BLOCKCHAIN

Ansari Mohammed Sajjad, Shaikh Aftab, Khan Abrar, Shaikh Yaseen, Usmani Mohammed Osama
Computer Department,
Anjuman.Islam.Abdul.Razzak.Kalsekar.Polytechnic, Panvel, India

***Abstract:* Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner.We also lay out possible future trends for blockchain.**
Digital world has produced efficiencies, new innovative products, and close customer relationships globally by the effective use of mobile, IoT (Internet of Things), social media, analytics and cloud technology to generate models for better decisions. Blockchain is recently introduced and revolutionizing the digital world bringing a new perspective to security, resiliency and efficiency of systems. While initially popularized by Bitcoin, Blockchain is much more than a foundation for crypto currency. It offers a secure way to exchange any kind of good, service, or transaction. Industrial growth increasingly depends on trusted partnerships; but increasing regulation, cybercrime and fraud are inhibiting expansion. To address these challenges, Blockchain will enable more agile value chains, faster product innovations, closer customer relationships, and quicker integration with the IoT and cloud technology. Further Blockchain provides a lower cost of trade with a trusted contract monitored without intervention from third parties who may not add direct value. It facilitates smart contracts, engagements, and agreements with inherent, robust cyber security features. This paper is an effort to break the ground for presenting and demonstrating the use of Blockchain technology in multiple industrial applications. A healthcare industry application, Healthchain, is formalized and developed on the foundation of Blockchain using IBM Blockchain initiative. The concepts are transferable to a wide range of industries as finance, government and manufacturing where security, scalability and efficiency must meet.
Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architechture firstly and compare some typical consensus algorithms used in different blockchains.

Introduction:
The introduction of cryptocurrencies, specifically Bitcoin, has brought the concept of blockchain technology into the mainstream. A blockchain is a continuously growing distributed database that protects against tampering and revision of data.The industry has already seen the power of a distributed system with Git Version control; blockchain builds on the same Merkle tree approach, but also adds consensus, which specifies rules on how data can be added and verified. Transactions are added in blocks and must follow the exact order in which they happened (thus the name blockchain).Bitcoin uses blockchain to maintain its public ledger of every single transaction ever made with Bitcoin. This Merkle tree approach allows for a greater hashing mechanism to provide efficient and secure verification of large amounts of data. This information is then used by Bitcoin to enforce their transactional checks.Though Bitcoin did not manage to completely disrupt the world market, the technology behind it has the potential to do so. Currently, blockchain is being used to solve problems other than cryptocurrencies–Nasdaq OMX is testing the technology for stock trading, while e-retail giant Overstock has released its digital bonds using blockchain. Blockchain is not just limited to the financial system; instead, it is a great solution for almost any platform or product that requires trust, such as keyless automobile entry authentication. Additionally, IBM and Samsung recently revealed a proof of concept that use blockchain as the backbone of the Internet of Things.The idea behind blockchain, in short, is to be able to establish and verify trust without the need of a centralized system. Instead, this power would be given to a decentralized network, making it not only more secure but also both more efficient and faster to scale. A decentralised marketplace can replace market leaders like Ebay, Amazon, and Uber. This would mean that trust, rules, identity, reputation, and payment choices would be embedded at the user level and participants arrive already trusted and decentrally acknowledged.Blockchain technology offers a lot of potentially disruptive power, and companies are already in the race for different product offerings. As the industry continues to evolve, blockchain stands out as the best investment for future returns.

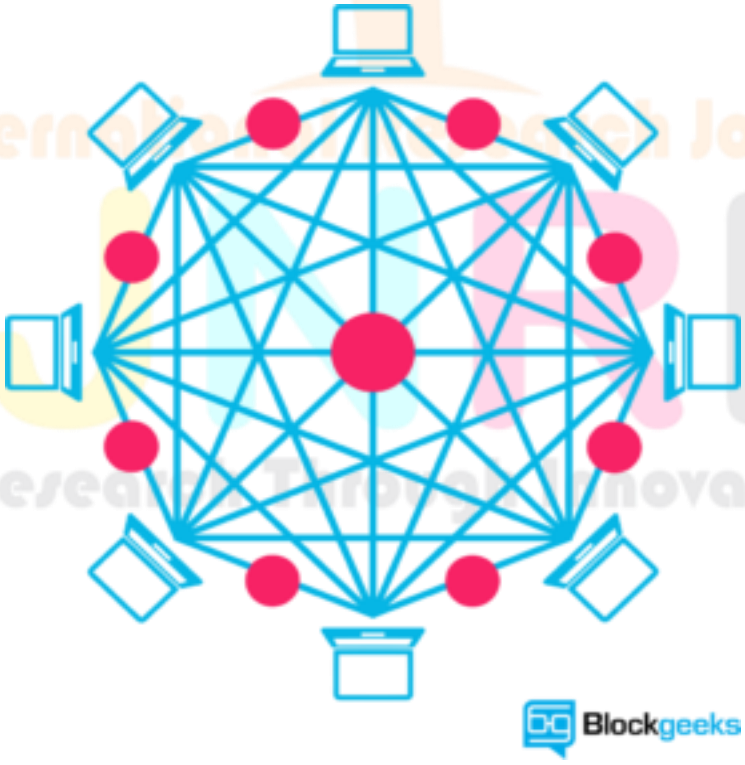
Blockchain:
By design, the blockchain is a decentralized technology. A global network of computers uses blockchain technology to jointly manage the database that records Bitcoin transactions. That is, Bitcoin is managed by its network, and not any one central authority.

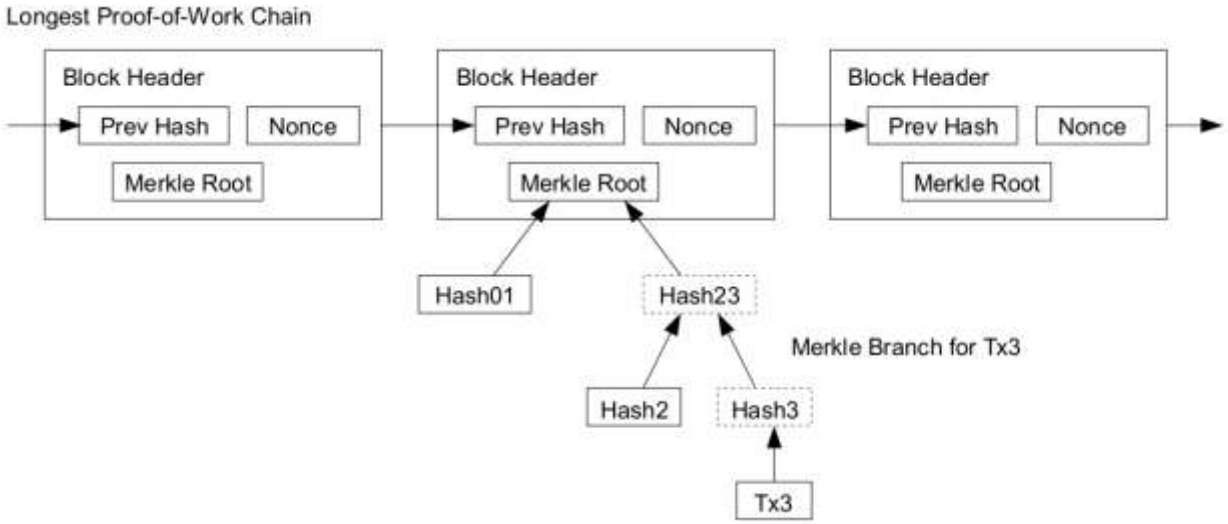
Blockchain also has the potential to improve upon systems already in use throughout society. A report done by the state of Virginia revealed that most voting machines put in practice between 2002 and 2014 used the passwords 'abcde' and 'admin,' meaning they could have easily been hacked from the parking lots outside of the polling stations. By implementing a blockchain-based voting system, elections can become much safer.

Definition - What does *Blockchain* mean?

A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions. Constantly growing as 'completed' blocks (the most recent transactions) are recorded and added to it in chronological order, it allows market participants to keep track of digital currency transactions without central recordkeeping. Each node (a computer connected to the network) gets a copy of the blockchain, which is downloaded automatically.

Originally developed as the accounting method for the virtual currency Bitcoin, blockchains – which use what's known as distributed ledger technology (DLT) – are appearing in a variety of commercial applications today. Currently, the technology is primarily used to verify transactions, within digital currencies though it is possible to digitize, code and insert practically any document into the blockchain. Doing so creates an indelible record that cannot be changed; furthermore, the record's authenticity can be verified by the entire community using the blockchain instead of a single centralized authority.

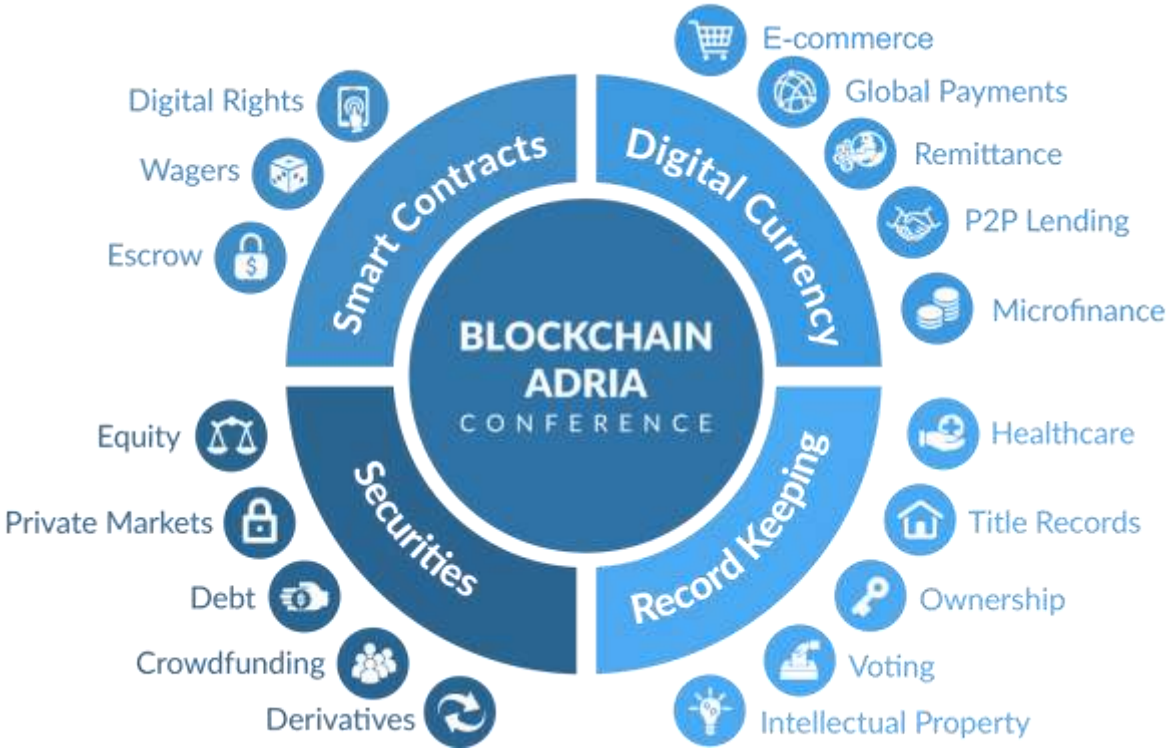




Block Diagram of Blockchain

Techopedia explains *Blockchain.*

The blockchain ledger helps to provide transparency for transactions. Although many bitcoin transactions are in some ways anonymous, the blockchain ledger can link individuals and companies to bitcoin purchases and ownership by allowing individual parties, called miners, to process payments and verify transactions. Rather than a central company presiding over the use of bitcoin, these blockchain originators serve central roles in the management and administration of this alternative currency system.

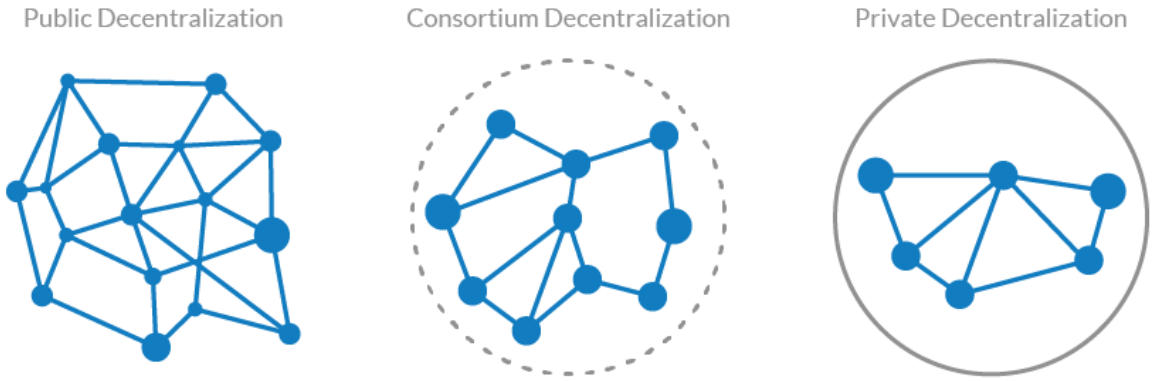


Types of Blockchain

There mainly three types of Blockchains that have emerged after Bitcoin introduced Blockchain to the world.

1.Public Blockchain Private 2.Blockchain 3.Consortium or Federated Blockchain

There are some more complicated types also such as public-permissioned blockchain, private-permissioned blockchain etc but I will keep it simple for this discussion. Now Let's discuss all the three one by one.



1. Public Blockchain

A public blockchain as its name suggests is the blockchain of the public, meaning a kind of blockchain which is-***' for the people, by the people and of the people'***Here no one is in charge and anyone can participate in reading/writing/auditing the blockchain. Another thing is that these types of blockchain are open and transparent hence anyone can review anything at a given point of time on a public blockchain.But a natural question that comes to our mind is that when no one is in charge here then how the decisions are taken on these types of the blockchain. So the answer is that decision making happens by various decentralized consensus mechanisms such as proof of work (POW) and proof of stake(POS) etc. Read more about POS and POW here. **Example:** Bitcoin, Litecoin etc On Bitcoin and Litecoin blockchain networks anyone can do the following things that make it truly public blockchain. Anyone can run BTC/LTC full node and start mining. Anyone can make transactions on BTC/LTC chain. Anyone can review/audit the blockchain in a Blockchain explorer

2. Private Blockchain

Private blockchain as its name suggests is a private property of an individual or an organization. Unlike public blockchain here there is an in charge who looks after of important things such as read/write or whom to selectively give access to read or vice versa. Here the consensus is achieved on the whims of the central in-charge who can give mining rights to anyone or not give at all.

That's what makes it centralized again where various rights are exercised and vested in a central trusted party but yet it is cryptographical secured from the company's point of view and more cost-effective for them. But it is still debatable if such a private thing can be called a 'Blockchain' because it fundamentally defeats the whole purpose of blockchain that Bitcoin introduced to us. **Example:** Bankchain. In such types of blockchain: Anyone can't run a full node and start mining. Anyone can't make transactions on the chain. Anyone can't review/audit the blockchain in a Blockchain explorer.

3. Consortium or Federated Blockchain

This type of blockchain tries to remove the sole autonomy which gets vested in just one entity by using private blockchains. So here instead of one in charge, you have more than one in charge. Basically, you have a group of companies or representative individuals coming together and making decisions for the best benefit of the whole network. Such groups are also called consortiums or a federation that's why the name consortium or federated blockchain. For example, let suppose you have a consortium of world's top 20 financial institutes out which you have decided in the code that if a transaction or a block or decision is voted/verified by more than 15 institutes then only it should get added to the blockchain. So it is a way of achieving thing much faster and you also have more than one single point of failures which in a way protects the whole ecosystem against a single point of failure. **Example:** r3, EWF.In such type blockchain: Members of the consortium can run a full node and start mining. Members of the consortium can make transactions/decisions on the chain.

Public Blockchain	Private Blockchain	Consortium or Federated Blockchain
Anyone can run BTC/LTC full node	Anyone can't run a full node	Selected members of the consortium can run a full node
Anyone can make transactions	Anyone can't make transactions	Selected members of the consortium can make transactions
Anyone can review/audit the blockchain	Anyone can't review/audit the blockchain	Selected members of the consortium can review/audit the blockchain

We require more types of blockchain because keeping such blockchains solves problems such as:-

1. One no longer need to rely upon huge servers.
2. They are cost effective and fast.
3. They reduce the need for more trusted parties because you can implement smart contracts instead of them.
4. Gives options for rights and access management while leveraging the same blockchain technology and reaping its benefits.

5. Reduces redundant work.
6. Distributed consensus between interested parties becomes fast even though you are geographically segregated.

Conclusion:

Blockchain technology has many benefits. In many cases, these benefits are worth those resources, which will be used to integrate it. However, there are also some disadvantages that we should not ignore and which the upcoming blockchain projects should try to either solve or avoid.