CHAPTER I

Introduction

BLOCKCHAIN

A Brief History

In the 1960s, the Internet started as a protocol that allowed computers to communicate with each other and by 1975, the US Department of Defense used cryptography for the first time in military history. They created the DES encryption algorithm for security purposes, which was monopolized and closed to others—other people were not allowed to analyze or to understand the structure of the algorithm. This was an incentive to develop another cryptography technique to be open and understood by all, and that happened in the 1980s with the development of Elliptic Curve Cryptography (ECC). In the late 1980s, an activist group of cypherpunks—people who are strongly interested in cryptography—started a cypherpunk forum where they could discuss and propose thoughts related to cryptography. Hashcash in 1997, B-money in 1998, and Bit Gold are solutions that proposed electronic cash systems. Bit Gold is a reusable form of Hashcash or proof-of-work system that is close to what we know as Blockchain today. In 2008 a user of the cypherpunk forum called Satoshi Nakamoto posted a white paper called “Bitcoin: A Peer-to-Peer Electronic Cash System”, which described the Bitcoin technology that is a combination of the previously mentioned solutions. In 2009, Satoshi released Bitcoin as open-source software for the community. Since then, developers have improved the Bitcoin network system which has become popular and has grown over time.[1]

The Concept of Blockchain

Blockchain is defined as several nodes or peers that communicate with each other in a decentralized environment with no single authority. Information is recorded in a ledger that is shared between the peers transparently, in which each node knows what is going on in the database. This can confirm trust between them even in an anonymous environment. Since the data is available to everyone in the system, this supports the immutability of data where no one can change or tamper with the transaction. [Figure1]

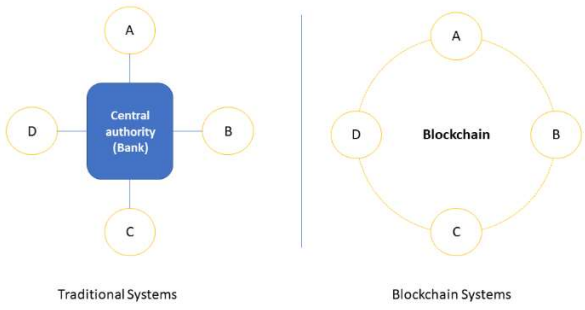

Figure 1:Blockchain Vs. Traditional systems

Blockchain has features which make it convenient for different applications. Since the information is seen by all the nodes, these transparent transactions increase trust and security between them. This has resulted in Blockchain technology being adopted for different applications. Money transfers or payment using Blockchain avoids the fees being paid to central authority banks. In addition, the Blockchain systems guarantee the charity gets to the intended recipient using the accountability of donations from benefactors. In political affairs, there are systems applying Blockchain technology to take votes and to ensure the best candidates win. Healthcare systems have started using Blockchain in patient medical record, in which the patient allows doctors and medical staffs to see his file anywhere and that can help to record a history of diseases and medical mistakes. Blockchain crowdfunding has the ability to change the industry. Because blockchain adds security to the funding

process, makes it accessible from anywhere, and completely transparent, blockchain can help to maximize the success of a project in crowdfunding platforms. Cryptocurrency is the largest and most common system that is associated with the beginning of Blockchain. Since its inception, it has been popular and it has recently been traded by some governments and businesses, and people have started to transfer money using Bitcoin. The other application that uses Blockchain is the Smart contracts, in which traditional contracts are performed digitally using some computation predefined protocols that are verified by the system community without third parties.

Blockchain Architecture

Blockchain is a combination of three main components: Cryptography, a P2P network, and Game theory as shown in Figure2.

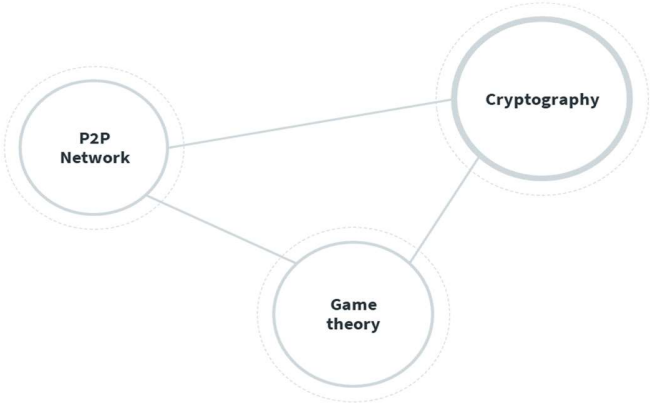

Figure 2:Components of the blockchain

Blockchain technology uses public key cryptography to ensure secure transfer transactions by performing the digital signature and hash function. Each node in the blockchain has public and private keys. The public key is used as an address for that node and other peers can use it to decrypt and verify the node transactions. Private keys are used for the digital signature where no one can tamper with or claim possession of the transaction. When a node wants to create a transaction in the blockchain, it possesses this transaction and before it propagates the transaction, it signs the transaction using the private key to ensure the identity, some

encryption process happen to ensure the confidentiality, and the hash function is applied to ensure the integrity of the message.

The second component of Blockchain is the P2P network, in which the nodes are connected to each other directly without using an authority. In P2P, the parties have the same capabilities, and any party can initiate a communication session. Each node has at least 8 outgoing peers or neighbors that it can send messages. Although the nodes are connected in P2P, each node has to hold an identical copy of the data of the network or so-called distributed ledger [Fig3].

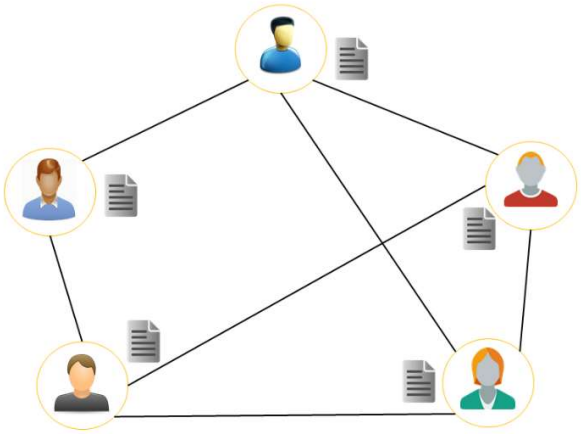

Figure 3:Nodes hold their identical copy of the ledger

The ledger contains all the information that the nodes create and transfer between them. It can be open for all and by using the cryptography hash function in a chain, no one can tamper or change the information recorded in the ledger.

The last component of the Blockchain architecture is Game theory. Game theory in Blockchain is defined as the consensus protocols that are used to make a decision by different participants and reach an agreement in a group. Since the participants are working on the P2P network, that means all have the same priority and no central authority can control the processes between them. Indeed, a consensus among those peers is required.

How Blockchain works

Blockchain has some terminologies that have to be highlighted before knowing how it works. A distributed ledger is an open database that shares information with all the nodes, which have all the data transferred between them. It consists of Blocks, and each block has a collection of data at any period of time. The Blocks are linked together using a cryptography hash function to ensure integrity and data manipulation. Any change in one block will affect all other linked blocks. Figure4 shows the structure of the blocks and how they are connected.

Figure 4:Structure of the blocks and how they are connected

The data is in the transactions that are created by nodes to process any intended goal, for example buying something or paying using cryptocurrency, or transferring an asset using a smart contract. Each transaction has to be broadcast to the peers, and to the transaction has to be approved and verified. The data block is structured using a Merkle tree, in which transactions represent the leaves of the tree and every two consecutive transactions are hashed together and the resulting hash is again hashed to the result of the next hash up to the root of the tree, which is considered the Block hash.

When node A wants to transfer some coins to node B, a transaction is created containing the details of this process like the amount coins that have to be paid and the sender and receiver addresses. This transaction is propagated to node A's peers using an advertisement technique. Once a peer receives a message from node A, it checks whether it has received this message before or not. If the node did not receive the message before, it will send a request message to node A to get the transaction. Node A subsequently sends the transaction to node B, and the process is repeated

to the remaining nodes. For a period of time, the transactions aggregated to form a so-called Block are linked to the head of the chain using a mechanism called a consensus. The consensus mechanism is the process to reach an agreement among all the nodes. When the block is ready to be chained, the nodes compete to solve a mathematical puzzle that is related to building the block compatible with the head chain. The complexity of the puzzle depends on the network size and the number of blocks; when the size of the Blockchain increases, the complexity increases and the required time to solve and computation power as well.

Security in Blockchain

Blockchain uses Asymmetric Cryptography or so-called Public Key Cryptography to ensure security in communications between the nodes. Specifically, Blockchain uses the ECDSA algorithm which stands for Elliptic Curve Digital Signature Algorithm, that has been applied especially for digital signatures. There are four basics to consider when transferring a message on a Blockchain network: confidentiality, integrity, non-repudiation, and authentication. When the transaction is sent to a peer, it must be kept hidden from other unauthorized parties by applying encryption and decryption. The integrity of the data means that no one has altered or tamper with the data, and that is achieved by using the hash function. As mentioned, a digital signature is applied using ECDSA to ensure the non-repudiation which means the node which is responsible for sending a message cannot claim the unlike that. The authentication property is fulfilled by public and private keys. When the message is received and decrypted the receiver is able to verify that the other party is really who sent this message. Figure 5 below describes the message transfer between the nodes.

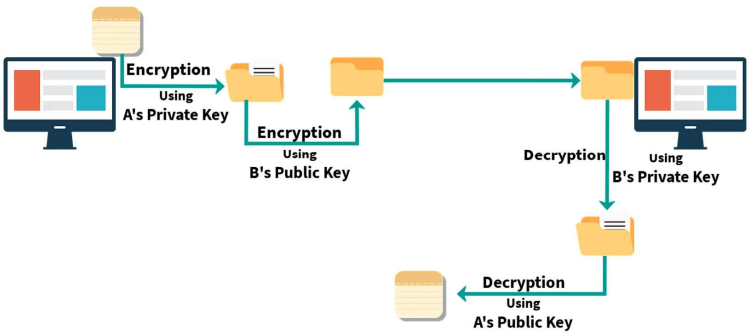

Figure 5:Transaction transfer between the nodes