Blockchain Technology and its Potential Areas of Implementation
(May 2019)

Rahul, Aditya, Ankit, Hrishikeh[1], *Dr* Sini Anna Alex[2], *Member, IEEE*
[1]B.E. Computer Science and Engineering, Ramaiah Institute of Technology, India
[2]Assistant Professor Computer Science and Engineering, Ramaiah Institute of Technology, India

***Abstract*— Blockchain in simple words is a distributed ledger of records that is immutable and verifiable. Since its advent in 2008, blockchain as a concept has been used in various ways. The largest impact or application is seen as a multitude of cryptocurrencies that have come up. However, with time it has become clear that blockchain as a technology is likely to have an impact much wider than just the cryptocurrency domain and much deeper than simple distributed ledger storage. Several initiatives that are already underway are driving its progression to an industrial solution which will yield several important benefits in the context of transfer of assets and flow of information inter and intra business networks. This research paper intends to bring together the key developments so far in terms of putting blockchain technology to practice and will explore the various domains where future implementations may be expected.**

Index Keywords: Blockchain Technology, Blockchain Taxonomy, Proof of Work, Proof of Stake, Applications.
Author for Correspondence E-mail :rahulnegi1409@gmail.com, Tel : +919560805564

I. INTRODUCTION

THE Blockchain technology has been especially identified to be capable of developing nations where ensuring trust is of a major concern which is predominantly seen in the developing countries like India. It has the potential for all participants in a business network to share a system of records which will provide consensus, provenance, immutability and finality around the transfer of assets and information flow. It can address certain drawbacks of the current processes by modernizing, channelizing and simplifying the traditional design of the financial sector infrastructure. Blockchain technology or the distributed, secure ledger technology has gained much attention in recent years. It has recently taken the worlds of finance and technology through its immense application in the modern crypto-currency Bitcoin, and more so because of the disruptive innovations it promises. While Bitcoin has been the most talked about application of the Blockchain technology to date, new applications such as Smart Contracts have tried to exploit more abstract nature of the platform. This paper presents a survey of blockchain technology and its potential areas of implementation.

Manuscript received October 9, 2001. (Write the date on which you submitted your paper for review.) This work was supported in part by the U.S. Department of Commerce under Grant BS123456 (sponsor and financial support acknowledgment goes here). Paper titles should be written in uppercase and lowercase letters, not all uppercase. Avoid writing long formulas with subscripts in the title; short formulas that identify the elements are fine (e.g., "Nd–Fe–B"). Do not write "(Invited)" in the title. Full names of authors are preferred in the author field, but are not required. Put a space between authors' initials.

F. A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (corresponding author to provide phone: 303-555-5555; fax: 303-555-5555; e-mail: author@ boulder.nist.gov).

S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp).

II. BLOCKCHAIN OVERVIEW

A. Blockchain Technology

The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually every data. A very significant advantage of the blockchain technology is that it solves two of the most dreaded problems of currency-based transactions, which have so long necessitated the requirement of a third party to validate the transactions. [1].

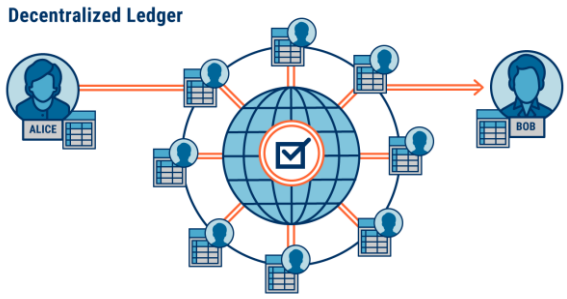
B. Blockchain Taxonomy

The original idea of blockchain implementation was propounded by Satoshi Nakamoto was of a public decentralized ledger and further introduced us to Bitcoin. In theory, based on who can access the blockchain network and how the permissions to write to the blockchain network are assigned, four types of blockchains can be defined as shown in Table 1.

Depending on the use case, one needs to select an appropriate architecture from those defined in the Table 1. Xu et al. [2] provide a further detailed taxonomy which can help in choosing architecture for a blockchain system.

Based on access to blockchain	Based on access to blockchain data
Permission less – Anyone with computing power can join	Public – All who access can modify
Permissioned –Approved users only	Private – Only specific users can write / modify

C. *Figures*



III. BLOCKCHAIN ARCHITECTURE

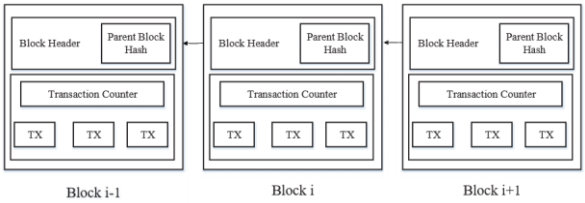


Fig. 1: An example of blockchain which consists of a continuous sequence of blocks.

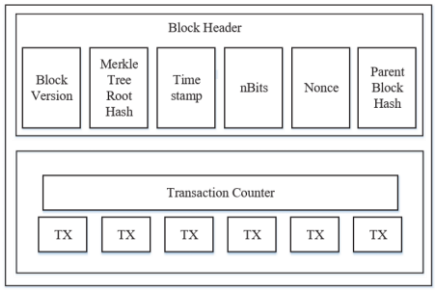


Fig. 2: Block structure

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [14]. Figure 1 illustrates an example of a blockchain. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in Ethereum blockchain. The first block of a blockchain is called genesis block which has no parent block. We then explain the internals of blockchain in details.

A. *Block.*

A block consists of the block header and the block body as shown in Figure 2. In particular, the block header includes:
(i)Block version: indicates which set of block validation rules to follow.
(ii) Merkle tree root hash: the hash value of all the transactions in the block.
(iii) Timestamp: current time as seconds in universal time since January 1, 1970.
(iv) nBits: target threshold of a valid block hash.
(v) Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in Section III).
(vi) Parent block hash: a 256-bit hash value that points to the previous block.
The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.

B. *Digital Signature*

Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: signing phase and verification phase. For instance, a user Alice wants to send another user Bob a message. (1) In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data. (2) In the verification phase, Bob validates the value with Alice's public key. In that way, Bob could easily check if the data has been tampered or not. The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm (ECDSA).

C. Key Characteristics of Blockchain

In summary, blockchain has following key characteristics.

• Decentralization. In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.

• Persistency. Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.

• Anonymity. Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint (details will be discussed in section

• Auditability. Bitcoin blockchain stores data about user balances based on the Unspent Transaction Output (UTXO) model [2]: Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent. So, transactions could be easily verified and tracked.

IV. BLOCKCHAIN PROTOCOLS

Proof of Work

PoW protocol requires all nodes on the network to solve cryptographic puzzles by brute force. For example, in case of Bitcoin blockchain, the new transactions are tentatively committed and then based on the PoW output, a selected block created by the winning node is broadcast to all the nodes, at specific synchronization intervals. Once the block is transmitted using peer to peer communication to all other nodes, the same is included in the blockchain and any tentative transactions are rolled back [3]. By rule of probability, the consensus is achieved as 51% of power rather than 51% of people count. Effectively the computing power used by all other nodes except the winning node, is wasted.

Proof of Stake

Proof of stake protocol of block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment. It is also an energy saving alternative [1, 11].

A variation of POS is the Delegated Proof of Stake (DPOS) algorithm. Delegated proof of stake (DPOS) is similar to POS, as miners get their priority to generate the blocks according to their stake. The major difference between POS and DPOS is that POS is a direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and validate a block. With significantly fewer nodes to validate the block, the block could be confirmed quickly, making the transactions confirmed quickly. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by the delegates. DPOS is implemented by Bit shares.

Practical Byzantine Fault Tolerance

An approach to deal with the Byzantine Generals problem is the Federated Byzantine Agreement (FBA). In this approach, it is assumed that the participants of the network know each other and can distinguish which ones are important and which ones are not. PBFT (Practical byzantine fault tolerance) is a replication algorithm which utilizes this principle. Hyperledger utilizes the PBFT as its consensus algorithm. There are designated validator (primary) nodes that are each associated with a group of nodes. The primary is responsible for multicasting requests to other replicas in its group. A service operation would be valid if it has received approvals from over 1/3 different replicas. Additionally, if a client does not receive the replies, it will send the request to all replicas instead of only sending it to the primary in case the primary is faulty. A primary is responsible for ordering the transaction and each replica commits the transaction in the same order. It has been seen that PBFT or its variations map well to the needs of various organizations like banks, supply chain or payroll systems.

V. COMPARISON OF BLOCKCHAIN CONSENSUS ALGORITHMS

Table 2: Blockchain Classification

Algorithm	Pros	Cons
Proof of Work E.g.: Bitcoin, Litecoin, Dogecoin, Namecoin	• Considered very secure, as less prone to Sybil attack unless a mining node acquires. • 51% of the pools computing power. • Miners get rewards (as Bitcoins). • Prevents unlawful forking of the chain.	• Quite slow at the moment, only 1 block added in 10 mins. • Driven by rewards assigned to solving the hash, may run into problems as rewards dwindle. • Consumes lot of electricity (mining likely to be centralized where electricity is cheap).

		• Decisions are not final till 6 blocks are confirmed.
Proof of Stake E.g.: Nxt, Mintcoin	• Less wasteful in terms of energy consumption. • Less chance of hardware centralization. • Potentially faster than Proof-of-work protocol. • Possibly reduced possibility of selfish mining attack.	• Miners are encouraged to hold on to their stake rather than converting it into at currency. • Economic penalties for fraudulent attempts.
Practical Byzantine Fault Tolerance E.g.: Stellar, Ripple	• Can tolerate 1/3rd of the nodes to be faulty or adversarial. • Fast and efficient. • Trust is decoupled from resource ownership, so small group can keep a powerful organization in check.	• Parties must agree to the exact participation of groups. • Comes at the cost of anonymity.

VI. BLOCKCHAIN APPLICATIONS

Currently most blockchains are used in the financial domain, more and more applications for different fields are appearing. Traditional industries could take blockchain into consideration and apply blockchain into their fields to enhance their systems. For example, user reputations could be stored on blockchain. At the same time, the up-and-coming industry could make use of blockchain to improve performance. For example, Arcade City [13] a ridesharing startup offers an open marketplace where riders connect directly with drivers by leveraging blockchain technology. A smart contract is a computerized transaction protocol that executes the terms of a contract [14]. It has been proposed for long time and now this concept can be implemented with blockchain. In blockchain, smart contract is a code fragment that could be executed by miners automatically. Smart contract has transformative potential in various fields like financial services and IoT.

Healthcare

The digitization of health records has brought about significant change in the public health sector, but it has been criticized for being complex on account of centralization and associated ethical issues. Blockchain technology can disrupt public health by creating a secure and flexible ecosystem for exchanging electronic health records (EHRs). This technology could also make the space more transparent by creating provenances for critical drugs, blood, organs, etc. In addition, by putting all medical licenses on a blockchain, fraudulent doctors can be prevented from practicing.

Education

Student records, faculty records, educational certificates, etc., are key assets in the education domain. Such records need to be shared with multiple stakeholders and it is imperative to ensure that they are trust worthy. The provenance of these records also needs to be determined accurately. Student records, faculty records and educational certificates can be maintained with the application of blockchain technology. Blockchain can also simplify certificate attestation and verification. It could even transform the manner in which the policy for educational inclusion is framed by bringing in base uniformity in the tracking of national metrics.

Public safety and justice

Blockchain could make the delivery of public safety more efficient by resolving the problem of interagency coordination by providing a unified source of truth that each agency independently interfaces with based on predefined conditions. Establishing a chain of custody for crucial evidence is often an important prerequisite for the evidence to be admissible; blockchain technology could help establish the provenance of the chain of custody for such evidence.

Agriculture

Blockchain technology can be used to increase transparency, reduce complexity and cost in food-based value chains by enabling trustworthy provenance and traceability from farmer to consumer. Other possible applications include the use of blockchain technology to record and manage agricultural land records as well as agriculture insurance.

Civil Registration

The civil registration process can be simplified through the application of blockchain technology to create distributed citizen registration platforms and even register vital events such as births and deaths on a blockchain. This can help make citizen records tamper-proof, resilient, secure and private, thus providing wide-ranging benefits for a variety of stakeholders.

Defense

Information regarding defense infrastructure and computer systems is critical to national security. For this reason, it is distributed across different locations to prevent unauthorized access and modification. Blockchain technology can be leveraged to provide consensus-based access for modifying

data and distributing access over multiple system resources such as networks, data centers and hardware equipment.

Governance

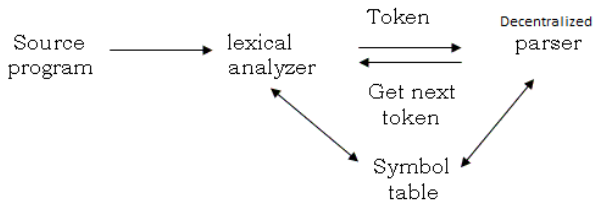
Government departments have functional interdependence but operate in silos, which impacts the availability of services and deteriorates citizen experience. Blockchain technology can be used to break the silos, check government corruption (if any), increase efficiency and transparency. Linking file and data movement between departments through a blockchain would increase visibility into the process and ensure that the data/file moves forward in real time.

Energy

Blockchain technology can be deployed to create a marketplace for electric power supply. Microgeneration of electricity through home power generation using solar energy supplements traditional power supply and promotes the use of renewable energy sources. Using smart meters, a record of produced and consumed electricity for each user in the grid can be maintained on a blockchain with credits/currency allocated to the user for surplus power supply and credits redeemed for power consumption. This essentially creates a transparent, hassle-free and efficient energy market.

Compiler Designs

Since Blockchain is decentralized we can make new compiled that does not req any kind of toolchain kits and also update stuff from scratch and see the top level security and hard to reverse engineer .Solc is the Solidity Compiler (Solidity is the programming language to write code on the Ethereum chain). A good number of Ethereum nodes natively includes a solc implementation, but it is also packaged as a standalone module for an offline compiling. So, you can decide to use web3.eth.compile.solidity to compile your Solidity files using your node, or you can start using a solc.compile that doesn't rely on any external node.



VII. POSSIBLE FUTURE DIRECTIONS

Blockchain has shown its potential in industry and academia. We discuss possible future directions with respect to four areas: blockchain testing, stop the tendency to centralization, big data analytics and blockchain application.

A. Blockchain testing

Recently different kinds of blockchains appear and over 700 cryptocurrencies are listed in [52] up to now. However, some developers might falsify their blockchain performance to attract investors driven by the huge profit. Besides that, when users want to combine blockchain into business, they have to know which blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different blockchains. Blockchain testing could be separated into two phases: standardization phase and testing phase. In standardization phase, all criteria have to be made and agreed. When a blockchain is born, it could be tested with the agreed criteria to valid if the blockchain works fine as developers claim. As for testing phase, blockchain testing needs to be performed with different criteria. For example, an user who is in charge of online retail business cares about the throughput of the blockchain, so the examination needs to test the average time from a user send a transaction to the transaction is packed into the blockchain, capacity for a blockchain block and etc.

B. Stop the tendency to centralization

Blockchain is designed as a decentralized system. However, there is a trend that miners are centralized in the mining pool. Up to now, the top 5 mining pools together owns larger than 51% of the total hash power in the Bitcoin network [53]. Apart from that, selfish mining strategy [10] showed that pools with over 25% of total computing power could get more revenue than fair share. Rational miners would be attracted into the selfish pool and finally the pool could easily exceed 51% of the total power. As the blockchain is not intended to serve a few organizations, some methods should be proposed to solve this problem.

C. Big data analytics

Blockchain could be well combined with big data. Here we roughly categorized the combination into two types: data management and data analytics. As for data management, blockchain could be used to store important data as it is distributed and secure. Blockchain could also ensure the data is original. For example, if blockchain is used to store patient's health information, the information could not be tampered and it is hard to stole that private information. When it comes to data analytics, transactions on blockchain could be used for big data analytics. For example, user trading patterns might be extracted. Users can predict their potential partners' trading behaviors with the analysis.

VIII. BLOCKCHAIN APPLICATIONS BEING EXPLORED IN INDIAN

A lot of Indian players have tested usage of Blockchain in the areas of Trade Finance, Cross-border Payments, Bill Discounting, Supply chain financing, Loyalty and Digital Identity areas. Some of the Indian banks, business conglomerates, and one stock exchange are among the pioneers for exploring Blockchain in India.

A. Trade Finance

A private sector bank in India and a leading banking group in Middle East successfully executed transactions in international trade finance and remittance using blockchain.

B. Supply Chain Financial

An Indian conglomerate has designed a cloud-based application to transform supplier-to-manufacturer trade finance transactions through a permissioned distributed ledger A lighting equipment manufacturer in India experimented with Blockchain to reduce the cycle time of Bill Discounting process for paying its suppliers from five days to almost real-time.

C. e-KYC Document Management

A leading stock market exchange in India is exploring blockchain for management of KYC documents in collaboration with some of the leading banks in India

D. Cross-Border Payments

Stellar has partnered with four financial institutions to enable low-cost global money transfers to the Philippines and cross border payments to and from India, Europe, Kenya, Ghana and Nigeria Two of the private sector banks in India are jointly testing Blockchain transactions focused mostly on cross-border remittance & trade settlements.

E. Employee Loyalty/Rewards

Deloitte India is working on a pilot on blockchain based rewards and recognition program.

IX. CONCLUSION

In a plethora of blockchain based applications and experiments, faith on the longevity of blockchain technology, is increasing. Scalability and consensus algorithms are areas of growing research in order to make blockchain more adaptable for businesses of larger scale. Areas like finance, taxation, education, insurance are yet to see a major overhaul through blockchain adoption and these can be the focus areas of future research in blockchain. Acceptance of blockchain and cryptocurrency by governments and establishment of regulations governing them are very important to ensure its ethical use. Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. In this paper, we present a comprehensive overview on blockchain. We first give an overview of blockchain technologies including blockchain architecture and key characteristics of blockchain. We then discuss the typical consensus algorithms used in blockchain. We analyzed and compared these protocols in different respects. Furthermore, we listed some challenges and problems that would hinder blockchain development and summarized some existing approaches for solving these problems. Some possible future directions are also proposed. Nowadays blockchain based applications are springing up and we plan to conduct in-depth investigations on blockchain-based applications in the future.

APPENDIX

Appendixes, if needed, appear before the acknowledgment.

ACKNOWLEDGMENT

The work described in this paper was supported by the National Key Research and Development Program (2016YFB1000101), the National Natural Science Foundation of India under (61472338), the Fundamental Research Funds for the Ramaiah Institute of Technology, Computer Science and Technology Research & Development under Grant No. 096/2013/A3. The authors would like to thank xyz. Hon for his constructive works and guide.

REFERENCES

[1] Peters G.W. Panayi E. 2016. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, Banking Beyond Banks and Money, Springer Sep 2016, pp. 239-278.

[2] Xu et al. 2017. A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3-7 April 2017

[3] Decker, Wattenhofer. 2013. Information Propagation in the Bitcoin Network, 2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P).B. Smith, “An approach to graphs of linear forms (Unpublished work style),” unpublished.

[4] Nir Kshetri, "Can Blockchain Strengthen the Internet of Things?," IT Professional, vol. 19, no. 4, pp. 68 - 72, May 2017

[5] Mahdi H. Miraz, "Blockchain: Technology Fundamentals of the Trust Machine," Machine Lawyering, Chinese University of Hong Kong, 23rd December 2017.

[6] Don Tapscott and Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 1st ed. New York, USA: Penguin Publishing Group, 2016.

[7] Maaruf Ali and Mahdi H Miraz, "Cloud Computing Applications," in Proceedings of the International Conference on Cloud Computing and eGovernance - ICCCEG 2013, Internet City, Dubai, United Arab Emirates, 2013, pp. 1-8.

[8] Maaruf Ali and Mahdi H. Miraz, "Recent Advances in Cloud Computing Applications and Services," International Journal on Cloud Computing (IJCC), vol. 1, no. 1, pp. 1-12, February 2014.3
[9] Xueping Liang et al., "ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," in Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid '17), Madrid, Spain, May 14 - 17, 2017, pp. 468-477.
[10] Mahdi H. Miraz, Maaruf Ali, Peter Excell, and Picking Rich, "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," in the Proceedings of the Fifth International IEEE Conference on Internet Technologies and Applications (ITA 15), Wrexham, UK, 2015, pp. 219 – 224.
[11] Mahdi H. Miraz, Maaruf Ali, Peter S. Excell, and Richard Picking, "Internet of Nano-things, Things and Everything: Future Growth Trends," (to be published) Future Internet, 2018.
[12] Mahdi H. Miraz and Maaruf Ali, "Blockchain Enabled Enhanced IoT Ecosystem Security," (accepted) in proceedings of the First International Conference on Emerging Technologies in Computing 2018 (iCETiC '18), London, UK, 23 August 2018.
[13] “Crypto-currency market capitalizations,” 2017. [Online]. Available: https://coinmarketcap.com
[14] “The biggest mining pools.” [Online]. Available: https:
[15] //bitcoinworldwide.com/mining/pools/ [54] N. Szabo, “The idea of smart contracts,” 1997.
[16]