**BRAC UNIVERSITY**



**Assignment**

**Course Code: CSE-707**

**Course Name: Distributed Computing System**

**SUBMITTED TO**

**Mr. Md. Safiuzzaman Rajib**

**CSE Department, BRAC University**

**SUBMITTED BY**

**Turzo Ahsan Sami**

**ID: 20166012**

**Date of Submission: 20/01/2020**

**Blockchain**

The innovation to probably have the best effect on the following scarcely any decades is here. It's not online networking or even man-made reasoning, it's the fundamental advancements in all cryptographic forms of money, for example, Bitcoin, and it's called Blockchain.

**History**: The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where document timestamps could not be tampered with. In 1992, Bayer, Haber and Stornetta incorporated Merkle trees to the design, which improved its efficiency by allowing several document certificates to be collected into one block.

**Decentralization:** By storing data across its peer-to-peer network, the blockchain eliminates a number of risks that come with data being held centrally. The decentralized blockchain may use ad hoc message passing and distributed networking.

Peer-to-peer blockchain networks lack centralized points of vulnerability that computer crackers can exploit; likewise, it has no central point of failure. Blockchain security methods include the use of public-key cryptography. Every node in a decentralized system has a copy of the blockchain,

**Types:**

Currently, there are at least four types of block chain networks —

* Public block chains
* Private block chains
* Consortium block chains
* Hybrid blocks chains.

**Block chain analysis**: The analysis of public block chains has become increasingly important with the popularity of bit coin, Ethereum, lite coin and other crypto currencies. A block chain, if it is public, provides anyone who wants access to observe and analyses the chain data, given one has the know-how. The process of understanding and accessing the flow of crypto has been an issue for many crypto currencies, crypto-exchanges and banks. A common belief has been that crypto currency is private and untraceable, thus leading many actors to use it for illegal purposes. This is changing and now specialized tech-companies provide block chain tracking services, making crypto exchanges, law-enforcement and banks more aware of what is happening with crypto funds and fiat crypto exchanges.