Domain: Cyber Security

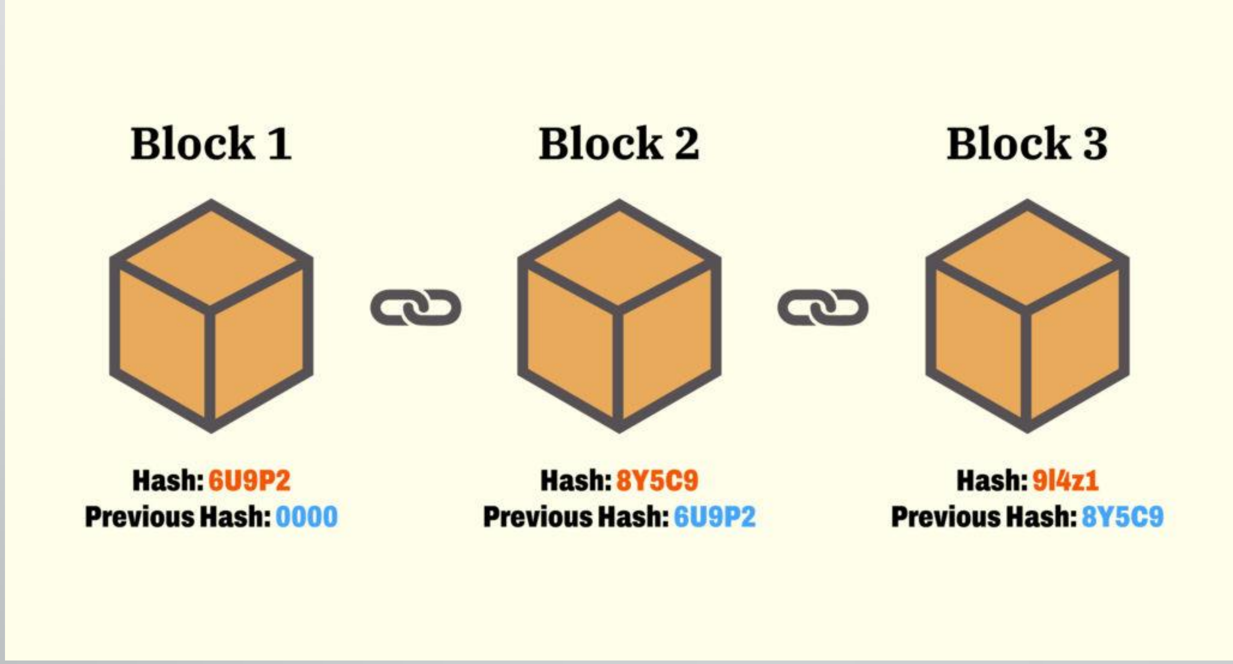
Mentor: Kalyan Das

Team Members: Digbijoy Dutta || Abhijan Mallick

Pranab Saha || Mahan Brata Raha

Project Ideation

- **Blockchain:** A distributed decentralized ledger which is transparent in nature to all the nodes in the network and any alteration is not possible after deployment.



Advantages:

□ Shared.
□ Immutability.
□ Integrity.
□ Verifiable, Visibility.
□ Control of data.
□ Security & Privacy.

Component of Blockchain

Node

- **<u>Full Node</u>:** Contains full copy of transaction. Able to validate, reject, accept transactions.
- **<u>Partial Node</u>:** Lightweight node. Contains hash. Transactions accessed using hash.

Ledger

Digital Database of information.

- Public Ledger
- Distributed Ledger.
- Decentralized Ledger.

Wallet

It is a digital wallet that allows user to store their cryptocurrency. Privacy of a wallet in a blockchain network is maintained using public and private key pairs.

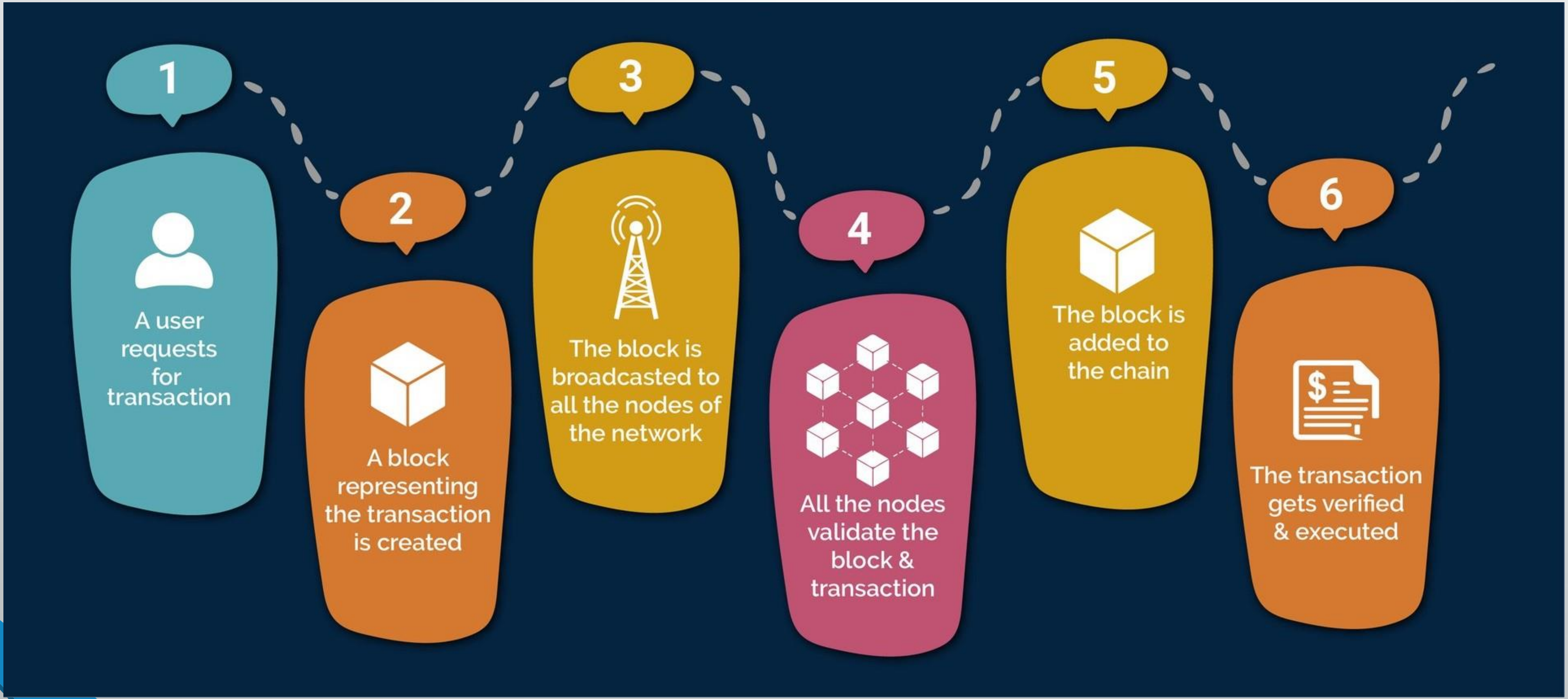
Nonce

The Nonce is a random whole number, which is a 32-bit (4 byte) field, which is adjusted by the miners, so that it becomes a valid number to be used for hashing the value of block. Nonce is the number which can be used only once.

Hash

The data is mapped to a fixed size using hashing. It plays a very important role in cryptography. In a blockchain network hash value of one transaction is the input of another transaction.

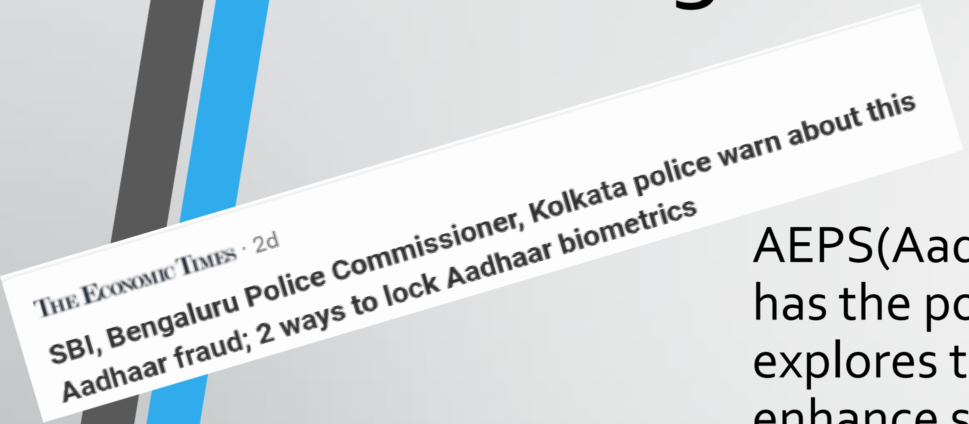
How transactions works in blockchain?



1
A user requests for transaction
2
A block representing the transaction is created
3
The block is broadcasted to all the nodes of the network
4
All the nodes validate the block & transaction
5
The block is added to the chain
6
The transaction gets verified & executed

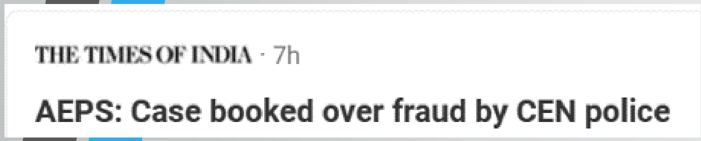
Topic: AEPS using Blockchain

Securing AEPS through Blockchain Technology



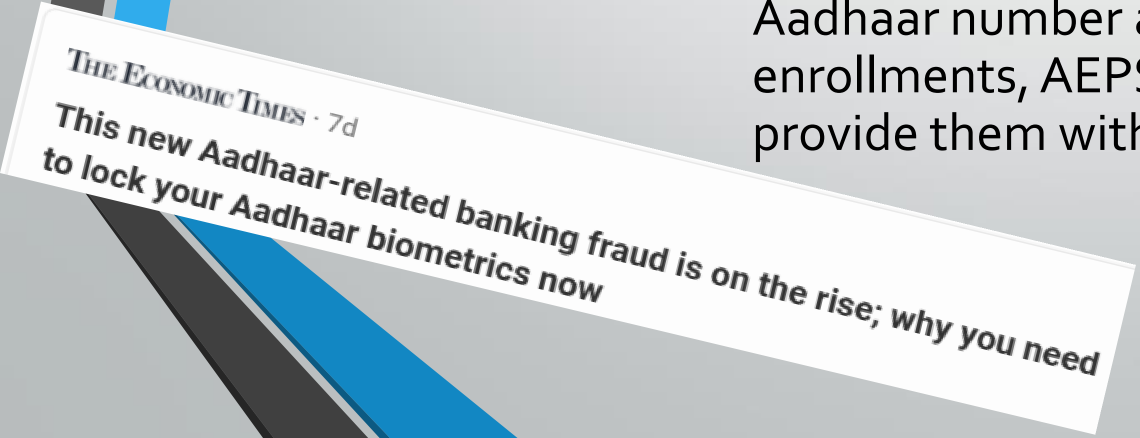
The Economic Times · 2d

SBI, Bengaluru Police Commissioner, Kolkata police warn about this Aadhaar fraud; 2 ways to lock Aadhaar biometrics



THE TIMES OF INDIA · 7h

AEPS: Case booked over fraud by CEN police



The Economic Times · 7d

This new Aadhaar-related banking fraud is on the rise; why you need to lock your Aadhaar biometrics now

AEPS(Aadhaar Enabled Payment System) is a revolutionary technology that has the potential to transform financial inclusion in India. This presentation explores the benefits of integrating blockchain technology with AEPS to enhance security, transparency, and efficiency in the financial ecosystem.

AEPS is a biometric-based payment system that allows individuals to access their bank accounts, make transactions, and withdraw cash using their Aadhaar number and fingerprint authentication. With over 1.2 billion Aadhaar enrollments, AEPS has the potential to reach the unbanked population and provide them with easy access to financial services.

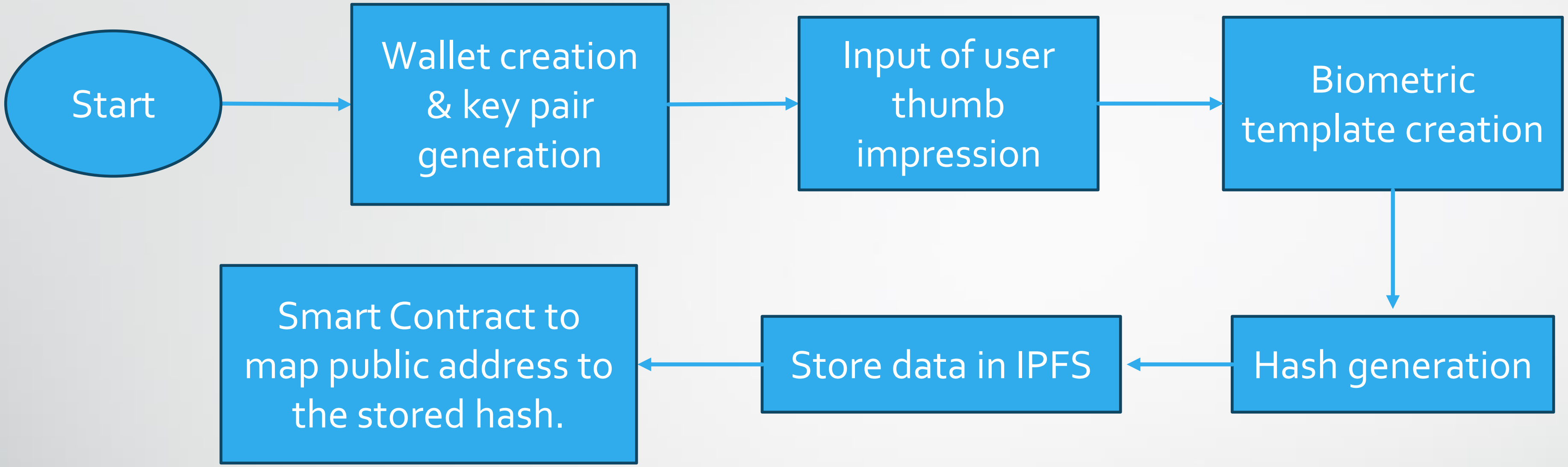
Continuation…

- Several frauds are led out across the country using the fingerprints collected. Such frauds, Man in the Middle attacks, all this could be easily handled by securing the transactions using Blockchain.
- The transactions would be secured since just getting the fingerprints would not help the attackers. They would require a private key along with the fingerprints to carryout the frauds.
- The hash of the fingerprint data would be used for the transactions, so even if there is slightest of chance of Man in the Middle attack, and the attacker getting the hash but there is no chance of getting the original data since hash is irreversible.

Encryption Concepts

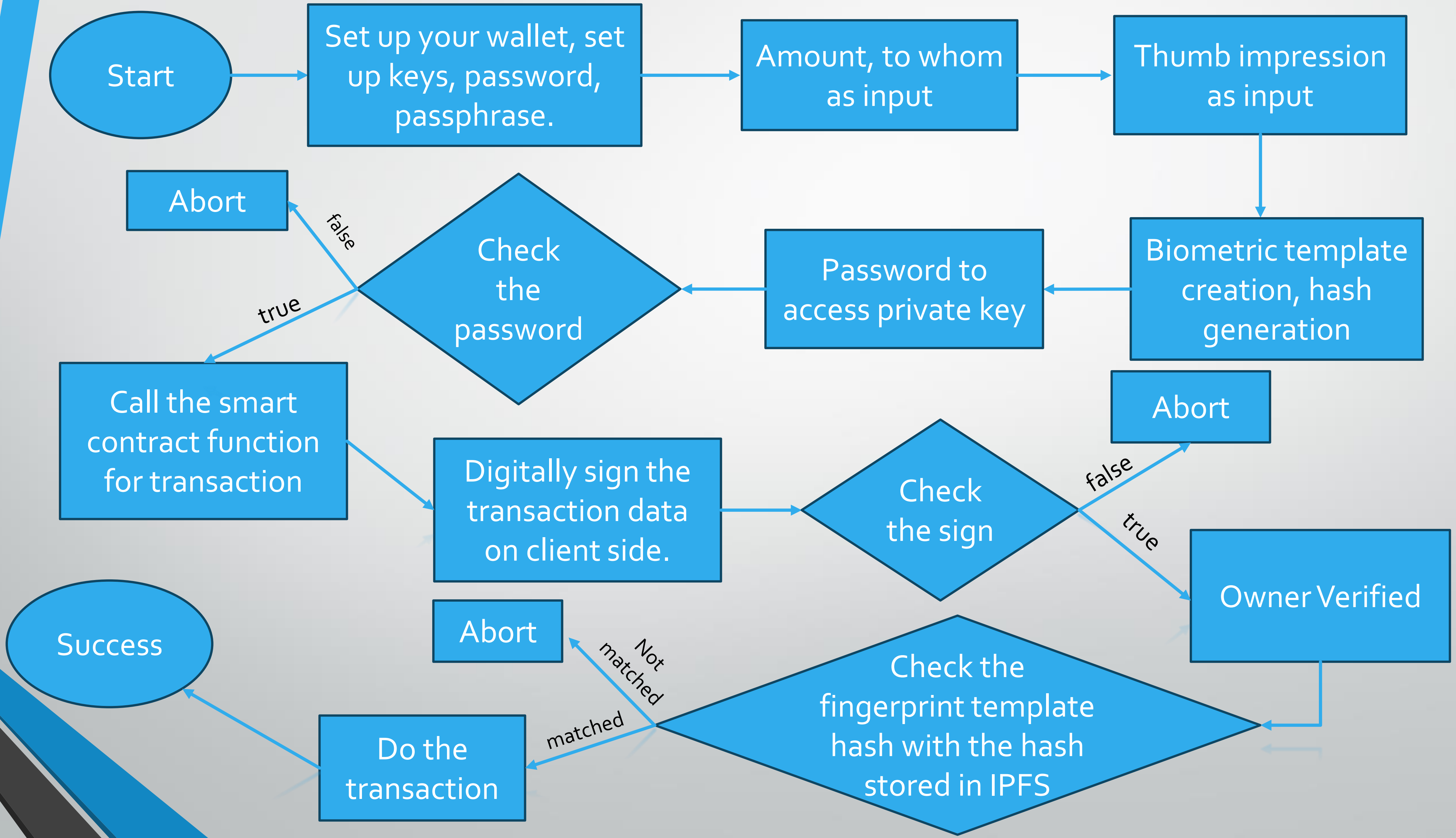
- Public key cryptography
- Digital signatures to authenticate owner.
- Hash
- Biometric Template
- Authentication(Identity) + Authorization(Access management)

Flowchart of User Registration


Start
Wallet creation & key pair generation
Input of user thumb impression
Biometric template creation
Hash generation
Store data in IPFS
Smart Contract to map public address to the stored hash.

- Points to be checked:
    - Whether the user already has registered.
    - Authenticity of the registration using digital signature.

Flowchart of Transaction



Start

Set up your wallet, set up keys, password, passphrase.

Amount, to whom as input

Thumb impression as input

Biometric template creation, hash generation

Password to access private key

Check the password

Abort

Call the smart contract function for transaction

Digitally sign the transaction data on client side.

Check the sign

Abort

Owner Verified

Check the fingerprint template hash with the hash stored in IPFS

Abort

Do the transaction

Success

Key Management

- To access the private key, Multi Factor Authentication should be used. (Password or Pin and OTP)
- Password should be changed at regular interval.
- A long security phrase (10-12 words long) can be used to recover wallet, this should be kept offline.
- Software should be updated regularly.
- If passwords or keys or phrases are stored locally, better to encrypt them with strong algorithms and store the encryption key offline.

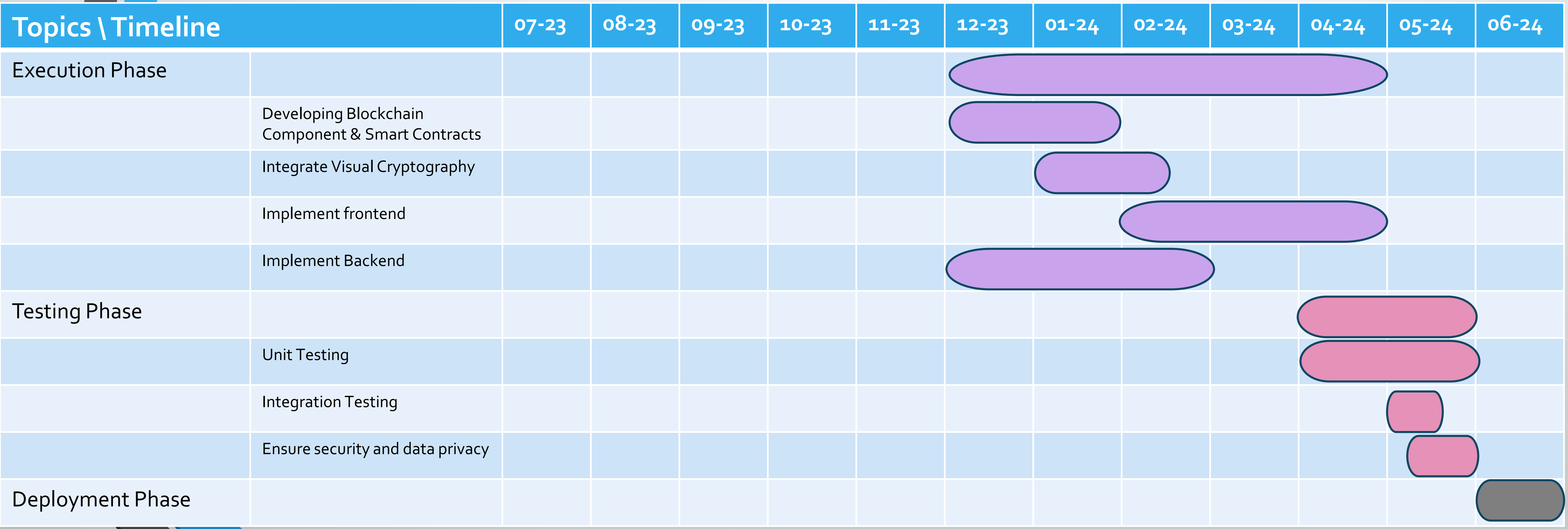
Technologies in use

- Solidity
- JavaScript
  - React.js
  - Web3.js
  - Node.js
  - Express.js
- Truffle
- Ganache
- Metamask

Gantt Chart

Topics \ Timeline		07-23	08-23	09-23	10-23	11-23	12-23	01-24	02-24	03-24	04-24	05-24	06-24
Requirement Gathering		■	■	■	■	■							
	Research Blockchain Technology	■	■	■									
	Study Encryption Method		■	■									
	Learn about visual cryptography				■								
	Understand smart contract implementation			■	■	■							
Project Planning				■	■								
	Define project scope			■									
	Identify project objectives			■									
	Develop a project plan			■	■								
Design Phase					■	■							
	Create system architecture					■							
	Develop a flowchart of the payment system				■								

Gantt Chart



Topics \ Timeline		07-23	08-23	09-23	10-23	11-23	12-23	01-24	02-24	03-24	04-24	05-24	06-24
Execution Phase							■	■	■	■	■		
	Developing Blockchain Component & Smart Contracts						■	■					
	Integrate Visual Cryptography							■	■				
	Implement frontend								■	■	■		
	Implement Backend						■	■	■				
Testing Phase											■	■	
	Unit Testing										■	■	
	Integration Testing											■	
	Ensure security and data privacy											■	
Deployment Phase													■

Thank You!