Blockchain-Based Website for Online Market

Introduction

A blockchain is a distributed software network that functions both as a digital ledger and a mechanism enabling the secure transfer of assets without an intermediary. Just as the internet is a technology that facilitates the digital flow of information, blockchain is a technology that facilitates the digital exchange of units of value. Anything from currencies to land titles to votes can be tokenized, stored, and exchanged on a blockchain network.

Existing System

The existing system provides online payment which can lead into online payment theft and fraud activities.

Proposed System

We propose a new free-ecommerce platform with blockchains that allows customers to connect to the seller directly, share personal data without losing control and ownership of it and apply it to the domain of shopping cart. Our new platform provides a solution to four important problems: private payment, ensuring privacy and user control, and incentives for sharing. It allows the trade to be open, transparent with immutable transactions that can be used for settling any disputes.

Problem statement

The intention of this shopping cart software is that it should be simple and as minimal as possible. You can download this free and customize it for your needs within minutes.

- Retrieve product information from the database.
- Create product gallery for the shopping cart.
- Manage cart items using the session.
- Handle add, edit, remove and empty cart actions.

Main Modules

Admin

- Login
- View Seller
    - View Products
- View Users
- View Bookings

Seller

- Register
- Login
- Manage Products
- Wallet generation
- View Bookings
    - View Payment
    - Update status to delivered

User

- Register
- Login
- View Products
    - Book Products
- View Orders
    - Make Payment
    - View Status
- Wallet generation

AES algorithm

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

Working of the cipher

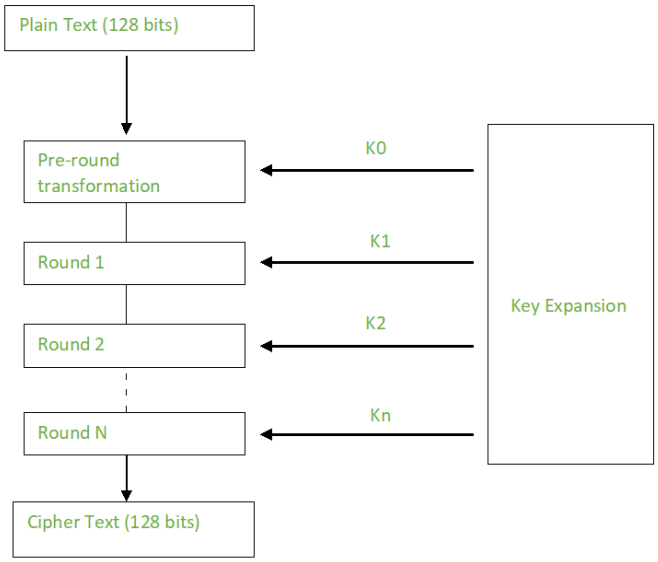
AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows :

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

Creation of Round keys

A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.



Encryption :

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.

[b0 | b4 | b8 | b12 |

| b1 | b5 | b9 | b13 |

| b2 | b6 | b10| b14 |

| b3 | b7 | b11| b15]

Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The last round doesn't have the MixColumns round.The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

SubBytes

This step implements the substitution.In this step each byte is substituted by another byte.(Its performed using a lookup table also called the S-box.This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte.The result of this step is a 16 byte (4 x 4) matrix like before.The next two steps implement the permutation.

ShiftRows

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)

[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3]

| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |

| b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 |

[b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]

MixColumns

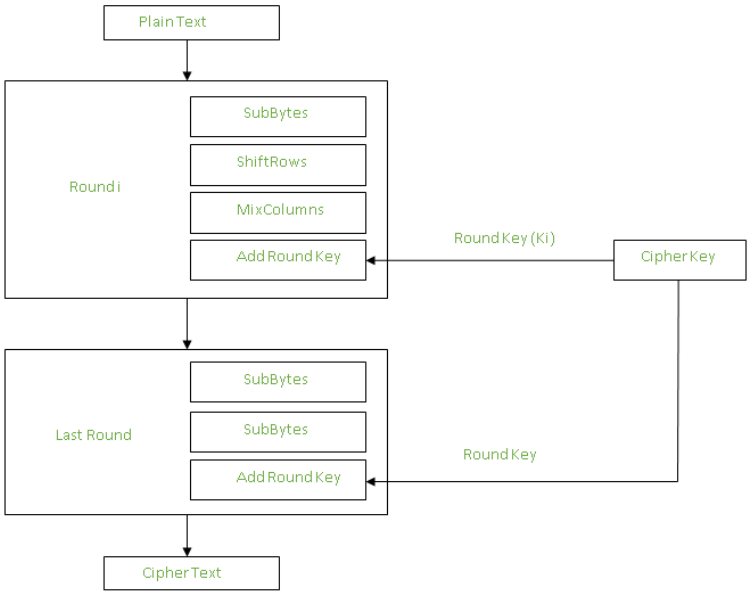
This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

This step is skipped in the last round.

$$\begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix}$$

Add Round Keys :

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.



After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Decryption :

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.

The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse MixColumns :

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

```
[ b0 ] =   [ 14  11  13  9 ]   [ c0 ]

| b1 | =   | 9   14  11  13 |   | c1 |

| b2 | =   | 13  9   14  11 |   | c2 |

[ b3 ] =   [ 11  13  9   14 ]   [ c3 ]
```

Inverse SubBytes

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

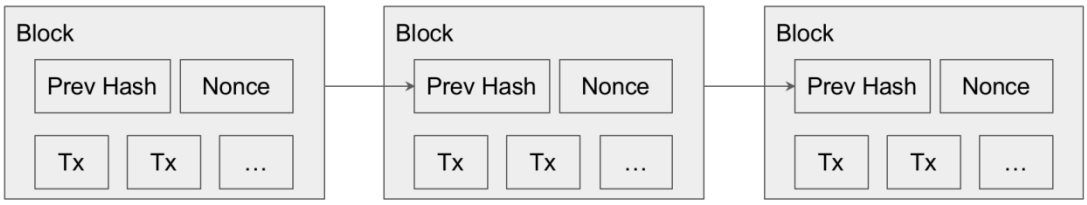
Summary

AES instruction set is now integrated into the CPU (offers throughput of several GB/s)to improve the speed and security of applications that use AES for encryption and decryption.Even though its been 20 years since its introduction we have failed to break the AES algorithm as it is infeasible even with the current technology. Till date the only vulnerability remains in the implementation of the algorithm.

Hashing and Blockchain's Cryptographic data

A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hashes. Hash functions are usually used to accelerate database lookup by detecting duplicated records, and they are also widely used in cryptography. A cryptographic hash function allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it by knowing the stored hash value.

Bitcoins uses a cryptographic hash function called SHA-256. SHA-256 is applied to a combination of the block's data (bitcoin transactions) and a number called nonce. By changing the block data or the nonce, we get completely different hashes. For a block to be considered valid or "mined", the hash value of the block and the nonce needs to meet a certain condition.



Blocks are chained together using the previous block's hash to form a Blockchain.

Conclusion

At one end of the spectrum of digital assets are cryptocurrencies like bitcoin used in payment networks such as the Bitcoin blockchain. Bitcoins are fungible: that is, one bitcoin is equal in value and function to every other bitcoin. So if you have a contract involving bitcoin, you could replace one bitcoin with another bitcoin without breaking the terms of your agreement.

Software Implementation Details

Platform: Python

Database: MySQL Server