**DIGITAL VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY**

MAYANK AGGARWAL

15BCE0751

KUNAL KALRA

15BCE0809

**ABSTRACT**

Democratic voting is a crucial and serious event in any country. The most common way in which

a country votes is through a paper based system, but is it not time to bring voting into the 21st

century of modern technology? Digital voting is the use of electronic devices, such as voting

machines or an internet browser, to cast votes. These are sometimes referred to as e-voting when

voting using a machine in a polling station, and i-voting when using a web browser.

Security of digital voting is always the biggest concern when considering to implement a digital

voting system. With such monumental decisions at stake, there can be no doubt about the

system’s ability to secure data and defend against potential attacks. One way the security issues

can be potentially solved is through the technology of blockchains.

Blockchain technology originates from the underlying architectural design of the cryptocurrency

bitcoin. It is a form of distributed database where records take the form of transactions, a block is

a collection of these transactions. With the use of blockchains a secure and robust system for digital voting can be devised. This report outlines our idea of how blockchain technology could

be used to implement a secure digital voting system.

**WHAT IS BLOCK CHAIN**

Blockchain technology was first used within Bitcoin and is a public ledger of all transactions. A

blockchain stores these transactions in a block, the block eventually becomes completed as more

transactions are carried out. Once complete it is then added in a linear, chronological order to the

blockchain.

The initial block in a blockchain is known as the ‘Genesis block’ or ‘Block 0’. The genesis block

is usually hardcoded into the software; it is special in that it doesn’t contain a reference to a previous block. Once the genesis block has been initialised ‘Block 1’ is created and when complete is attached to the genesis block. Each block has a transaction data part, copies of each transaction are hashed, and then the hashes are paired and hashed again, this continues until a single hash remains. The block header is where the merkle root is stored. To ensure that a transaction cannot be modified each block also keeps a record of the previous blocks header, this means to change data you would have to modify the block that records the transaction as well as all following blocks.

A blockchain is designed to be accessed across a peer-to-peer network, each node/peer then

communicates with other nodes for block and transaction exchange. Once connected to the

network, peers start sending messages about other peers on the network, this creates a

decentralised method of peer discovery. The purpose of the nodes within the network is to

validate unconfirmed transactions and recently mined blocks, before a new node can start to do

this it first has to carry out an initial block download. The initial block download makes the new

node download and validate all blocks from block 1 to the most current blockchain, once this is

done the node is considered synchronised.