Blockchain:The new era of Technology

Riya Sapra
Department of Computer Science
and Technology
Manav Rachna University
Faridabad, Haryana, India
riya@mru.edu.in

Parneeta Dhaliwal
Department of Computer Science
and Technology
Manav Rachna University
Faridabad, Haryana, India
parneeta.cst@mru.edu.in

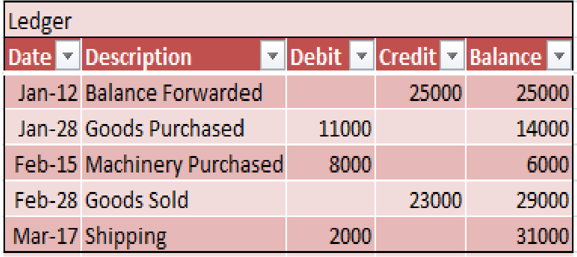
***Abstract*---Now a days many applications are being built using the immutability and robustness of blockchain. Blockchain is a new class of information technology which combines cryptography and distributed ledger that already exists. The model is composed of a group of computers that collaborate towards maintaining a secured database, without storing the data at any central unit. It is the technology behind all the crypto currencies like Bitcoin, Litecoin, Etherum and now finding its way to record everything possible. This paper focuses on the basic framework of blockchain model, its development history, pre-requisites and challenges of blockchain. Finally, various current real time applications of the technology are discussed.**

Keywords---blockchain, bitcoin, distributed ledger, merkle root, applications, consensus, challenges, pre-requisites.

I. INTRODUCTION

Blockchain has become a buzzword in IT sector. The technology behind blockchain has become so powerful that applications are being built on top of them which will automatically make them decentralized, block based and resistant to censorship. Various new initiatives are being launched that are based on blockchain principle. The popularity of Bitcoin has resulted in all these initiatives. Bitcoin [12] is a digital money ecosystem where users transfer bitcoins for buying/selling of goods. Unlike traditional currencies, bitcoins are entirely virtual i.e. no physical coins. The coins [5] only signify the transfer value from sender to receiver.

Basically a blockchain [24] is a chain of blocks which include all the valid transactions happening in the chronological order to be maintained in public ledgers, secured by hashes and validated through distributed consensus. The technology behind blockchain works by maintaining the transaction ledger [1] with all the members in the blockchain. Whenever there is a new transaction, the transaction ledger is updated without any involvement of third party. This provides a way to many applications like supply chain [21, 22], financial trading [20], banking [25], cross border payments [21], health care [23] and many more.



Ledger

Date	Description	Debit	Credit	Balance
Jan-12	Balance Forwarded		25000	25000
Jan-28	Goods Purchased	11000		14000
Feb-15	Machinery Purchased	8000		6000
Feb-28	Goods Sold		23000	29000
Mar-17	Shipping	2000		31000

Fig.1 Ledger

Ledger [10] is a book or a computer file for recording and totaling all economic transactions as debit/credit transactions, a starting and ending monetary balance for each account as shown in Fig 1. In blockchain, the ledger records transactions like exchange of capital or data. Blockchain ledger is decentralized [24] as it is replicated to many network participants, who collaborate in its maintenance. Also the information in blockchain is append-only [1], which guarantees that if a transaction is added to the ledger, no one can modify it.

Each block is represented by a hash value [24] called the merkle root [12] of the block as shown in

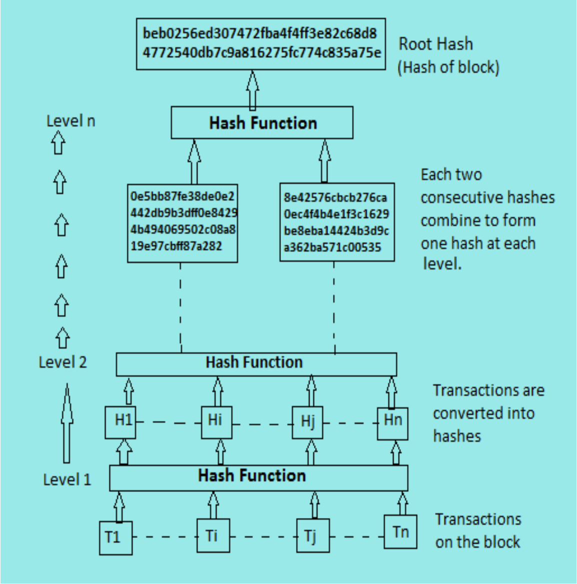


Fig. 2 Merkle root evaluation

978-1-5386-6026-3/18/$31©2018 IEEE

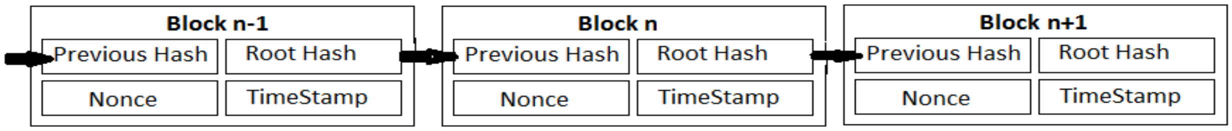


Fig. 3 Blockchain architecture

Fig.2. The root hash is evaluated by converting all the transactions into a hash value using a hash function. The hash function [25] takes any length string as input and provides a unique fixed length output known as hash of that transaction. For example if we have 4 transactions in a block, at Level 1, every transaction will be converted into its unique hash. For level 2 to level n-1, two hashes will be converted into one unique hash and so on till we get one single hash for all the transactions in the block as shown in Fig.2.

Each block [12] stores its own root hash, nonce, timestamp and hash of previous block as shown in Fig. 3. Nonce [1] is a unique random number in every block which is used as an authentication protocol so that no old transactions are redone. The timestamp [1] is the time when block is created.The blocks in blockchain are connected via hashes to form a chain.If anyone attempts to tamper any transaction in the block, its hash will change and so will the root hash. This will make the blockchain invalid and hence the changes will be reversed using the valid blockchain available on the network.

The paper gives a review of blockchain technology, its challenges and various application areas of blockchain technology. The paper is organized as follows. Section III explains the 3 types of blockchain. Section IV and V gives the detail of various pre-requisites and challenges of blockchain. Section VI explains numerous real time applications of blockchain in industries. Finally section VII concludes the article.

II. RELATED WORK

The concepts of distributed computing, public ledgers, cryptography are decades old but blockchain gained popularity just recently after the release of Bitcoin. Bitcoin [12] is the first implementation of the concept of blockchain.

Blockchain is being used effectively for storing and exchanging information over internet. A design scheme [9] for securing copyright information is proposed by integrating blockchain with digital watermarking, perceptual hash function, Inter Planetary File System (IPFS) and Quick Response (QR) code. A peer to peer network is used to integrate copyright management and its distribution without the need of any centralized authority.

Blockchain technology is proposed to build secure public key infrastructure (PKI) systems [11] to replace certificate authorities for issuing, validating and cancelling X.509 certificates. Ethereum [3] smart contracts and restful services are used to provide verification of digital certificates issued.

A model [4] has been proposed for using blockchain as a decentralized platform for managing and controlling personal data like medical records. A mobile application provides fine grained access control to the user to monitor how and where its data is used. The access rights are stored in blockchain and users can alter the permissions any time.

MedRec [13] is a novel and decentralized record management system which uses blockchain to handle electronic medical records (EMRs). It provides the patients a comprehensive and immutable log of medical records with an easy access to the treatment sites. Through blockchain, MedRec manages the confidentiality and authenticity of the information.

Sia [25] is a blockchain based decentralized cloud storage system where various peers rent their storage spaces. It provides agreements/smart contracts between the clients and storage provider by using Bitcoin protocol.

A scheme [6] has been proposed to store sensitive data in blockchain as it prevents unauthorized access and make data tamper-proof by using secured cryptographic algorithms like Secure Hash Algorithm [16, 23], Scrypt [26].

An energy blockchain [15] has been proposed for the security of energy trading system. It proposes a credit-based payment system for fast energy trading to be used in P2P energy eliminating the need of any trusted intermediary.

Blockchain Covert Channel (BLOCCE) [19] has been proposed for covert communication. Covert communication channels [17] are used in military communication or in authoritarian government for secret communications. Covert messages are securely embedded to the blockchain using steganography and cryptography.

ControlChain [7] is a blockchain-based architecture for managing IoT access authorizations. The proposed architecture is fully decentralized, fault tolerant, user transparent, scalable, user friendly and compatible with a many access control models of IoT. It establishes a secure relationship between a group of users and devices providing high privacy and confidentiality among them.

Hawk [14] has been proposed as a decentralized system for smart contracts to retain transactional privacy by designing a compiler which automatically implements cryptography on the smart contract written by the programmer. The contractual parties interact with each other using cryptographic primitives like zero-knowledge proofs [4] and thereby defining a formal model for applications design atop decentralized blockchains.

III. TYPES OF BLOCKCHAIN

There can be following three types of blockchain on the basis of permissions to access or write the transactions:

a) *Public blockchain:* In public blockchain such as Bitcoin [12], Dash [8], Ethereum [3] transactions are transparent. Anyone can execute transactions via network and can read the transaction on public block explorer [25]. Hence the transactions can be audited by anyone. These blockchains [24] are preferable in cryptocurrencies.

b) *Federated or Consortium Blockchains:* Consortium Blockchains [18] are partly decentralized blockchain as they don't allow anyone to participate in the verification of transactions. They are faster, provide better transaction privacy and have higher scalability as compared to public blockchain. These blockchains are preferable in the banking sector. Corda [22] is a partly decentralized federated blockchain.

c) P*rivate Blockchain:* In private blockchains such as Ripple [21], write permissions are only meant for an individual or an organization and read permissions may be public or restricted to few authorized persons. Private or permissioned [1] blockchains provides different access rights to people in the same network for providing privacy of data. This makes it useful for collecting, storing or sharing of sensitive information, auditing, database management etc.

IV. PRE-REQUISITES OF BLOCKCHAIN

a) *Transaction verification and validity checking:* Whenever someone is doing a transaction, there must be a protocol for commitment of transaction so that the transaction is fully committed or discarded. The Proof of Work (PoW) [12] or Proof of Stake (PoS) [24] algorithms are needed to create blocks of transactions by verifying by legitimacy of transactions.

b) *Consistency maintenance:* As all the nodes on the network holds a copy of public ledger, the consistency of the data needs to be maintained. Consensus algorithm [18] is required so that an identical and updated copy of the data is maintained.

c) *Security and Integrity of data:* Data distributed in public ledgers cannot be hacked or manipulated as it is append-only data. In case of permissioned Blockchain, methods need to be designed for accessing the sensitive data by only authorized users of the Blockchain.

d) *Hashing algorithm:* Transactions in Blockchain are stored as hash values. Various hashing algorithms like Secure Hash Algorithm (SHA) -256 [16], SHA-1 [23], The Algorithm X11[8], Scrypt [26] should be used to hash the transactions of Blockchain.

e) *Decentralized network*: One of amazing feature of blockchain is decentralization of the data which secures it from any single point of failure. Decentralization brings designing of lots of rules and protocols for information exchange and update. These protocols should be defined and tested before implementation.

f) *No double spending*: Double spending is using the same digital money in more than one transaction. The risk of double spending is very common in digital currencies. Protocols need to be defined for the verification and authentication of each transaction and digital currency used.

V. CHALLENGES

Decentralization brings a lot of challenges. As there is no central authority so every participating node needs to process every transaction, maintain a copy of the system and update it as and when required.

a) *Storage***:** All the data in blockchain needs to be stored on every participating node in the network, there is high requirement of data storage and as the size of block or blockchain grows, storage requirement will increase many folds. Various storage optimization techniques need to be devised for handling this issue.

b) *Processing Speed:* All the transactions are happening in real time and need to be updated at every node. Moreover as users of blockchain increases, the number of transaction per second will increase, resulting in requirement of high processing speed.

c) *Security***:** Blockchain has a 51% attack problem [1, 7]. If someone has a control of 51% of the block, he/she will be able to manipulate the block. This problem needs to be addressed.

d) *Scalability*: As the size of blockchain increases, storage requirements may increase many folds. Faster computations and higher power will be required.

e) *Environment Impact*: To run blockchain, high amount of electricity is required. Environmental friendly means need to be designed to cater the high power demand of blockchain.

VI. APPLICATIONS

Blockchain is being used in various public and private sector organizations. The various services where blockchain has its applications can be broadly classified in following categories:

A. Financial Services

- ICICI bank [18] became the first bank to perform banking transactions using Blockchain to provide electronic and paperless financial transactions within the country and abroad.
- Bajaj Finserv [18] is also using blockchain to fasten its services of settling claims and travel insurances.
- A blockchain based platform “chain.com” [20] uses Blockchain for private equity exchange.
- Corda [21, 22] is an open source Blockchain platform that connects supply chain to global network, insurance providers to their authoritative record and much more.
- Other application areas could be asset management [25], foreign exchange [25], fraud control [18].

B. Smart Healthcare

- The NITI Aayog, India [27] is trying to solve the issue of fake medicines using blockchain technology.
- Medchain [23] is building a blockchain based platform for health information exchange for hospitals.

C. Smart Property

- Microsoft and Ernst & Young [28] are developing blockchain project for content rights and management of royalties.
- Ujo Music [30] is a music platform which uses blockchain for music licensing.
- ChromaWay [29] is using blockchain for land registry to track property ownership.
- Everledger [30] is a blockchain based diamond certification database to keep track of original, owner, VAT charges etc.

D. Smart Government

- BitID, Onename, Bithandle are various blockchain based digital identity [21] verification platforms.
- Estonia, Europe [31] is the first nation to use blockchain to provide e-residency to anyone by issuing e-ID which allows them to do any commercial activity within the nation.

E. Smart Contracts

- Eris Industries [30] provides a platform to create smart contracts by writing their own programs which can be executed in a distributed manner.
- Bob’s Repair [34] use smart contracts and Blockchain 2.0 for providing various repair services, publish all the transactions and reviews by the customers.
- Bit & Coin AG [36] provides smart contracts with European energy suppliers to get best price for green energy.
- Block and chain game studios [35] uses smart contracts for their gaming platform providing a new virtual experience.
- Ethereum [3] uses smart contracts to provide a platform to build decentralized application on top of it.

F. Data storage and protection

- Emercoin [21] is a provider of blockchain based IT services like data storage security, data protection and creation of various distributed services.
- Storj [2] is a decentralized cloud storage platform which allows user to share and transfer data without having third party reliance.

G. Commerce

- Bitcoin [12] was the first real application of blockchain. Various other crytocurrencies [25] like Ripple [21], Litecoin [32], Dodgecoin [5] etc. originated after Bitcoin’s success.
- HomeSend [21] which is meant for cross border payments is also finding its use case in Blockchain.
- Six international banks joined Utility Settlement Coin (USC) [33] blockchain based project, which will streamline the inter-bank settlements.

VII. PROPOSED RESEARCH ISSUE TO BE HANDLED

Blockchain can be used to integrate all the user’s identities and their various records like job details, property records, criminal records, PAN number, aadhar no., voter id etc. on one platform. It will act as a bibliography of the citizens of nation and can be used to identify any fake id-cards and frauds in any transactions. Facilities like bank loans, visa approvals, credit cards etc. can be issued after looking at the history of one’s assets and transactions.

VIII. CONCLUSION

Blockchain technology is going to transform the internet era. It is addressing the major privacy and security concerns of the new age technologies like cloud computing, Internet of Things etc. Smart contracts have already changed the way doing businesses by enforcing strict laws and automation of the transactions. Industries and organizations are embracing the technology and looking for use cases and usage of the technology for their work.

The technology is still in very early phases. A lot of research and development is going on to optimize its working algorithms for cleaner and greener environment. Apart from private organizations, the technology is getting accepted by the government in various countries like Europe for e-residency and India in healthcare. The technology surely has much more to deliver in the years to come.

REFERENCES

[1] Niranjanamurthy, M., Nithya, B.N. and Jagannatha, S. (2018) “Analysis of blockchain technology: pros, cons and SWOT”. Cluster Computing, 1–15. https://link.springer.com/article/10.1007/s10586-018-2387-5#aboutcontent.

[2] Wilkinson, S., Boshevski, T., Brandoff, J., Buterin, V. “Storj a peer-to-peer cloud storage network”. Technical report, Storj Labs Inc. (2014)

[3] Ethereum Team. Ethereum White Paper—“A Next-Generation Smart Contract and Decentralized Application Platform”. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 29 December 2017).

[4] Feige, Uriel, Amos Fiat, and Adi Shamir. "Zero-knowledge proofs of identity." Journal of cryptology 1, no. 2 (1988): 77-94.

[5] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Sebastopol, CA, USA:O’Reilly Media, Inc, 2014.

[6] Abhishek Jain, Aman Jain, Nihal Chauhan, Vikrant Singh, Narina Thakur, "Seguro Digital storage of documents using Blockchain," International Research Journal of Engineering and Technology (IRJET), vol. 5, no. 4, Apr- 2018.

[7] O. J. A. Pinno, A. R. A. Gregio and L. C. E. De Bona, "ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6.doi: 10.1109/GLOCOM.2017.8254521

[8] Duffield, E., Diaz, D. “Dash: A Privacy-Centric Crypto-Currency.” No Publisher (2015) https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf.

[9] Meng, Zhaoxiong, et al. "Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain." 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2018.

[10] Hamida, E.B., Brousmiche, K.L., Levard, H., Thea, E.: Blockchain for enterprise: overview, opportunities and challenges. In: The Thirteenth International Conference on Wireless and Mobile Communications-IEEE ICWMC (2017)

[11] A. Yakubov, W. Shbair, A. Wallbom, D. Sanda et al., “A blockchain-based pki management framework,” in The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018, 2018.

[12] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[13] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25-30. doi: 10.1109/OBD.2016.11

[14] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839-858.doi:10.1109/SP.2016.55

[15] Li, Zhetao, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang. "Consortium blockchain for secure energy trading in industrial internet of things." IEEE Transactions on Industrial Informatics (2017).

[16] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In Security and Privacy Workshops (SPW), 2015 IEEE, pp. 180-184. IEEE, 2015.

[17] Partala, Juha. "Provably Secure Covert Communication on Blockchain." Cryptography 2, no. 3 (2018): 18.

[18] Sheetal, Ms, and K. A. Venkatesh. "Necessary requirements for Blockchain Technology and its Applications." (2018).

[19] Partala, Juha. "Provably Secure Covert Communication on Blockchain." Cryptography 2, no. 3 (2018): 18.

[20] Zhao, J. Leon, Shaokun Fan, and Jiaqi Yan. "Overview of business innovations and research opportunities in blockchain and introduction to the special issue." (2016): 28.

[21] Olleros, F. Xavier, and Majlinda Zhegu, eds. Research handbook on digital transformations. Edward Elgar Publishing, 2016.

[22] Brown, Richard Gendal. "The Corda Platform: An Introduction." (2018).

[23] Rouhani, Sara, Darryl G. Humphery, Luke Butterworth, Ralph Deters, and Adam D. Simmons. "MediChain TM: A Secure Decentralized Medical Data Asset Management System."

[24] Lin, Iuon-Chang, and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and Challenges." IJ Network Security 19, no. 5 (2017): 653-659.

[25] Singh, Sachchidanand, and Nirmala Singh. "Blockchain: Future of financial and cyber security." In Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on, pp. 463-467. IEEE, 2016.

[26] Fernández-Caramés, Tiago M., and Paula Fraga-Lamas. "A Review on the Use of Blockchain for the Internet of Things." IEEE Access (2018).

[27] Balsari, Satchit, Alexander Fortenko, Joaquín A. Blaya, Adrian Gropper, Malavika Jayaram, Rahul Matthan, Ram Sahasranam et al. "Reimagining Health Data Exchange: An application programming interface–enabled roadmap for India." Journal of medical Internet research 20, no. 7 (2018).

[28] Xu, Ruzhi, Lu Zhang, Huawei Zhao, and Yun Peng. "Design of network media’s digital rights management scheme based on blockchain technology." In Autonomous Decentralized System (ISADS), 2017 IEEE 13th International Symposium on, pp. 128-133. IEEE, 2017.

[29] Kshetri, Nir, and Jeffrey Voas. "Blockchain in Developing Countries." IT Professional 20, no. 2 (2018): 11-14.

[30] Mattila, Juri. "The blockchain phenomenon." Berkeley Roundtable of the International Economy (2016).

[31] Sullivan, Clare, and Eric Burger. "E-residency and blockchain." Computer Law & Security Review 33, no. 4 (2017): 470-481.

[32] M. Swan, Blockchain: Blueprint for a New Economy; O’Reilly Media: Newton, MA, USA, 2015.

[33] http://fortune.com/2017/08/31/banks-ubs-blockchain-settlements/

[34] https://bobsrepair.com/

[35] https://www.blockandchain.games/

[36] http://www.bit-coin.ag/