IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005144|

Review on Functional Block chain Approach towards Approximation Problems in Commerce

Shivani Sharma, Pallavi Shahane, Sanchana Pawaar, Priya Lingot, Vaishanavi Suple, J.S.Wankhade

Department of Computer Science Engineering, P. R. Pote Patil College of Engineering and Management, Amravati, Maharashtra, India

ABSTRACT: Blockchain-based technologies are predicted as major disruptors for numerous business applications and processes, which bears huge implications for ecommerce. Given the ability of blockchain and related technologies to create socalled "trustless systems" with idiosyncratic properties, various business models and established processes that have emerged over the years to ensure trust, reliability and enforceability in business-to-consumer (B2C), business-tobusiness (B2B), business-to-government (B2G) and consumer-to-consumer (C2C) relations need to be questioned and potentially adjusted. Blockchain has the potential to shake the foundation of e-commerce by enabling exchange relations that are trustless and operate without dedicated intermediaries or even central authorities in the case of permissionless blockchains. Furthermore, the exchange of information and value between companies and consumers might change considerably by enabling unified access to immutable data along the entire supply chain. In this paper, a framework and 19 high-level research questions are developed to inspire researchers to closely investigate the potential impact of blockchain on e-commerce. The main categories include (a) technological, (b) legal and (c) organizational and quality issues as well as (d) consumer issues. This paper illustrates how blockchain potentially impacts different elements of e-commerce in these respective areas.

KEYWORDS: Blockchain, Distributed Ledger Technology, E-Commerce

I. INTRODUCTION

Blockchain was invented by a person using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The identity of Satoshi Nakamoto is unknown. The invention of the blockchain for bitcoin made it the first digital currency to solve the doublespendingproblem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains that are readable by the public are widely used by cryptocurrencies. Blockchain is considered a type of payment rail. Private blockchains have been proposed for business use. Sources such as Computerworld called the marketing of such blockchains without a proper security model. however the nodes of a blockchain are logically centralized, as the entire blockchain is a distributed network performing certain actions programmed into it. so much time and effort is currently wasted on identity verification. using the decentralization of blockchains, the verification of online identity will be much quicker. online identity data in a central location will vanish with the use of the blockchain smart contracts. computer hackers will no longer have centralized points of vulnerability to attack. data storage is tamper-proof and incorruptible when backed by blockchain. all over the world, the blockchain is leading to big improvements in the verification of identity. The city of zug in switzerland uses a decentralized application (dapp) for the verification of its citizens' electronic identities. another producer of dapps, for identity verification is oraclizein estonia. it markets a dapp to solve the kyc (know your customer) problem. Blockchain technology is a revolutionary computer protocol used for digital recording and storing information on multiple computers or multiple nodes. One of the most important elements of Blockchain is the so-called
"Ledger", which is similar to a relational database. A Blockchain is a list of encrypted digital record or transaction, called a block. Each block is then "chained" to the next block, in a linear, chronological order, using a cryptographic signature. The blocks contain a copy of the last transactions since the last block was added. Thus, the shared block, or ledger, is linked to all participants who use their computers in a network to validate or confirm transactions, removing the need for a third- party.

Blockchain is used to secure and distribute data in a new and unique way.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005144|

II. BACKGROUND HISTORY

It took the Internet several decades to transform from a network that was primarily used for communication purposes at and between military and educational institutions into a technological platform that was able to host and realize commercial applications. However, after the introduction of the World Wide Web, it took only a few more years before commercial websites were soaring and e-commerce became a worldwide business model, with retail ecommerce sales amounting to 4.89tn US dollars in 2021 with an expected growth of up to 6.39tn US dollars by 2024, which has been amplified by the global COVID-19 outbreak as indicated by early research. In comparison, the total market capitalization ofcryptocurrencies amounted to 566.26bn US dollars in 2017, 128.78bn US dollars in 2018, 237.1bn US dollars in 2019 and 758.06bn US dollars in 2020, showing a strong decline after the 2017 hype, but also a rapid recovery and growth afterwards. Payments with cryptocurrencies only have a 2% share of digital payment transactions, but are growing in importance.

The following sections briefly describe the advent of e-commerce and highlight several important research topics that have emerged. Next, relevant developments in the area of blockchainare summarized that even surpass the speed of the ecommerce era with respect to expectations and, to an extent, also market adoption. The focus of the discussion lies particularly on those characteristics of blockchain that have the potential to significantly impact e-commerce.

III. RELATED WORK

As the cyber-attacks are critically growing nowadays, the data breaches issues are getting vital for the individuals and organizations trying to ensure their privacy and security. Based on the research, the data breaches had increased at an unexpected rate, the data breaches issues in 2016 recorded as 36.6 million increased to 197.6 million in 2017, then created a new high record as 446.5 million data exposure issues in the next year. The data breaches issues not only occur on the bigger companies but small businesses at the same time because they are easier to attack and ransom. The attackers threatened and ransomed the companies with the data that were stolen. For example, Uber paid $100,00 to the hacker to delete the stolen data and settle the data breaches issue in 2016. Data breaches issues of organizations will threaten the customer loyalty and the public's trust because the customers value their data privacy, especially if it is related to personal information and transaction history. The online store system of Under Armour also experienced unauthorized access to the database in March 2018 and the more than 150 million of customers' username, emails and encrypted passwords were compromised. Fortnite, an online video game which has 200 million users worldwide also attacked and exposed players' personal account information and eavesdropped on the game chatter. The news proved the cyber-attacks are growing exponentially in the online platform and it needed to be controlled and monitored to minimize the loss of organizations. Blockchain technology should be implemented to ecommerce based organizations to protect the highly sensitive data of an organization and reduce the data breaches issues efficiently.

IV. OBJECTIVE OF THE SYSTEM

For e-commerce, finance, and energy, it applies blockchain technology in the following business scenarios.

(1) It realizes blockchain-based evidence certification platform. The key information, such as hash value of evidence file, is write to blockchain to realize evidence collection of important document in the whole process.
(2) Blockchain-based payment clearing and settlement improve operating efficiency.
(3) Blockchain-based supply chain finance application is achieved.
(4) Blockchain-based trust system application is realized.
(5) It applies blockchain in material bidding process to record the performance of suppliers and bidders, and provides basis for credit evaluation.
(6) It realizes visual display and monitoring of block node information, such as block height, block hash, transaction information, time, etc.

V. REVIEW OF LITERATURE

The use of blockchain technologies in online shopping has been evolved beyond decentralized digital payments towards blockchain-based online and offline services. The following highlights the benefits of blockchains in the context of e-commerce.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005144|

5.1 High Security

Blockchains provide transactions to be immutable due to the implementation of the technology. In the event that a block is altered, the block would be rejected by most of the nodes and the information would not persist in the ledger. This is because the block is hashed using the hash of the previous block which would link the blocks together and creating a chain. If a block is altered the data would also affect the hash for the subsequent block which in turn causes the nodes in the network to reject it. This ensures that the information has not been tampered with which would ensure ecommerce ecosystems for customers, suppliers, sellers, and shipping companies to highly protected. In addition, the use of smart contracts eliminates an external third-party entity when doing a transaction exchange, without compromising the security in the midst of the transaction process. Smart contracts are designed to automate tasks based on the preset rules, omitting any forms of interference by any signatories.

5.2 Lower Transaction Cost

Retailers are often required to pay commission fees to use e-commerce platform. This is inevitable if they want exposure to a large audience that an e-commerce platform provides. These fees do not yet include the cost of using payment gateways such as PayPal and credit card which would further decrease their profit margin. Retailers will have little choice but to increase the price of these products to gain profit from selling on the platform. These increase in price would also cost customers to pay more for the product. With the introduction of blockchain technologies into these, it would remove the need for the intermediaries, and these payments can be made directly between the retailer and customer reducing the cost of the product and increasing profit.

5.3 Traceability

Tracing an order item back to its root origin proves to be an arduous task when products are traded using a centralized traditional E-commerce platform. Therefore, with blockchains, it allows an audit trail whenever an action is done during the transaction. This help to verify the authentication of the transaction, preventing frauds. This is especially useful for order tracking as blockchain allows immutable tracking. This means that customers are able to locate where their products, whether their products are genuine and what is contained etc. This helps to maintain the integrity and authenticity of products.

5.4 Trustless

In traditional forms of e-commerce platforms, information used by retailers is owned by the platform. These platforms offer guarantees and reviews of seller whereas, for payment gateways, they offered to keep safe of the transaction amount till its verified. This undeniably gives absolute controls to these platforms and gateways over their customers. Furthermore, trusting these platforms and gateways to store huge amount of confidential data posed a risk in terms of privacy issues, which is why these companies are the choice of targets for fraud and hacking attempts. Therefore, blockchain can be employed to create a system where trust is no longer required. The cryptography in blockchain can completely eliminate the external intermediary.

VI. PROPOSED METHODOLOGY

- The number ofrounds shown in Figure is for the case when the encryption key is 128bitlong.

- Before any round-based processing for encryption can begin, the input state array isXORed with the first four words of the key schedule. The same thing happens duringdecryption — except that now we XOR the cipher text state array with the last four wordsof thekeyschedule.

Forencryption, eachround consistsof thefollowingfoursteps:

1) Substitute bytes, 2) Shift rows, 3) Mix columns, and 4) Add round key. The last stepconsists of XORing the output of the previous three steps with four words from the keyschedule.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005144|

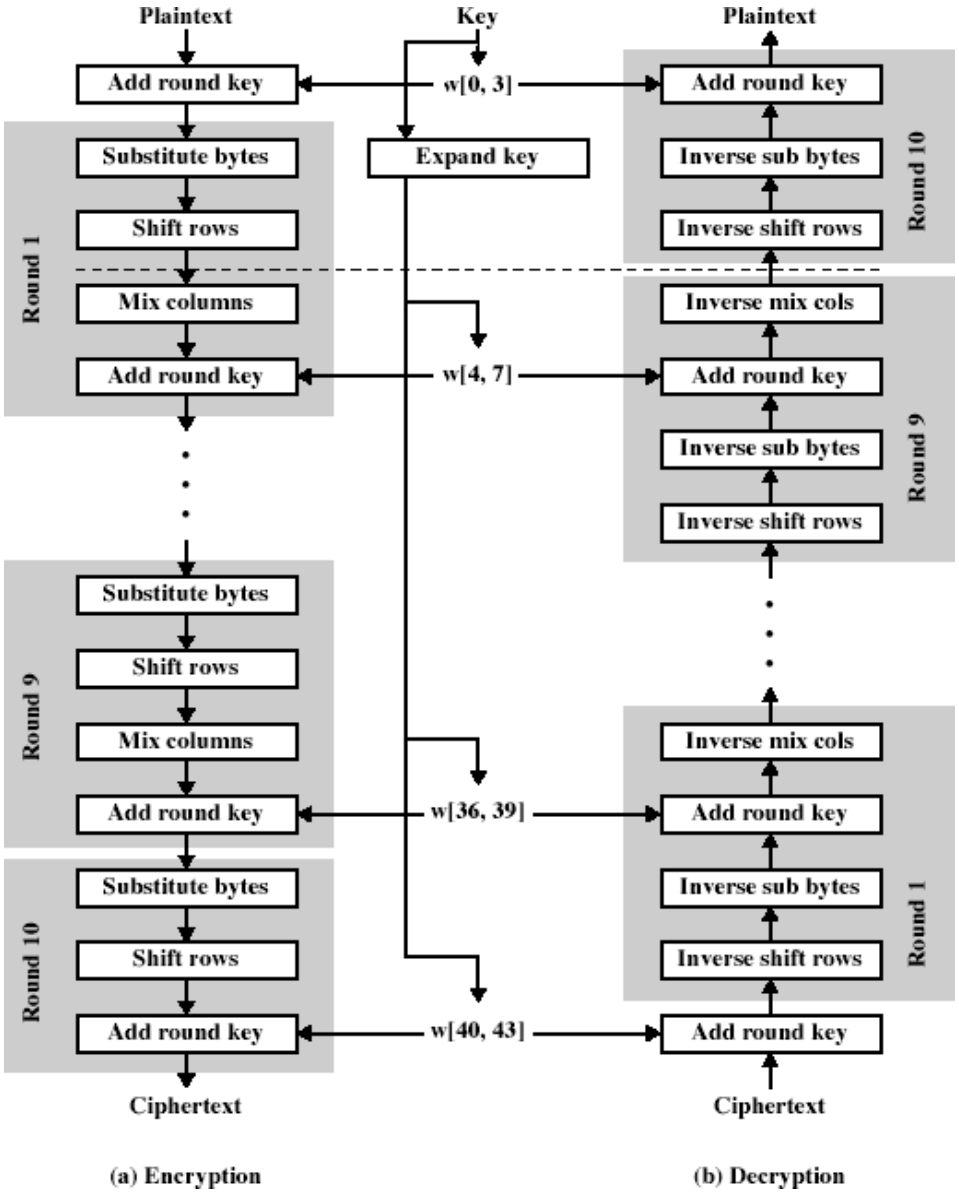

Figure 4.1: - SYSTEM ARCHITECTURE

• For decryption, each round consists of the following four steps: 1) Inverse shift rows, 2) Inverse substitute bytes, 3) Add round key, and 4) Inverse mix columns. The third stepconsists of XORing the output of the previous two steps with four words from the keyschedule. Note the differences between the order in which substitution and shifting operations are carried out in a decryption round vis-a-vis the order in which similar operations are carried out in an encryption round.

• The last round for encryption does not involve the "Mix columns" step. The last roundfordecryption doesnot involvethe "Inversemixcolumns"step.

TheFourStepsIn EachRoundOfProcessing:

STEP 1: (called SubBytes for byte-by-byte substitution during the forward process) (The corresponding substitution step used during decryption is called Inv Sub Bytes.)

• This step consists of using a 16 × 16 lookup table to find a replacement byte for a givenbyteinthe input

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005144|

statearray.

• The entries in the lookup table are created by using the notions of multiplicative inverses in GF(28) and bit scrambling to destroy the bit-level correlations inside eachbyte.

STEP 2: (called Shift Rows for shifting the rows of the state array during the forward process) during decryption is denoted In v Shift Rows for Inverse Shift-Row Transformation.)

• The goal of this transformation is to scramble the byte order inside each 128-bit block.

STEP 3: (called Mix Columns for mixing up of the bytes in each column separately duringthe forward process) (The corresponding transformation during decryption is denoted In vMix Columns and stands for inverse mix column transformation.) The goal is here is to further scramble up the128-bitinputblock.

• The shift-rows step along with the mix-column step causes each bit of the cipher text todependon everybitof theplain-text after 10rounds ofprocessing.

• In DES, one bit of plaintext affected roughly 31 bits of cipher text. But now we wanteachbitoftheplaintexttoaffect everybitoftheciphertextinablockof128bits.

STEP 4: (called Add Round Key for adding the roundkey tothe output of the previousstep during the forward process) (The corrresponding step during decryption is denoted Inv Add Round-Key for inverse addround key transformation.)

5.Flowchart:

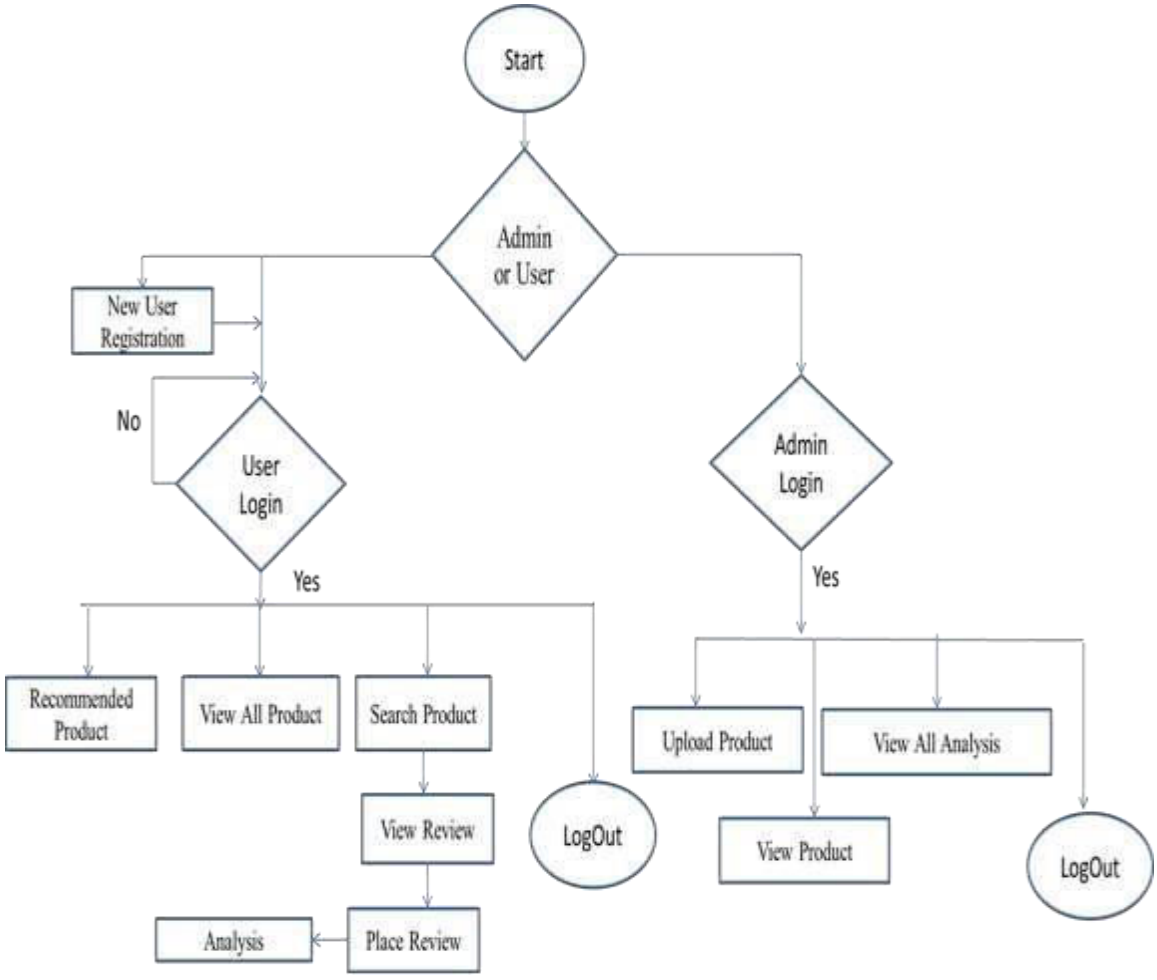

Figure 5.1: -Functional Block Chain Approach towards Approximation Problem in E-Commerce Website

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005144|

VII. CONCLUSION AND FUTURE SCOPE

Blockchain is a shared, replicated ledger, blockchain can openup bus in ess networks by taking out cost, improving efficiencies and increase accessibility. Blockchain addresses an exciting and topical set of business challenges, which cross every industry. Blockchain helps in reducing time delay and also extra costs.before thebackdropoftheresearchquestion,how"trust-free"systemsbasedonblockchaintechnology may impact the reputation economy in ecommerce, the study demonstrates that the underlying trust issues can be heal their competition amongst brands

VIII. FUTURE SCOPE

Faceted search is a technique for accessing information that allowing users todigest, analyse and navigate through multidimensional data. Multiple dimensions means,Data that is comprised of many data types, For example, a product datasetcould havedata types of name, price, photo and product-id. The word framework indicates that weimplementa system in which we can getfacetsfromthe query logof users. The querylog is the record of user searched data or request. The log is collection of large record justlikeadatabase

REFERENCES

1. **https://blockgeeks.com/guides/what-is-blockchain-technology**
2. **(http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2709713).**
3. Condos,James, William H. Sorrell, and Susan L.Donegan. 2016.Blockchain *Technology:OpportunitiesandRisks*.Montpellier,Vermont.
4. Beck,R., Stenum Czepluch,J., Lollike,N., Malone,S., 2016.Blockchain.
5. Gatewaytotrust-freecryptographicTransactions.In:ECIS2016Proceedings.
6. Chang, M.K., Cheung, W., Tang, M., 2013. Building trust online: interactions among trust building mechanisms.
7. Chen, Y., and Xie, J. Third-party product review and firm marketing strategy.MarketingScience, 24, 2(2005),218–240.
8. Connolly, A.J., Kick, A., 2015. What differentiates early organization adopters ofbitcoinfromnon-adopters?.In:AMCIS2015Proceedings.pp.1–6.doi:10.13140/RG.2.1.4730.8645.
9. Davidson, S., De Filippi, P., Potts, J., 2016. Economics of Blockchain. Soc. Sci.Res.Netw. 1–23. https://doi.org/10.2139/ssrn.2744751.
10. Hawlitschek, F., Notheisen, B., Teubner, T., The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy, Electronic Commerce Research and Applications,Volume29,2018.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details