INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.488

A Study on Features and Application of Blockchain Technology

Mithun Vishnu Mhatre, Ranjeet Ramesh Pawar

Incharge HOD, Dept. of Computer Technology, BVIT, Navi Mumbai, India.

Incharge HOD, Dept. of Information Technology, BVIT, Navi Mumbai, India.

ABSTRACT: Blockchain technology has become popular due to its successful adoption of cryptocurrencies such as Bitcoin. This distributed digital ledger has many advantages as it can keep track of all data or money transactions made between two parties in a secure, immutable and transparent manner. Blockchain applications go far beyond cryptocurrencies and bitcoins. With its ability to create greater transparency and fairness while saving companies time and money, technology is influencing a variety of industries in ways ranging from how contracts are enforced to making government more efficient.

KEYWORDS: Application of Blockchain technology, cryptocurrency, distributed, Smart Contract, Bitcoin.

I. INTRODUCTION

Blockchain technology, essentially a virtual ledger capable of recording and verifying a large volume of digital transactions, is now spreading through a wave of industries. Blockchain technology has gone far beyond its beginnings in the banking and cryptocurrency industry: Annual global spending on blockchain applications has almost tripled since 2017. Annual spending on blockchain solutions will reach nearly $ 16 billion by 2023, according to Market. CB Insights sizing tool. Industries ranging from insurance to gaming to cannabis are starting to see blockchain applications. The popularity of Bitcoin has helped demonstrate the application of blockchain in finance, but entrepreneurs have come to believe that blockchain could transform many more industries. Ultimately, the use cases for a transparent and verifiable transaction data ledger are practically endless, especially since the blockchain operates through a decentralized platform that does not require central oversight, making it resistant to fraud. Blockchain technology is incorporated into business solutions to ensure greater security. While many may only be familiar with the applications of the cryptocurrency blockchain, new formats of the technology have emerged and will continue to advance. "In the next five years, you will see a blockchain economy," said Robin Raskin, former president of Living in Digital Times, which has produced several shows. "We will find great use cases for blockchain in shipping, identifying counterfeit products and other applications."

II. RELATED WORK

In this paper [4], a blockchain incentive mechanism has been presented to preserve privacy in crowd-sensing applications, where a cryptocurrency built into blockchain is used as a secure form of incentive. High quality tax payers will receive their payments recorded in blocks of transactions. The miners will verify the confirmation based on the criteria for the evaluation of the survey data published by the server. [5], In this paper proposes the digital platform and governance regime interplay as an important factor for dis-ruptive derivatives to be developed. The governance model in public administration is centralized, and that introducing a new digital platform like Bitcoin could foster new disruptive derivative services in public sector, but at the same time could challenge the centralized governance model. E-Government researchers must wake up and see the promising potential in the Bitcoin technology and start researching ways for the illustration of potential use of Bitcoin technology in public sector a selected use case with special relevance to public sector has been studied. [7]The health blockchain is a good solution to address the problem of monopoly of physiological data and improve the robustness of storing these data, and has a broad application prospect in the area of healthcare system [7]. The author addressed the problem of protecting private physiological data. The core problem is designing an effective key management scheme. In the paper, they merged the BSN and the health blockchain, A BSN is composed of tens of biosensor nodes that are deployed on or into the human body.in [8], the author has proposed an incentive mechanism based on blockchain for distributed P2P applications that applies a crypto currency such as Bitcoin to encourage users to cooperate. Proposed a secure validation method and a pricing strategy and integrated them into the incentive mechanism. They design a real incentive mechanism based on Blockchain able to satisfy the different needs of users in dynamic and distributed P2P environments and introduce a

secure validation method to keep the content that must be verified secretly by miners in the Blockchain P2P system, author also proposed a pricing strategy to prevent selfish users from showing selfish actions and to defend the resulting collusion attacks.

III. BLOCKCHAIN AND KEY FEATURES

Blockchain is a distributed cryptographically designed distributed ledger. Records all transactions made on a network. It is a chronological chain of blocks where each block consists of a block header. The block header records the hash of the previous block along with a Merkle root and a date / time of the current block. This helps ensure the integrity of the blocks and allows the block chain to detect any invalid block, which makes it extremely secure. In this paper, we illustrate how the use of a blockchain-compatible peer-to-peer examination system can solve the problems identified in the security domain [1] and the integrity of current examination systems. We propose a framework to conduct a decentralized exam using blockchain for better evaluation and maintenance of exam records, so that records are more credible, reliable and secure than the current exam system. The current examination system suffers from extreme cases of manipulation of scores in the database, both by students [1], external security criminals or privileged information with administrative access. These concerns can be addressed by the proposed blockchain-based system.
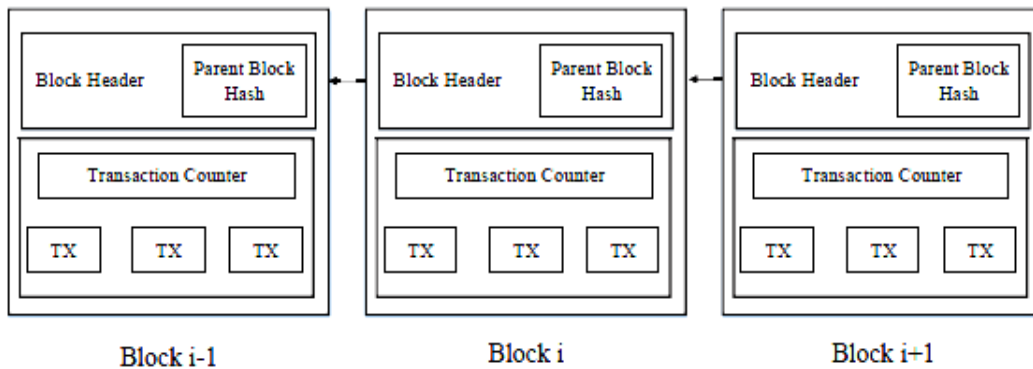
Blockchain Architecture

Fig. 1.1: An example of blockchain which consists of a continuous sequence of blocks.

Blockchain is a sequence of blocks, which contains a complete List of transaction records as a normal public record[14] Figure 1.1 shows an example of a blockchain. With a hash of the previous block contained in the block header, a block It has a single parent block. The hashes have also been memorised (the children of the ancestors of the block) in the chain of ethereum blocks [11]. The first block of a blockchain, It's called a genetic block that does not have a main block.

(A)Block

block contains the block header and the block body as shown in Figure 1.2. The block header contains:
(i) Block version: identify which set of block validation rules to follow.
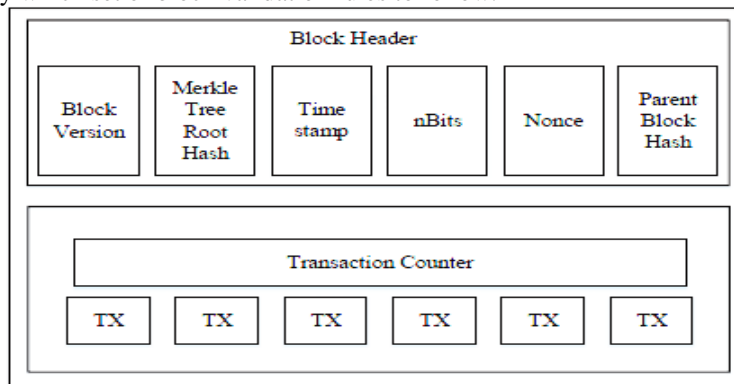

Fig 1.2 Block Structure

(iii nBits: target beginning of a valid block hash
(iv) Root Hash of the Merkle tree: the hash value of all transactions in the block
(iv)Timestamp: current time as seconds in universal time from 1 January 1970.
(v) Nonce: a four byte of field, which generally begins with 0 and increases 4 each hash calculation.
(vi) Parent Block Hash: hash value of the previous block which is a 256-bit that points to the previous block.

vi) Transaction counter: consists of a transaction and the extreme number of transactions that a block can enclose depends on the size of the block and the size of each transaction.[12].

(B) Digital signature

Each user has a private and public key pair. The private key that will be kept confidential is used to sign transactions. The basically digital signature is involved in two phases: firstis signature phase and second is verification phase. For example, an A1user wants to send a message to another B1 user. (1) In the signing phase, A1 encrypts their data with own private key and sends B1 ,the encrypted result and the original data. (2) In the verification phase, Bob validates the value with Alice's public key. In this way, B1 could easily check whether the data was tampered with or not. The typical digital signature algorithm used in blockchains is the digital signature algorithm of the elliptic curve (ECDSA) [12].

Key Features OfBlockchain

A. **Decentralized Database:** A distributed database is a database in which storage devices are not all attached to a common processor. It may be stored in multiple computers, located in the same physical location; or may be dispersed over a network of interconnected computers. With the use of a decentralized and encrypted communication protocols, messages can be transferred, stored and retrieved at any time without any form of intervention from the government and a distributed database system consists of loosely coupled sites that share no physical components. Decentralized Database also allows both decentralized and secure manner of data exchange. If required, information can be published and distributed across a huge number of computers in an encrypted manner thereby eliminating the ability of a single entity to censor.

B. **Eliminating Third Party:** It records and stores every transaction that occurs in the network, essentially eliminating the need for "trusted" third parties such as payment processors. Blockchain proponents often describe the innovation as a "transfer of trust in a trust less world," referring to the fact that the entities participating in a transaction are not necessarily known to each other yet they exchange value with surety and no third-party validation.

C. **Smart Contracts**: Smart contact is a term used to describe computer program code that is capable of facilitating, executing, and enforcing the negotiation or performance of an agreement (i.e. contract) using blockchain technology. The entire process is automated can act as a complement, or substitute, for legal contracts, where the term of the smart contract is recorded in a computer language as a set of instructions. These smart contracts employ the use of the _if-this-then-that 'logic. The execution of smart contracts does not involve the use of any human in any way. This signifies that Smart contracts are decentralized and they tend to operate without any middleman or third-party regulation. Furthermore, they employ the use of a distributed database so that participants can verify that there is an occurrence of a digital event without requiring any middleman or third party.

D. **Self-Executing Systems**: Blockchain-based smart contracts are self-executing. They can solve the problems of counterparty trust in the sense that they automatically implement the terms of an agreement between parties on pre-set logic without the need for intermediaries. They are executed by a computer network that uses consensus protocols to agree upon the sequence of actions resulting from the contracts 'code. Coded contracts introduce efficiency of automatically generating contracts based on mutually agreed-upon patterns and syntax amongst counter parties. This is a major overhaul from how things are currently done i.e. manual documentation. Prior to blockchain, for an agreement of this type, parties would have had to maintain separate databases. Blockchain however, allows the shared database to have self-executing smart contracts where all participants can validate the outcome instantly without requiring an intermediary.

E. **Best-Fit Scenarios**: A good fit for blockchain enabled smart contracts could be a scenario where frequent transaction happen between a network of participants and manual mechanical tasks are performed repetitively for each transaction. Smart contracts are particularly well suited for the permissioned/private blockchain network. For the financial and securities sectors, such a code-based compliance would save a lot of time and money. Syndicated loans are a $4 trillion plus market that still run primarily on faxes, emails and Excel spread sheets. It can definitely see improvement with this technology.

F. **Faster Settlement:** By eliminate the need of third-party regulator to a large extent, since the rules and regulations would be in built and required to follow every time in order to make your transactions official (as a part of the blockchain), so in this case the network acts as a regulator for every single transaction. This would not only reduce huge costs levied on customers in terms of commissions, but would also speed up the process resulting in much faster transaction settlements. Also, given the number of intermediaries in the

system gets reduced, the costs associated with them like trades record keeping, audits, and trade verifications also gets eliminated. For example, in the current system, 1% processing fee might not seem like much but add a number of intermediaries and the cost mounts up significantly creating an impact in the long run. This also restricts access to a lot of small players. Blockchain removes this hurdle.

G. **Better Security:** Theblockchain addresses the fundamental flaws of security by taking away the human factor from the equation, which is usually the weakest link. By leveraging a distributed ledger and taking away the risk of a single point of failure, blockchain technology provides end-to-end privacy and encryption while still ensuring convenience for users. Blockchain technologies are here to stay. It is probably going to help us protect as individuals, companies and governments. Even the pentagon already thinks the blockchain technology can be used as cybersecurity shield.

IV. BLOCKCHAIN APPLICATIONS

Blockchain technology can be used in multiple industries, including financial services, healthcare, government, travel and hospitality, retail, and CPG. Financial Services - In the financial services industry, Blockchain technology has already been implemented in many innovative ways. Blockchain technology simplifies and streamlines the entire process associated with asset management and payments by providing an automated business lifecycle where all participants would have access to the exact same data in a transaction. This eliminates the need for brokers or intermediaries and ensures transparency and efficient management of transactional data.

A. **Blockchain In Education System(BIES):**Educational technology (edtech) has made great strides over the last 20 years, but there is still a long road ahead to full modernization. Technologies like blockchain are here to speed up the process. Ledger tech, along with AI, smartphones and tablets, are rapidly replacing bulky desktop computers and antiquated textbooks as the preferred method of teaching.

B. **Smart Contracts Use Cases**
Smart contracts are like regular contracts except the rules of the contract are enforced in real-time on a blockchain, which eliminates the middleman and adds levels of accountability for all parties involved in a way not possible with traditional agreements. This saves businesses time and money, while also ensuring compliance from everyone involved. Blockchain-based contracts are becoming more and more popular as sectors like government, healthcare and the real estate industry discover the benefits. Below are a few examples of how companies are using blockchain to make contracts smarter.

C. **Healthcare.**
Blockchain can play a key role in the healthcare sector by increasing the privacy, security and interoperability of the healthcare data. It holds the potential to address many interoperability challenges in the sector and enable secure sharing of healthcare data among the various entities and people involved in the process. It eliminates the interference of a third-party and also avoids the overhead costs. With Blockchains, the healthcare records can be stored in distributed data bases by encrypting it and implementing digital signatures to ensure privacy and authenticity.

D. **Government**
Blockchain technology holds the power to transform Government's operations and services. It can play a key role in improving the data transactional challenges in the Government sector, which works in siloes currently. The proper linking and sharing of data with Blockchain enable better management of data between multiple departments. It improves the transparency and provides a better way to monitor and audit the transactions.

E. **Money Transfer Use Cases**
pioneered by bitcoin, cryptocurrency transfer apps are exploding in popularity right now. blockchain is especially popular in finance for the money and time it can save financial companies of all sizes.By eliminating bureaucratic red tape, making ledger systems real-time and reducing third-party fees, blockchain can save the largest banks $8-$12 billion a year, according to a recent article by ComputerWorld. we'll take a deeper dive into four companies using blockchain to efficiently transfer money.

F. **Internet Of Things Use Cases**
The Internet of Things (IoT) is the next logical boom in blockchain applications. IoT has millions of applications and many safety concerns, and an increase in IoT products means better chances for hackers to steal your data on everything from an Amazon Alexa to a smart thermostat. Blockchain-infused IoT adds a higher level of security to

prevent data breaches by utilizing transparency and virtual incorruptibility of the technology to keep things "smart." Below are a few US companies using blockchain to make the Internet of Things safer and smarter.

G. **Personal Identity Security Use Cases**

According to identity theft expert LifeLock, more than 16 million Americans complained of identity fraud and theft in 2017 alone, with an identity being stolen every two seconds. Fraud on this scale can occur via everything from forged documents to hacking into personal files. By keeping social security numbers, birth certificates, birth dates and other sensitive information on a decentralized blockchain ledger, the government could see a drastic drop in identity theft claims. Here are a few blockchain-based enterprises at the forefront of identity security.

H. **PG And Retail**

There is a huge opportunity for Blockchain technology to be applied in the retail sector . This includes everything from ensuring the authenticity of high value goods, preventing, fraudulent transactions, locating stolen items, enabling virtual warranties, managing loyalty points and streamlining supply chain operations.

I. **Travel and Hospitality**

The application of Blockchain can radically change the travel and hospitality industry . It can be applied in money transactions, storing important documents like passports/ other identification cards, reservations and managing travel insurance, loyalty and rewards.

Table 1. Global Top 20 Public Companies and their Blockchain Use Case Plan

Rank	Public Company Name	Company Category	Country	Blockchain Application Use Case	Website
1	Industrial and Commercial Bank of China (ICBC)	Banking	China	Trying to verify digital certificatesusing Blockchain	http://www.icbc-ltd.com/icbcltd/en/
2	China Construction Bank	Banking	China	Using IBM Blockchain for financial products	http://www.ccb.com/en/home/indexv3.html
3	JPMorgan Chase	Financial Services	United States	Contributed to Quorum Project	https://www.jpmorganchase.com/
4	Berkshire Hathaway	Conglomerate	United States	Blockchain base supply chain	http://www.berkshirehathaway.com/
5	Agricultural Bank of China	Banking	China	Unsecured agricultural loans on Blockchain for e-commerce merchant	http://www.abchina.com/en/
6	Bankof America	Banking	United States	Trying to use EthereumBlockchain to automate issue of letters of credit	https://www.bankofamerica.com/
7	Wells Fargo	Financial Services	United States	Member of R3 and trying to simplify tracking of securitized home mortgages.	https://www.wellsfargo.com/

8	Apple	Technology	United States	Registered a patent to timestamp data using Blockchain	https://www.apple.com/
9	Bank of China	Banking	China	Working with Tencent to develop financial solutions using Blockchain.	www.boc.cn/en/
10	PingAn Insurance Group	Insurance	China	Member of R3 and working with various insurance firm to develop Blockchain solution	http://www.pingan.cn/en/index.shtml
11	Royal Dutch Shell	Oil & Gas	Netherlands	Funding Blockchain projects and working with BP to develop Energy Commodities Platform	https://www.shell.com/
12	Toyota Motor	Automotive	Japan	Founder member of Blockchain Mobility Consortium and developing Blockchain based payment system for self-driving cars	https://www.toyota-global.com/
14	Samsung	Conglomerate	South Korea	Own Nexledger platform to track global supply chains	https://www.samsung.com
19	BNP Paribas	Banking	France	Blockchain platform for internal treasury operations	https://group.bnpparibas/en/
20	Microsoft	Technology	United States	Offering Blockchain as a services on Azure Platform	https://www.microsoft.com

V. CONCLUSION AND FUTURE WORK

The purpose of this paper is ,This decentralized blockchain system is going to change your life from the way you transact business or manage assets ,to the way you use your machines, vote, rent a car,IOT,smart contract, and even prove who you are. Along the way, it will transform banks and other financial institutions, hospitals, companies, and governments among others.It's important to note that for the blockchain to work, the node-to-node network must be motivated and agree to work under ethical standards. Once, and only if, these standards are adhered to, the blockchain could become a powerful tool for improving business, conducting fair trade, democratizing the global economy, and helping support more open and fair societies.

REFERENCES

[1] Alex Rohr's, Cristiano André da Costa, Rodrigo da Rosa Righi Journal of Biomedical Informatics 71 (2017) 70–81. "OmniPHR: A distributed architecture model to integrate personal healthrecords".
[2] Qi Xia, Emmanuel BoatengSifah, Kwame OmonoAsamoah, Jianbin   Gao, Xiaojiang Du and Mohsen Guizani IEEE DOI: 10.1109/ACCESS.2017.2730843July 2017 "Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain".
[3] JianbinGao 1, Kwame Omono Asamoah2, Emmanuel Boateng Sifah2, GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid".

[4] Jingzhong Wang1, (Member, Ieee), Mengru Li 1, Yunhua He1, (Member, Ieee), Hong Li2, (Member, Ieee), Ke Xiao1, And Chao Wang1 "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications"

[5] SveinØlnes, Vestlandsforsking (Western Norway Research Institute), February 27, 2018, Beyond Bitcoin "Public Sector Innovation Using the Bitcoin Blockchain Technology"

[6] Wei Yin ,Qiaoyan Wen, Wenmin Li, Hua Zhang, (Member, Ieee), And ZhengpingJin, February 28, 2018. "An Anti-Quantum Transaction Authentication Approach in Blockchain".

[7] Huawei Zhao ,Peidong Bai, Yun Peng, Ruzhi Xu 17th January 2018," "Efficient key   management scheme for health blockchain".

[8] Yunhua He 1, (Member, Ieee), Hong Li2, (Member, Ieee), Xiuzhen Cheng3, (Fellow, Ieee), Yan Liu4, (Member, Ieee), Chao Yang5, (Member, Ieee), And Limin Sun2, (Member, Ieee) China April 2, 2018, "A Blockchain Based Truthful Incentive Mechanism For Distributed P2p Applications".

[9] Lijing Zhou, Licheng Wang, Yiru Sun and Pin Lv , 8, AUGUST 2015 "BeeKeeper: A Blockchain-based IoT System with Secure Storage and Homomorphic Computation".

[10] Yanqi Zhao 1, Yannan Li2, (Student Member, Ieee), Qilin Mu3,Bo Yang1, (Member,   IEEE), And Yong Yu1, March 19, 2018. (Member, IEEE "Secure Pub-Sub: Blockchain- Based Fair Payment With Reputation For Reliable Cyber Physical Systems".

[11] Oliver, Miquel; Moreno, Joan; Prieto, Gerson; Benítez, David 4thAugust 2018   "Using Blockchain As A Tool For Tracking And Verification Of Official Degrees: Business Model".

[12] Shangping Wang1, Yinglong Zhang 1, And YalingZhang , June 24 2018 "A Blockchain-Based Framework For Data Sharing With Fine-Grained Access Control In Decentralized Storage Systems".

[13] https://builtin.com/blockchain/blockchain-education

[14] M. Conoscenti, A. Vetro, J. C. D. Martin, Blockchain for the internet of ` things: A systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1–6. doi:10.1109/AICCSA.2016.7945805.

[15] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303. doi:10.1109/ ACCESS.2016.2566339.

[16] J. Sun, J. Yan, and K. Z. K. Zhang, ``Blockchain-based sharing services:Whatblockchain technology can contribute to smart cities," Financial".

[17] Blockchain in Education, JCR Science for Policy Report. A. Grech, A.F. Camilleri.2017.Innov., vol. 2, no. 1, p. 26, Dec. 2016. [Online]. Available: http://j_nswufe.springeropen.com/articles/10.1186/s40854-016-0040-y

[18] Blockchain and the Future of Digital Learning Credential Assessment and Management. MerijaJirgensons, JānisKapenieks. Published Online: 2018.

[19] MuhamedTurkanovi. , Marko Hölbl , Kristjan Ko.I,MarjanHeri.Ko, And Aida Kami.Ali January 5, 2018,."EduCTX: A Blockchain-Based Higher Education Credit Platform ".

[20] T.P. George, D.L. Hopla, Advantages Of Personal Health Records, Nursing 2015Crit. Care 10 (6) (2015) 10–12.Yanqi Zhao 1, Yannan Li2, Qilin Mu3,Bo Yang1, (Member, IEEE), And Yong Yu1, (Member, IEEE).

[21] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008). URL https://bitcoin.org/bitcoin.pdf

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING