**A Secure and Privacy Data Sharing with Example**

**ABSTRACT**:

Blockchain is a progressive innovation technology that permits individuals to record message exchanges or transactions on an advanced, decentralized, distributed ledger, with no central controlling authority as in case of financial banking systems. Recorded transactions are seen to all users within the blockchain network and cannot be modified by any user or node. Blockchain has become popular with many other applications including IoT, healthcare, industry, supply chain management etc. Blockchain technology is ready to change almost every aspect of our advanced digital lives. By obviating third parties, blockchains guarantee to make our frameworks more effective. By going around oversight, they guarantee to make our frameworks more impartial. Also, if appropriately executed, they could make our frameworks more dependable and secure. The purpose of this review is to understand blockchain technology and challenges associated with its security and privacy

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * Privacy Leakage Actors had opinion that blockchain offers higher privacy while managing important and sensitive data. In blockchain, actors or users may want to generate address with in preference to their identity * . MITM Attack Man in The Middle Attack [14] where a user comes in the middle and compromises the transactions between two nodes. MITM attack tries to impersonate as valid user and gain access to transmission data * Distributed Denial of Service (DDoS) Attack Distributed Denial of Service attack [14] targets to deal with one particular system which may be a program under execution, computer system, webpage, server or other resources of the network resulting in controlling the targeted system or node resulting in powering off the system or damage the system related files to slow down the processing capability. In blockchain such attack can damage the business. | * . Traceable and unforgeable Each transaction carried out on a blockchain network shall have a time stamp. This permits every node to maintain the order of transactions so that data or the transactions are traceable * In blockchain network, all users share transactional records and find the data in nodes in a decentralized manner. The blockchain technology makes certain that nodes correctly capture and forward transactional data and related information. Transparency is exiting in the network with transactions and data sharing. Decentralization The blockchain consists of P2P node blocks, each of these nodes shall have potential to generate data and save all transactional data. In a decentralized network, all nodes participate in all activities and transactions |
| **EXISTING ALGORITHM**  Consensus algorithm | **PROPOSED ALGORITHM:-**  Hash pointer,DIGITAL SIGNATURE |
| **ALGORITHM DEFINITION:-**  Consensus algorithm is defined to ensure that the transactions written on ledger are same as data on the minor nodes. Set of rules defining consensus is a process that makes the declaration of all blockchain nodes in the same post, which can ensure that the new block has been effectively added to the chain | **ALGORITHM DEFINITION:-**  The head of the blockchain which is the first block is called as genesis block and this block doesn’t contain a link to any other block in the network of chains.  o ensure that the transactions are valid, Digital signatures are used in blockchain technology. Each node has a private secrete key and known to all public key. Every node sign transactions using secrete private key and other nodes validate this signature using public key of the signer |
| **DRAWBACKS:-**   * Scalability * Privacy Leakage * MITM Attack * Distributed Denial of Service (DDoS) Attac. | **ADVANTAGES:-**   * Decentralization * Detrusting * Transparency * Traceable and unforgeabl. |

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE

**System Architecture.**



