Block chain and Cryptography Communication System

Project ID:22MP0D48

Group Members RA1811003030185 Koustubh Saxena
RA1811003030202 Satwik Srivastava RA1811003030204 Rachit Gupta
RA1811003030302 Deeptanshu Yadav Supervised By Dr. Premananda Sahu

Department of Computer Science & Engineerin Faculty of Engineering & Technolog SRM Institute of Science & Technology

May 10, 2022

Table of Contents I

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

Comments

- Make your Objectives concise and to the point.
- Make your PPT more discriptive.
- Use LateX to create presentation, and use the template provided

Action Taken

- Defined a precise obective and made the objective clear.
- Added more slides.
- Used the template provided.

Objectives & Motivation

A prototype of fast and secure communication of the data over the internet is achieved by using military grade encryption followed by passing the data using Blockchain technology

Literature Survey

- A systematic review of blockchain-based applications across multiple domains.
- We identify the characteristics that can revolutionise "business-as-usual" practices.
- We provide a framework to determine the fitness of blockchainn per application.

Blockchain

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blackchains. Each block in the chain contains a number of transactions, and every time a new transactions occurs on the blockchain, a record of that transaction is added to every participant's ledger.

BLOCKS

What Is a Block (Blockchain Block)? Blocks are (data structures within the blockchain database, where transaction data in a cryptocurrency blockchain are permanently record.) A block records some or all of the most recent transactions not yet validated by the network. Once the data are validated, the block is closed.

Blockchain

```
import datetime
import hashlib

class Block:
    blockNo = 0
    data = None
    nextp = None
    hashb = None
    nonce = 0
    previous_hash = 0x0
    timestamp = datetime.datetime.now()

    def __init__(self, data):
        self.data = data

    def hash(self):
        h = hashlib.sha256()
        h.update(
        str(self.nonce).encode('utf-8') +
        str(self.data).encode('utf-8') +
        str(self.previous_hash).encode('utf-8') +
        str(self.timestamp).encode('utf-8') +
        str(self.blockNo).encode('utf-8')
        )
        return h.hexdigest()

    def __str__(self):
        return "Block Hash: " + str(self.hash()) + "\nBlockNo: " + str(self.blockNo) + "\nBlock Data: "
+ str(self.data) + "\nHashes: " + str(self.nonce) + "\n--------------"
```

Blockchain

```
class Blockchain:

    diff = 20
    maxNonce = 2**32
    target = 2 ** (256-diff)

    block = Block("Genesis")
    dummy = head = block

    def add(self, block):

        block.previous_hash = self.block.hash()
        block.blockNo = self.block.blockNo + 1

        self.block.next = block
        self.block = self.block.next

    def mine(self, block):
        for n in range(self.maxNonce):
            if int(block.hash(), 16) <= self.target:
                self.add(block)
                print(block)
                break
            else:
                block.nonce += 1
```

Output

```
        print(blockchain.head)
        blockchain.head = blockchain.head.next
```

```
Block Hash: 4e2de909f53740a3d92cac0df4881b2f25c7a5c17f5036f70645
BlockNo: 1
Block Data: Block 1
Hashes: 169477
--------------
Block Hash: ff79fc1b9726fb68f95fb98468c9f093df96172e7fd17d78c6f08
BlockNo: 0
Block Data: Genesis
Hashes: 0
--------------
Block Hash: 4e2de909f53740a3d92cac0df4881b2f25c7a5c17f5036f70645
BlockNo: 1
Block Data: Block 1
Hashes: 169477
--------------
```

Crytography

Cryptography is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data from the private messages during a communication process. Cryptography is also made up of two ancient Greek terms, Kryptos and Graphein, the former meaning "hidden" and latter being "to write".
Encryption It is a process of plaintext (normal text) to a ciphertext (random sequence of bits).
Decryption The inverse process of encryption, conversion of ciphertext to plaintext.

Use of Cryptography in Blockchain

Blockchains make use of two types of cryptographic algorithms, asymmetric-key algorithms, and hash functions. Hash functions are used to provide the functionality of a single view of blockchain to every participant. Blockchains generally use the SHA-256 hashing algorithm as their hash function.

Application of Cryptography

Hashing, public-private key pairs, and the digital signatures together constitute the foundation for the blockchain. These cryptographic features make it possible for blocks to get securely linked by other blocks, and also ensure the reliability and immutability of the data stored on the blockchain. There are a huge number of applications of blockchain technology, and cryptography makes it possible. One of the major real-world applications of cryptography in the blockchain is cryptocurrencies.

Cryptography hash function in Blockchain

Cryptographic hash functions provide the following benefits to the blockchain:

- *Avalanche effect* – A slight change in the data can result in a significantly different output.
- *Uniqueness* – Every input has a unique output.
- *Deterministic* – Any input will always have the same output if passed through the hash function.
- *Quickness* – The output can be generated in a very small amount of time.
- *Reverse engineering is not possible*, i.e. we cannot generate the input by having the output and the hash function.

RSA

RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers

Code

```
LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
LETTERS = LETTERS.lower()

def encrypt(message, key):
    encrypted = ''
    for chars in message:
        if chars in LETTERS:
            num = LETTERS.find(chars)
            num += key
            encrypted +=  LETTERS[num]

    return encrypted

def decrypt(message, key):
    decrypted = ''
    for chars in message:
        if chars in LETTERS:
            num = LETTERS.find(chars)
            num -= key
            decrypted +=  LETTERS[num]

    return decrypted
```

Output

```
    main()
```

```
Enter your message: attack china
Enter you key [1 - 26]: 20
Encrypt or Decrypt? [E/D]: E
unnuwewbchu
```

```
main()
```

```
Enter your message: unnuwewbchu
Enter you key [1 - 26]: 20
Encrypt or Decrypt? [E/D]: D
attackchina
```

```
[ ]
```

References

- https://www.investopedia.com/terms/b/blockchain.asp
- https://www.ibm.com/in-en/topics/what-is-blockchain
- https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain
- https://en.wikipedia.org/wiki/Blockchain
- https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html
- https://builtin.com/blockchain
- Nakamoto, Satoshi (October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System"