Chapter 1 Introduction

Brief history

For any process of buying and selling commodities through the internet, there is a need for a trusted third party to deal with to complete the process of buying and selling. As a consequence, there is a need to trust those third parties and provide them with private information only for verification processes while exposing most information is not necessary. As a result, there was an attempt to protect users' privacy in the late 1980s under the name of CypherPunk. The goal of this act is to protect the privacy and security of people's information by using cryptography technologies. As Erick Hughes, a CypherPunk activist posted in 1993, "in the electronics age" people should have a choice to reveal their private information to whom they want and hide it from whom they want in the network. Indeed, this idea spread widely even though it was against laws causing large illegitimate internet actions [1]. The first implementation of this concept was in 1999 by a music sharing app called Napster which was founded by Sean Parker and Shawn Fanning with a protocol known as peer 2 peer protocol. A lot of music was shared illegally by using Napster.

Another sharing file system called BitTorrent was founded by Bram Cohen in 2001. BitTorrent works by using BitTorrent Client for connecting with other clients. Swarms in BitTorrent exchange by requesting pieces of files (download) and send files that were requested (uploading). But with all its popularity, it still has one vital weakness, which is that the client's IP address can very easily be exposed.

In addition to the previous two attempts, there were many other attempts that tried to share data through the network. The two closest to what is known as Blockchain are B-money and Bit-Gold.

B-money was published in 1998 by Wei Dai. This publication was the first distributed system that dealt with hash cash. Wei described two protocols of which the first one is not practical [2]. In the second protocol, every one of the

participants is known in the network by just a public key. The public key acts as an ID for each one in the network. All the participants in the network are known by maintaining a database that contains all participants' IDs, which is distributed separately. The creation of money happened by solving computational problems and the amount is determined by the difficulty of the problem. The transferring of money in B-money had similar functionalities that exist nowadays in common crypto currencies. Wei used a consensus protocol in which each party of the network must approve the transaction. He used also digital signatures to verify the identity of the sender and receiver. Unfortunately, his protocols remained as a proposal and were never applied in a real environment. Nevertheless, Satoshi referenced Wei Dai's proposal in his paper as one of the inspirations for Bitcoin

The second idea was Bit-Gold. A crypto system that appeared in 1998 by Nick Szabo with also the same idea as Bitcoin. However, it was not applied like B-money. Some researchers said it was a precursor of the bitcoin because it was based on the Proof of Work (POW) protocol and used a Byzantine Fault Tolerance peer to peer network. Differing from Bitcoin, Bit-Gold used a method that depends on a quorum of addresses that was vulnerable to Sybil attack[3].

What is Blockchain

Blockchain technology is a general name of an intelligent idea that emerged in 2008 by an unknown person named Satoshi Nakamoto[4]. The main concept of the Blockchain is building a trust-based decentralized network and eliminating any rules of centralized authority inside it.

The word Blockchain contains two parts. A block, which refers to the container that holds all the data in the network during a period of time and chain which refers to the process of stacking each block to the previous one to perform a chain. Blockchain is based on a decentralized peer 2 peer system which adopts ledgers to keep a record of all transactions that took place inside the network. The main properties of Blockchain are transparency and immutability, where transparency

means that each node inside the blockchain network has a copy of the same data shared over the network, which means that all the data is shared transparently. For this reason, the data is immutable so changing or tampering it is nearly impossible.

Within a specific timeframe, all the transactions will be contained in a single block. An algorithm is initiated to find this block and then that block will be stacked with other blocks to create a chain.

All the nodes in the blockchain network also act as witnesses as a result of having a copy of all the information of events inside the network which makes block tampering nearly impossible. For this reason, utilizing of blockchain technology evolved very quickly after initiating the first blockchain application[5].

Blockchain applications

In the early days of Blockchain, it was not known to the public and it was not until digital currencies appeared, that use blockchain technology came to the surface. One of the most popular applications of blockchain is Bitcoin.

Bitcoin

The author Satoshi defined Bitcoin in his white paper as "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."[1] The valuable digital unit in the Bitcoin is called a Bitcoin. Users can use the digital Bitcoin unit to buy and sell assets, transfer money, and exchange bitcoin with other cryptocurrencies.

Ethereum

In 2015, Vitlaik Buterin launched Ethereum which is the first programmable digital currency. The digital unit of the Ethereum is called ETH. It is also completely decentralized. Ethereum spreads quickly because it uses a smart contract. The core difference between Bitcoin and Ethereum is that Ethereum is based on a smart

contract that the programmer can build in an application to accomplish a user's demands, and the application can be used in a decentralized network. Ethereum has many applications now like financial applications, games and decentralized market applications[6][7].

Besides these two applications of Blockchain, Blockchain technology is not restricted to only cryptocurrency, it also used in economics, medicine, software engineering, and the internet of things.

Components of Blockchain

Blockchain stands for three parts.

Cryptography**,** which uses ECC (Elliptic Curve Cryptosystems) that is based on PKI (Public Key Infrastructure). It uses two public and private keys. A public key is represented as a locker for data while the private key is represented as a key that can open the lock. In addition, Blockchain uses a specific algorithm in ECC which is called Elliptic Curve Digital Signature Algorithm (ECDSA). This algorithm helps in proofing the user's ownership of the signature without exposing the private key. ECDSA works by using the private key to encrypt a message and the public key to verify the signed message as encrypted from that private key (see Figure 1).

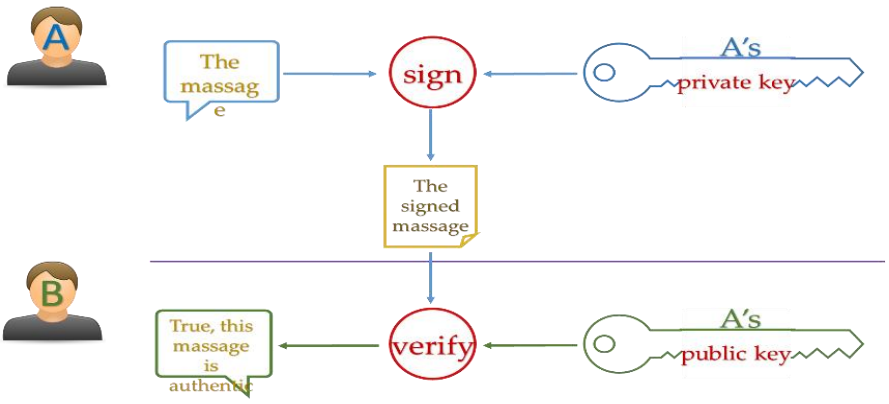

Figure 1 Sign and verify a message by using a digital signature

Peer 2 peer. This concept is based on eliminating the role of third parties for providing the process of verification and building trust. As a result, each participant in the network can connect and share data directly with other participants by following specific rules that were found to ensure trust amongst all of them. Figure 2.

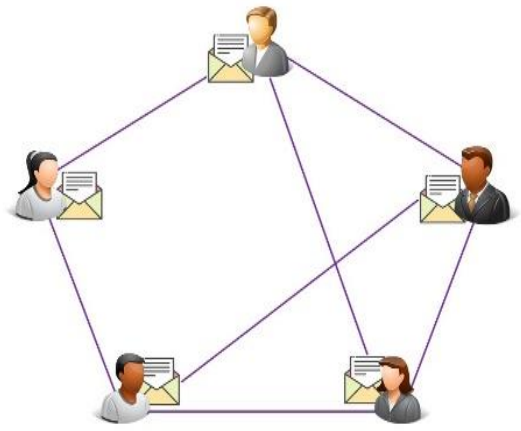

Figure 2 Peer 2 peer network

Game theory A consensus algorithm's goal is to reach an agreement amongst most of the nodes in the network for every process confirmation. The two most popular types of consensus protocols are Proof of Work (POW) and Proof of Stake (POS)

that are used in Bitcoin and Ethereum respectively. POW works by solving hash puzzles that need huge computational power to find a hash with a SHA256 algorithm which meets difficulty requirements. On the other hand, POS works by locating the nodes with a higher amount of currency. According to POS, the one who owns more money in POS has less chance to be an attacker and a higher chance to be a new block initiator. In addition, there are many other protocols used in digital currencies. All those protocols work to ensure that all nodes are in a consensus statement.

Blockchain Structure

As previously mentioned, Blockchain is based on a decentralized network that does not need a third party. All nodes work as a distributed ledger. Blockchain contains chains of blocks and every block can be known by a hash algorithm in its header. Each block header also refers to a previous block or a parent block until reaching the genesis block which is the first block in the chain (see Figure 3) [7].

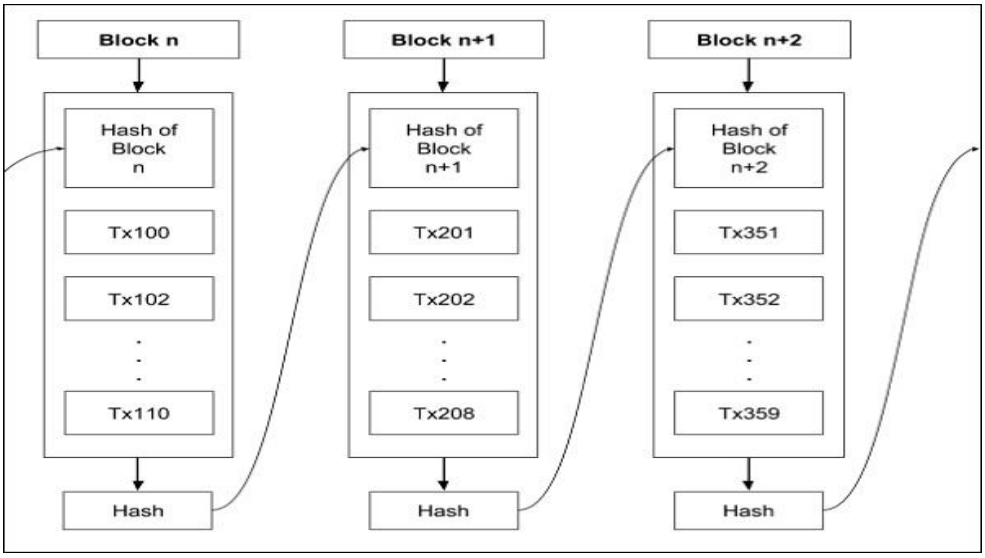

Figure 3 Chain of blocks representing each hash depends on previous hashes

Each block performs a number of transactions that contain the processes for transferring services from one node to another node. In addition, the transactions in the blocks will be performed in a tree called a binary tree (see Figure 4). Every two transactions will be hashed in one parent until it ends up with only one root hash called the Merkle tree which is used to provide immutability and integrity.

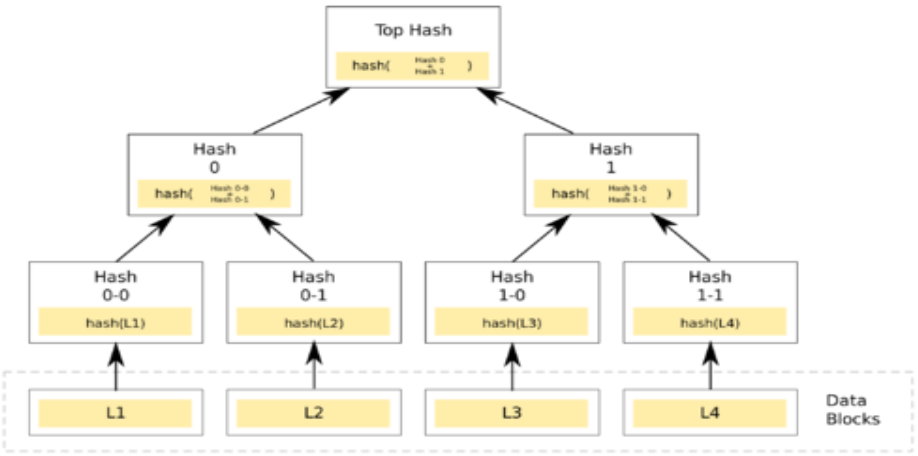

Figure 4 Binary Tree