Overview of Block Chain Technology

Rita Patil, Neha Patil, Yamini Jadhav, Rohini Jadhav, Pooja Kale, Rohidas B. Sangore.

Department of Information Technology, K. B. C. North Maharashtra University, Jalgaon, India.

Shram Sadhana Bombay Trust's College of Engineering & Technology, Bambhori, Jalgaon, Maharashtra, India.

Corresponding Author:rohinij81296@gmail.com

Abstract: -"Many sectors, like finance, medicine, manufacturing, and education, use blockchain applications to profit from the unique bundle of characteristics of this technology. Blockchain technology (BT) promises benefits in trust ability, collaboration, organization, identification, credibility, and transparency. In this paper, we conduct an analysis in which we show how open science can benefit from this technology and its properties. For this, we determined the requirements of an open science ecosystem and compared them with the characteristics of BT to prove that the technology suits as an infrastructure. We also review literature and promising blockchain-based projects for open science to describe the current research situation. To this end, we examine the projects in particular for their relevance and contribution to open science and categorize them afterwards according to their primary purpose".

Key Words: — *Blockchain, Centralized, Decentralized, Distributed.*

I. INTRODUCTION

Blockchain is a decentralized, distributed, public ledger system. Next thing in industry is blockchain as internet has affected all many industries in some way blockchain will also affecting it that question may be two year or three years blockchain will be there why it is so important. If you hurt about bitcoin or ypu might have hurt about blockchain as well so the word on bitcoin is started 2008 with pseudo name it may be person or group of people and pseudo name is "Santoshi Nakamoto". That person or pseudo name has created bitcoins with blockchain. So, the technology behind bitcoin is blockchain but what exactly bitcoin gives you bitcoin is basically a digital crypto currency and it works on peer-to-peer network which can also called it as distributed system so there is no central system.

For example: You want transfer money now you have bank in between bitcoins don't have any central bank anything is distributed.

When we talk about distributed there is problem the first problem is security and second is trust how can you trust this technology and how was security now this one solution for security we can use cryptography now we can use concept of asymmetric cryptography and we can achieve security but how what trust someone that you ask data or sending money to how can you trust data which is available from internet. Because when you say all the entire internet one person is transferring money to other person who is maintaining database. It has issue because let I send 5 bitcoins to you how can you sure that you have 5 bitcoins I have and I don't have

those 5 bitcoin which I send you who is maintaining the system so that's where this ledger come to the picture now what is that ledger. It is normal database nothing about it we can have a central database that's a problem because we are talking about distributed system and in distributed why need you something in central that's one problem what if every node what node here if there are 5 people working with bitcoin and 5 people in this network and every machine we will call it as machine so can you maintain the ledger on every machine. We can do that but how can trust them because this is one problem you have ledger there anyone can tempered you are confusing with ledger imagine a simple database or a simple file if we talk about government in government we have lot of corruption and everyone want to stop corruption and one way if that is look at database what they have work and everything is store in database. So, now we normal people see in database we can do that they have power to change database while change history of database we want something where should not be change so we want ledger which will available any machine but no one should able to change it so that's where should blockchain come to picture.

II. HISTORY

The first major blockchain innovation was bitcoin, a digital currency experiment. The market cap of bitcoin now hovers between \$10–\$20 billion dollars, and is used by millions of people for payments, including a large and growing remittances market.

The second innovation was called blockchain, which was essentially the realization that the underlying technology that operated bitcoin could be separated from the currency and used for all kinds of other inter organizational cooperation. Almost every major financial institution in the world is doing blockchain research at the moment, and 15% of banks are expected to be using blockchain in 2017.

The third innovation was called the "smart contract," embodied in a second-generation blockchain system called ethereum, which built little computer programs directly into blockchain that allowed financial instruments, like loans or bonds, to be represented, rather than only the cash-like tokens of the bitcoin. The ethereum smart contract platform now has a market cap of around a billion dollars, with hundreds of projects headed toward the market.

The fourth major innovation, the current cutting edge of blockchain thinking, is called "proof of stake." Current generation blockchains are secured by "proof of work," in which the group with the largest total computing power makes the decisions. These groups are called "miners" and operate vast data centers to provide this security, in exchange for cryptocurrency payments. The new systems do away with these data centers, replacing them with complex financial instruments, for a similar or even higher degree of security. Proof-of-stake systems are expected to go live later this year. The fifth major innovation on the horizon is called blockchain scaling. Right now, in the blockchain world, every computer in the network processes every transaction. This is slow. A scaled blockchain accelerates the process, without sacrificing security, by figuring out how many computers are necessary to validate each transaction and dividing up the work efficiently. To manage this without compromising the legendary security and robustness of blockchain is a difficult problem, but not an intractable one. A scaled blockchain is expected to be fast enough to power the internet of things and go head-to-head with the major payment middlemen (VISA and SWIFT) of the banking world.

III. WHY BLOCKCHAIN

First of all, there are certain issue with current technology which you working. For example, internet we are using now its amazing technology it has change business work it has created different type of domain or business think about google, facebook they are all running because of feature of internet. Now internet has mentally open to everyone but internet is actually control by few companies and we don't want central power because it is good up now. You can change this block but can we because you have block anyone can change it that's not how bitcoin works. So what bitcoin do is they use concept of hashing what is hashing now so hashing means we use different algorithm to generate a simple

hash key it can be any algorithm we can use MD5, SHA512. We can use this algorithm for specific input my name is shital so if this is input you can perform operation which will give you a key now the awesome thing is it doesn't matter how big input is it can simple line like my name is shital or it can be entire keep a database.

IV. WHAT IS CRYPTOCURRENCY

Fig.1. Cryptocurrency

Cryptocurrency is a type of money which is completely virtual, like an online version of cash which exists digitally. While you can use some, such as Bitcoin, to buy products and services, not many shops accept it and some countries have banned it altogether. Cryptocurrencies, such as Bitcoin, are basically computer files which are stored in a digital wallet on a smartphone or computer. They can be sent between digital wallets, with every single transaction recorded on a list called the Blockchain. Some people like the fact cryptocurrencies are generally not controlled by the government or banks. But is it secure? While every transaction is recorded, cryptocurrency2 can potentially be stolen if a thief were to get access to a wallet. BBC journalist Monty Munford had £25,000 worth of Ethereum stolen after mistakenly storing his password in an email. It is possible to lose your Bitcoin wallet or delete your Bitcoins and lose them forever. There have also been thefts from websites that let you store your Bitcoins remotely.

V. TYPES OF BLOCKCHAIN

The code to operate a Public Blockchain is openly This gives anyone the right to participate in the process that decides which blocks get added to the chain as well as the current shape and size of the Blockchain. Anyone can perform transactions on the network. The transactions, as long as they are valid, will go through. With a block explorer, anyone can gain access to and read transactions.
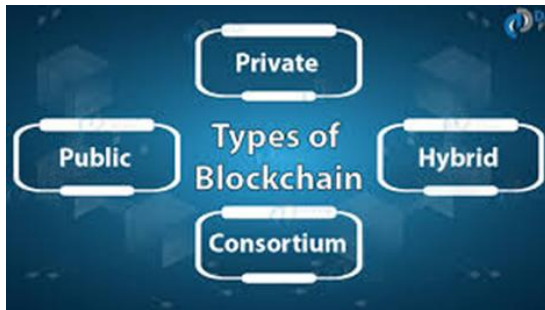
Fig.2.Public Blockchian

Transactions are anonymous and transparent. Anyone can participate on a public Blockchain, without permission. Examples include Bitcoin, Ethereum, Monero, Dash, Litecoin, among others.This nature of the Public Blockchain presents two major implications. Everyone can potentially disrupt prevalent business models through the reduction in the use of intermediaries.

A. Private Blockchain:

In a Private Blockchain, edit permissions are kept centralized to one organization. Read permissions may be public or restricted to varying degrees. Private Blockchains are mostly used in database management, auditing among other fields. There uses are internal to a single company, and so the companies will not want the data to be accessible to the public. They use Blockchain technology by setting up groups and participants who can verify transactions internally. However, Private Blockchains may scale better and comply better with governmental data security and privacy regulations. The important benefits of Private Blockchains are a reduction in transaction costs and data redundancies as well as easier data-handling and more automated compliance functionalities.

B. Consortium Blockchain

The consortium blockchain is a system that is semi-private and has a controlled user group, but works across different organizations. There are many benefits to consortium systems, and many blockchain platforms are setting themselves up as a backbone for these cross-company and cross-discipline solutions. A blockchain consortium of like-minded companies can leverage information to improve workflows, accountability, and transparency.

IS BLOCKCHAIN PRIVATE:

Anyone can view the contents of the blockchain, but users can also opt to connect their computers to the blockchain network as nodes. In doing so, their computer receives a copy of the blockchain that is updated automatically whenever a new block is added, sort of like a Facebook News Feed that gives a live update whenever a new status is posted. Each computer in the blockchain network has its own copy of the blockchain, which means that there are thousands, or in the case of Bitcoin, millions of copies of the same blockchain. Although each copy of the blockchain is identical, spreading that information across a network of computers makes the information more difficult to manipulate. With blockchain, there isn't a single, definitive account of events that can be manipulated. Instead, a hacker would need to manipulate every copy of the blockchain on the network. This is what is meant by blockchain being a "distributed" ledger. Looking over the Bitcoin blockchain, however, you will notice that you do not have access to identifying information about the users making transactions. Although transactions on the blockchain are not completely anonymous, personal information about users is limited to their digital signature or username.

IS BLOCKCHAIN SECURE:

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well. Here's why that's important to security. Let's say a hacker attempts to edit your transaction from Amazon so that you actually have to pay for your purchase twice. As soon as they edit the dollar amount of your transaction, the block's hash will change. The next block in the chain will still contain the old hash, and the hacker would need to update that block in order to cover their tracks. However, doing so would change that block's hash. And the next, and so on. In order to change a single block, then, a hacker would need to change every single block after it on the blockchain. Recalculating all those hashes would take an enormous and improbable amount of computing power. In other words, once a block is added to the blockchain it becomes very difficult to edit and impossible to delete.

What Is Blockchain Architecture Works:

For starters, let's first learn what is blockchain technology. Logically, a blockchain is a chain of blocks which contain specific information (database), but in a secure and genuine way that is grouped together in a network (peer-to-peer). In other words, blockchain is a combination of computers linked to each other instead of a central server, meaning that the whole network is decentralized [3].

International Journal of Progressive Research in Science and Engineering
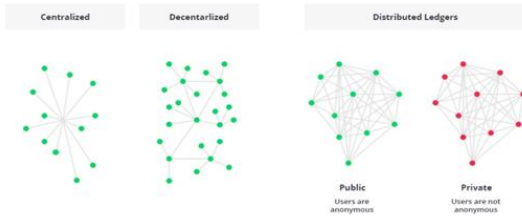Volume-1, Issue-3, June-2020
www.ijprse.com

Fig.3. Centralized, Decentralized, Distributed Ledger

To make it even simpler, the blockchain concept can be compared to work done with Google Docs. You may recall the days of tossing over doc. documents and waiting for other participants to make necessary edits. These days, with the help of Google Docs, it is possible to work on the same document simultaneously. The blockchain technique allows digital information to be distributed, rather than copied. This distributed ledger provides transparency, trust, and data security. Blockchain architecture is being used very broadly in the financial industry. However, these days, this technology is employed not only for crypto currencies, but also for record keeping, digital notary, and smart contracts.

VI. ADVANTAGES

- In financial systems and businesses, this adds an unprecedented layer of accountability,
- In comparison to traditional financial services, blockchain facilitates faster transactions by allowing P2P cross-border transfers with a digital currency.
- Blockchain is far more secure than other record keeping systems because each new transaction is encrypted and linked to the previous transaction.

VII. DIS-ADVANTAGES

- Blockchain is not indestructible.
- It's hard to enter into legacy system.
- Blockchain implementation is costly process.

VIII. APPLICATIONS

Payment processing and money transfers:
The main use for blockchain is as a means to expedite the transfer of funds from one party to another. As noted, with banks removed from the equation, and validation of transactions ongoing 24 hours a day, seven days a week, most

transactions processed over a blockchain can be settled within a matter of seconds.
Retail loyalty rewards programs:
More than 1 billion people worldwide face identity challenges.
Healthcare:
Blockchain has a wide range of applications and uses in healthcare.

Smart contracts:
Blockchain based smart contracts are proposed contracts that can be partially or fully executed or enforced without human interaction. One of the main objectives of a smart contract is automated escrow.

IX. FUTURE SCOPE

In the current day there are endless opportunities for blockchain developers as UMPTEEN number of jobs with good salaries are available. The demand of for blockchain developers is now at an all-time high. Being considered as the second most demand company in the market after robotics specialists, blockchain development will only grow higher in popularity. This is not just speculation. With blockchain technology become more and more in demand in industries such as business.

X. CONCLUSION

Blockchain is a new name in the world of technologies but it is definitely the one to last. Even in the early stages, the technology has gained huge popularity starting with their very first application of crypto currencies. More areas of applications are being discovered and tested with each passing day. Once the technology is adopted and accepted on a global level, it'll transform the way we live today.

REFERENCES

[1]. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform

[2]. Bellare, Mihir; and Rogaway, Phillip. (September 21, 2005). "Introduction." In Introduction to Modern Cryptography

[3]. Medium.com/coinmonks/asset-tokenization-on-blockchain-explained-in-plain-english-f4e4b5e26a6d.

[4]. S. Underwood, "Blockchain beyond bitcoin", Commun. ACM, vol. 59, no. 11, pp. 15-17, 2016.