Blockchain Technology and Decentralized Applications Using Blockchain

Mohd. Osama Iqbal, Ahmed J. Obaid, Parul Agarwal, Tabish Mufti, and Ahmed R. Hassan

Abstract A blockchain is a collection of blocks, each of which contains a set of transactions that are verified using an encryption algorithm. The blocks are constantly adding to each other, forming a chain of blocks. Blockchain technology is widely used for security and smart contracts, financial and non-financial spheres, a large variety of blockchain systems are used. Decentralized applications (DApps) are in their early stages of development, and several critical issues which services, the Internet of Things (IoT), healthcare services, and supply chain to name a few. This paper throws light on several aspects of blockchain technology, the linkage between blockchain and DApps. It also illustrates working of blockchain transaction process and Ethereum transaction. It also elaborates on the working of smart contracts. Furthermore, this paper also discusses the making of decentralized application in detail and enlighten the architecture of DApps. Moving ahead this paper also discusses the implementation of DApps in various sectors in industry like health care, banking and stock market. It also puts light on the challenges of implementing decentralized application in the present centralized market and its scalability as well. We have also discussed the future of decentralized application and its growing market demand due to its various unique features. The actual user interaction in the projects is exceedingly small: in fact, even the five major applications in any sector, be it games or exchanges, have roughly over 1 k users. However, the marketplace for DApps is expected to increase substantially in the near future.

Keywords Blockchain · Decentralized applications · Blockchain applications · Ethereum · Smart contract

Mohd. O. Iqbal · P. Agarwal (✉) · T. Mufti
Department of CSE, Jamia Hamdard, Hamdard Nagar, New Delhi-62, India
e-mail: pagarwal@jamiahamdard.ac.in

A. J. Obaid
Faculty of Computer Science and Mathematics, University of Kufa, Kufa, Iraq

A. R. Hassan
National University of Science and Technology, Nasiriyah, Iraq

M. Tuba et al. (eds.), *ICT Infrastructure and Computing*, Lecture Notes in Networks and Systems 520, https://doi.org/10.1007/978-981-19-5331-6_57

1 Introduction

Blockchain enables peer-to-peer digital asset transfer without the use of intermediaries [1]. Blockchain was designed to aid in the development of a very well-acknowledged Cryptocoin Bitcoin. Bitcoin as a Cryptocoin was first conceived in 2008, and it was first used in 2009, thanks to the work of Satoshi Nakamoto [2]. The chain continues to develop as additional chunk blocks are added to it. Blockchain operates in a decentralized environment, which is made possible by the use of a number of core technologies, including virtual signatures, cryptographic hashes and allocated consensus methods. Decentralization, privacy, immutability and auditability are just a few of the major qualities of blockchain [3].

DApp allows developers to create applications that are completely open to users and run independently of any external body. To abstain from a single point of system failure, the contents and code of that program are stored securely and controlled by a decentralized blockchain. This represents a DApp's overall architecture.

The data is kept on the Ethereum blockchain system under this design. Smart contracts are used to construct the application logic, which is then published and controlled on the blockchain. EVM is in charge of executing any smart contract code in this case [4].

In this architecture, the smart contract functions as the backend. The code for this backend is saved on, handled and operated by the blockchain, which makes it completely decentralized. The user must contact a blockchain network node in the ability to engage with the smart contract. If a node goes down, other nodes are notified and substituted for that node. In addition, the Ethereum-based DApp profits from ETH, a cryptocurrency. This coin can be used to create financial applications or to quickly include monetary activities into DApps [5].

The paper is structured as follows: Section 2 throws the light on the background process of the blockchain technology live various transaction processes and smart contracts. Section 3 discusses the decentralized application in detail and its various uses in different industries. Section 4 puts light on the making of decentralized application and building its core architecture. Section 5 illustrates the challenges of decentralized application in current market which in centralized in nature. Section 6 discusses the future of decentralized application and its growing demand due to various unique feature. Section 7 provides the limitations of the decentralized applications. Section 8 provides the conclusion while discussing some aspect of decentralized application and its use in present market and in different industries.

2 Background Review

A node in a decentralized blockchain network initiates a transaction by creating a digital signature using private key cryptography. A transaction on the blockchain network is a data structure that reflects a digital asset exchange between peers. When

the miners have verified and validated the transaction, it is put in a block. Miners are people who pool their computing power to search for blocks [6].

2.1 Blockchain Transaction Process

A blockchain transaction is a small portion of a larger operation that is recorded in a public ledger. These data are also known as blocks [7]. These chunks are then created, implemented and recorded here on blockchain for every miner to see and verify. The status of any past transaction can be examined at whatever time, but it cannot be changed [8]. Blockchain processing and voting solutions that primarily use a hashing algorithm can be used to address security concerns. The SHA-256 algorithm, for example, is indeed a 256-bit cryptographic hashing algorithm used by Bitcoin. Words, digits, letters, or maybe a system-generated document of any type can be created from any type of data. Bitcoin may generate 256 bits or 64 bytes output.

2.2 Ethereum Transaction

Ethereum brought the theory of an institution as a protocol component that acts as both the sender and receiver of a transaction. As a result, transactions directly change account balances rather than retaining state. In Bitcoin, UTXOs allow for the movement of responsibilities, information and data between accounts, which can give outcome as state transitions [9]. Ethereum has similar properties to Bitcoin, such as the preceding block hash, nonce and transaction data. All produced transactions will be checked by looking at the time stamp, nonce combination, and whether there are adequate fees for execution.

2.3 Smart Contracts

Smart contracts comprise software programs that run on the Ethereum platform. They, like vending machines, can enforce some sorts of contracts between participants, even though they have no fundamentally direct relationship with legal contracts.

An Ethereum smart contract had already grown in popularity to the point where it has supplanted the term's original definition, resulting in a number of misinformation about what blockchain can do. What is the significance of the term "contract"? It was created with the goal of serving as a kind of settlement across parties [10].

3 Decentralized Applications (DApps)

Decentralized applications are frequently referred to as a trustless network with the distinction that they are not controlled by a single server or organization, as in a client–server model. We recognize the smart contract's appealing features and the platform's adaptability.

However, it is necessary to evaluate what goes into a modern centralized application in order to grasp it.

3.1 What Distinguishes a DApp from a Centralized Application?

A commonly modernized software application that must include at least one user interface (UI), such as a mobile application downloaded from an android market, a blog (opened from just a smart device), or a desktop application installed on a computer network. In most cases, data is involved. This information could come from a single source, such as a weather application that incorporates data from a national weather organization. Finally, it necessitates database operations or computation [11].

The blockchain is at the heart of a DApp's processing and storing of data. A smart contract is used to do this. A typical website model is currently used to construct the UI for a DApp. As a result, a fully functional DApp can be compared to a website that contains one or more smart contracts. The fundamental difference seems to be that the blockchain is responsible for both data and processing [11].

3.2 Decentralized Application and Blockchain

The following examples given are some of the benefits of utilizing blockchains decentralization for DApps:

Before calling a function or providing any data, the client will see what would happen.

1. An interaction cannot be retracted, tampered with, or erased once it has been done by the user. These characteristics are useful in and of themselves. At the protocol level, this embodies decentralization. This, on the other hand, promotes another sort of decentralization, which is a major motivation for DApps:
2. Administration can be decentralized, allowing application users to directly engage in its management. Another of the more well-known decentralized applications is CryptoKitties. It's an Axiom Zen game in which users can trade, nurture, acquire and sell digital cats. In CryptoKitties, these digital items are

stored on the blockchain [12]. The decentralized autonomous organization (DAO) is another example of a DApp.

3.3 The Case for DApps

In the DApp sector, a variety of applications are being pursued. So far, they've generally fallen into the following categories:

- Initial Coin Offerings (ICOs)
- Exchanges and marketplaces
- Know your customer (KYC) & Anti-money laundering (AML)
- Banking and accounting services
- Games are just a few examples.

We'll look at a few of these applications presently. In a preliminary decentralized application environment, the major obstacle is entry to just provide finance or securities operations like a bank or stock exchange is high. The regulatory compliance, staffing, infrastructure and institutional linkages that are required to run a business are enormous. Anyone with the ability to write programs can use a smart contract-based framework to create a system that safely maintains large amounts of assets, with deposits regulated by publicly available computer code. In 2016, an enterprising software developer called EtherDelta established a successful Bitcoin exchange [13]. At its peak, the exchange smart contract contained more than a billion dollars in ETH and tokens. A few applications of DApps are mentioned below:

Health care—The use of decentralized blockchain technology has the potential to revolutionize health care. One of the main priorities in the healthcare business is maintaining patient data security.

Energy Industry—Microgrids are by far the most often used blockchain applications in the energy sector. Blockchain can also be used in microgrids to ease, register and confirm transactions between power buyers and suppliers.

Stock Market—Connectivity, reliability and integrity are all difficulties that decentralized market systems face. Blockchain technology may be successful in overcoming these issues. It can improve the stock exchange's efficiency by decentralizing and automating it.

Voting—Blockchain may be used in a variety of fields to solve problems that a traditional database could have. Voting is one example of such an issue. It recently came in the knowledge that a major voting machine vendor in the USA had placed different remote support software with some of its machines.

Insurance—Insurance businesses can utilize the blockchain to negotiate, buy, and register policies, file and handle claims, and assist reinsurance activities.

Identity Management—Self-identity can be validated in the real-world using identification credentials like a driver's license, ID card or country passport. Djuri Baars et al. propose a new self-sovereign decentralized identity management architecture based on blockchain technology (Table 1).

Table 1 Applications of decentralized applications in various sectors

Description	References
Health care	[14]
Energy market	[15]
Stock market	[16]
Voting	[17]
Insurance	[18]
Identity management	[19]

4 Making of Decentralized Application (DApps)

Most of those technologies being used to construct and use DApps are still in their infancy. To engage with just a DApp like a user, you'll need a way to create and maintain a network identity. In a typical application, access credentials (username and password) are stored on a server. In a DApp, your account is a cryptographic hash key recorded on your local hard drive or in your smartphone's memory. There are gadgets that can help you keep track of your keys. The most useful methodology for controlling DApp (Ethereum) profiles and communicating with DApps is MetaMask, a browser plugin for Chrome, Firefox and Opera.

Furthermore, the revolutionary DApp framework, which includes icons, words and actions, may be confusing to new users. Other popular web-based wallets, such as MyEtherWallet, allow you to conduct transactions without downloading any software [4].

However, instead of just interacting with DApps, it is primarily meant for dealing with Ethereum as a coin. To contact a DApp, you must repost obscure programming language into the web form. Solidity is a suite of tools for software developers that includes implementation tools (IDEs) like Remix, checking mechanisms like Truffle and Ethereum's fundamental programming language.

5 Challenges in Decentralized Application (DApps)

5.1 Obligation of Laws

Regulatory frameworks are essential considerations when creating various applications that wish to transfer to the blockchain. Let's take a look at several of the realtor tokenization cases. If Alice provides Bob a token that represents a share in a piece of Tokyo real estate, these transactions can take place in a way that is guaranteed and verified by the technology. Bob may see if he pays the price, and if he does, the token will be handed to his possession. Nothing can make Alice refuse to hand over the tokens or Bob refuse to pay. In this case, the blockchain takes the position of

a reliable party's escrow service. It's doesn't, however, negate the reality that rules tying a portion of the property to a digital token are required [20].

5.2 Scalability

Ethereum, Bitcoin, emerged spontaneously as a test. The demands for technology increase as even more people connect to the network. The system's scalability refers to its ability to fulfil those rising demands. Understanding the pricing model surrounding transaction and block formation is helpful in framing the concerns of scalability. The current goal block formation time is 12 s between blocks, which is a balance among security, efficiency and actual network limits. The main problem of mining difficulty is automatically changed by the Ethereum network and software as mining power is added or detachment from the network to maintain this pace.

The following are some of the most important aspects of scalability:

- Transaction processing speed
- Cost of computation
- Data archiving.

6 The Future of Decentralized Application (DApps)

We've focused on Ethereum, but there are variety of other competing technologies under development, among which Ethereum is there. But not all of those innovations will catch on. We anticipate some of these conflicting and redundant systems to merge in the months and years ahead of blockchain innovation. Polkadot, for example, is a platform that combines and connects many blockchains and subnetworks. The use of blockchain with IoT in transforming the education sector can also be done [21]. Under a shared security mechanism, Bitcoin and Ether could trade with one another.

7 Limitations

Apart from several advantages, there are certain limitations too. Due to those major limitations, the adoption of culture of decentralization of applications is slow. Some major limitations are given.

Maintenance issue—Maintenance is quite tough in decentralized application as the code when published is hard to modify for updates and error.

Performance overhead issue- Performance overhead is quite a bit and scaling decentralized application is quite tough. The output that Ethereum is looking is quite tough to get.

Network congestion issue- Currently, there is slow transaction rate which is about 10–15 s per transaction due to lack of users.

8 Conclusion

Applications have grown into DApps as a result of blockchain technology. DApps are superior to standard applications in that they have the ability for becoming self-sustaining resources by enabling stakeholders to contribute in DApp development. DApps will be favoured over presently offered traditional applications for a variety of purposes in the near future, including payments, storage, cloud computing and so on. The adoption of blockchain is unavoidable, and many present processes will become obsolete as a result. Banking services are already preparing to implement blockchain in the near future, which will enable them to operate with trustless, self-sustaining and decentralized networks.

References

1. Aste T, Tasca P, Di Matteo T (2017) Blockchain technologies: the foreseeable impact on society and industry. Computer 50(9):18–28
2. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Decentralized Business Rev 21260
3. Kouhizadeh M, Sarkis J (2018) Blockchain practices, potentials, and perspectives in greening supply chains. Sustainability 10(10):3652
4. Farnaghi M, Mansourian A (2020) Blockchain, an enabling technology for transparent and accountable decentralized public participatory GIS. Cities 105:102850
5. Six N, Herbaut N, Salinesi C (2022) Blockchain software patterns for the design of decentralized applications: a systematic literature review. Blockchain: Res Appl 100061
6. Kroll JA, Davey IC, Felten EW (2013) The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: Proceedings of WEIS, vol 2013(11)
7. Tschorsch F, Scheuermann B (2016) Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun Surv Tutorials 18(3):2084–2123
8. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData congress), pp 557–564
9. Wood G (2014) Ethereum: a secure decentralized generalised transaction ledger. Ethereum Project Yellow Paper 151:1–32
10. Mohanta BK, Panda SS, Jena D (2018) An overview of smart contract and use cases in blockchain technology. In: 2018 9th international conference on computing, communication and networking technologies (ICCCNT), IEEE, pp 1–4
11. Casino F, Dasaklis TK, Patsakis C (2019) A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics Inform 36:55–81
12. Metcalfe W (2020) Ethereum, smart contracts. DApps. Blockchain and Crypt Currency, pp 77
13. Nguyen H, Pham T, Nguyen T, Do N, Nguyen H (2019) KardiaChain-the first decentralized interoperable and self-optimised blockchain ecosystem
14. McGhin T, Choo KKR, Liu CZ, He D (2019) Blockchain in healthcare applications: Research challenges and opportunities. J Netw Comput Appl 135:62–75

15. Lasseter RH, Paigi P (2004) Microgrid: a conceptual solution. In: 2004 IEEE 35th annual power electronics specialists conference (IEEE Cat. No. 04CH37551), vol 6. IEEE, pp 4285–4290
16. Lee L (2015) New kids on the blockchain: How bitcoin's technology could reinvent the stock market. Hastings Bus LJ 12:81
17. Pawlak M, Poniszewska-Marańda A (2021) Trends in blockchain-based electronic voting systems. Inform Process Managem 58(4):02595
18. Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V (2018) Blockchain and smart contracts for insurance: is the technology mature enough?. Future Internet 10(2):20
19. Tan E, Mahula S, Crompvoets J (2022) Blockchain governance in the public sector: a conceptual framework for public management. Government Inform Quart 39(1):101625
20. Fatima N, Agarwal P, Sohail SS (2022) Security and privacy issues of blockchain technology in health care—a review. ICT Anal Appl 193–201
21. Agarwal P, Idrees SM, Obaid AJ (2021) Blockchain and IoT technology in transformation of education sector. Int J Online Biomed Eng 17(12)