JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BLOCK CHAIN TECHNOLOGY

[1]Amit Kumar Gupta, [2]Dr. Devesh Katiyar, [3]Mr. Gaurav Goel

[1]Student, [2,3]Assistant Professor, Faculty of Computer & Information Technology, Dr. Shakuntala Misra National Rehabilitation University, Lucknow, India

1. *ABSTRACT*

Blockchain technology has emerged as a hot research topic and a viable technological option for many businesses and industrial communities. Blockchain, due to its distributed, decentralised, and trust less nature, can provide businesses with new opportunities and benefits such as increased efficiency, lower costs, increased integrity and transparency, improved security, and improved traceability. Although blockchain's most prominent applications have been in finance and banking, we are now seeing experiments and proposed applications in a variety of fields. This paper provides an overview of blockchain technology; it brings together all of the key design features, characteristics, and benefits of blockchain that make it a superior and unique technology; and it presents the most popular consensus protocols and blockchain system taxonomy. Furthermore, the paper examines blockchain-based applications in finance, insurance, supply chain management, energy, advertising and media, real estate, and healthcare. It intends to investigate the industries' key issues, blockchain solutions, and use cases. The paper discusses three major limitations of blockchain technology: scalability, security, and regulation, and how these issues may affect blockchain application and adoption.

Keywords: *Blockchain, Distributed Ledger, Cryptocurrency, Smart Contracts, Decentralized Applications*

2.INTRODUCTION

The blockchain concept was first introduced in November 2008 and was implemented in January 2009. Satoshi Nakamoto, a presumed pseudonymous person or persons, created the virtual currency bitcoin and published the bitcoin white paper. A decentralised, publicly available, and cryptographically secure system based on a chain of blocks was proposed in this paper, allowing peer-to-peer digital currency trading while eliminating the need for centralised financial institutions to enable currency issuance or transaction settlement (Dai & Vasarhelyi, 2017; Murray, 2018; Nakamoto, 2008). Bitcoin and the blockchain aren't the same thing. Blockchain is the infrastructure for recording and storing bitcoin transactions; it has many applications other than bitcoin. Bitcoin is the first blockchain application (M. Gupta, 2017; V. Gupta, 2017).

According to M. Gupta in Blockchain for Dummies, Bitcoin is actually built on the foundation of blockchain, which serves as bitcoin's shared ledger. Consider blockchain to be an operating system, similar to Microsoft Windows or MacOS, with bitcoin being just one of many applications that can run on it.

Furthermore, blockchain should be viewed as a broader concept that encompasses a variety of technologies and applications. The blockchain concept can be compared to the Internet, which has numerous technologies and applications. It is predicted that blockchain will transform business in the same way that the Internet did. Blockchain has the potential to positively disrupt central banking platforms as well as numerous business models and use cases such as trading, wealth management, distribution networks, business process re-engineering, health information sharing, and logistics and distribution. In contrast to a distributed database, users in a distributed ledger do not trust one another and independently verify transactions. A distributed ledger is a synchronized, replicated, decentralised, and cryptographically secure record of data and transactions shared by contracting parties. Distributed ledgers are broadly

classified into two types: those that seek to minimise the role of trusted third parties and those that continue to rely on those third parties to handle some of the system's properties.
Blockchain is commonly classified as a distributed ledger technology. All decentralised systems for documenting transactions and sharing data across various servers, organisations, or nations are included in this category. Although blockchain is a distributed ledger, not all distributed ledgers are blockchains, nor are all distributed ledgers built on a chain of blocks. Blockchain is a new technology, and its underlying technical components are difficult to grasp, especially for non-specialists. This technology is supported by complex algorithms and computer protocols. However, early adopters of technology tools report that becoming a coding expert is not required to use this technology. Businesses and organisations, like any other modern technology, do not need to comprehend the technical fundamentals of the technology to recognise its benefits.

While there are many survey studies on the blockchain, only a handful have addressed its applications across multiple domains. The bibliography includes some of these survey works. This study examines blockchain applications across multiple domains, with an emphasis on fields and industries having the greatest potential for blockchain application success. The goals of this paper are as follows: first, to address the characteristics and benefits of blockchain that make it a technological option for many individuals, businesses, and institutions; and second, to discuss latest progress of said technology in a number of domains; covering several blockchain applications and some developed technological tools for these applications. An in-depth explanation of blockchain's technological elements is beyond the scope of this poll.

3.Blockchain Technology

Nakamoto (2008) offered two technological and inventive ideas in the white paper Bitcoin: A Peer-to-Peer Electronic Cash System. The original concept was bitcoin, a digital money that can be traded without the intervention of a central financial authority. The concept of blockchain was the second idea. Blockchain, as the name implies, is a chain of blocks linked together by complex computational encryption algorithms. The core concept of this technology is to store digital assets of any kind in blocks, which are connected by a digital fingerprint known as a hash and kept in an infinite number of places on a distributed database. Blockchain is a "distributed ledger technology that establishes transparency and trust for a new generation of transactional applications" (Linn & Koo, n.d., p. 2).

According to Koshechkin et al. (2018), blockchain is both a peer-to-peer network and a public database that operates without a central server.The basic notion behind blockchain is that it is a secure register or list for data records and the storing of past transactions, which are validated and confirmed by blockchain parties. The primary feature of blockchain is the accurate representation of reality at any given time, which fosters confidence among business partners. Blockchain can be viewed of as a state machine; it saves the status of events, then updates that status while keeping a permanent record of past states. These previous states are nearly impossible to modify (Adams et al., 2017).

"Hashing" is one of blockchain's primary strengths. Each block contains information that must be kept, and each new block added to the chain is encoded with a "hash," a code created arithmetically from the block's date. "Hashing" is a well-known method for securing passwords. Furthermore, each newly inserted block incorporates the previous block's hash in the same block hash. Falsifying fresh or old blocks becomes extremely tough in this manner. Because the hashes of prior blocks affect the hashes of later blocks, changing a single block would need rewriting the entire network. Tampering is extremely tough with this approach of combining the pieces into a chain (Hughes & Morrow, 2019; White, 2017).

Figure 1 illustrates how blockchain was initially developed for the safe exchange and storage of the cryptocurrency bitcoin. The Blockchain 1.0 technology that made it possible to issue, distribute, and deal in digital currencies is represented by this application. Later, it underwent further development, enabling Turing-complete programming languages. Blockchain 2.0 is this advancement, which enables users to create smart contracts that can operate on the blockchain. Ethereum is the most widely utilised blockchain-based system that enables smart contracts (Li et al., 2017; Oh & Shong, 2017). The Blockchain 3.0 era is characterised by the expansion of blockchain applications beyond finance and commerce (Aras & Kulkarni, 2017).

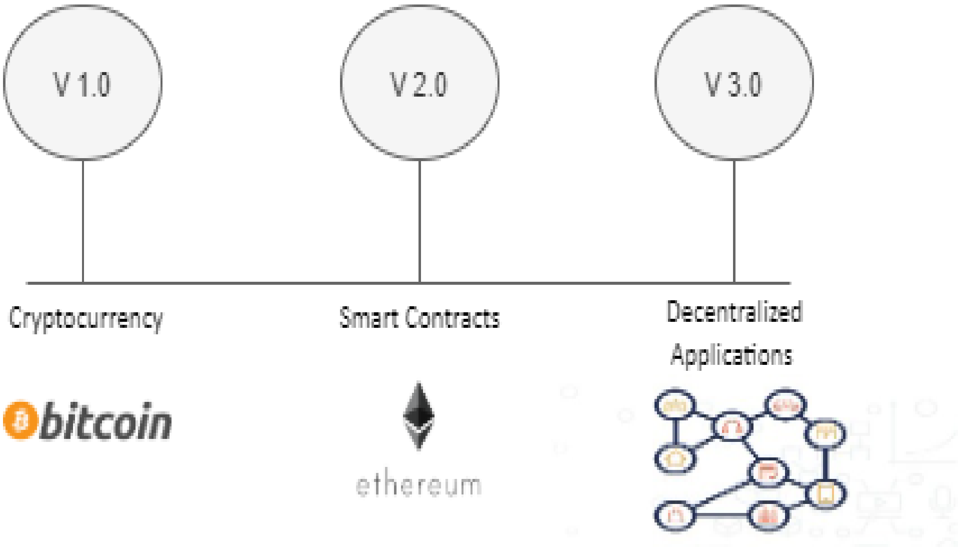

Figure 1 Development of blockchain

4.Blockchain-Based Design Features

The key attributes of a blockchain-based design are critical to the technology's superiority and uniqueness. According to Perkinson and Miller (2016), these design features are highly valued, particularly in environments where transaction verification, reconciliation and settlement, and dispute resolution consume an inordinate amount of energy and resources; they summarised these features as follows.

- *Transaction confirmation: Blockchain is supported by protocols that require users to verify transactions as a precondition for posting, ensuring transaction validity.*
- *Settlement verification: As counterparties confirm transaction details, blockchain instantly verifies the pre-transaction ownership of the underlying asset being exchanged, allowing the asset's transfer to be settled as the transaction is completed.*
- *Permanent timestamp: Once blocks are created, added to the chain, accurately ordered, and timestamped, an immutable record of the chain's sequence and timing is created.*
- *Smart contract automation: Although it is not a built-in feature of blockchain technology, blockchain ledgers can support smart contracts that run automatically under certain conditions. Smart contracts are covered in greater detail later in this section.*

5.Benefits of Blockchain Technology

Even though blockchain technology is still in its infancy, it has already transformed many businesses and become an attractive technology for many industries. Some of the most important advantages of blockchain application are as follows (Beck, 2018; Herlihy, 2019; Kumar, 2019; Workie & Jain, 2017):

- **Transparency:** *In a blockchain, a complete history of transactions is kept permanently and is available to all network users at the same time. All users involved in a transaction are aware of any actions taken on any data or transactions carried out, resulting in increased transparency.*

- **Business Continuity:** *All businesses must ensure the availability and continuity of their services. Because blockchain technology lacks a single point of failure, the system is never down, even if some parts fail, ensuring business continuity.*

- **Disintermediation:** *Because blockchain infrastructure is truly decentralised, it allows for significant disintermediation. Because of decreased trust, technology protocols and elements can replace intermediaries, increasing efficiency and lowering friction-related direct and indirect costs between individuals and organisations.*

- **Trust:** *The foundational idea behind the blockchain technology is the creation of a reliable record between unknown parties. The robust cryptographic properties and well-designed blockchain-embedded protocols strengthen confidence and facilitate verification.*

- **Smart Contracts:** *Ledgers can be enhanced with additional functionality because most blockchain apps include scripting languages. For instance, while Ethereum offers a language similar to JavaScript, a Turing-complete imperative language, bitcoin contains a crude stack-based language. These programmes, referred to as smart contracts, are computer codes or software created to digitally facilitate, confirm, and enforce the negotiation or performance of the business logic. Smart contracts automate the execution of reliable transactions and actions (such as the exchange of assets, money, shares, or anything else of value) when the terms of agreements are met, without the need for a mediator. Although smart contracts can be used in traditional systems, blockchain is the ideal technology platform because of data integrity and data accessibility for all stakeholders.*

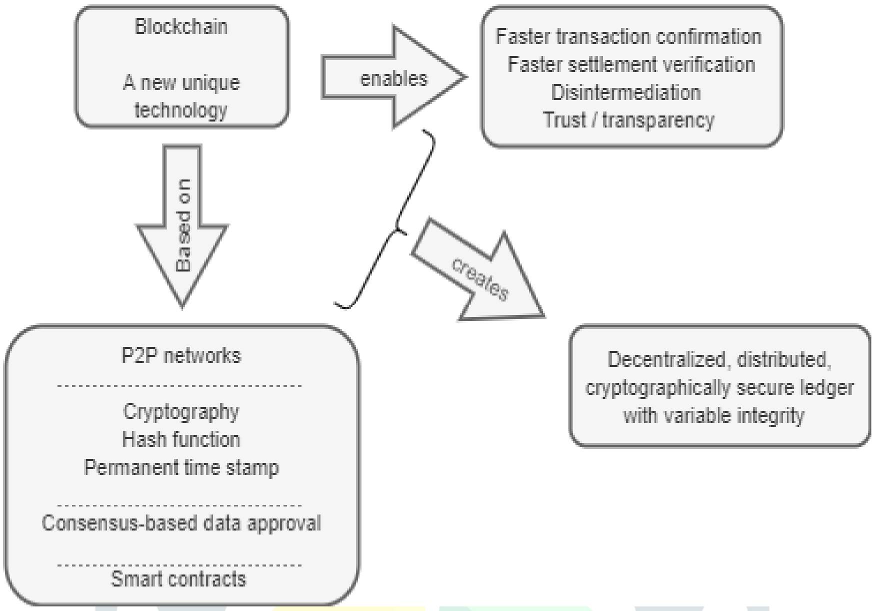
Blockchain
A new unique technology
enables
Faster transaction confirmation
Faster settlement verification
Disintermediation
Trust / transparency
Based on
creates
P2P networks
Cryptography
Hash function
Permanent time stamp
Consensus-based data approval
Smart contracts
Decentralized, distributed, cryptographically secure ledger with variable integrity

Figure 2 A combination of key design features, characteristics, and benefits of blockchain technology

6. Types of Blockchain Systems

Bitcoin, a peer-to-peer electronic cash system and decentralised public ledger, was the first blockchain-based system proposed by Nakamoto in 2008. However, there are now a number of blockchain solutions available to both people and companies. The two basic criteria that may be used to categorise these various blockchain systems are access to the blockchain system (permissionless and permissioned blockchains) and access to the blockchain data (public and private block chains) (BitFury Group, 2015; Peter & Panayi, 2015).

- **Permissionless blockchains:** *In these blockchains, transaction verification can be done by any participant. Users are free to create blocks without constraints or permission from a higher authority. Only a small group of carefully chosen known users can add to or validate transaction blocks on these blockchains.*

- **Permissioned blockchains***: Only a small group of carefully chosen known users can add to or validate transaction blocks on these blockchains.*

- **Public blockchains:** *Anyone can join the network, access the data, and contribute transactions in these blockchains.*

- **Private blockchains:** *In these blockchains, access to data, viewing of transactions, and submission of transactions are all restricted to specific people within one organisation or a small number of related organisations.*

7.APPLICATIONS OF BLOCKCHAIN

Many industries and professions could be disrupted and revolutionised by blockchain technology. Although blockchain applications have moved to other industries, blockchain-based cryptocurrency applications are well known and used. Numerous businesses recognise its value and began researching its potential. Today, we are beginning to see certain blockchain use cases outside of finance and banking, including supply chain management, advertising verification, energy conservation, and healthcare. With the creation of user-friendly interfaces and new use cases, it is anticipated that we will see more beneficial applications in the future. (Appelbaum & Smith, 2018; Anjum et al., 2017) Businesses and sectors are motivated to explore and build blockchain-based applications for a variety of reasons, including access to information, data integrity, and operational resilience (Klimos, 2018).

7.1.Financial Applications

The success of blockchain-based cryptocurrency platforms has paved the way for numerous possible applications in various financial sectors. Trusted intermediaries typically handle financial transactions between people and institutions. Blockchain can replace the services offered by these reliable middlemen, particularly the avoidance of duplicate financial transactions and the registration and confirmation of financial activity, according to its enabled design features and characteristics (Al-Jaroodi & Mohamed, 2019). The following are some instances of blockchain-based financial applications that eliminate the need for banks and other financial institutions to perform essential services.

7.2.Payments

Since its introduction, blockchain technology has significantly increased its trust due to its openness, security, and use. For improved operation, various industries have started to believe in and utilise blockchain technology. Blockchain is now being used successfully in industries like bitcoin trading, entertainment, healthcare, and more. However, employing blockchain as the foundation of payment systems is its most desired use.

Blockchain is the technology of the future, and it has the potential to completely change how we conduct daily financial transactions. Over the years, our generation has witnessed the entire elimination of currency from our financial system. Another such transition, where the centralised, middleman-based payment networks are going to be supplanted, is about to happen in the upcoming years. Replacing them will be a decentralized, peer-to-peer system i.e. blockchain.

7.3.Stock Trading

Traditionally, a centralised organisation like an exchange market oversees stock trading. All trades and settlements are monitored by this centralised management. This type of approach is linked to higher costs and delayed payouts (Al-Jaroodi & Mohamed, 2019). In this regard, some blockchain-based solutions have been created (Monrat et al., 2019). For instance, the blockchain technology start up Polymath5 is creating a market and platform to enable the trading of digital securities. The company will introduce security tokens on its platform in collaboration with Block trade, Corl, and Ethereum Capital (How Blockchain Could Disrupt Banking, 2018). Another such is Overstock's tZERO6 trading platform. In October 2018, tZero raised $134 million in a personal digital token offering. In January 2019, these tokens were put up for trade on tZero (Elliott, 2018). Additionally, Chain Company launched the integration of live blockchain transactions between the financial systems of Citi and the NASDAQ stock market after being incorporated into a new business called Interstellar (How Blockchain Could Disrupt Banking, 2018).

7.4.Internet of Things

One of the most advanced information and communication technologies is the internet of things (IoT) (ICT). IoT is "a network of networks of individually identifiable endpoints (or "things") that communicate utilising IP connectivity, whether locally or internationally, without human contact" (Lund et al., 2014, p. 2). Globally, the use of IoT-based services has been rising tremendously, especially in telemedicine, manufacturing, and urban areas to create smart cities. Many issues are resolved by IoT technology without the assistance of a human staff. Makhdoom et al., 2019; Kumar & Mallick, 2018). By 2020, it was predicted that IOT would link 30 billion devices (Lund et al., 2014).

IoT is a collection of numerous technologies that collaborate to achieve smartness; it is not a single technology (Kumar & Mallick, 2018). Lee & K. Lee (2015) emphasised the several complex technologies needed for the successful implementation of the IOT concept and the creation of IoT-based goods and services. These include wireless sensor networks (WSN), middleware, cloud computing, and Internet of Things application software. The Internet of Things has several uses. The common applications for RFID and near field communication (NFC) in telehealth include smart parking, smart homes and workplaces, smart grids and logistics management (Miorandi et al., 2012; Shah & Yaqoob, 2016).

7.5.Supply Chain Management Applications

Blockchain technology can improve supply chain systems' accountability and transparency (Ahram et al., 2017; Hewa & Liyanage, 2020). Better quality, results, and performance are made possible by blockchain in efficient supply chain management (SCM) procedures. Tracking data become unchangeable once they are added to a blockchain ledger. Due to the ability for all suppliers in the chain to track shipments, deliveries, and progress, blockchain fosters greater supplier trust. Due to the elimination of middlemen auditors, blockchain improves efficiency, reduces costs, and allows suppliers to perform their own checks and balances at any time (Koetsier, 2017; Kshetri, 2018; Pournader et al., 2020). The measurement of product quality during transportation can be improved via blockchain. Supply chain stakeholders, for instance, can identify whether a product was not in the proper location or was stored for an excessive amount of time simply by reviewing information on the shipping course and duration of the product.

When it comes to refrigerated items, which demand more particular and careful handling, these difficulties are crucial. This is how blockchain-based solutions may be used to guarantee the authenticity and calibre of goods (Kshetri, 2018).

8.LIMITATIONS OF BLOCKCHAIN

Because blockchain is a new technology, there are various difficulties in implementing and using it. The fact that people do not understand this technology or how it operates sufficiently is a barrier that needs to be overcome. Blockchain growth and acceptance are severely hampered by the complete lack of blockchain competence in many enterprises (Bizarro et al., 2018). There are still more blockchain-related problems that need to be solved. One has to do with the blockchain's scalability. Other obstacles to overcome are those related to legislation and security.

8.1.Lack of Awareness

Blockchain is a topic that is frequently discussed, but most people are unaware of its genuine benefits and how they may use it.

8.2.Limited availability of technical talent

These days, it's easy to find developers who have a wide range of skills across many industries. However, there aren't as many developers with specific knowledge in blockchain technology as there are in other fields. Therefore, it is difficult to construct anything on the blockchain due to a dearth of developers.

8.3.Immutable

We are unable to change any of the records in immutable. If you want to maintain a record's integrity and make sure that no one ever tampers with it, it is incredibly beneficial. However, immutability has a downside.

In the event that you decide to change anything or go back and make any reversals, we can understand this. For instance, you may need to go back and modify a payment that you have already processed.

8.4.Key Management

Since cryptography is the foundation upon which blockchain is built, it follows that there are many keys, including both public and private keys. When using a private key, there is also a chance that someone could misplace it and no longer have access to it. In the beginning, when bitcoin wasn't worth much, it frequently occurs. People would just accumulate a significant amount of bitcoin before forgetting the key, and those may now be worth millions of dollars.

8.5.Scalability

Similar to bitcoin, blockchains have consensus mechanisms that mandate that each participating node confirm the transaction. The amount of transactions a blockchain network can process is constrained by this. As a result, Bitcoin was not created to handle the massive numbers of transactions that many other organisations perform. The current maximum transaction rate for bitcoin is seven per second.

8.6.Consensus Mechanism

We are aware that a block can be created on the blockchain every ten minutes. It's because each transaction must guarantee that the consensus for every block in the blockchain network. The amount of time and resources required for *the back-and-forth communications necessary to reach consensus can vary greatly depending on the size of the network and the number of blocks or nodes involved in a blockchain.*

9.CONCLUSION

Because of its decentralised infrastructure and peer-to-peer nature, blockchain is a technology that has a bright future. Through its architectural features, the blockchain has shown its ability to simplify complicated procedures like transaction verification, reconciliation and settlement, and dispute resolution. Additionally, blockchain can revolutionise traditional business because to its essential features like distribution, anonymity, immutability, and audibility. Blockchain uses a decentralised consensus mechanism for transaction processing and validation because it was created to do away with the need for middlemen, notably in the world of financial transactions.

The most often employed consensus mechanisms by the current blockchain systems are PoW, PoS, PBFT, and DPoS. Initiated as a decentralised public ledger, blockchain has evolved into a number of different sorts of systems. A blockchain network could be consortium, private, or public. The selection of blockchain systems is influenced by important elements like investment capacity, privacy requirements, and objectives. For instance, financial institutions are more interested in private blockchains because they value the secrecy component. Companies who share similar objectives and activities, however, are more prepared to split costs and data and may use consortium blockchains.

Blockchain proved its value through cryptocurrency applications, but today its uses extend beyond the world of virtual money. As this study illustrated, blockchain may be used in a variety of industries with the similar properties, including advertising and media, energy, real estate, healthcare, and many more. The key advantages of blockchain—transparency, business continuity, disintermediation, and trust—have piqued the curiosity of these many businesses, and they have begun to investigate its potential and applicability.

We are seeing a lot of proposed smart contract applications in various fields as blockchain provides smart contract capability. We are all aware of how powerful blockchain technology can be in solving issues. But we are also beginning to notice some of the problems that blockchain is encountering, particularly in terms of scalability, security, and legislation. It is essential to overcome the blockchain's current constraints so that it becomes effective and more resilient.

10. REFERENCES

[1] "Who Owns Medical Records: 50 State Comparison." Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. Aug. 20, 2015. [Online] Available: http://www.healthinfolaw.org/comparative-analysis/whoowns-medical-records-50-state-comparison

[2] U.S. Department of Health and Human Services, Office of Civil Rights. (2013). 45 CFR Parts 160, 162, and 164. "HIPAA Administrative Simplification." [Online] Available: http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

[3] Office of the National Coordinator for Health Information Technology. (2015). Report to Congress. "Report on HealthInformationBlocking."[Online]Available: https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf

[4] "FHIR Overview." HL7 International. Oct. 2015. [Online] Available: https://www.hl7.org/fhir/overview.html

[5] "Fact Sheet: Obama Administration Announces Key Actions to Acclerate Precision Medicine Initiative." The White House Briefing Room. Feb. 25, 2016. [Online] Available: https://www.whitehouse.gov/the-press-office/2016/02/25/fact-sheet-obamaadministration- announceskey-actions-accelerate

[6] "InterSystems Unveils Major New Release of Caché." InterSystems. Feb. 25, 2015. [Online] Available: http://www.intersystems.com/who-we-are/newsroom/news-item/intersystems-unveils-majornew-release-cache/