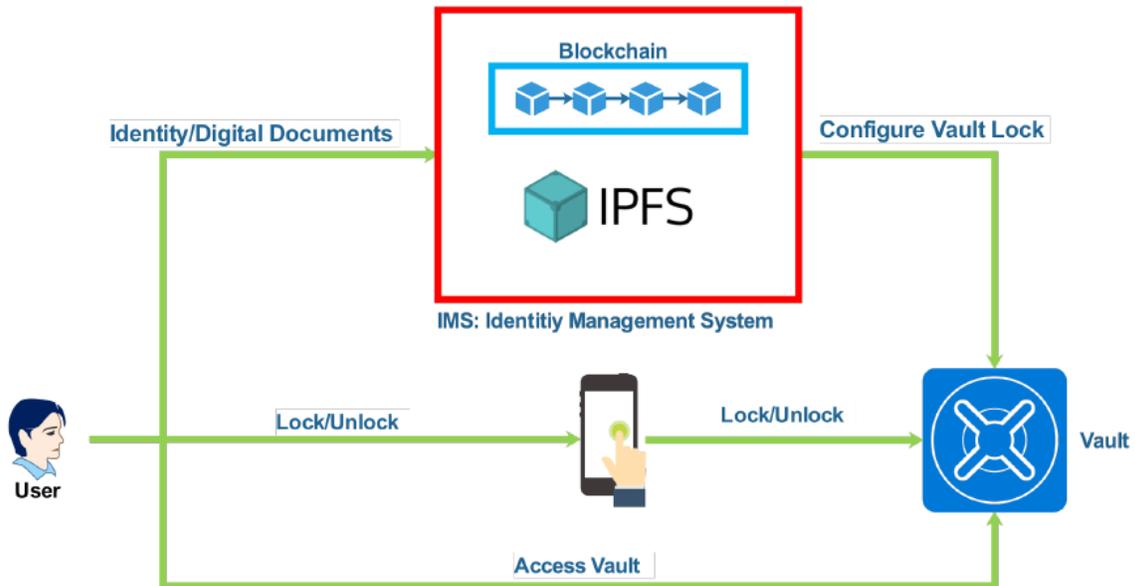# IDENTITY MANAGEMENT SYSTEM (IMS) USING BLOCKCHAIN & IOT TECHNOLOGY

DIGITAL IDENTITY RESEARCH INITIATIVE (DIRI), INDIAN SCHOOL OF BUSINESS (ISB)

IMS ARCHITECTURE

The architecture focuses upon secure and efficient management of confidential/personal identity data. This system integrates Inter Planetary File System (IPFS), Internet of Things (IoT) and Blockchain Technology. The user credential is securely stored in the blockchain and the nature of blockchain prevents unauthorised modifications. Confidential documents can be uploaded as scanned images into the immutable database called IPFS. This architecture also provides a digital locker for the user to store his/her data physically using his/her password from the blockchain using IoT technology.

STEPS FOR CREATING IMS

1. The user registers by providing his/her basic details like username, address, phone, password etc., which is stored in Blockchain, to be accessed later.
2. The user can login using his/her username and password, which is cross-checked with data stored in Blockchain (provided at the time of registration). Depending on the match or mismatch, the user is given access or rejected respectively.
3. On logging in, the user can upload scanned images of documents, which are stored in IPFS, with corresponding hash code stored in the Blockchain.
4. Authenticity of the documents are validated using Digital Signature. The user can view his/her documents using the hash code.
5. The user can keep the hard copies of documents in a physical vault by entering his/her username and password on the keypad provided on the vault, which are verified with the one stored in Blockchain, thus integrating it with IoT; and by placing one's finger on the fingerprint scanner.

Blockchain
A blockchain is a growing list of records, called blocks, which are linked using cryptography. Blockchains which are readable by the public are widely used by cryptocurrencies. Private blockchains have been proposed for business use. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree root hash).

By design, a blockchain is resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority.

Though blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

Internet of Things (IoT)
The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables them to connect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions.

IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled. With the arrival of driverless vehicles, a branch of IoT, i.e. the Internet of Vehicle starts to gain more attention.

Inter Planetary File System (IPFS)
IPFS is a protocol and network designed to create a content addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. IPFS was initially designed by Juan Benet and is now an open-source project developed with help from the community.

Raspberry pi
Raspberry Pi is a series of small single-board computers developed initially in UK by the Raspberry Pi Foundation to promote teaching of basic computer science in schools. The original model became far more popular than anticipated, selling outside its target market for uses such as robotics.

Fingerprint Scanner
Fingerprint scanner is a recognition device based on unique fingerprint biometric technology.