Internet Banking Networks

(IB-NET)

Ganesh T S	– ESD18I006
Karthika Rajesh	– EDM18B026
Manas Kumar Mishra	– ESD18I011

IIITD&M
Kancheepuram

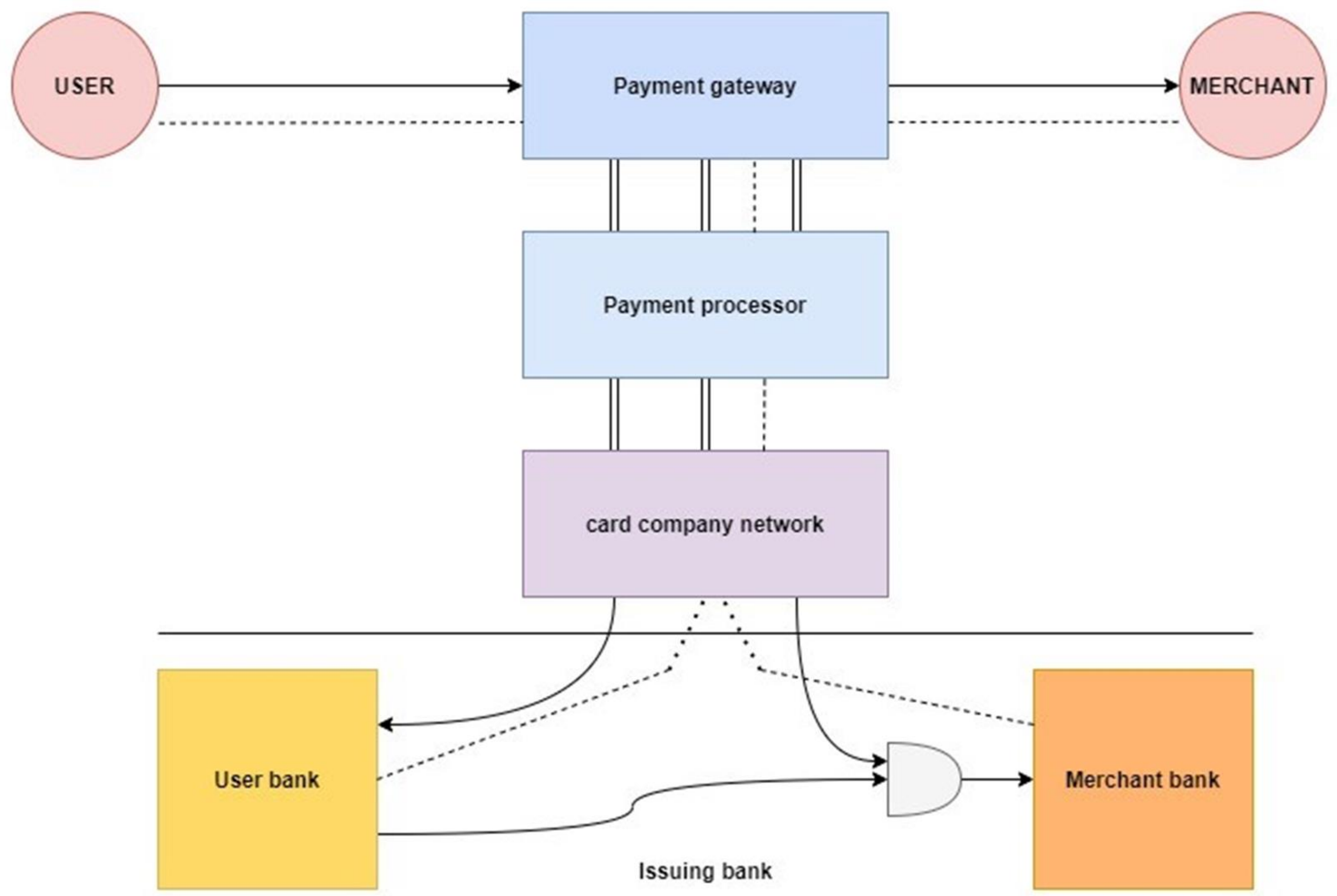
WHY?

Why are we doing this?

To understand the internet banking network through day-to-day digital transaction process.

How?

How actually transactions take place?


USER
Payment gateway
MERCHANT
Payment processor
card company network
User bank
Merchant bank
Issuing bank

WHAT ?

There are six separate modules of this project

1 . USER and MERCHANT

2. Payment Gate-ways

3. Payment processor

4. Card company

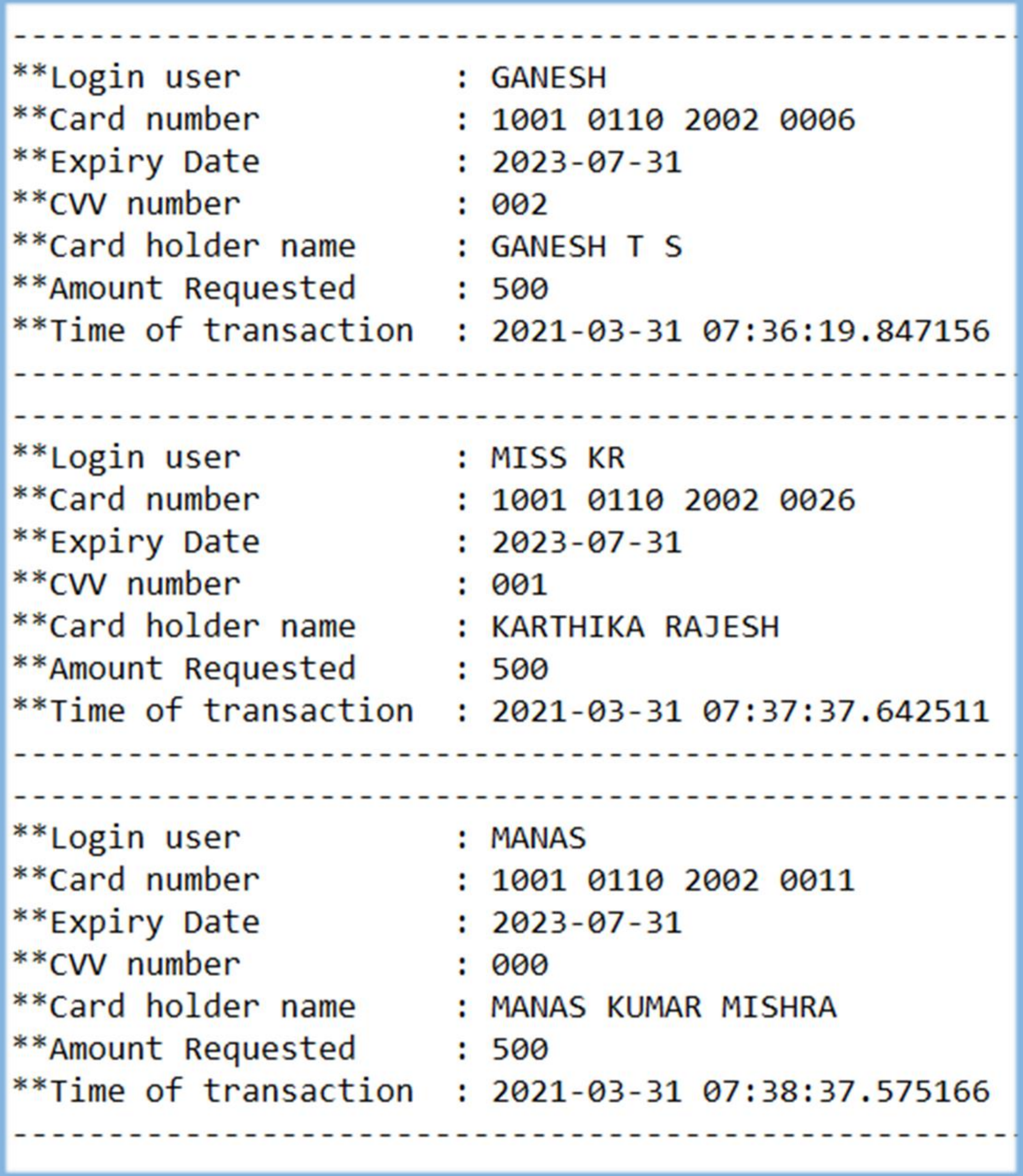
5. Banks (TPS)

6. Feedback

Source:- Internet

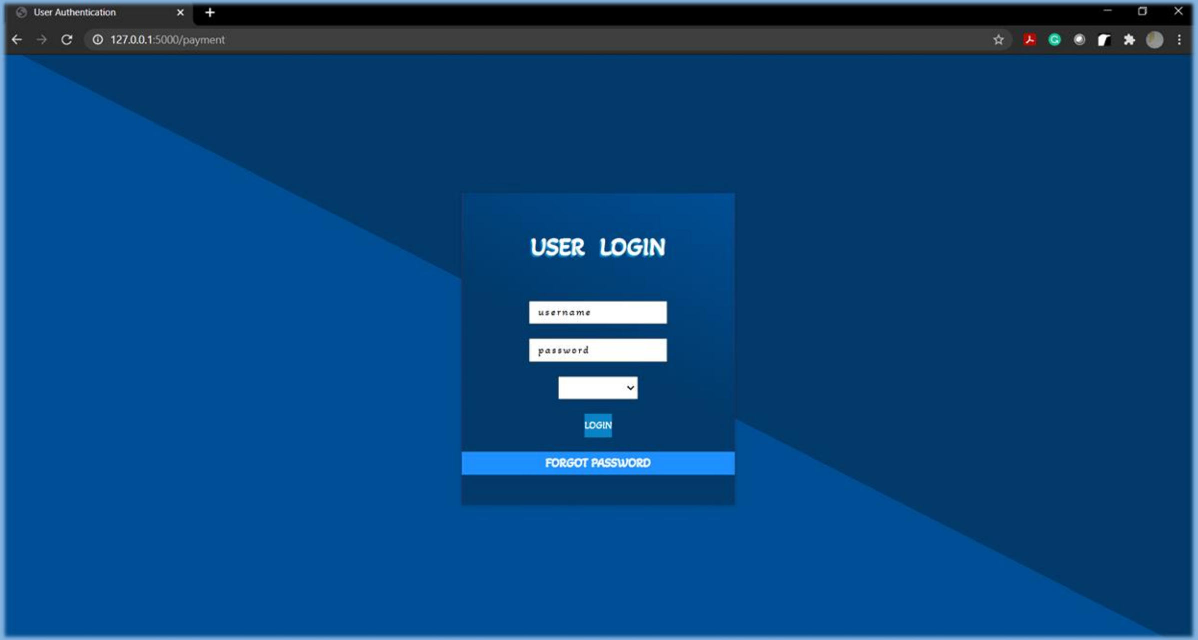
USER and MERCHANT

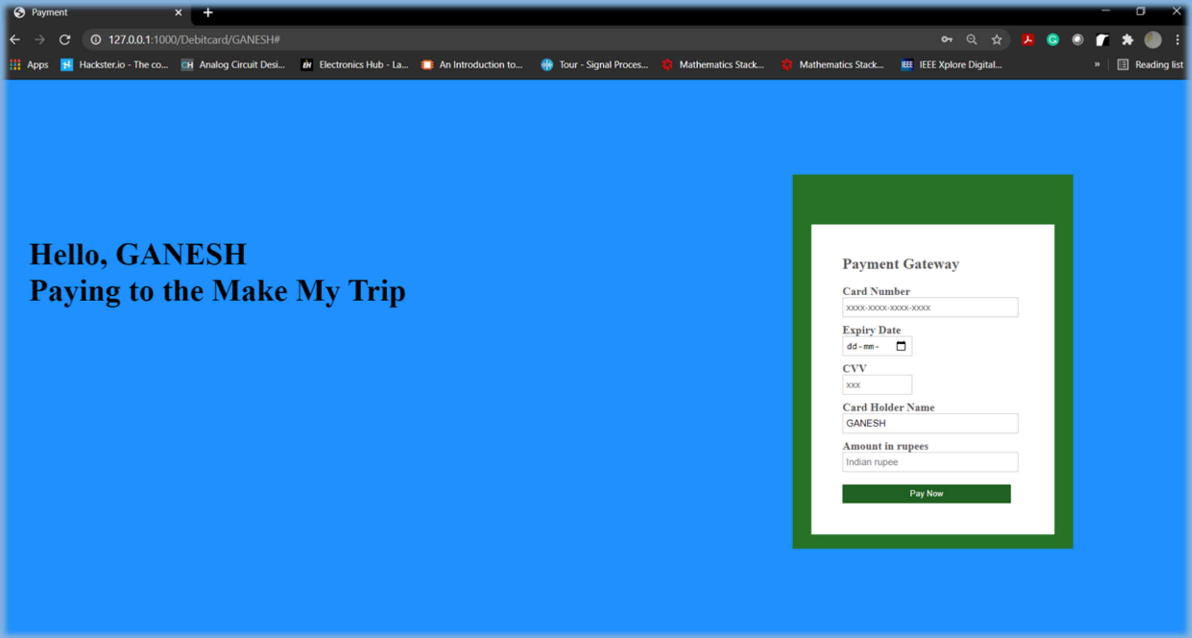
Normal people like us



```
----------------------------------------------------
**Login user            : GANESH
**Card number           : 1001 0110 2002 0006
**Expiry Date           : 2023-07-31
**CVV number            : 002
**Card holder name      : GANESH T S
**Amount Requested      : 500
**Time of transaction   : 2021-03-31 07:36:19.847156
----------------------------------------------------
----------------------------------------------------
**Login user            : MISS KR
**Card number           : 1001 0110 2002 0026
**Expiry Date           : 2023-07-31
**CVV number            : 001
**Card holder name      : KARTHIKA RAJESH
**Amount Requested      : 500
**Time of transaction   : 2021-03-31 07:37:37.642511
----------------------------------------------------
----------------------------------------------------
**Login user            : MANAS
**Card number           : 1001 0110 2002 0011
**Expiry Date           : 2023-07-31
**CVV number            : 000
**Card holder name      : MANAS KUMAR MISHRA
**Amount Requested      : 500
**Time of transaction   : 2021-03-31 07:38:37.575166
----------------------------------------------------
```

PAYMENT GATEWAY





Hello, GANESH
Paying to the Make My Trip

Payment Gateway

Card Number: xxxx-xxxx-xxxx-xxxx

Expiry Date: dd-mm-

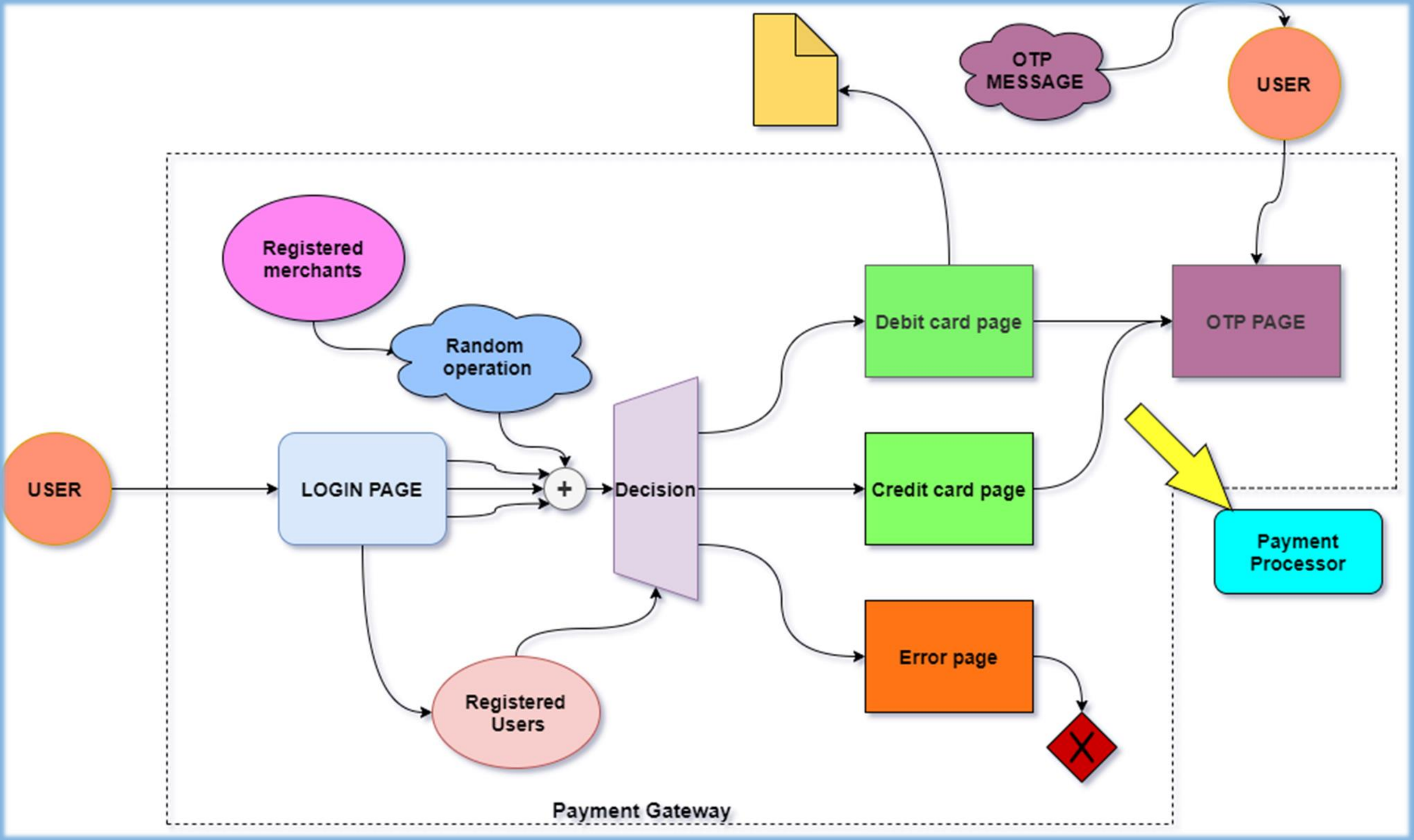
CVV: xxx

Card Holder Name: GANESH

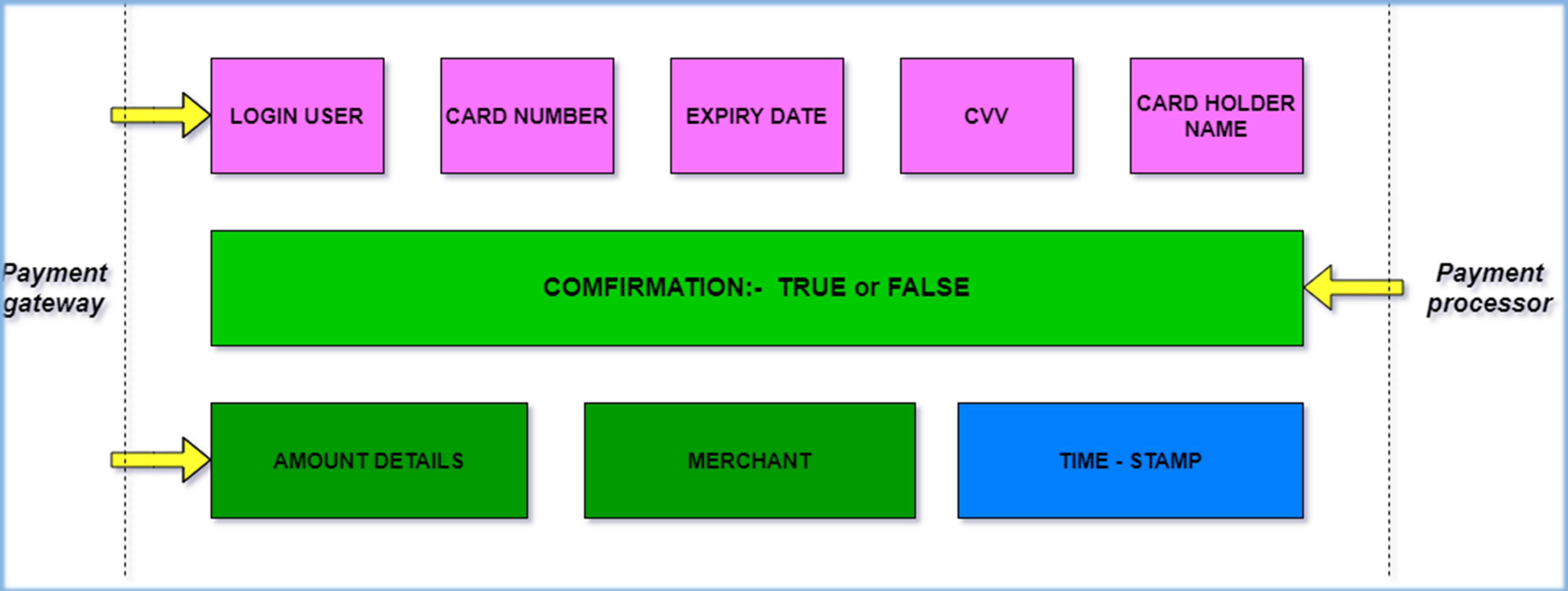
Amount in rupees: Indian rupee

Pay Now

PAYMENT GATEWAY and USER



PAYMENT GATEWAY and PAYMENT PROCESSOR

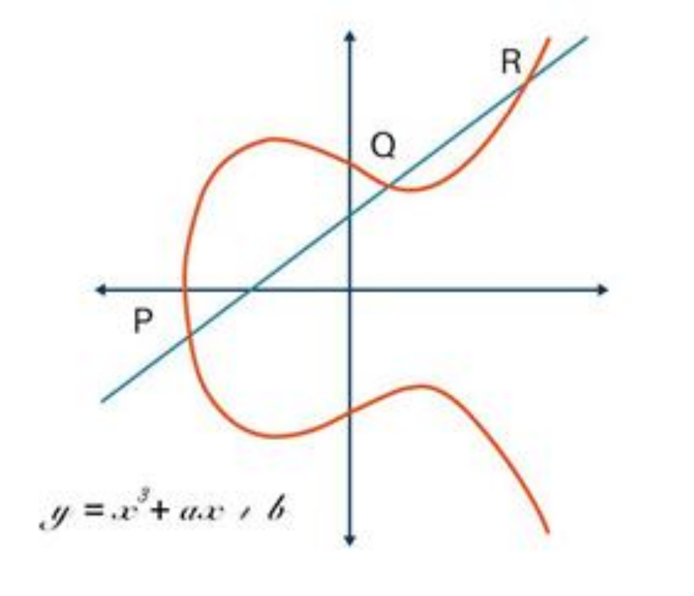


SECURITY LAYER

- Key Generation and Exchange
- Data Transfer Across Network
- Encryption and Decryption

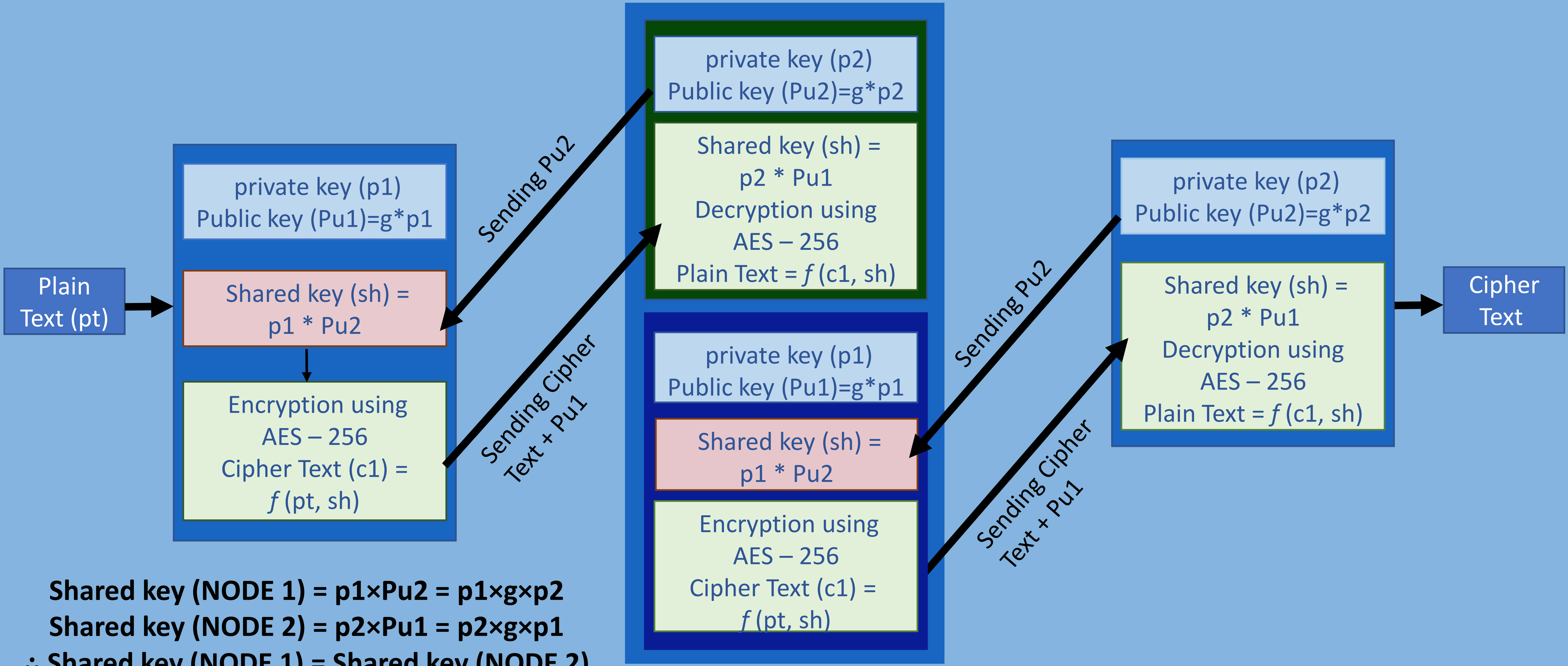
KEY GENERATION AND EXCHANGE

Elliptic Curve Diffie–Hellman Key Exchange → Public Key encryption



- Choice of Elliptic curve
- Private key generation
- Public key generation

DATA TRANSFER ACROSS NETWORK



Plain Text (pt)
private key (p1)
Public key (Pu1)=g*p1
Shared key (sh) = p1 * Pu2
Encryption using AES – 256
Cipher Text (c1) = *f* (pt, sh)
Sending Pu2
Sending Cipher Text + Pu1
private key (p2)
Public key (Pu2)=g*p2
Shared key (sh) = p2 * Pu1
Decryption using AES – 256
Plain Text = *f* (c1, sh)
private key (p1)
Public key (Pu1)=g*p1
Shared key (sh) = p1 * Pu2
Encryption using AES – 256
Cipher Text (c1) = *f* (pt, sh)
Sending Pu2
Sending Cipher Text + Pu1
private key (p2)
Public key (Pu2)=g*p2
Shared key (sh) = p2 * Pu1
Decryption using AES – 256
Plain Text = *f* (c1, sh)
Cipher Text

Shared key (NODE 1) = p1×Pu2 = p1×g×p2

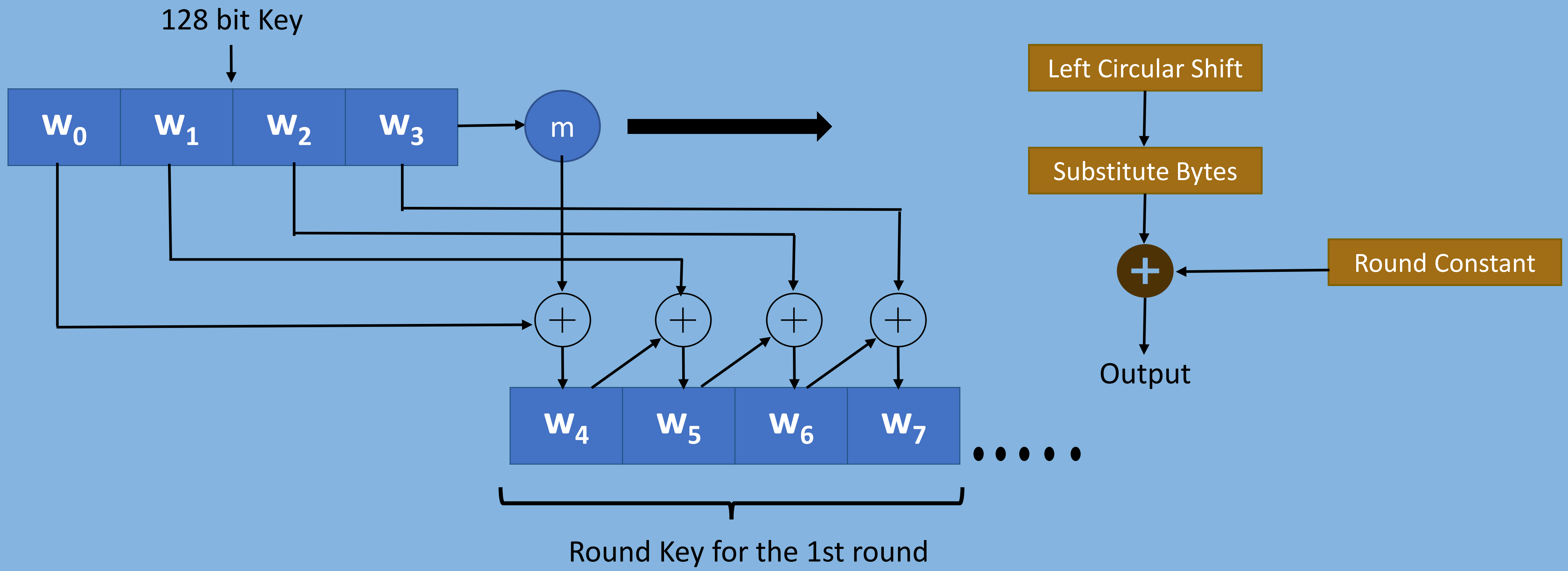
Shared key (NODE 2) = p2×Pu1 = p2×g×p1

∴ Shared key (NODE 1) = Shared key (NODE 2)

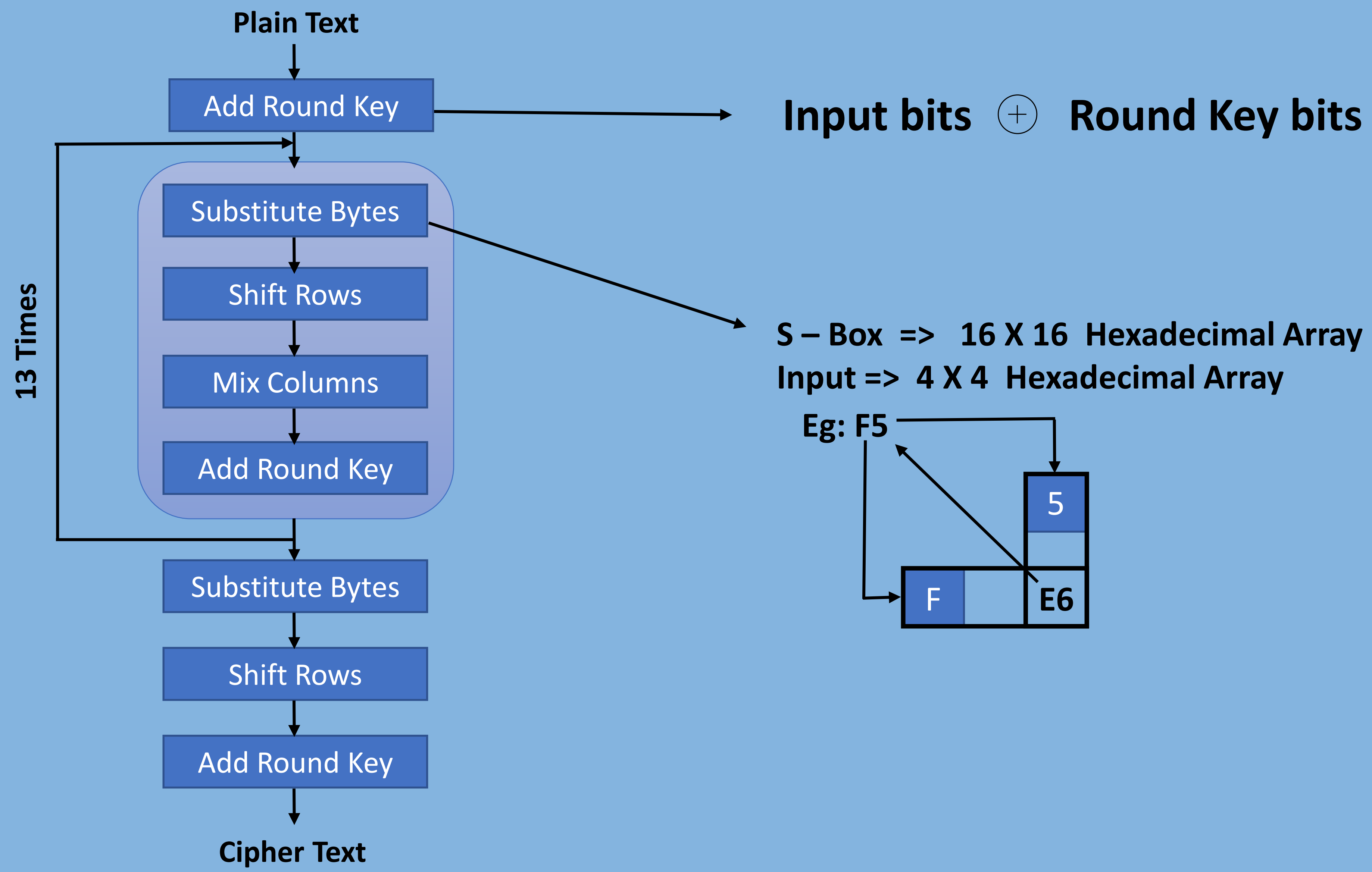
ENCRYPTION AND DECRYPTION

- AES – Advanced Encryption Standards
- A symmetrical key Block cipher
- Key length 256 bits
- 14 Rounds
- 256 bits => 128 bits +128 bits
- Last round of Encryption

ENCRYPTION AND DECRYPTION – Round Key Scheduling



ENCRYPTION AND DECRYPTION



Plain Text

Add Round Key

Substitute Bytes

Shift Rows

Mix Columns

Add Round Key

13 Times

Substitute Bytes

Shift Rows

Add Round Key

Cipher Text

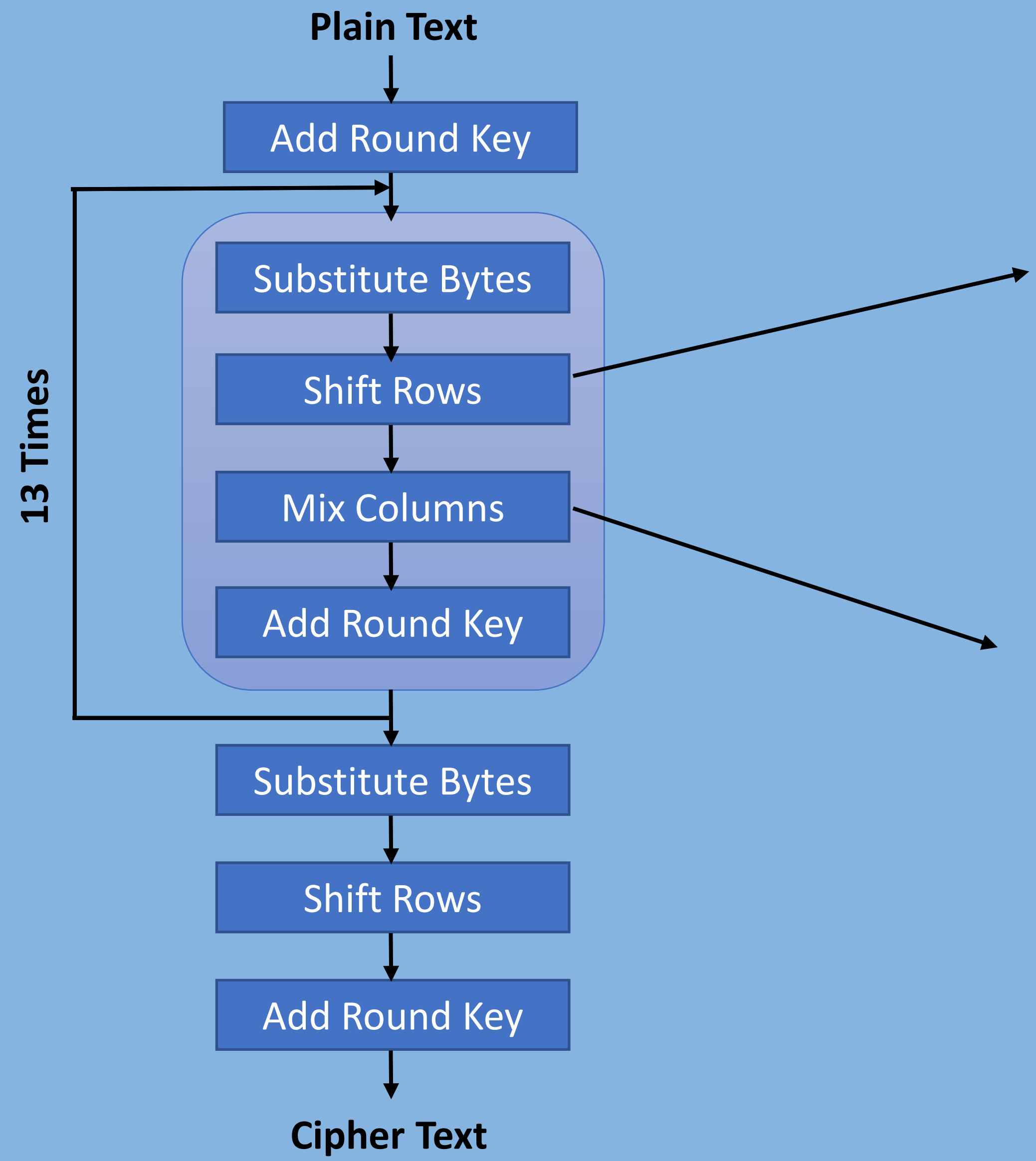
Input bits ⊕ Round Key bits

S – Box => 16 X 16 Hexadecimal Array

Input => 4 X 4 Hexadecimal Array

Eg: F5

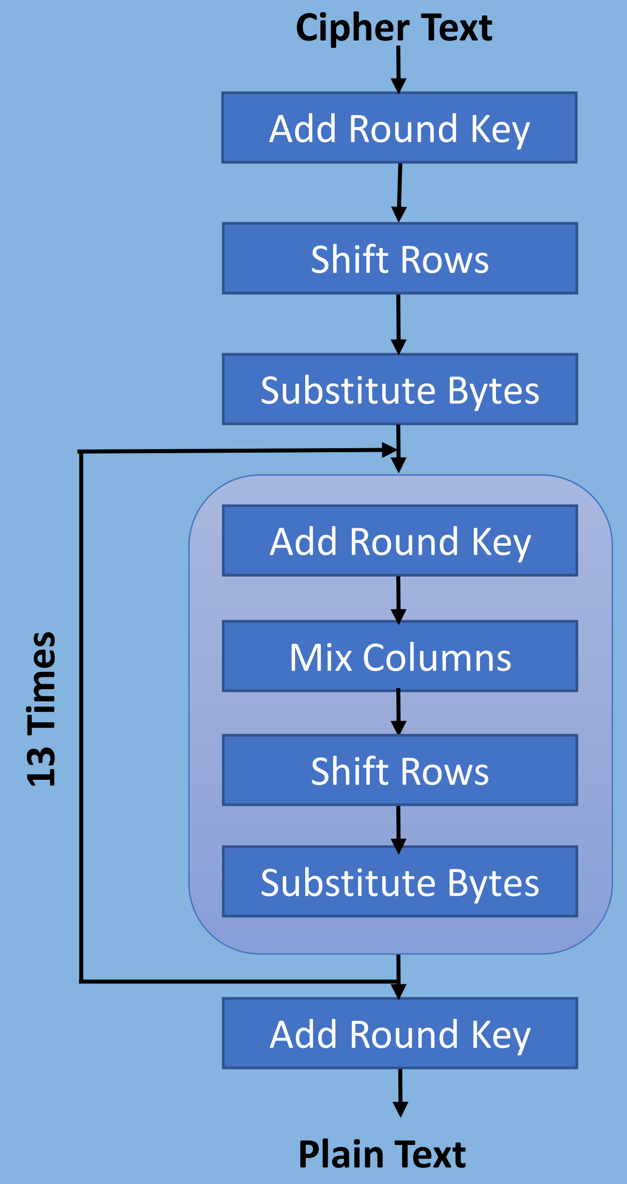
ENCRYPTION AND DECRYPTION



$$\begin{array}{c|cccc}
0 & S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\
1 & S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\
2 & S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\
3 & S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3}
\end{array}
\Rightarrow
\begin{array}{cccc}
S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\
S_{1,3} & S_{1,0} & S_{1,1} & S_{1,2} \\
S_{2,2} & S_{2,3} & S_{2,0} & S_{2,1} \\
S_{3,1} & S_{3,2} & S_{3,3} & S_{3,0}
\end{array}$$

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \times \begin{pmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{pmatrix}$$

ENCRYPTION AND DECRYPTION



DATABASE ON PHPMYADMIN

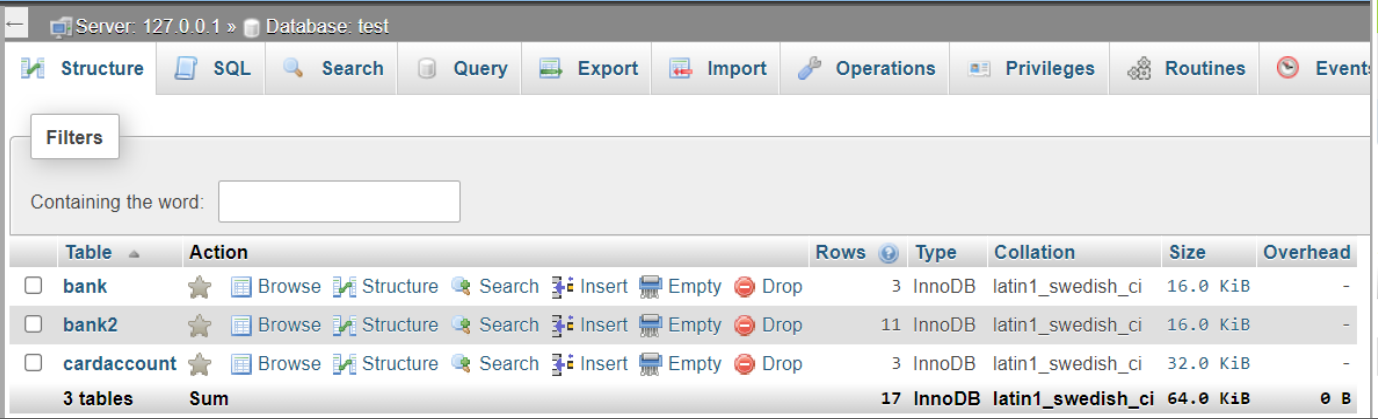
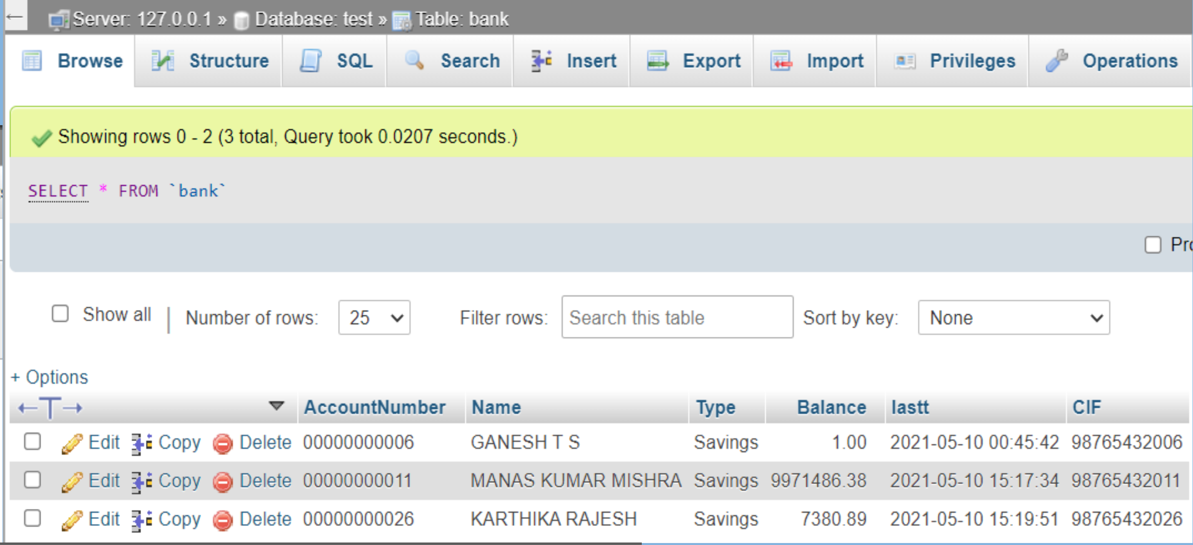


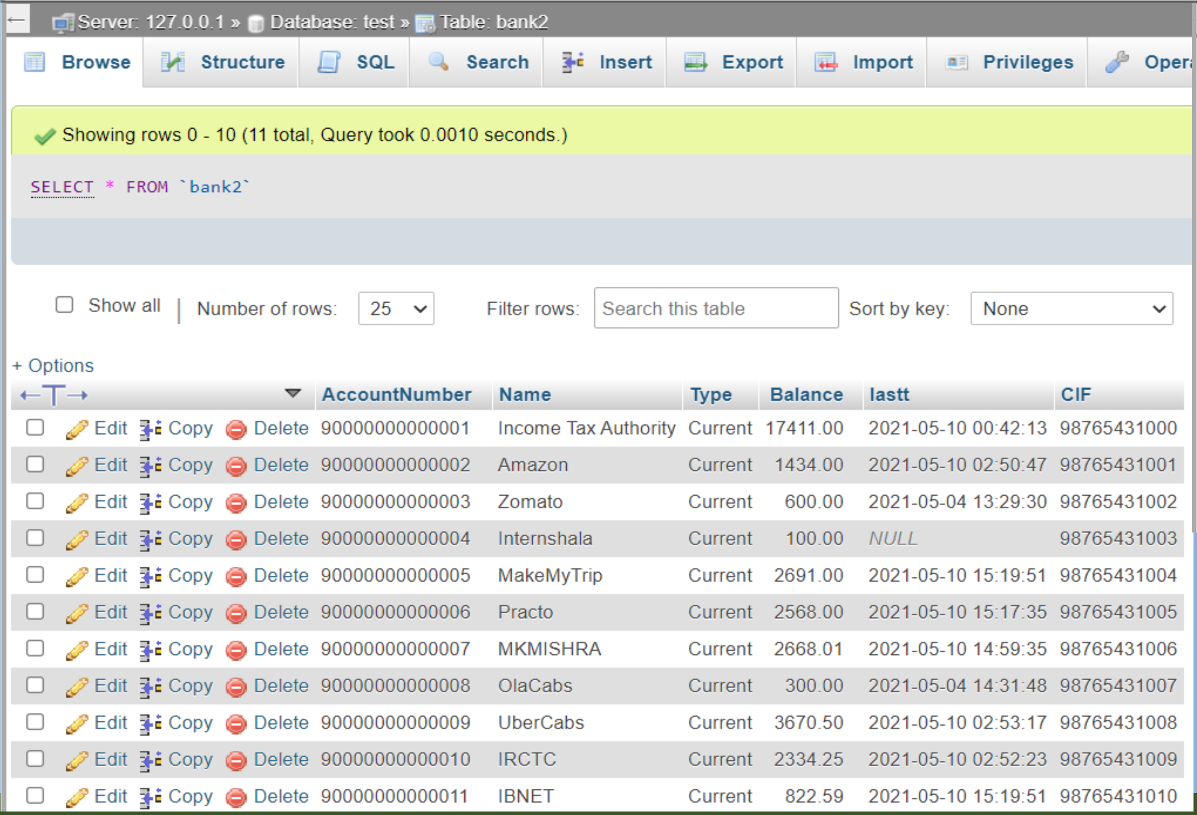
	Table	Action	Rows	Type	Collation	Size	Overhead
□	bank	Browse Structure Search Insert Empty Drop	3	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	bank2	Browse Structure Search Insert Empty Drop	11	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	cardaccount	Browse Structure Search Insert Empty Drop	3	InnoDB	latin1_swedish_ci	32.0 KiB	-
	3 tables	Sum	17	InnoDB	latin1_swedish_ci	64.0 KiB	0 B



✓ Showing rows 0 - 2 (3 total, Query took 0.0207 seconds.)

```
SELECT * FROM `bank`
```

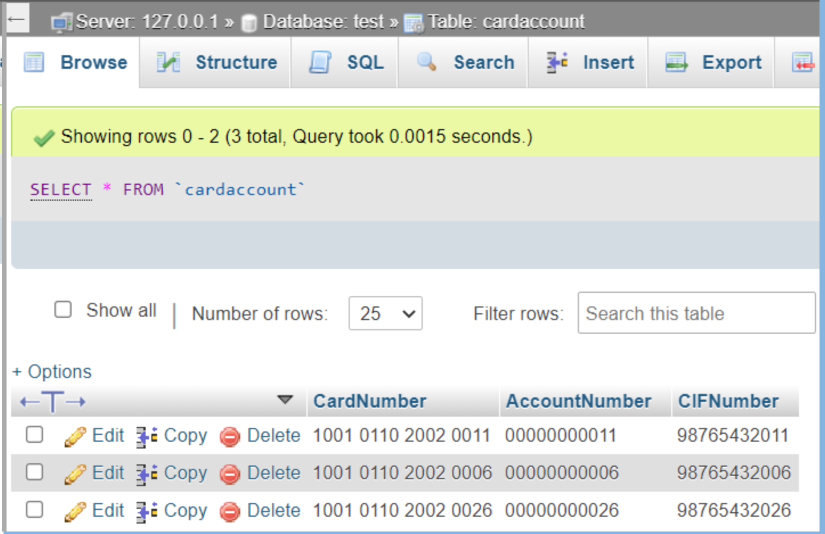
		AccountNumber	Name	Type	Balance	lastt	CIF
□	Edit Copy Delete	00000000006	GANESH T S	Savings	1.00	2021-05-10 00:45:42	98765432006
□	Edit Copy Delete	00000000011	MANAS KUMAR MISHRA	Savings	9971486.38	2021-05-10 15:17:34	98765432011
□	Edit Copy Delete	00000000026	KARTHIKA RAJESH	Savings	7380.89	2021-05-10 15:19:51	98765432026



✓ Showing rows 0 - 10 (11 total, Query took 0.0010 seconds.)

```
SELECT * FROM `bank2`
```

		AccountNumber	Name	Type	Balance	lastt	CIF
□	Edit Copy Delete	90000000000001	Income Tax Authority	Current	17411.00	2021-05-10 00:42:13	98765431000
□	Edit Copy Delete	90000000000002	Amazon	Current	1434.00	2021-05-10 02:50:47	98765431001
□	Edit Copy Delete	90000000000003	Zomato	Current	600.00	2021-05-04 13:29:30	98765431002
□	Edit Copy Delete	90000000000004	Internshala	Current	100.00	NULL	98765431003
□	Edit Copy Delete	90000000000005	MakeMyTrip	Current	2691.00	2021-05-10 15:19:51	98765431004
□	Edit Copy Delete	90000000000006	Practo	Current	2568.00	2021-05-10 15:17:35	98765431005
□	Edit Copy Delete	90000000000007	MKMISHRA	Current	2668.01	2021-05-10 14:59:35	98765431006
□	Edit Copy Delete	90000000000008	OlaCabs	Current	300.00	2021-05-04 14:31:48	98765431007
□	Edit Copy Delete	90000000000009	UberCabs	Current	3670.50	2021-05-10 02:53:17	98765431008
□	Edit Copy Delete	90000000000010	IRCTC	Current	2334.25	2021-05-10 02:52:23	98765431009
□	Edit Copy Delete	90000000000011	IBNET	Current	822.59	2021-05-10 15:19:51	98765431010

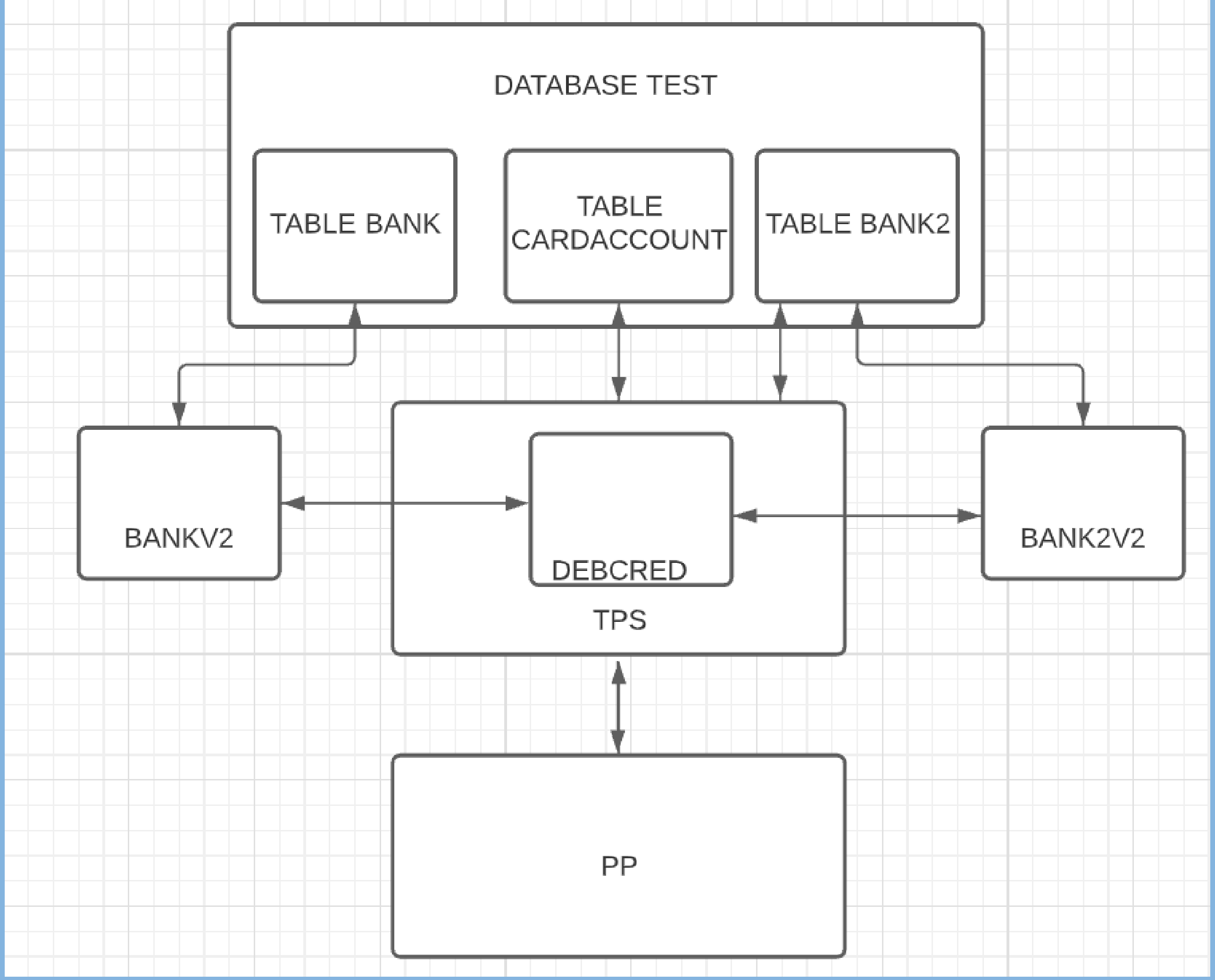

Server: 127.0.0.1 » Database: test » Table: cardaccount
Browse
Structure
SQL
Search
Insert
Export
Show all
Number of rows: 25
Filter rows: Search this table
+ Options

✓ Showing rows 0 - 2 (3 total, Query took 0.0015 seconds.)

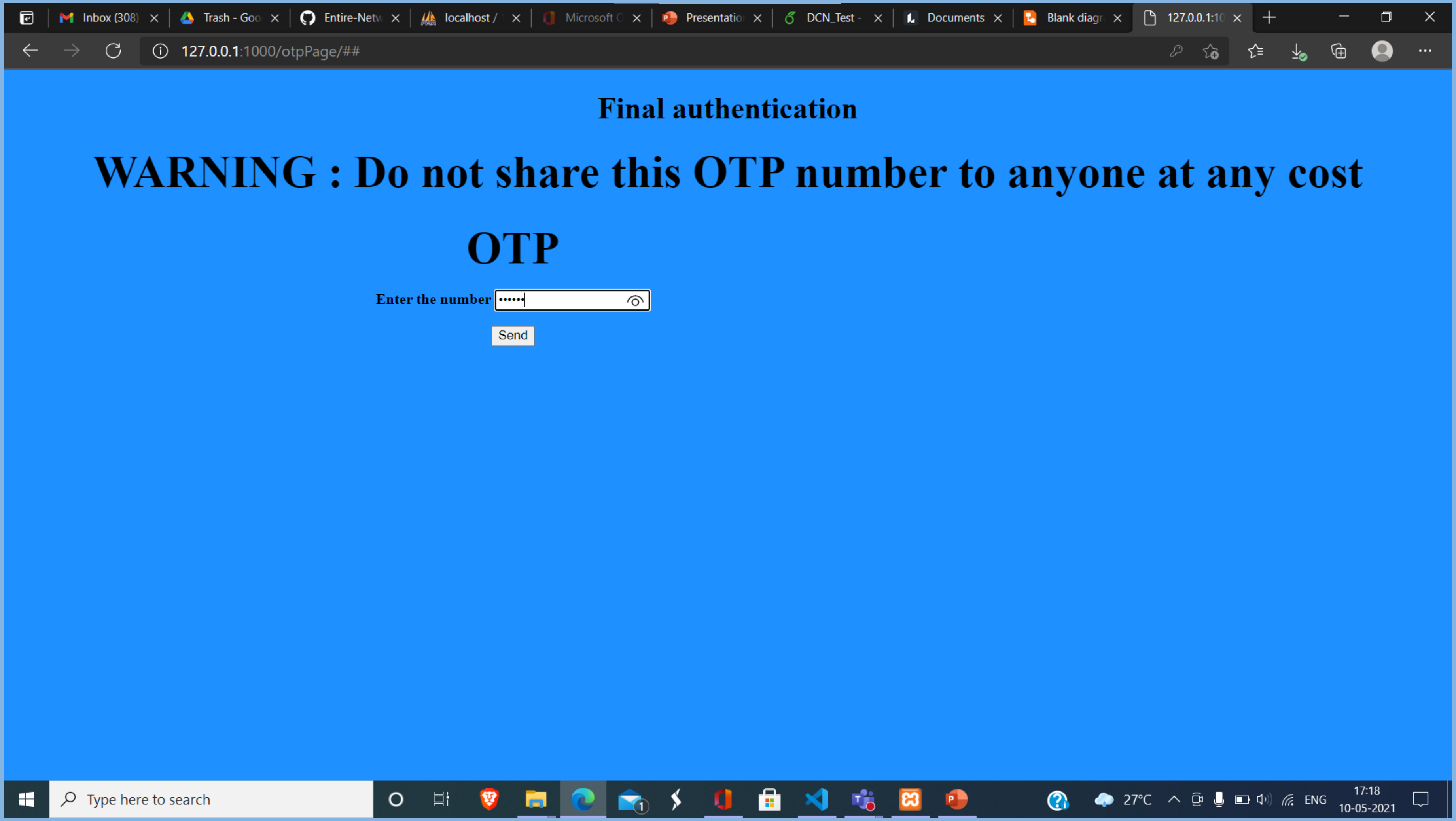
```
SELECT * FROM `cardaccount`
```

		CardNumber	AccountNumber	CIFNumber
□	Edit Copy Delete	1001 0110 2002 0011	00000000011	98765432011
□	Edit Copy Delete	1001 0110 2002 0006	00000000006	98765432006
□	Edit Copy Delete	1001 0110 2002 0026	00000000026	98765432026

TPS-BANKS-DATABASE



OTP INPUT PAGE



Final authentication

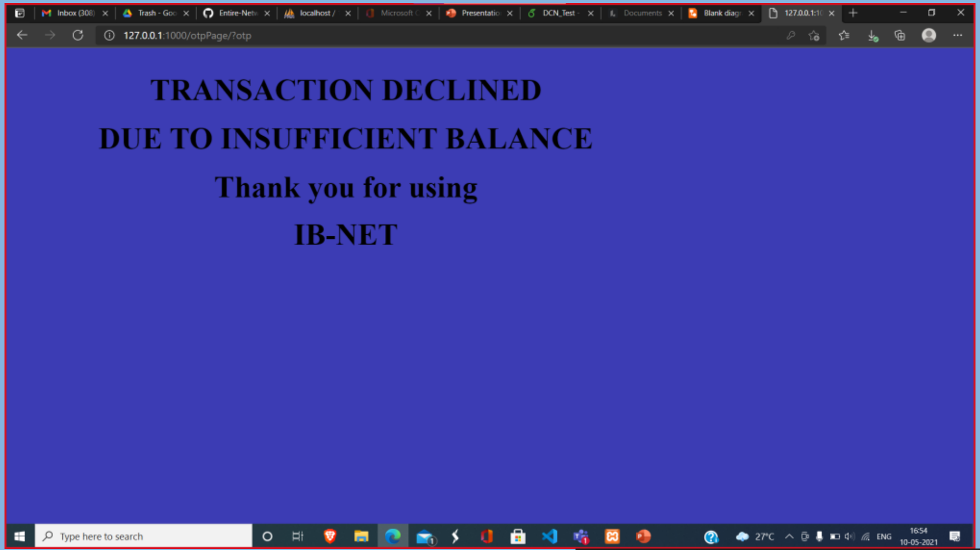
WARNING : Do not share this OTP number to anyone at any cost

OTP

Enter the number ••••••

Send

FEEDBACK

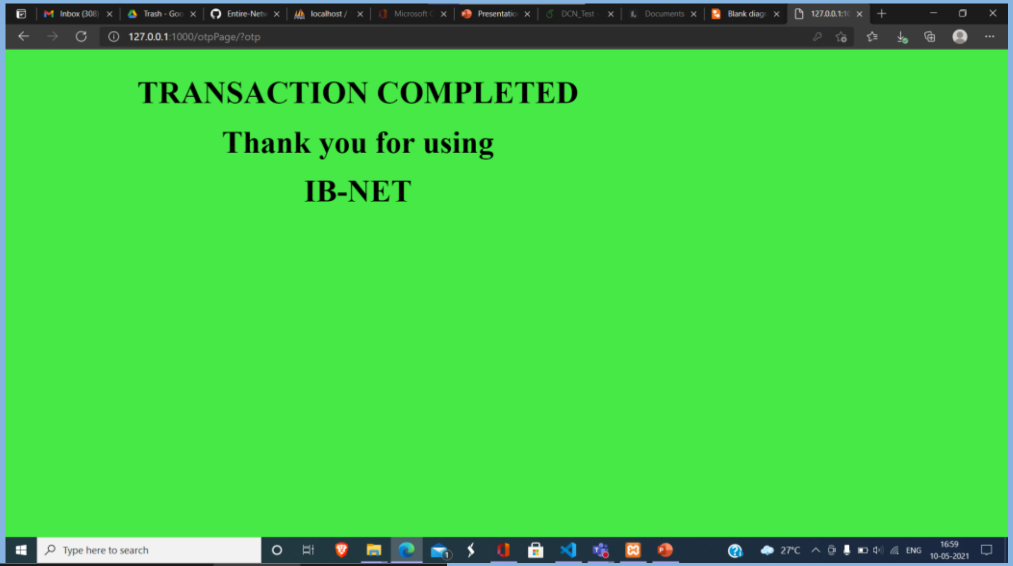


TRANSACTION DECLINED

DUE TO INSUFFICIENT BALANCE

Thank you for using

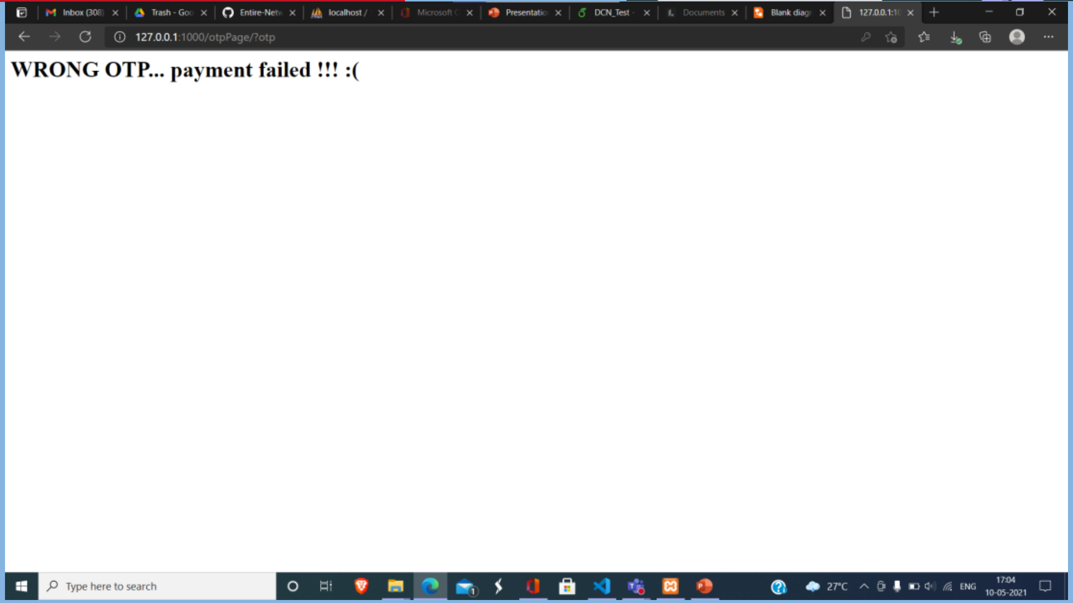
IB-NET



TRANSACTION COMPLETED

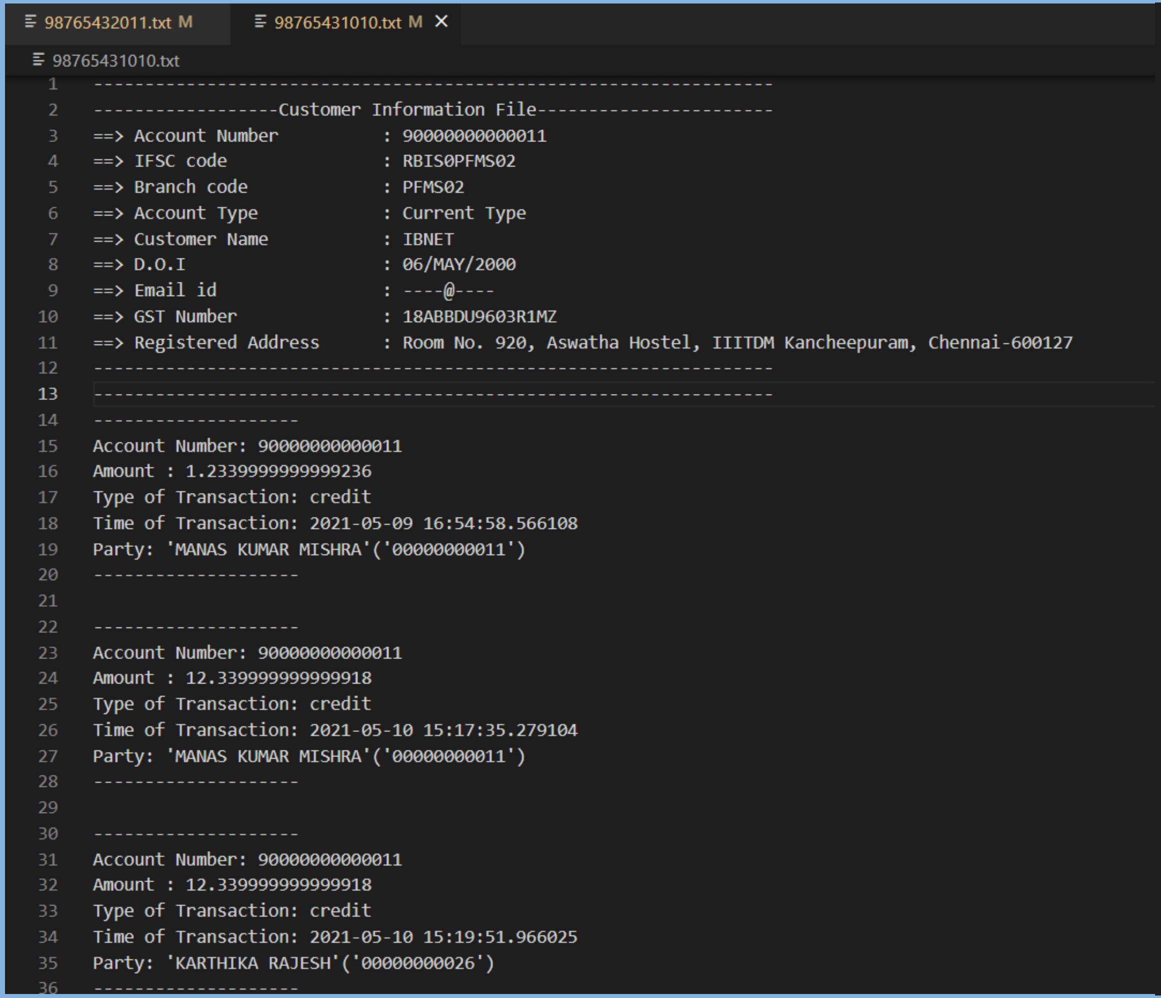
Thank you for using

IB-NET

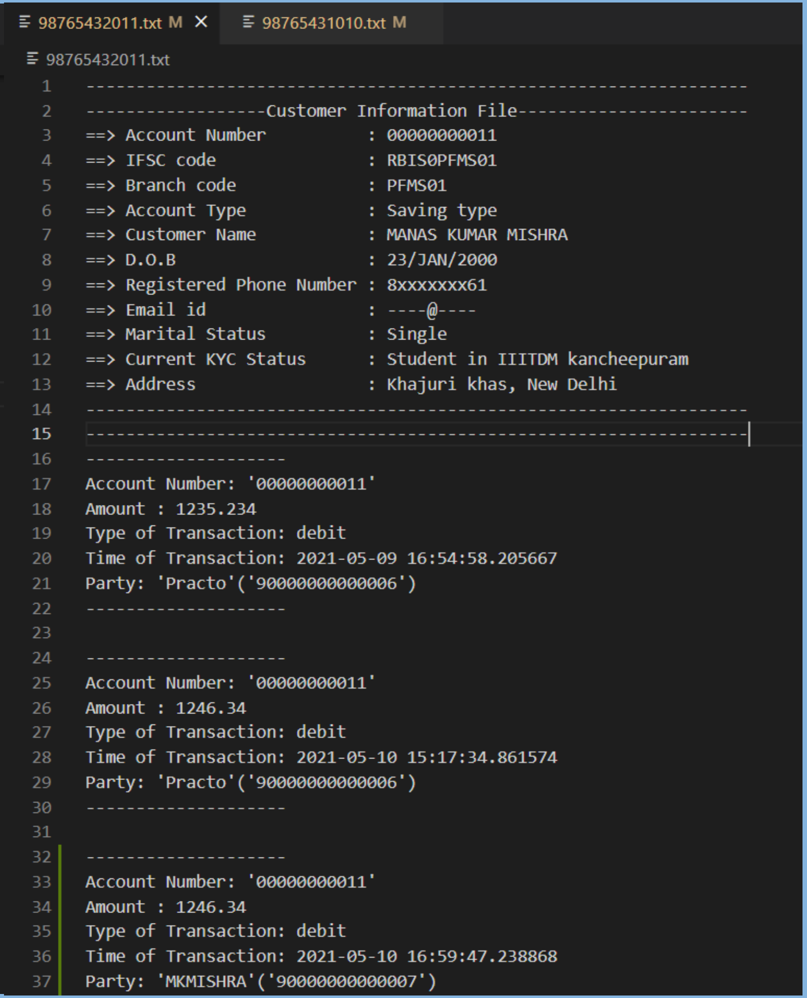


WRONG OTP... payment failed !!! :(

CIF



```
------------------------------------------------------------------
------------------Customer Information File-----------------------
==> Account Number          : 90000000000011
==> IFSC code               : RBIS0PFMS02
==> Branch code             : PFMS02
==> Account Type            : Current Type
==> Customer Name           : IBNET
==> D.O.I                   : 06/MAY/2000
==> Email id                : ----@----
==> GST Number              : 18ABBDU9603R1MZ
==> Registered Address      : Room No. 920, Aswatha Hostel, IIITDM Kancheepuram, Chennai-600127
------------------------------------------------------------------
------------------------------------------------------------------
--------------------
Account Number: 90000000000011
Amount : 1.2339999999999236
Type of Transaction: credit
Time of Transaction: 2021-05-09 16:54:58.566108
Party: 'MANAS KUMAR MISHRA'('00000000011')
--------------------

--------------------
Account Number: 90000000000011
Amount : 12.339999999999918
Type of Transaction: credit
Time of Transaction: 2021-05-10 15:17:35.279104
Party: 'MANAS KUMAR MISHRA'('00000000011')
--------------------

--------------------
Account Number: 90000000000011
Amount : 12.339999999999918
Type of Transaction: credit
Time of Transaction: 2021-05-10 15:19:51.966025
Party: 'KARTHIKA RAJESH'('00000000026')
--------------------
```

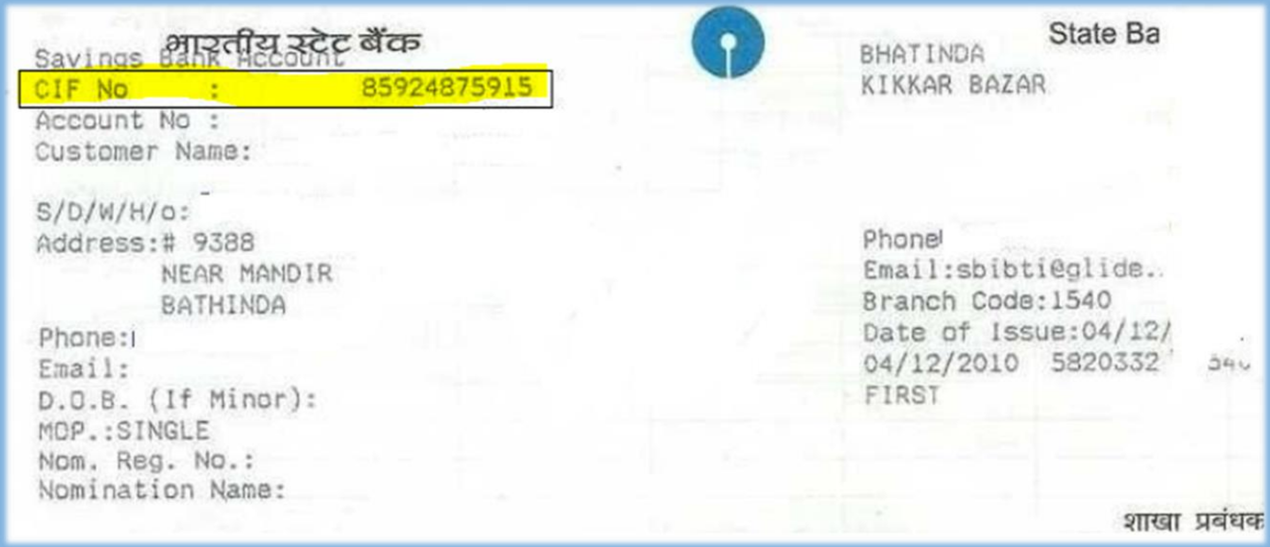


```
------------------------------------------------------------------
------------------Customer Information File-----------------------
==> Account Number          : 00000000011
==> IFSC code               : RBIS0PFMS01
==> Branch code             : PFMS01
==> Account Type            : Saving type
==> Customer Name           : MANAS KUMAR MISHRA
==> D.O.B                   : 23/JAN/2000
==> Registered Phone Number : 8xxxxxxx61
==> Email id                : ----@----
==> Marital Status          : Single
==> Current KYC Status      : Student in IIITDM kancheepuram
==> Address                 : Khajuri khas, New Delhi
------------------------------------------------------------------
------------------------------------------------------------------
--------------------
Account Number: '00000000011'
Amount : 1235.234
Type of Transaction: debit
Time of Transaction: 2021-05-09 16:54:58.205667
Party: 'Practo'('90000000000006')
--------------------

--------------------
Account Number: '00000000011'
Amount : 1246.34
Type of Transaction: debit
Time of Transaction: 2021-05-10 15:17:34.861574
Party: 'Practo'('90000000000006')
--------------------

--------------------
Account Number: '00000000011'
Amount : 1246.34
Type of Transaction: debit
Time of Transaction: 2021-05-10 16:59:47.238868
Party: 'MKMISHRA'('90000000000007')
```

CIF number and IFSC code

CIF :- Customer Information File

A centralized way of keeping track of user data
(Personal data, Transaction data, and Account data)



भारतीय स्टेट बैंक

State Ba

Savings Bank Account

CIF No : 85924875915

Account No :

Customer Name:

-

S/D/W/H/o:

Address:# 9388
NEAR MANDIR
BATHINDA

Phone:ı

Email:

D.O.B. (If Minor):

MOP.:SINGLE

Nom. Reg. No.:

Nomination Name:

BHATINDA
KIKKAR BAZAR

Phone!

Email:sbibti@glide..

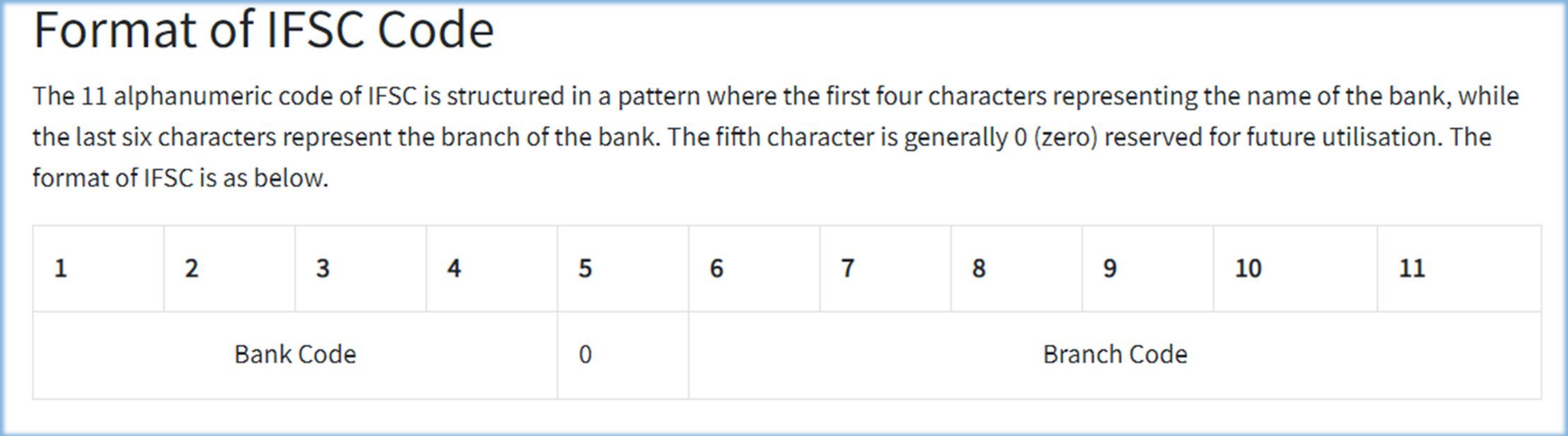
Branch Code:1540

Date of Issue:04/12/

04/12/2010 5820332 54ᴗ

FIRST

शाखा प्रबंधक

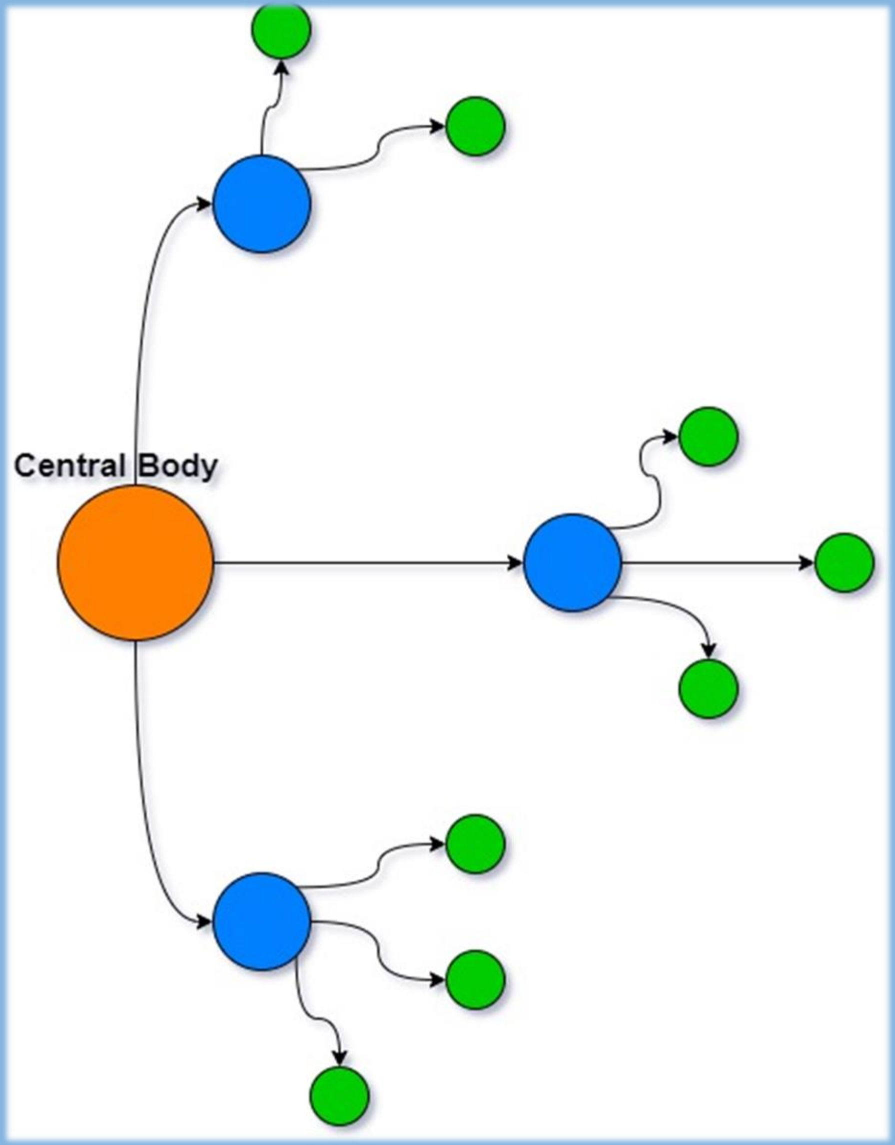


Format of IFSC Code

The 11 alphanumeric code of IFSC is structured in a pattern where the first four characters representing the name of the bank, while the last six characters represent the branch of the bank. The fifth character is generally 0 (zero) reserved for future utilisation. The format of IFSC is as below.

1	2	3	4	5	6	7	8	9	10	11
Bank Code				0	Branch Code					

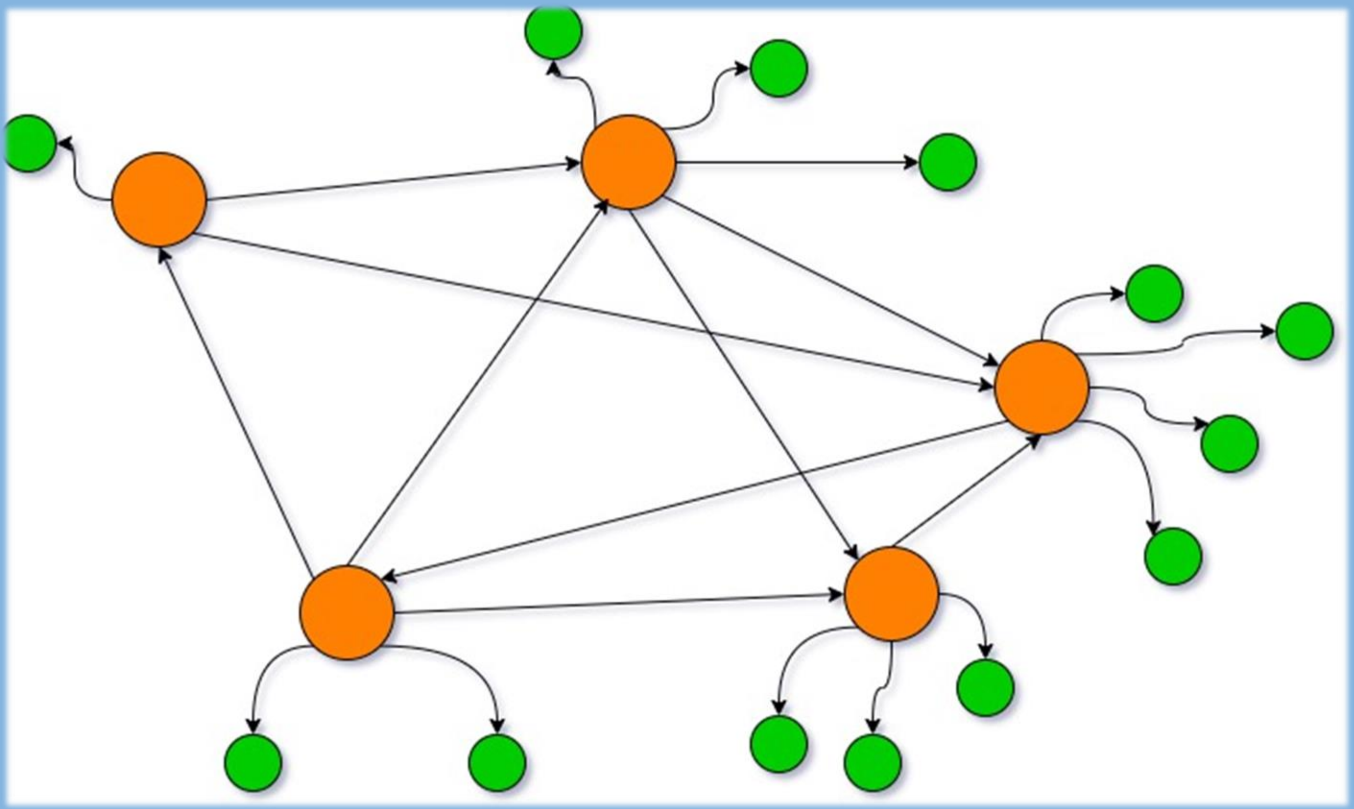
Centralized Network



Advantages

Disadvantages

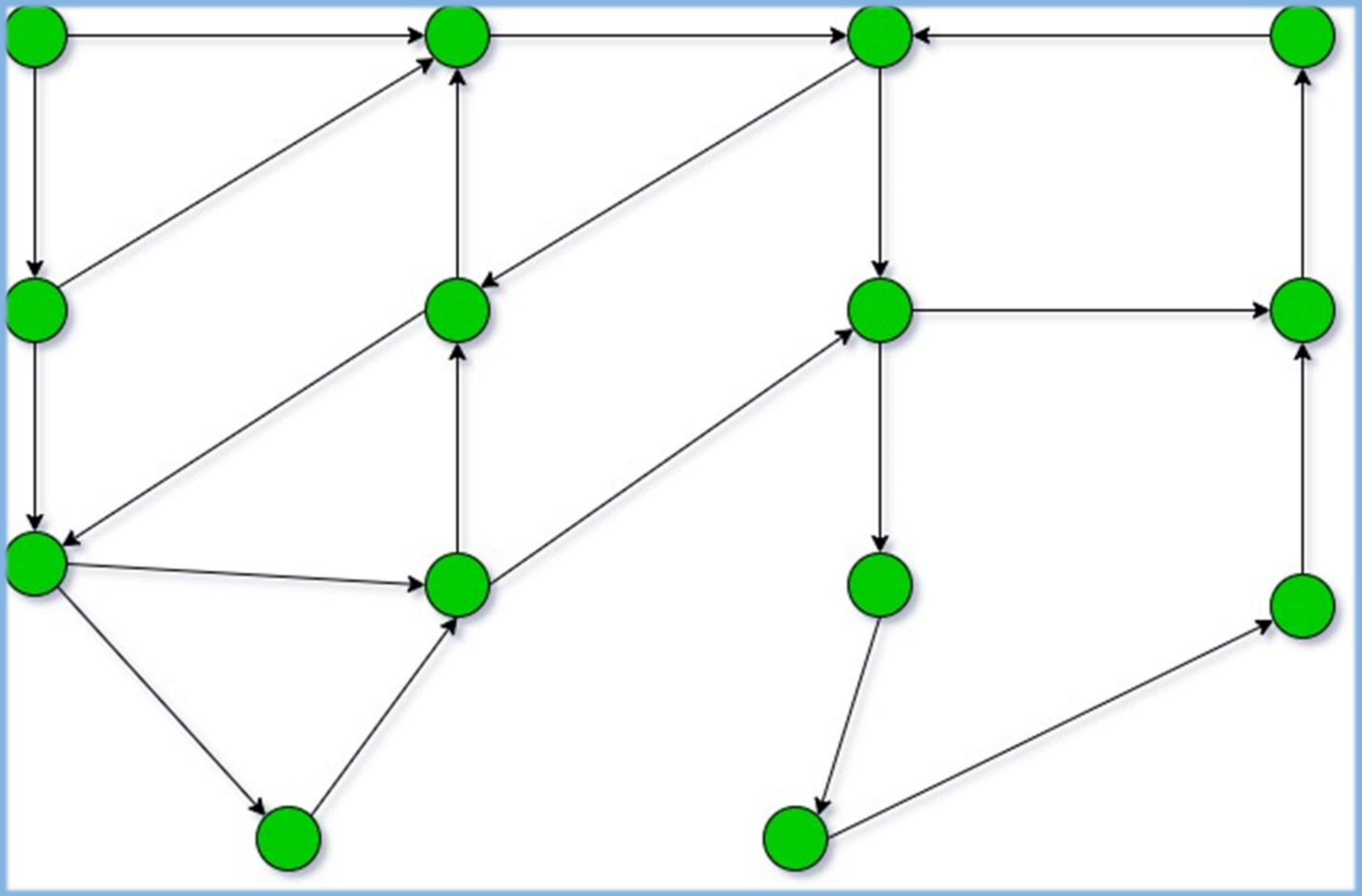
Decentralized Network



Advantages

Disadvantages

Distributed Network



Advantages

Disadvantages

Ledger

A maintained Documentation about every transaction.

Trust

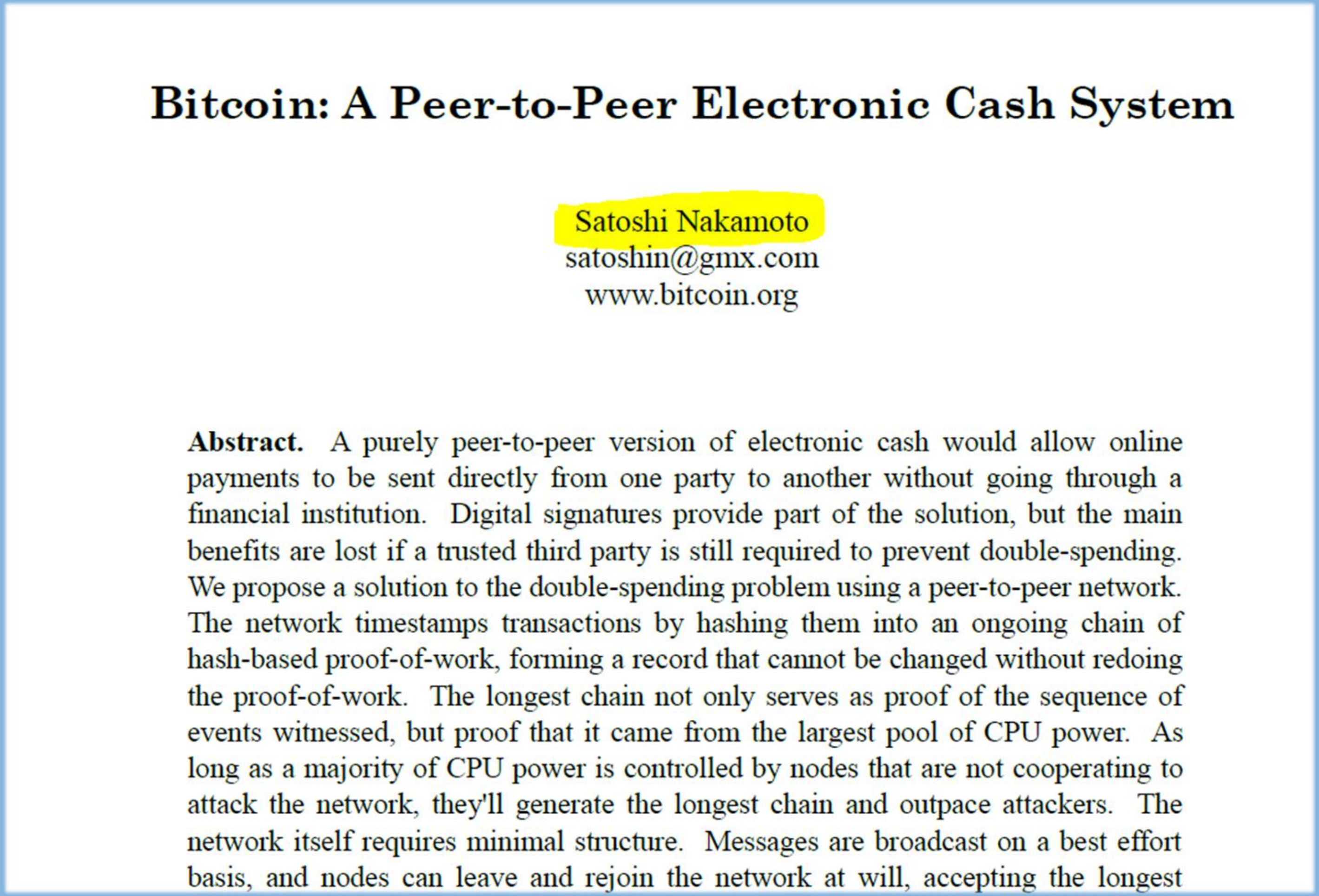
Signature(message, sk) = Digital signature

Verify(message, sk, pk) = True/False

Cryptography

Hash Function, Proof of work

A solution by Satoshi Nakamoto



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest

Timestamp Server.

Proof of work

Network (peer to peer)

Incentive (Block-chain Mining)

Payment Verification

Thank you