Glimpse On Blockchain Technology And Applications

Dr. V. Chandra Shekhar Rao¹, Johnson Kolluri², M.S.B.Pridviraj³, Syed Abdul Moed⁴, Dr. C. Srinivas⁵

¹Associate Professor, Kakatiya Institute of Technology and Science, Warangal, India.
²Assistant Professor, Kakatiya Institute of Technology and Science, Warangal, India.
³Assistant Professor, Kakatiya Institute of Technology and Science, Warangal, India.
⁴Assistant Professor, Kakatiya Institute of Technology and Science, Warangal, India.
⁵Associate Professor, Kakatiya Institute of Technology and Science, Warangal, India.

¹vcsrao.cse@kitsw.ac.in

Abstract: The term blockchain pasteurizes the chain of blocks like linked lists which will be linked to the previous block. A blockchain is a distributed ledger of digital transactions which is decentralized and no individual, team or company has its controllability over it. However, with time, the use of blockchain has come into existence. It has wide range of applications including risk management, credit money, Internet of Things (IoT), social networks, and financial resources. Blockchain has many benefits like decentralization, persistency, anonymity, audit ability. Blockchain is trustable one and it is very efficient. In particular, this paper gives us the detailed information about the blockchain and its applications.

Keywords: Blockchain, cryptocurrency, ethereum, bitcoin.

1. Introduction
It first came into action in 2008 by Satoshi Nakamoto, the best known digital currency [1]. The first and foremost application of blockchain is Bitcoin. Bitcoin got succeeded and made the people know about blockchain and it is leading to the trust worthy transactions. Blockchain is having mainly three pillars decentralisation, transparency, immutability. This survey consists of all the domains where blockchain impacts and where the upcoming changes will occur using blockchain. Section 2 provides the information about the technology before blockchain. Section 3 gives us the brief explanation about blockchain and its concepts. Section 4 includes the principles of blockchain. Section 5 shows us the Blockchain Architecture. Section 6 has the categories of blockchain. Section 7 contains the applications of blockchain. Section 8 shows us the challenges and other related works of blockchain. Section 9 concludes the paper shows the future ways to expand blockchain.

2. Antecedent Technology Of Blockchain
The technology proceeding blockchain is the technology which is centralised. Blockchain eliminates the problem of double spending with the help of a cryptographic public key, whereby each member is assigned a public key shared with all other members.

3. Overview Of Blockchain
The two most critical problems of currency based transactions can be solved by blockchain technology. Both are popularly regarded as the dilemma of the Byzantine Generals and the dilemma of...
the Double spend problem. With the occurrence of blockchain, the progress of cryptoeconomics increased. The works of pilkington[2] has been highlighted each and every aspect. The paper shows how blockchain is applicable to a non-tokenized scheme.

The paper also explains about blockchain classification and how the permission less blockchain has become less important than the permission blockchain because permission less ledger seems to be risky. There are three layers of blockchain stack explained by swan[3]. They are, first, the underlying blockchain application infrastructure, second, the Bitcoin protocol, i.e., which makes transaction possible by using Bitcoin blockchain’s network machine programme and, lastly, the Bitcoin Digital currency itself (denominated as BTC) which is the basis of value. Swan’s book is about the history of blockchain technologies in three decades. The digital currency application 1.0, the deployment of blockchain for smart contracts and distributed applications (Dapps) is called Blockchain 2.0 and eventually the platform outside the currency and economy is detailed as Blockchain 3.0.

4. Principles Of Blockchain

- **Decentralisation and Distribution**: The data is stored in multiple computers in blockchain is called decentralisations because of the absence of the central control and any modifications of data on one computer is distributed across the network to all computers.
- **Secure**: Blockchain is highly advanced in security because each block has link to its previous block which makes blockchain secure.
- **Smart contracts**: Smart contracts are protocols that implements a transaction that participants should follow. These smart contracts make sure that all the parties follow the rules which are present on the blockchain.
- **Consensus Algorithm**: Before the transactions there must be an agreement between the parties. The transaction is verified to the ledger through various means of the consensus algorithm. Consensus algorithm has Proof of work and Proof of shake.
- **Immutable**: Once the data has been given to a block it can’t be tampered.
- **Anonymity**: Blockchaintenchnology overcome the confidence issue from node to node, since data sharing can be private, only people need to know the blockchain address.

5. Blockchain Architecture

Blockchain is the chain of blocks[5], like linked lists which will be linked to the previous block. Here the block structure of blockchain contains Parent block hash, Merkle tree root, nBits,Nonce, Blockversion, Timestamp..

![Block Structure](image)

**Figure 1 Block Structure**

**Digital Signature**

Here every user in the blockchain has a private key and a public key. Consider Figure as an example. Alice requires a transaction[8], produces a hash value taken from a transaction and this hash is encrypted with her private key and transfers it to another user, Bob. This Bob compares the decrypted
hash (by using a public key) and the hash value taken from the obtained info. Here, if I blocks are present, the initial block is represented as the genesis block and the hash for the first block and the genesis block is null. Then the hash for the second block is stored in the first block and in the same lines, I block hash is stored in the (i-1) block and the chain begins.

Figure 2 Usage of Digital signature in blockchain

6. Blockchain Categorization

6.1 Public Blockchain:
Public blockchain is available to everyone. It is a peer to peer transaction and run on consensus and each transaction is stored in a block which has unique identity called hash which will be linked to the previous block. Public blockchain can be accessed to anyone i.e, anybody can see any transaction details. In public blockchain not only particular blocks but all blocks can be accessed by anyone. It is not having any restrictions of availability means it is public so called public blockchain.

Figure 3. Public Blockchain

6.2 Private Blockchain:
Private blockchain cannot be accessed by everyone and it is restricted. It is available to only the persons who are having transactions in blockchain. It has a strict management on data access. In private blockchain not only limited blocks but all the blocks are not available to everyone.

Figure 4. Private Blockchain

6.3 Consortium Blockchain:
The word consortium resembles association. It is the association of both public blockchain and private blockchain. And this consortium blockchain is not fully decentralized unlike public blockchain and private blockchain. This consortium blockchain has both public and private nature i.e, some blocks can be accessed by everyone but some blocks are restricted to particular people.
7. Applications Of Blockchain

**Bitcoin**: Bitcoin is the first application of blockchain[1] . It was introduced by Satoshi Nakamoto in 2008. Blockchain public ledger used by Bitcoin to perform transaction in peer to peer manner unlike centralized transactions. Bitcoin is a decentralized form of currency that individuals could trade directly without the need for an intermediary. Each blockchain transaction is validated and confirmed by the entire Bitcoin network.

**Ripple**: A currency swap, deposit and realtime gross settlement system is known as ripple[9]. Ripple mainly focuses on banking market. A peer to peer network is used by ripple protocol which is decentralized exchange.

**Ethereum**: It was suggested at the end of 2013 and brought to life in 2014 by Vitalik Buterin, then co-founder of Bitcoin Magazine. Ethereum is the do-it-yourself framework for open services which is also known as mobile applications. Ethereum is a distributed infrastructure for handling decentralised systems. It’s a site for an ethereum programming language the data in the blockchain is not tampered[10].

**Hyperledger**: Hyperledger is a open source community of communities which is used to develop blockchain technologies. In a very simple way, Hyperledged can be thought of as a software which everyone can use to create own personalized blockchain service. It is a linux based project which enables blocked automation for business, banking, internet of things.

8. Challenges

A challenge is a call for proof. Some of the serious challenges are listed below.

a) **Scalability** is one of the challenge. If there are N blocks in a chain then the (N-1) block is get validated after the validation of (N-2) block. Transaction decay may become a problem because of size of blocks in chain.

b) Memory expansion of blockchain is another challenge in scalability. To overcome this challenge, cryptocurrency scheme was introduced in 2014[12]. In this new one the old transactions are removed and account tree is used to maintain the non-empty addresses [13]and redesigning of blockchain is another challenge.

c) Privacy leakage is another challenge i.e, the data in the public blockchain[12] is not secure because the transactions and advances are visible to everyone. Moreover the study revealed that one block is linked to the other block to reveal users’ particulars.

d) Bitcoin's consensus protocol and certain other blockchains could be the biggest impediment to universal acceptance. Bitcoin mining used the same amount of electricity as Denmark’s entire country in 2017. We're clearly having a crisis. In order to mature the blockchain, existing consensus protocols need to be supplemented with implementations that do not involve power.
hungry server farms. It is yet to be seen what such ideas could be, but here lies a big challenge for creativity to push DLT to the next level of upgradation. In several ways, blockchain is uncomfortable. The blockchains of tomorrow will, you can be sure, bear no similarity to those of today. The immutability of chained records, along with allowed access and traceability, will, of course, always be there. But maybe that's when the comparisons end. Somewhere down the way, consensus protocols will arise that will not tax the planet's power grid. Industry-specific standardisation would streamline the phase of R&D. And, perhaps most notably, blockchain is going to achieve mainstream recognition. The blockchain technology challenges of today are the achievements that wise businesses will rely on for tomorrow's success stories.

e) Selfish mining is another challenge for blockchain. In general, if the nodes are having 51% of computing power then the blockchain data is tampered for happened transaction[12]. Selfish miners don’t broadcast the mined blocks and the private block is accessed to public only if some restriction are satisfied. Honest miners waste their time on useless blocks unlike selfish miners and selfish miners get more revenue. We also see the these challenges in 5G for IoT and IoT and.

9. Future Directions
Blockchain has the potential to expand in given areas.

- Blockchain testing
- Stop the tendency to centralization
- Big data analytics
- Smart Contracts
- Artificial Intelligence

10. Conclusion
Blockchain provides platform for decentralization and peer to peer network. Decentralised, Distributed, Immutable, Secure, Smart contracts, Consensus Algorithm are the characteristics of blockchain. There are different types of blockchains are there based on their accessibility. Public, private and consortium blockchains are secure than public. If we can overcome the challenges of present blockchain then there will be very less cons than pros then it will become the leading technology or world driving technology.

11. References
[1] Satoshi Nakamoto,—Bitcoin: A Peer-to-Peer Electronic Cash Systeml, 2008
[2] Pilkington Mark 2016 Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations, Social Science Research Network
[3] Swan Melanie 2015 Blockchain: Blueprint for a new Economy, O'reilly Publications
[4] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends” 2017 IEEE 6th International Congress on Big Data
[5] Handbook of Digital Currency, 1st ed, Elsevier
[6] ANext-Generation Smart Contract and Decentralized Application Platform, White Paper
[7] NRI Survey on Blockchain Technologies and Related Services, Technical Report Omohundro, S ‘Cryptocurrencies, smart contracts, and artificial intelligence’, AI Matters
[8] Johnson, D, Menezes, A and Vanstone, S ‘The elliptic curve digital signature algorithm (ECDSA)’, International Journal of Information Security, Vol 1, No 1, pp36–63
[9] Hou, —The application of blockchain technology in government in china, l in ICCCN IEEE, 2017, pp1–4
[10] Vitalik Buterin, —Ethereum and The Decentralized Future” Future Thinkers Podcast 2015-04-21 Retrieved 2016-05-13
[11] Rao, V Chandra Shekar, Chinthapally Akanksha, and Voore Subba Rao “Applications of NANO-
RK in Internet of Things (IoT)” No 2457 EasyChair, 2020

[12] Dr V Chandra Shekhar Rao and VooreSubba Rao and SVenkhatramulu “Secure Architecture For 5G Network Enabled Internet Of Things(IoT)”, No16171, Algorithms for Intelligent Systems(AIS), Springer 2020

[13] Dr V Chandra Shekhar Rao, Dr P Kumaraswamy MSBPhridviraj3, Dr S Venkatramulu, VSubba Rao, “5G enabled Industrial Internet of Things(IIoT)Architecture for SmartManufacturing’, Springer, 4th International conference Data Engineering and Communication Technology (ICDECT-2020), September 25-26, KITS, Warangal