

CIS4630 - Understanding the computation behind Blockchain

Last Name: _____ First Name: _____ Date: _____

Goal: The purpose of this topic is to introduce students to Blockchain and the encryption computation behind this revolutionizing disruptive technology. In 2009, Bitcoin became the first popular (decentralized) peer – to peer crypto- currency application. Currently, 1-Bitcoin is equivalent to \$4,026 USD. The success of blockchain is mainly due to the usages of Cryptography; Blockchain is a growing list of records, called **blocks** which are link using cryptography. Each block contains a cryptographic hash of the pervious block, a time stamp, and transaction data. During this hands on we will examine the mathematical computation of the encryption process of blockchain: RSA, Merkle tree, and SHA256.

Blockchain use RSA which involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct large random [prime numbers](#) p and q
2. Compute $n=pq$
 - o n is used as the [modulus](#) for both the public and private keys
3. Compute the [totient](#): $\phi(n) = (p-1)(q-1)$
4. Choose an integer such that $1 < e < \phi(n)$, and e and $\phi(n)$ share no factors other than 1 (coprime)
 - o e is released as the public key exponent
5. Compute d to satisfy the [congruence relation](#) $de \equiv 1 \pmod{\phi(n)}$ ie: $de = 1 + k \cdot \phi(n)$ for some integer k .
 - o d is kept as the private key exponent

The **public key** (e, n) consists of the modulus and the public (or encryption) exponent .

The **private key** (d, n) consists of the modulus and the private (or decryption) exponent which must be kept secret.

Compute the following:

1. $p = 11$
 $q = 3$

2. $p = 23$
 $q = 13$

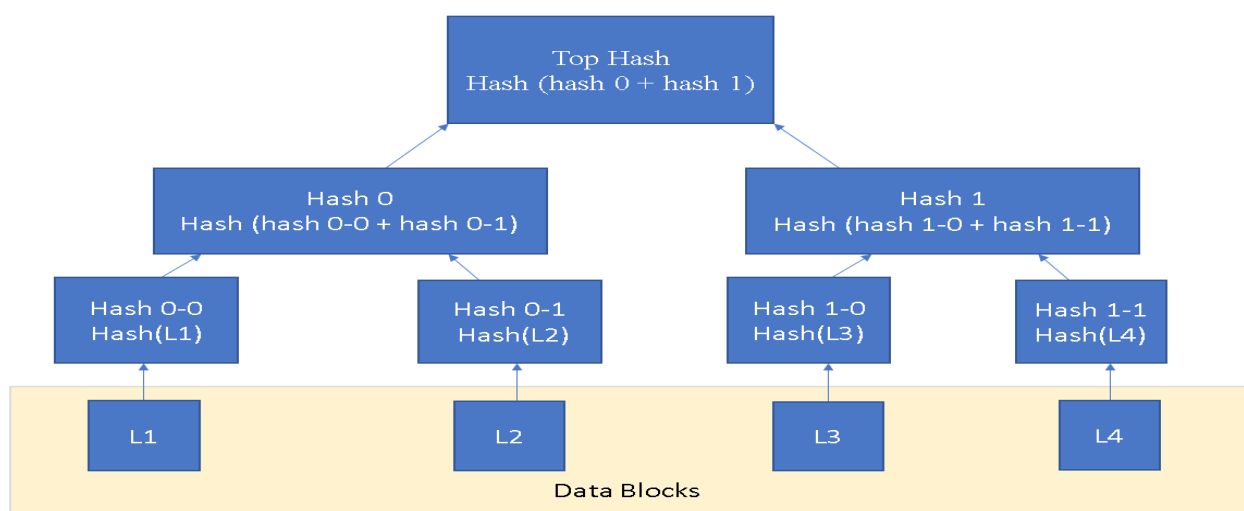
Merkle tree – Merkle trees are a fundamental part of blockchain technology. Merkle tree is a structure that allows for efficient and secure verification of content in a large body of data. This structure helps verify the consistency and content of the data. Merkle trees are used by both Bitcoin and Ethereum.

A Merkle tree summarizes all the transactions in a block by producing a digital fingerprint of the entire set of transactions, thereby enabling a user to verify whether or not a transaction is included in a block.

Merkle trees are created by repeatedly hashing pairs of nodes until there is only one hash left (this hash is called the Root Hash, or the Merkle Root). They are constructed from the bottom up, from hashes of individual transactions (known as Transaction IDs).

Each leaf node is a hash of transactional data, and each non-leaf node is a hash of its previous hashes. Merkle trees are binary and therefore require an even number of leaf nodes. If the number of transactions is odd, the last hash will be duplicated once to create an even number of leaf nodes.

See example below:



1. Complete the Merkle tree below:



SHA (Secure Hash Algorithm) – A set of cryptographic hash designed by United State National Security Agency in 1995. This hash function takes an input and output a cryptographic hash block. One- way hash that can produce a message to produce a condensed representation called a message digest or hash. Once the process through the hash function, any changes in a message or downloaded results in a different digest or hash. Therefore, these algorithms can be used to validate the integrity of the message. SHA256 can handle messages digest of size 2^{64} or less. Each block consists of 16 32-bit words. The resulting hash 8 32 bits words, for a total of 256 bits.

- Use to following site <https://passwordsgenerator.net/sha256-hash-generator/> to enter the following phase

1. HelloWorld!_____
2. HelloWorld:_____
3. Alice paid bob \$100:_____
4. Bob paid Alice \$100:_____

1. What is Blockchain Technology?

2. What is encryption? What role does it play in Blockchain?

3. Why Blockchain is a trusted approach?

4. How does Bitcoin use Blockchain?

5. Is it possible to modify the data once it is written in a block? Why?
