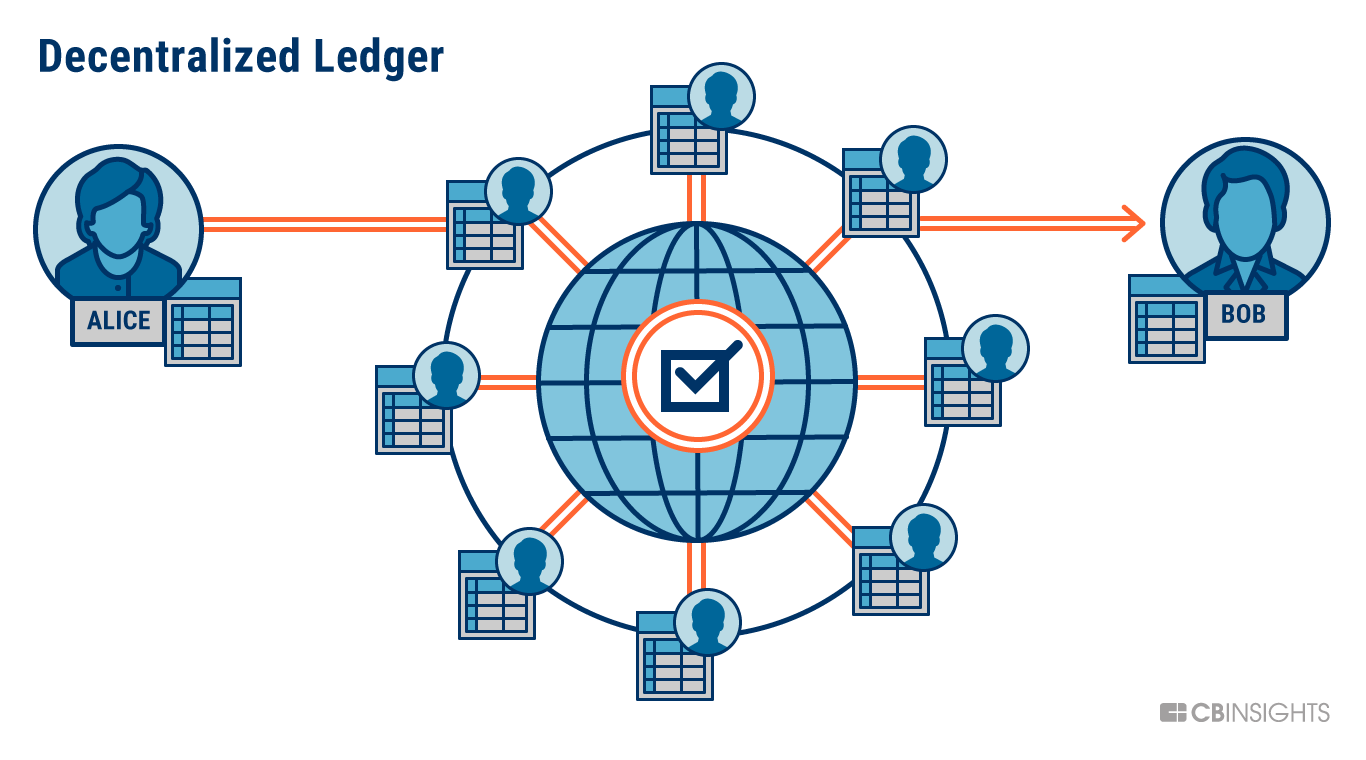
**A REVIEW ON BLOCKCHAIN TECHNOLOGY AND BLOCKCHAIN PROJECT’S FOSTERING OPEN SCIENCE**

**Blockchain**

Blockchain is a rapid growing technology in various field of science and technology. Blockchain is an immutable ledger or simply a linked list which is distributed and verified by every computer that is connected or a part of blockchain. It is distributed in a peer to peer network .One of the famous blockchain application is bitcoin which is a cryptocurrency and used as alternative to standard money and transactions are maintained in blockchain. But that’s not blockchain is made for blockchain is a ledger which maintains the transactions not specifically for money but for the data we want to be highly secured and shareable to everyone. Blockchain data is encrypted first by a highly secured algorithm called sha256 algorithm which is a one way going algorithm and cannot be retrieved back the data which is encoded and this makes blockchain secured Technology which is a major concern of today. In the ledger we just not store transaction but we can also Store text files documents and images as well in encrypted form. This makes blockchain technology helpful in other fields such as medical real estates currency exchange etc.

**Basic Terms of Blockchain:**

* **Transaction:** Any type of action or request made is a transaction in the blockchain all the transactions are then forwarded to a unconfirmed transaction. It is just not a monetary transaction but any type of data we want to store in the ledger in encrypted form that we want to record.
* **Node:** All those computers which are apart of network or connected to blockchain are called node every node is provided be a public and private key to encrypt the data.
* **Miners:** Miners are those who possess powerful computers CPU or GPU which actually solves the problem every transaction is a complex mathematical problem which when solved then only a transaction will be added to the block and that block will be added to the blockchain and that problem should be solved in least amount of time to make the transaction successful so miners chose transaction which provide good fees to them and solve that transaction problem. Use CPU and GPU consume a lot of energy and the energy consumed is even comparable to the total amount of energy used by sum of some countries. So transaction is that difficult to be then successful. Simple computer as are not made for such purposes. There are even new hardwares made that are only invented to solve those problems.
* **Ledger:** Ledger is nothing but a linked list which stores data and the next data block is somehow connected with the previous block in such a way that if previous block gets corrupted then it will affect the nose ahead of it. in this way if among any computer in blockchain gets hacked then it will lose the integrity and when it will get updated for the next time then it will not match with all other nodes and it will know that something went wrong so will delete the corrupted list all the ledger and correct it with the new one in this way it is nearly impossible disturb the list.



* **Consensus protocol:**
* Consensus protocol come into play when 2 miners at the same time solve the mathematical problem then it is quite difficult to decide whose block should be added to blockchain in such case the minor who propagated the block to the maximum nodes in the blockchain will be the winner or who carry the longest chain will be the winner. And the other miner who created block that block will be released and called as orphan block. It follows Byzantine fault tolerance principle.

**Difficulty in hacking or disturbing a Blockchain System which makes blockchain more strong**

* Blockchain follows Byzantine fault tolerance which tells that if more than 50% of the participants agree on the wrong agreement or any wrong condition then only system will fail otherwise it will not to make the system corrupt so as we know there are thousands of nodes connected in the blockchain and if we hack one of the computer and try to alter the data in the blockchain then also it will not affect anyone because every time updating the ledger with their neighbour nodes so it is quite difficult to alter the data to change anything in very least amount of time and that also more than 50% of the nodes all together.
* Since the data is encrypted in sha256 algorithm it is quite difficult to read what is in the blockchain every data in blockchain is present in just 256 bytes even if the file is in text multimedia or any other format the data is represented in 256 bytes so we cannot retrieve the data.
* Transactions in the blockchain are publicly available but in encrypted form and the sender and receiver are also represented by address not by their names or email. User is provided with some address and public and private key so directly no one can understand show records are available but normal people cannot make any conclusion from that.
* Ethereum based projects(blockchain with features) are agreed upon some contract and that contract are managed by the blockchain. So if someone tries to cheat or steal money then also it is not possible to do so. In this way blockchain can be used to make strict applications where there is a chance of some illegal activity.
* No middleman is present in blockchain system even in the banks there is a chance that some traitor change the data and the whole system or cooperation security and data is affected. All the people unknown to each agree on some rules and that makes it reliable no one can change it.

**Applications of blockchain**

Blockchain is highly used when we want to store an immutable data which we don't want to get corrupted or hacked by someone and not disturbed over a long. of and if some kind of failure occurs then it should maintain its integrity and follow some recoverability rules. In standard client server architecture if some server fails or server is hacked then it can bring huge loss while in blockchain the data is maintained and distributed over a network and gets updated time to time every node is somehow linked to the next node and the same next node is linked with some rules to its next node then the first note leaves a mark on every node so if something gone wrong whole ledger will be disturbed but other computers when update next time will correct it because they We have to maintain Data integrity and correctness. And where there is a need be a proof of work.

**Various Fields where blockchain is leveraged**

**Banks:** For the transaction of money and maintaining records.

**Hospitals:** secure the highly sensitive data which if altered can be life threating and where previous records are also important to analyse the disease or past results.

**Real Estates:** Many a times it happens that plot registered by two people due to some mistake done by the authority in such cases blockchain is the perfect solution.

**Building decentralized applications** which involves multiple computer save data and update time to time blockchain provide us the way Ethereum and hyperledger are the build rebuild blockchains which are helpful in making such systems.

For making **Immutable smart contracts** which cannot be changed accessed by anyone non authorized person.

If We want who built a **application private** for some specific community then hyperledger is a good platform where it works completely as a blockchain but not everyone by choice can participate in it. Only the legitimate users will be able to be a part of it.

**Blockchain Fostering Open Science**

Open science is an initiative or step to make the researches and material related to some subject publicly available or to a group of people through some Technology and digitalization. So blockchain can help a lot in fasting open science some of the ways are digitally signed documents can be created so that

No one can change the data because blockchain immutable. Since research data is precise and highly important it is a must do job to do make it unchangeable by some kind of hacking activity.

If we go for private blockchain then group of people who are legitimate and only needed in the group and access through the data and not all can participate or see the Private data.

The rights and the Possession of work is totally secured in blockchain so there will be no confusion regarding the possession of document and plagiarism can be found.

Since there will be no middle man so there are less chances of cheat and robbery.

The content can be preserved over a long period of time and if one node gets corrupted then also the data is maintained by all the nodes so there is no chance of data loss.

No one server is maintained so there is less chance of traffic and server down situations instead data will be accessible to everyone and with the new technology of IPFS(used to store the data online ) we can make the application serverless but available to everyone.

Through Smart contracts we can define the rules and regulations for the system in open science and then no one can go against the rules we made. In this way a discipline community can be maintained which cannot go against the laws and no illegal activity can be done.

So all these leads to a strong open science organisation and structure which is transparent and error free and can be totally relied upon since blockchain can be integrated with web applications and mobile applications so use of blockchain can be made very simple and growth of open science can reach very high