CUSTOMER DATA PRIVACY AND SHARING USING BLOCKCHAIN TECHNOLOGY

Aim: To design an integrated banking kiosk system which automatically checks for authentication via blockchain based KYC.

Components: R-Pi board incorporating blockchain technology, biometric scanner used for authentication, GSM module to add a 2 way security protocol, IOT module to store database on cloud server and a display panel.

Problem we target: KYC is mandatory in all banks nowadays as it is applicable for the following - *Customer Admittance, Customer Identification, Monitoring of banking activity, Risk management*, etc.

Despite being accepted globally, KYC faces some challenges such as - Disparity in specifications(Every bank has their own specifications they adhere to, lack of standardisation), Stringent regulations, Adverse impact on customer relationships, *Escalating cost*, etc.

Blockchain is an immutable distributed ledger shared in the public domain. Every participant interacts with the blockchain using a public-private cryptographic key combination.

In its essence, since it is devoid of any single central authority, we plan on developing a system wherein banks will use blockchain technology and it applications to solve the hassles created by the present use of the KYC process.

For KYC operations, banks can use a either a private or a public blockchain. In a private one, the bank uses it for its internal audit and regulatory compliance. In a public one, where it shares data and control with other institutions.

We plan on implementing an intra-bank blockchain based KYC system, where each customer will have their details secured in a blockchain with the help of an unique identification key. Basis this, KYC can be done across various branches of the bank with just customer authentication across any of the branches.

Solution we provide:

Blockchain technology :

Whenever a new customer enters into the ecosystem, the ‘Trusted Party’ i.e. the bank verifies the documents. Once checked, the bank uploads this data onto the blockchain. Whenever any new data is needed to be appended, the ledger could enable encrypted updates to the ledger. These updates can be accessed by other entities in real time as and when required.A Digital Identity — analogous

to a digital passport — of the on-boarded customer can then be used as a trust sign for future transactions.

Advantages:

DATA QUALITY-Data alterations can be tracked and monitored — chances of misuse and fraud are reduced. Since all data is stored in a homogeneous blockchain, resulting better governance and use of data would help banks detect fraud at an earlier stage.

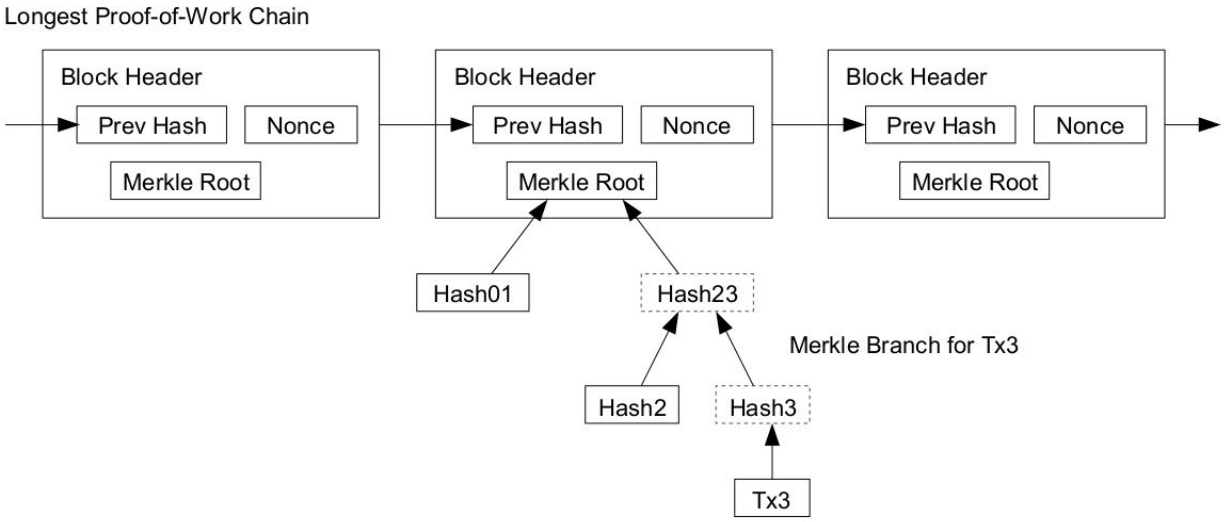
LOWER TURNAROUND TIME-Direct access to the KYC data could save huge amount of time for institutions.The hassle of disparity in specifications can thus be eliminated.

CIRCUMVENTING MANUAL EFFORT-Required compliance reports can be automatically generated from the data of the blockchain. This would help reduce non-compliance penalties.Manual error while performing the KYC initiation can be avoided.

Distributed: The ledger is replicated across a number of computers, rather than being stored on a central server. Any computer with an internet connection can download a full copy of the blockchain.

Immutable: The blockchain can be changed in append only fashion. In other words, votes can only be added to the blockchain but cannot be deleted or modified.

Use of Proof of Work (PoW)

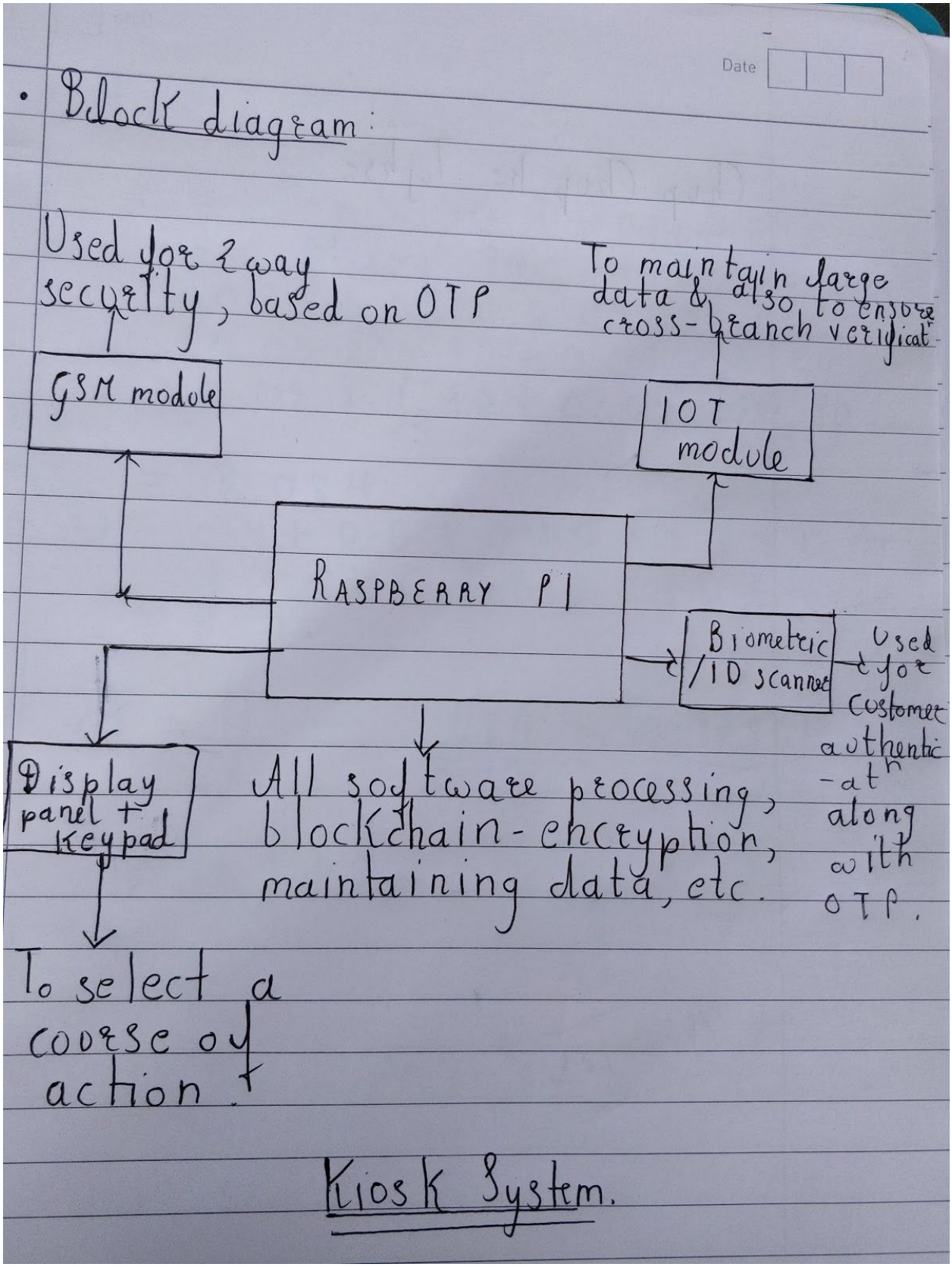


Hardware: We plan to implement a banking kiosk on a R-Pi board, with integrated display board and keypad. We will have different applications (say opening a FD, applying for loan ,etc). Based on any of the applications, a background check will be done using Blockchain encrypted KYC. The data encrypted in a ledger will be stored on a cloud server, which we will implement using an IOT module. Via this we aim to achieve a higher processing speed at hardware level and would avoid the case of overloading the hardware because of a heavy database. If valid information is found corresponding to ID recognition (biometric/ID scanner), permission to proceed further will be granted. The idea behind interfacing a scanning device is used for the purpose of customer authentication/identification so as to maintain no bogus activities. We also aim at using the biometric details to collect the necessary personal information for further security check(say AADHAR details,valid Voter id, etc.). The initial plan is to work on small data set and then extend it with more datasets.

Our system will incorporate the following case apart from pan-branch KYC, suppose a person wants to access their bank account for a certain procedure from a state X in the country but their account is set up in another state(say state Y), they will only require to add their biometrics and all the above info will be retrieved. A security otp msg will be sent via GSM module. The fingerprint will be cross checked with blockchain hosted on cloud, IOT based.

Software: The Blockchain algorithm will be implemented using Python, JSON and Flask library in Python. Customer authentication will be achieved using a biometric sensor, where simple but powerful ML algorithms will be deployed for training the data set.

Blockchain will include name, age, address proof, income proof photo where did the person first do kyc (say which branch), digital signature, etc.


Date
• Block diagram:
Used for 2 way security, based on OTP
To maintain large data & also to ensure cross-branch verificat
GSM module
IOT module
RASPBERRY PI
Biometric / ID scanner
Used for Customer authentic -ath along with OTP.
Display panel + keypad
All software processing, blockchain-encryption, maintaining data, etc.
To select a course of action.
Kiosk System.

CUSTOMER DATA PRIVACY AND SHARING USING BLOCKCHAIN TECHNOLOGY