Journal of Artificial Intelligence and Capsule Networks (ISSN: 2582-2012)
www.irojournals.com/aicn/

A Brief Analysis of Smart Contracts and Applications of Blockchain Technology

Rishi Matura[1], Kunal[2]

Computer Science Engineering, Chandigarh University, Mohali, India

E-mail: [1]rishimatura27@gmail.com, [2]Kunalsingla009@gmail.com

Abstract

Blockchain refers to a distributed system or ledger that is shared via a computer network. For storing data, a blockchain serves as a digital database. The most well-known use of Blockchain technology is to maintain a secure and impartial record of every transaction made using Bitcoin and other types of cryptocurrency. By assuring the security and integrity of a data record, a blockchain encourages confidence without the need for a trustworthy third party. This paper discusses the various aspects and implications of Blockchain technology in modern society.

Keywords: Blockchain, system, database, digital, cryptocurrency, Bitcoin, smart contract

1. Introduction

Back in 2008, a mysterious person known by the alias Satoshi Nakamoto initially introduced the ideas of Bitcoin and Blockchain, outlining how a digital money application may be made using encryption and an open distributed ledger [1]. The incredibly high volatility of bitcoin and the perceptions of many nations regarding its intricacy slightly slowed down its development, but the benefits of blockchain, the technology that underpins bitcoin, drew more and more attention. The distributed ledger, decentralization, information exchange, impenetrable design, and accessibility of blockchain are some of its benefits [2]. The unison of a preponderance of the system's consumers verifies all transactions on the public ledger through people called miners. Additionally, information/digital data cannot be manipulated once it is fetched in the network. Every transaction ever made is contained in a particular verifiable record on the blockchain. To take a simple comparison, it is simpler to steal candy from a

DOI: https://doi.org/10.36548/jaicn.2023.1.004
Received: 07.02.2023, received in revised form: 07.03.2023, accepted: 22.03.2023, published: 01.04.2023

container maintained in a secret location than it is to do the same in a public space where hundreds of people may see you.

Figure 1. Blockchain Insights [3]

The most well-known example of a Blockchain technology-related product is Bitcoin [3]. It is also said that Blockchain was initially created to support the movement of bitcoin and keep it secure. It's also more problematic since it helps to create an anonymous, multimillion-dollar industry independent from any authority of any state or nation throughout the world. Henceforth every government institute has tried to tie it down with scores of regulations [4]. However, the technology behind blockchains is not debatable; it has operated without a hitch for years and is now being effectively used in both monitory [5] and non-pecuniary applications [6]. Not a long ago, the Blockchain distributed agreement model was cited as the most significant invention, since the Internet itself, by Marc Andreessen, the dean of Silicon Valley investors. In the Quintessence magazine [7], Johann Palychata from BNP Paribas presented that the blockchain, the program that powers bitcoin should be seen as a breakthrough with the potential to change other industries, comparable to the steam or combustion engine. The truth is that by entrusting a third unknown party to safeguard the privacy and security of digital assets, people live dangerously in the digital world. It is nonetheless a truth that these external sources are susceptible to hacking, manipulation, and compromise. Blockchain technology is useful in this situation. Establishing a distributed agreement where any online pact, present, and past, including virtual assets, may be fixed at any moment in the time ahead, has the capability to wholly change the virtual environment. It achieves this without compromising the privacy of the parties or digital assets. Anonymity and decentralized consensus are two crucial aspects of Blockchain technology.

Figure 2. Blocks of data in a blockchain [7]

The foundation of the ongoing digital thrift is its dependence on a recognized authority. All online transactions depend on the belief that the people dealt with, speak the truth. This may be an electronic mail provider confirming that an email has been received or an enfranchisement body confirming that a specific digital object is genuine. Alternatively, a social media company like Facebook may inform the user i.e., that his posts are reliable by using a trust-worthy certificate relating to his life events that have only been disclosed to his pals, or a bank may inform the user that his loved ones are in a faraway nation have dependably received the money.

The high volatility of bitcoin and the complexity of its technology slowed down its development. The anonymous and decentralized nature of blockchain technology has made it difficult for governments to regulate it. The reliance on trusted third parties to safeguard the privacy and security of digital assets has made the digital world vulnerable to hacking and compromise. Blockchain technology has the potential to change various industries, but its adoption may face some challenges due to the resistance to change and the need for regulatory frameworks. The use of Blockchain technology in both monetary and non-monetary applications has introduced new possibilities and opportunities.

2. The History of Blockchain

In 2008, a person named Satoshi Nakamoto proposed the concept of the fundamental decentralized Blockchain. By storing blocks without needing that a foreign entity signs them, the developer significantly enhanced the architecture. To date, no one knows the real identity of Satoshi Nakamoto. A few months later, a 50-coin Genesis block-based open-source application was made available and implemented, and the new protocol was made available. Installing this open-source tool enables anyone to join the peer-to-peer Bitcoin network. Since then, it has become more well-known. Table 1 given below shows how Blockchain technology progressed through the years [8].

Table 1. Events that led to the rise of blockchain [9]

Year of interest	Event
1991	Dr. S. Haber and Dr. Scott report the first series of blocks that is cryptographically protected
1998	Dr. N. Szabo develops the decentralized virtual currency "bit gold"
2000	Dr. S. Konst releases his theory of cryptographically secured chains along with suggestions for use
2008	Developers using the alias Satoshi Nakamoto, published a white paper outlining the framework for a blockchain
2009	Satoshi establishes the rudimentary blockchain as an open-source database for Bitcoin proceedings
2014	The prospective blockchain mechanism for other monetized and organizational transactions are reviewed once the money component has been removed. Blockchain 2.0 emerges, alluding to uses outside of cash.

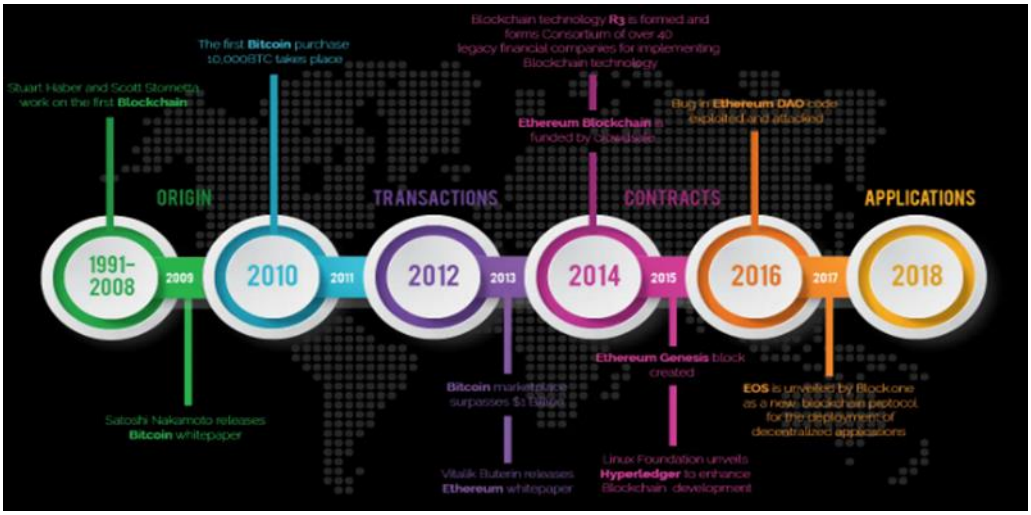

Figure 3. The history of Blockchain throughout the years [10]

3. Structure of a Blockchain

The foundational component of the Bitcoin Blockchain is transaction, broadcasting, and the validation of transactions. A block is made up of many transactions, and a chain of boxes is connected by a digital data connection. To decide which block will be the next to be added to the chain, blocks go through a unison procedure. The chosen block is examined before being added to the running chain. The consensus and validation procedures are taken care of by

specialized users known as miners. They are strong machines running the blockchain protocol software [11].

An Unspent Transaction Output, or UTXO, is a key idea in the Bitcoin network. The state of the Bitcoin Blockchain was defined by a collection of all Unspent Transaction Outputs in a Bitcoin web. UTXOs are referred to be in an agreement as inputs. Unspent Transaction Outputs are outputs produced as part of a transaction. The participant nodes store all the UTXOs in a system database. According to the request made by the sender, the transaction takes the quantity provided by one or more than one UTXO and transfers it to at most one recently generated output UTXO. A particular UTXO has a fairly straightforward construction. The UTXOs unique transaction identifier, an index (where it appears in the transaction output list), and value (how much it is good for) are all included. And a permissive script that specifies the circumstances refers to one or more previously created inputs, a reference number for the current agreement, Unspent Transaction Outputs, references to one or more previously generated output UTXOs, and the total input and output amounts are all included in the transaction itself.

The word "blockchain" comes from the manner that maintains transaction data in blocks connected by links to form a chain. The blockchain expands as transactions are made. The timing and order of transactions are recorded and confirmed in blocks, which are subsequently added to the blockchain and regulated by the rules established by the network's users. Each block includes the preceding block's hash, timestamped bundles of current, legitimate transactions, and a hash (a digital fingerprint or unique identification). A block cannot be changed or put between two existing blocks because of the prior block hash, which connects the blocks. The process makes Blockchain impervious to tampering, in principle.

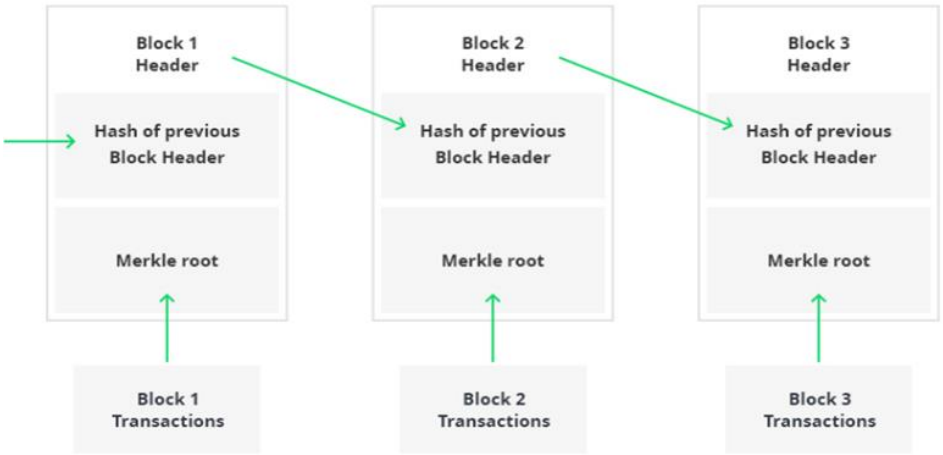

Figure 4. The architecture of a Blockchain [12]

In a transaction using blockchain, there are two major participants. Respondents, known as miners, who choose to perform additional toil which include calculation to confirm transactions, broadcasting transactions, contending for the right to produce a block, working to achieve an agreement by validating the block, broadcasting the recently formed block, and competing for the right to construct blocks, and the other who initiates a value transfer by creating a transaction. Bitcoins are used as compensation for the miners' work maintaining the network. Through blockchain research and forfeiture, the US federal authorities were able to confiscate part of the bitcoin used by the lawbreaker operation Silk Road, which used to run on a dark web browser.

4. Applications of Blockchain Technology

4.1 Cryptocurrency

Most cryptocurrencies record transactions using Blockchain technology. For instance, blockchain is the foundation of both the Ethereum network and the Bitcoin network [9][10]. On May 8, 2018, Facebook announced that David Marcus, who formerly oversaw Messenger, will lead a brand-new blockchain group. On June 18, 2019, Facebook publicly unveiled Libra (now called Diem), their next cryptocurrency platform.

Figure 5. Cryptocurrency in Blockchain [13]

4.2 Smart Contracts

Smart Contracts are one of the numerous benefits of bitcoin. Automated escrow is one of a smart contract's primary goals [11][12]. The contract is carried out by the blockchain network by itself, with smart contracts eliminating the requirement for an entrusted third party (such as an agent) to function as a mediator among the involved parties. This may make it easier for entities to move value with less friction, which might then pave the way for more advanced transaction automation. According to a 2018 IMF staff debate, blockchain-based

smart contracts may lessen jeopardy and improve the usage of agreements. However practical smart contract solutions are yet to be derived.

4.3 Insurance

Blockchain may be used to register assets that can be uniquely identifiable by one or more IDs that are challenging to copy or delete. This may be used to trace the history of transactions as well as confirm who owns an asset. Any item (intact or virtual, including properties, cars, assets, computers, and other goods) [14] may be recorded in the blocks, and the proprietary rights and agreement history could be verified by anybody, particularly insurance.

Figure 6. Blockchain in the Insurance sector [14]

4.4 Logistics

A new decentralized and transparent transaction mechanism in business and industry is made possible by Blockchain technology [15]. Through openness in all data, products, and financial transactions, this technology's features build trust. Blockchain technology makes it simple to offer safe company logistical operations. The technological platform generates a continuous mark that can be distributed and is open to the public and is built on a decentralized approach.

4.5 Healthcare

According to the analysis [16][17], there are several applications for Blockchain in the medical sector, including the administration of electronic medicinal accounts, the control of medication research, distant patient monitoring, and health data analysis.

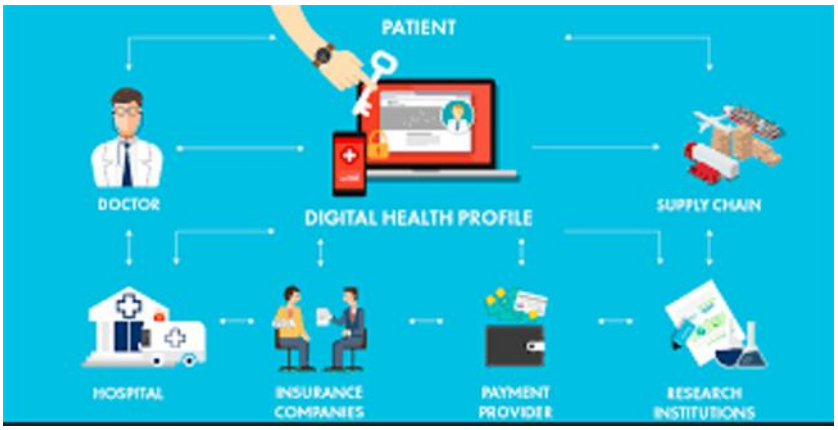

Figure 7. Blockchain in the Healthcare sector [16]

Numerous healthcare applications based on blockchain are available based on new advancements in the field including blockchain, smart contracts, etc. To comprehend, define, and assess the value there has to be more research done on the use of Blockchain technology in healthcare more thoroughly.

4.6 Accounting

In comparison to other industries, some of which have been significantly impacted by the developments of Blockchain technology, the digitalization of the accounting system is still in its infancy [17]. By lowering maintenance costs, offering a highly secure environment, and reconciling ledgers, auditors expand the potential of the accounting profession by using blockchain to improve audit efficiency [Swan (2015)]. Traceable audit trails, automated accounting and reconciliations, asset ownership tracking, and transaction authentication are all made possible by Blockchain.

A tabulation highlighting the applications of Blockchain technology, along with its role in each application, challenges, and advantages is given below.

Table 2. Applications of blockchain and its challenges and advantages

Application	Role of Blockchain	Challenges	Advantages
Banking and Finance	Secure transactions, reducing the risk of fraud	Integration with legacy systems, regulatory compliance	Transparency, reduced transaction costs
Supply Chain Management	Enhanced traceability, reducing counterfeiting	Implementation costs, integration with legacy systems	Improved efficiency, reduced fraud
Healthcare	Secure and transparent data sharing, protecting patient privacy	Regulatory compliance, interoperability with existing systems	Improved patient outcomes, reduced costs
Real Estate	Secure transactions, reducing fraud	Lack of standardization, integration with existing systems	Faster transaction times, reduced costs
Voting	Secure and transparent voting process, reducing fraud	Lack of standardization, scalability	Improved trust in the voting process, increased voter turnout
Digital Identity	Secure and decentralized identity management, protecting personal data	Adoption, interoperability with existing systems	Increased privacy, reduced identity theft

5. Smart Contracts

Smart Contracts are one of the numerous benefits of Bitcoin. The main distinction between smart contracts and traditional contracts is that smart contracts are entirely digital [8]; in reality, they are computer programs that are recorded in blockchain. A smart contract does away with the need for a third party to validate an agreement.

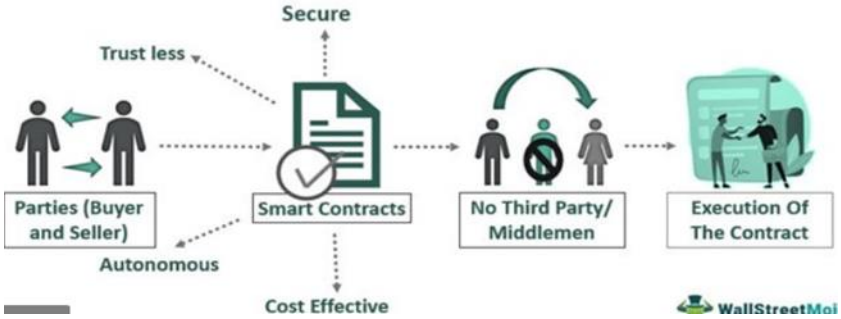

Figure 8. Diagramatic explanation of smart contracts [17]

For instance, if firm A needs to raise money from the public for a project, it may make smart contracts that can hold the money in reserve until the objective is met. Now, in this scenario, the smart contract may keep donations made by the donors and send the money to the business when a particular objective is met. However, if a circumstance arises where the objective is not reached, then the program redirects the funds back to the donors.

Smart contracts inherit certain intriguing qualities from being recorded in a blockchain, such as being immutable and distributed. A smart contract cannot be altered after it has been formed since it is immutable. Additionally, because the contracts are distributed, everybody in the network must check their output, making it nearly difficult to tamper with them. Smart contracts are not just useful for crowdfunding; they can be used for many different purposes. It can be used by banks, for instance, to offer automated payments or make loans. It can be used by insurance firms to handle some claims. It might be used by postal services for cash on delivery and other purposes.

There are now a few blockchains that enable smart contracts, but Ethereum is by far the most popular. It was constructed with the support of smart contracts in mind. Solidity is a unique programming language that may be used to create smart contracts. The grammar of this language, which was developed especially for Ethereum, is similar to JavaScript. Also worth mentioning is that while Bitcoin has enabled smart contracts, its capabilities are far more constrained than those of Ethereum.

Smart Property:

Another similar idea is smart property, which involves utilizing smart contracts on the blockchain to manage ownership of a building or other asset. The asset might be materialistic (like a car, a house, a phone, etc.) or can be immaterial (like shares in a company).

Perception of Blockchain Technology:

Banks and investment organizations no longer consider Blockchain technology to be a danger to current company procedures. The major banks in the world are investigating cutting-edge blockchain technologies to find potential in this space. Rain Lohaus of the LHV bank in Estonia recently stated that for several banking and finance-related applications, blockchain is considered to be the most tried-and-true and safe technology. This paper focuses on the various implications of Blockchain technology on the current stature of markets across the globe. This emergence in the field of the digital economy can very well revolutionize the way one perceive the society, and economy, shortly.

6. Discussion

In the research area, Blockchain technology is a new topic for researchers. The summarized data for the five primary blockchain publication sources, is shown in Figure 10. The number of blockchain papers released in each of these five sources was taken into account when compiling the list. In comparison to other sources, IEEE access has distinguished itself with a sharp growth until 2020. While their quantity has decreased in sources like Sensors Switzerland and the Journal of Physics Conference Series, publications tend to rise in Sustainability Switzerland and Applied Sciences Switzerland.

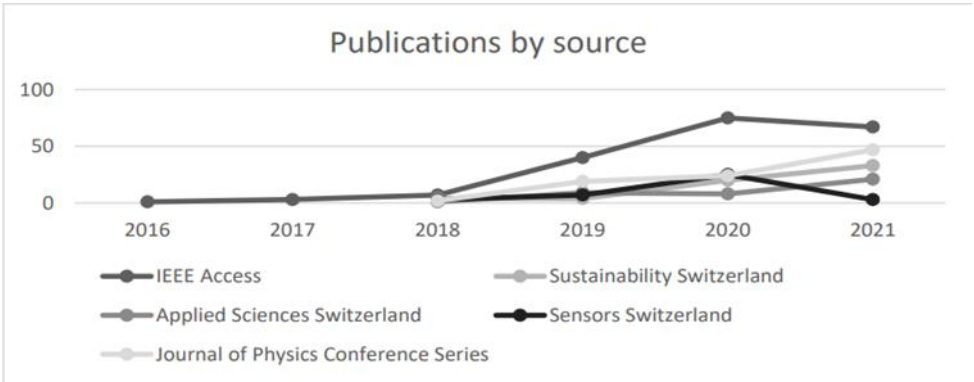

Figure 9. Number of Publications [17]

7. Conclusion

This review paper has discussed various aspects of Blockchain technology and its implication in modern society. Moreover, how its perception changed in the eyes of the masses as well as modern-day billionaires, and how since its inception is on the rise in the global

market, have been summarized. As studied, it is used in various fields like insurance, cryptocurrency, the accounting sector, and drafting smart contracts. This technology carries various advantages with it like secure and traceable transactions, more efficiency, more transparency, and faster transactions. And according to the research, technology will be on the rise in the near future.

References

[1] Ahram, T. et al., (2017). Blockchain technology innovations. 2017 IEEE Technology & Engineering Management Conference (TEMSCON) (Jun. 2017), 137–141.

[2] Yli-Huumo, J.; Ko, D.; Choi, S.-J.; Park, S.; Smolander, K. Where Is Current Research on Blockchain

[3] Romano, D.; Schmid, G. Beyond Bitcoin: A Critical Look at Blockchain-Based Systems. Cryptography2017,1,15.Technology?—A Systematic Review. PLoS ONE 2016, 11, e0163477.

[4] Wang, H.; Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X. Blockchain challenges and opportunities: a survey. IJWGS2018, 14, 352.

[5] Adams, R.; Parry, G.; Godsiff, P.;Ward, P. The future of money and further applications of the blockchain.Strat. Change 2017, 26, 417–422. [CrossRef]

[6] Forrest P., (2016). Blockchain and non-financial services use cases.

[7] Ashta A, Biot-Paquerot G (2018) FinTech evolution: strategic value management issues in a fast changing industry. Strategic Change-Briefings in Entrepreneurial Finance 27(4):301–311.

[8] Fanning, K. & D.P., Centers, (2016). Blockchain and Its Coming Impact on Financial Services", Journal of Corporate Accounting & Finance, 27(5), pp. 53–57.

[9] Hassani, H.; Huang, X.; Silva, E. Big-Crypto: Big Data, Blockchain and Cryptocurrency. BDCC 2018, 2, 34.

[10] Glaser, F. & Bezzenberger, L., (2015). Beyond Cryptocurrencies—A Taxonomy of Decentralized Consensus Systems. 23rd European Conference on Information Systems, Munster, 1-18.

[11] Savelyev S. (2017). Contract law 2.0:‘Smart’contracts as the beginning of the end of classic contract law. Information & Communications Technology Law.

[12] Peters, G.W.; Panayi, E. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. SSRN J. 2016, 1, 239–278.

[13] Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J. Med. Syst. 2018, 42, 130.

[14] Gatteschi, V.; Lamberti, F.; DeMartini, C.; Pranteda, C.; Santamaria, V. Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? Future Internet 2018, 10, 20.

[15] Gstettner, Stefan (30 July 2019). "How Blockchain Will Redefine Supply Chain Management". Knowledge@Wharton. The Wharton School of the University of Pennsylvania. Retrieved 28 August 2020.

[16] Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain Technology Applications in Health Care.Circ. Cardiovasc. Qual. Outcomes 2017, 10, e003800.

[17] Tapscott, D., & Tapscott, A., (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World. New York, NY: Penguin Random House.