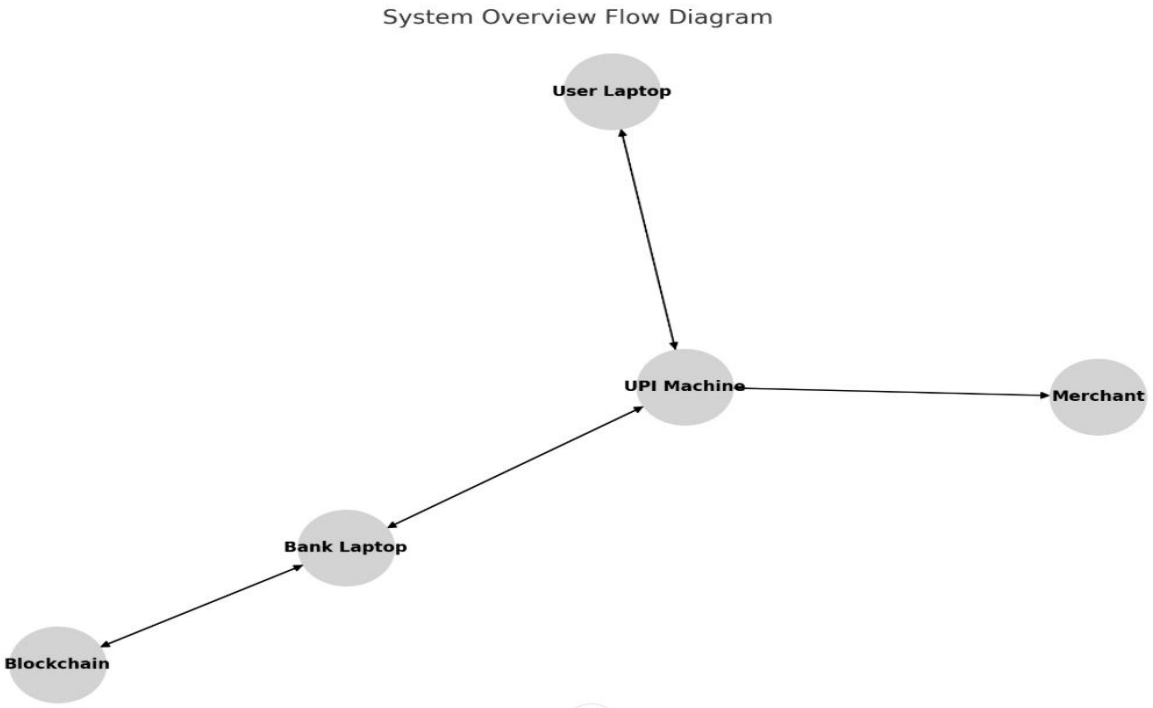
In the current financial ecosystem, ensuring high-level security for UPI transactions is essential due to increasing cyber threats. The integration of **Blockchain**, **Lightweight Cryptography (LWC)**, and **Quantum Cryptography** is proposed in this system to ensure data confidentiality, prevent tampering, and maintain trust among users. The system will leverage Blockchain technology for maintaining secure and immutable transaction records, LWC for ensuring lightweight and fast encryption processes, and Quantum Cryptography using Shor's Algorithm to identify potential vulnerabilities in user credentials like PIN and MMID.

This document outlines a detailed problem statement to design a **Centralized UPI Payment Gateway**, describing the core functionalities, data flow, encryption methods, and technical requirements. Furthermore, we describe the role of each participating entity, the process of payment initiation, the security infrastructure, and the expected challenges, ensuring maximum security and efficiency in digital transactions.

2. System Overview

The **Centralized UPI Payment Gateway** aims to simulate a complete digital transaction system in a secure and verifiable manner. This system will be designed using three physical devices acting as separate entities:

- **UPI Machine:** This device will act as the central processing machine mimicking the behavior of sound-box machines used by merchants for payment validation. It is responsible for encrypting merchant info and communicating with the bank server and user.
- **User Laptop:** This device will act as a user platform where the user initiates a payment by scanning a QR code, entering their transaction amount, MMID, UPI ID, and PIN.
- **Bank Laptop:** This device acts as a banking terminal allowing bankers to access transaction data of the bank.



The system consists of the following critical processes:

- **Bank Registration:** There are 3 banks in our system HDFC bank, ICICI and SBI. Each bank has 3 branches which can be identified by their unique IFSC code, merchant and users will open their account in any one of these branches.
- **Merchant Registration:** Merchants are required to register with the bank by providing their name, IFSC code, password to access account, and amount in account. The bank then generates a 16 digit **Merchant ID (MID)** which is their account number. MID is formed using their name, time of account creation and password hashed using **SHA256** algorithm and converted into a 16 digit hexadecimal number. This is unique to every merchant and shouldn't be shared.
- **User Registration:** Users also need to have their bank account in any branch of the bank. The registration is similar to a merchant. But the bank also stores a PIN that will be set by users for doing UPI transactions. The **16 digit number** is referred to as **UID**. Users use UID and mobile number to create their MMID which is used in UPI transactions.
- **QR Code Generation:** Merchant enters his/her Merchant ID, the machine should encrypt it using LWC algorithm and generate a qr code which upon scanning reveals the encrypted number.
- **Payment Process:** The user scans the QR code using their phone, providing MMID, transaction amount and PIN to initiate the transaction. This data is hashed and sent to the UPI machine.
- **Transaction Processing:** The UPI machine decrypts the merchant ID from the QR code, forwards the request to the bank, and waits for transaction approval.
- **Bank Processing:** The bank decrypts the user credentials and validates the transaction amount, MMID, and PIN. If successful, the transaction is recorded in the blockchain, and funds are transferred to the merchant.

The integration of Blockchain ensures that each transaction is immutable and transparent, Lightweight Cryptography guarantees fast and secure encryption.

3. Entities Involved

The system is designed to interact between four key entities: the **Bank**, **Merchant**, **User**, and **UPI Machine**. Each entity has a unique role and responsibility in ensuring the successful processing of a transaction.

3.1 Bank

The **Bank** is the central governing body responsible for managing the financial accounts of both users and merchants. It acts as the ultimate decision-maker for processing payments, validating credentials, and ensuring funds availability.

Responsibilities of the Bank:

- **Merchant Registration:** The bank registers the merchant by collecting the following details:
    - **Merchant Name**
    - **Password**
    - **Initial account balance**
    - **IFSC Code**
- **User Registration:** The bank registers the user and by linking their mobile number to a **Mobile Money Identifier (MMID)** generates a UPI ID.
- **Generating Virtual Merchant ID (VMID):** Mechant enters his MID in upi machine which uses LWC algorithm to generate a VMID.
- **Transaction Verification:** During any payment request, the bank verifies the transaction details including MMID, PIN, and available balance.
- **Blockchain Ledger Maintenance:** All valid transactions are securely stored in a blockchain ledger ensuring immutability and transparency.

3.2 Merchant

The **Merchant** is an individual or business entity willing to accept payments from users through the UPI system.

Responsibilities of the Merchant:

- **Providing Bank Details:** The merchant shares their bank account details including Account Number, IFSC Code, and personal information.
- **QR Code Generation:** The merchant receives a QR code from the UPI machine containing the hashed VMID. This QR code is displayed for payment.
- **Transaction Confirmation:** After payment, the merchant receives a success/failure message from the bank via the UPI machine.

3.3 User

The **User** is the individual initiating the payment by scanning the QR code and entering the payment details.

Responsibilities of the User:

- **Providing Payment Details:** The user provides their MMID, PIN, and Transaction Amount during the payment process.
- **Authorizing Payment:** The user confirms the payment after scanning the QR code.
- **Receiving Confirmation:** The user receives a success/failure message from the bank through the UPI machine.

3.4 UPI Machine

The **UPI Machine** acts as an intermediary between the **User**, **Merchant**, and **Bank**. It ensures encrypted communication and relays transaction requests to the bank.

Responsibilities of the UPI Machine:

- **Encrypting Merchant ID:** The UPI machine encrypts the merchant ID from the QR code.
- **Relaying Transactions:** The UPI machine sends transaction requests to the bank and waits for approval.
- **Providing Confirmation:** Based on the bank's response, it notifies both the user and merchant regarding payment success/failure.

4. Role of Lightweight Cryptography (LWC)

LWC is used for:

- Generating Virtual Merchant ID (VID) from Merchant ID and timestamp.
- Ensuring lightweight computational overhead to reduce transaction processing time.
- Encrypting Merchant ID in the QR code.
- Use SPECK (Simple Permutation Encryption) algorithm for lightweight cryptography designed for high-speed encryption in resource-constrained environments.

5. Role of Quantum Cryptography

Quantum Cryptography is introduced in the following manner:

- The system simulates **Shor's Algorithm** to break the User's PIN and ID.
- This highlights the vulnerability of classical cryptography in UPI systems.
- The implementation will use Quantum Cryptographic libraries to demonstrate the potential breach.

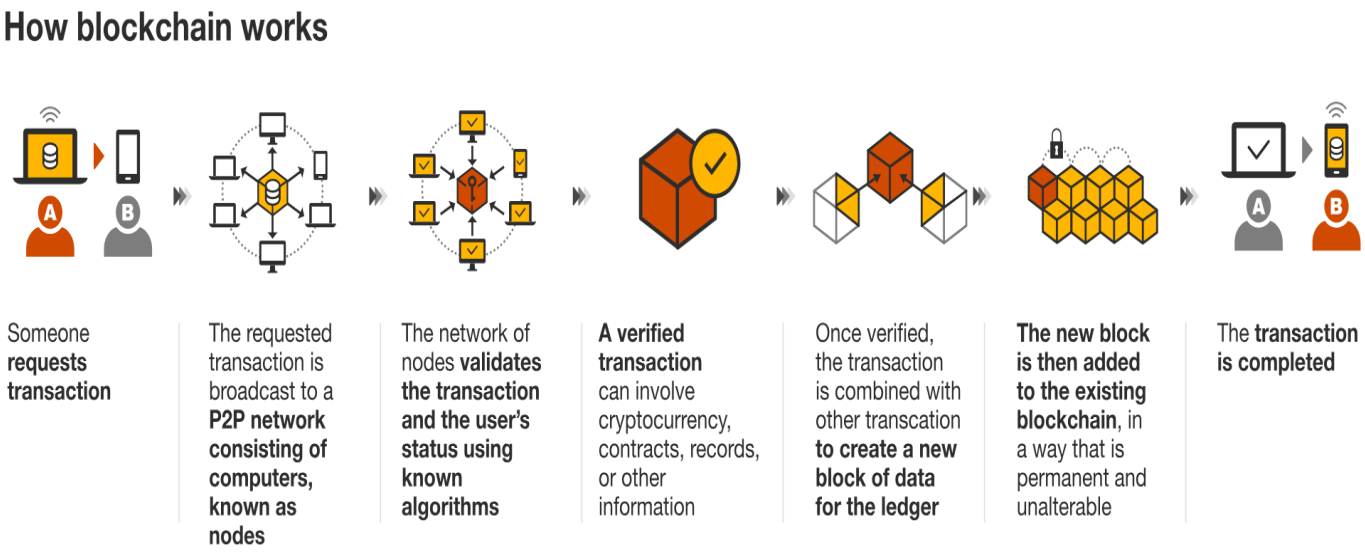
6. Role of Blockchain

Each bank maintains a Centralized Blockchain Ledger where valid transactions are recorded.

Transaction Block Structure:

- Transaction ID (Hash of UID, MID, Timestamp, Amount)
- Previous Block Hash
- Timestamp
- Every valid transaction creates a new block.

This ensures immutability and transparency in UPI transactions.



7. Outcomes of the Project

By the end of this project, the following outcomes will be achieved:

- A fully functional centralized UPI Payment Gateway mimicking real-world UPI transactions.
- Lightweight Cryptography (LWC) for VID generation and hashing.
- Quantum Cryptography Simulation (Shor's Algorithm) to demonstrate PIN vulnerabilities.
- Blockchain Integration for secure transaction logging and validation.

8. Further Reading

- **What is LightWeight Cryptography ?**
- **SPECK Algorithm**
- **SPECK Algorithm Paper**
- **WTF is The Blockchain? | HackerNoon**
- **Shor Algorithm Explained**

9. Deliverables

Submit your source code and a README file as a single .zip or .tar file. Please name your file as **BITSF463_Team_99** (assuming your team number is 99. You can find your team number from the google sheet). The readme should contain a brief explanation of the project, steps to run the code, and the list of team members. **Deadline: 11:59 PM, April 11th, 2025.** The exact date and demo schedule will be intimated later. From a team, **only one team member needs to do the submission**.

The students are advised not to resort to any sort of copying of code from others. Marks will be reduced for copying.

For queries regarding the assignment, the students may approach the **TA** of the course
1. **Nishchay Deep** (**f20213144@hyderabad.bits-pilani.ac.in**)