

Blockchain in E-Commerce

KetalaSnehal Kumar

Department of Data Science and Business
Systems,

SRM Institute of Science and Technology,
Kattankulathur, Tamil Nadu, India
kk3929@srmist.edu.in

DaivikGururajPelathur

Department of Data Science and Business
Systems,

SRM Institute of Science and Technology,
Kattankulathur, Tamil Nadu, India
dp6697@srmist.edu.in

M. Prakash

Department of Data Science and Business
Systems,

SRM Institute of Science and Technology,
Kattankulathur, Tamil Nadu, India
prakashm2@srmist.edu.in

Abstract—The new digitization trends have completely transformed or altered industries and traditional business models. Blockchain technology is now poised to completely transform and disrupt sectors, particularly those that depend on trust, like the financial industry. This innovation depends on the possibility that it is a public, shared, and sealed record that lets individuals who don't have the foggiest idea about one another or trust each other convey data in a reliable record where any sort of irrelevant, important data can be kept.

This work gives a hypothetical structure to looking at the impacts of blockchain innovation on the monetary area specifically and the writing overall. This thesis recognizes that blockchain innovation can possibly raise straightforwardness, decrease gambles by tying up less resources during exchanges, increment efficiency, and diminish costs like monetary exchange charges. While brilliant agreements are one of the most aggressive uses of blockchain innovation, the monetary area may likewise profit from different applications. It is still too soon to precisely foresee what the blockchain innovation will actually want to do, despite the fact that the innovation has a huge potential to upset the ongoing monetary framework. The most extreme hypothesis is that banks are not generally needed in light of the fact that to blockchain innovation. This thesis contends that, rather than becoming outdated as a result of blockchain technology, financial institutions are more likely to benefit from it. As an addition, we will map the data to blockchain wallets and also employ NFT smart contracts in place of conventional smart contracts to produce hash addresses, after which the data is transferred to an online IPFS server.

Keywords—Smart contracts, the financial sector, and blockchain technology.

I. INTRODUCTION

Information technology has already had a significant impact on industry and business procedures (Jaki& Marin, 2015). Then again, the internet has prompted the improvement of an extensive variety of novel business techniques and, surprisingly, entirely different monetary subsectors that were unbelievable only a couple of years prior. The genuine advantage of data innovation is that it makes altogether new and more powerful method for connection among individuals and organizations. Blockchain technology is the technology that deserves your attention right now. This relatively new technology will enable less secure and safer ways to conduct business alongside the Internet. This thesis inspects extra applications for the blockchain, which is regularly distinguished as the innovation behind the virtual money bitcoin. This thesis will rapidly make sense of what bitcoin is and why it might work as an elective money surrendered that bitcoins make virtually each of the information in present day blockchains. Regardless of this, the proposition expects to exhibit that the innovation isn't limited to only this application. In mark of reality, there has been a ton of analysis evened out at the utilization of this innovation in bitcoin for being fairly

prohibitive. As per TheEconomist (2016b), it is vital for make a differentiation between the possibility of blockchains overall and the particular innovation that controls the virtual currency bitcoin. Buterin (2015), then again, underlines the qualification among public and private blockchains.

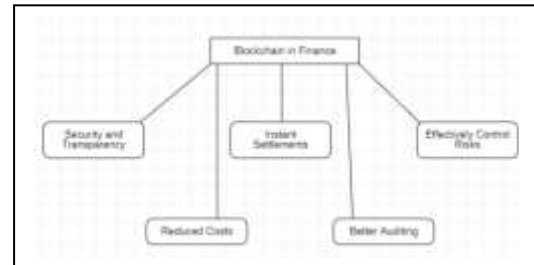


Fig.1: Example figure

Numerous applications made possible by technology need for cooperation and common standards across participants in the financial industry. As a result, this thesis briefly analyses the collaboration between a group of over 50 financial institutions worldwide and the financial technology start-up R3. This collaboration aims to advance blockchain technology and hasten its application to the financial industry. In the highly competitive banking industry, they are working together to establish clear guidelines for the use of this technology. Trautman attests that blockchain technology can possibly overturn and rebuild the financial business, notwithstanding every one of the difficulties it faces.

Blockchain technology will have a much broader impact than bitcoin, according to this thesis. Notwithstanding, it is too early to know precisely exact thing the blockchain will permit or when it will be utilized in the monetary area on the grounds that the innovation is still in its outset. Notwithstanding, there is a critical opportunity that it will disturb the current financial structure. By eliminating ineffective and costly middlemen from, for example, stock trading or international payments, financial institutions stand to benefit from cost reduction as well as increased productivity. Additionally, because blockchain-based procedures require less cash, risks are reduced. Nonetheless, the blockchain's dependability and openness help to increase public confidence in the financial system. Because some services may be more appropriate for the technology than others, it is important to underline that not all useful information should be included in blockchains. But according to this concept, financial institutions would benefit more from automating international payments and securities trading first because those processes have already been proven to be effective.

II. LITERATURE OVERVIEW

1. *Blockchain and Bitcoin: Regulatory responses to cryptocurrencies:*

This essay investigates Bitcoin from a legal and regulatory standpoint, providing significant insights. They start out by defining Bitcoin and highlighting its significance. They discuss issues with Bitcoin's use as a cryptocurrency implementation strategy. With this background on cryptocurrencies, we may now address the inescapable question: Is it legal? What are the currency's regulatory responses? Can it be controlled? They clearly explain why virtual currencies are important, why self-regulation has failed, and what can be gained from this. Finally, they arrive at practical and mostly permanent conclusions on the use of virtual currencies in general, the viability of mining currency on blockchains, and the depth of Bitcoin in relation to the advancement of block chain technology. They come to the conclusion that, much as Bitcoin may be Second Life a decade from now, blockchains might be a really revolutionary social technology similar to Web 2.0 social networks.

2. *The Future of Banking: The Role of Information Technology:*

This article looks at how information technology (IT) is changing both explicit foundations and the financial area overall. Albeit the essential financial matters of banking have not adjusted, technological advancements might entice establishments to participate in exchange banking (because of IT-driven cost efficiencies). Banks shouldn't, be that as it may, forsake relationship banking. If all else is equal, banks should adapt to customers' shifting tastes for IT-driven products and encourage IT advancements to update or maybe completely rethink relationship banking. Due to the introduction of FinTech startups and IT corporations into conventional banking industries, significant changes are also about to occur in the banking industry. Banks are given greater time to adapt thanks to government action and regulation. JEL L86, O33, G20, and G21.

3. *Market Design for Trading with Blockchain Technology:*

The so-called distributed ledger, which entails keeping a decentralized record of all transactions for a security, is a fundamental aspect of blockchain technology. Anyone with access to a distributed ledger may look up asset holdings using (anonymous) IDs. They contend in this study that the mapping between IDs and end-investors should be a decision made during market design. They investigate the impacts of the utilization of IDs and the connected straightforwardness of possessions on trading behaviour, trading costs, and investor welfare government assistance while integrating qualities of blockchain innovation into a hypothetical model of intermediated and peer-to-peer trading. They discover that, notwithstanding the possibility of front-running, the setup with the most transparency results in the greatest investor welfare. In the absence of complete transparency and low levels of liquidity in the intermediated market, investors' welfare will be at its highest if they are forced to consolidate their assets under a single identity.

4. *Bitcoin: A peer-to-peer electronic cash system:*

Online payments can be done effortlessly from one party to the next without going through a banking institution using a peer-to-peer kind of electronic cash. Automated markings improve the arrangement in certain ways, but the main advantages are lost if a reliable outsider is still required to reduce copy spending. As a remedy to the double-spend issue, we suggest a distributed organization. By encrypting trades in a persistent chain of hash-based work verification, the organization timestamps transactions. This creates a record that cannot be altered without rehashing the evidence of work. Both the source of the most CPU and the request for times seen are supported by the longest chain. The hubs that aren't working together to seek the organization will create the longest chain and outlast rivals as long as they have the majority of the CPU. The actual organization doesn't need a lot of construction. Hubs could leave the company at any time and come back, using the longest confirmation of work chain as evidence of their absence. The best effort principle governs the transmission of messages.

III. METHODOLOGY

As every current application works on a single centralized server and if this server is hacked or crashes due to a heavy load of requests, the services will not be provided, we are using Blockchain technology in financial applications in this project. We can utilize decentralized Blockchain technology to solve this issue since it maintains data across numerous servers or nodes, ensuring that consumers can still access services even if one node goes down.

Blockchain stores data as blocks or transactions and assigns each block a distinct hash code. Before storing any new block, Blockchain verifies the hash codes of all existing blocks to ensure that no blocks have been attacked or altered. If this verification is successful, Blockchain will only then store a new block. Blockchain is said to be immutable since it cannot be attacked or have its data changed from the backend if the verification process fails because it won't store any new data. Verification will fail if altered.

The aforementioned benefits of blockchain are driving businesses to move from centralised servers to decentralised networks.

Customers and service providers are the two types of users we are creating for this project.

- 1) **Service Providers:** Service providers may register and log in to the application to see orders from customers, add new items, and more.
- 2) **Users:** Users may register and log in to the application, access all information about service providers, contribute funds to their wallets, and explore product descriptions to make purchases.

Blockchain uses smart contracts to store data, and SOLIDITY programming is used to create these contracts. Utilizing Truffle, SOLIDITY code may be deployed on Ethereum's blockchain. Once deployed, the contract will

yield an ADDRESS, which can be entered into a Python application to access the contract and save and receive data from the blockchain.

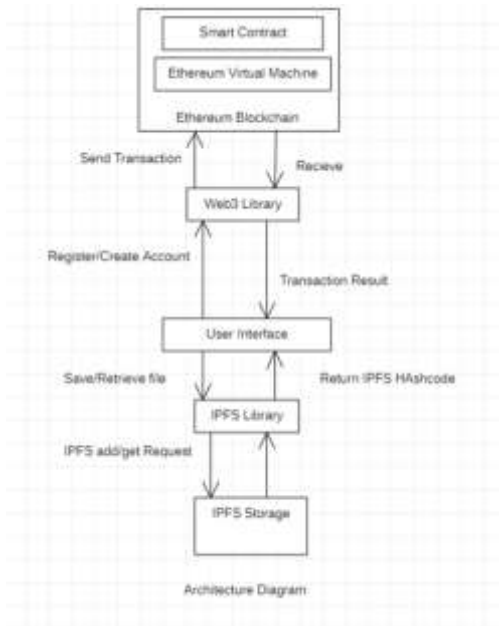


Fig.2: System architecture

In light of blockchain innovation, BITCOIN is a computerized cash that can be utilized for the purpose of trade without the need of an outsider that can be relied upon, similar to a bank. Alternatives to fiat currencies, virtual currencies function similarly to cash. The most popular and widely utilised virtual money nowadays is bitcoin.

Basically, BLOCKCHAIN TECHNOLOGY is a public, disseminated, and dependable record that is open to anybody. Furthermore, it is sealed, and that implies that whenever information is placed into the blockchain, it can't be changed without being seen. Technically, the ledger may include any sort of valuable intangible information. Because there is no need for trust between users of the blockchain technology, it is possible to conduct transactions without a middleman.

DISTRIBUTED LEDGERS are unmanaged, open databases. They are instead supported by several participants. In a distributed ledger, information is dispersed over thousands of locations as opposed to being centralised. A distributed ledger's characteristic is the blockchain technology.

The type of money that is currently used the most is the FIAT CURRENCY, which is a currency that is theoretically worthless but has been given value by a law or a government. Notes, which are really just pieces of paper but have gained value nonetheless, are examples of fiat currency.

Peer-to-peer networks are reliant upon hubs, or PCs all through the globe that are answerable for keeping up with the organization. It is a decentralized organization where hubs speak with each other and trade data without having a focal power.

IV. TECHNOLOGY

1. Ganache

Ganache is a private blockchain for quick creation of Corda and Ethereum distributed applications. Ganache may be used throughout the whole development cycle, allowing you to create, distribute, and test your dApps in a secure and predictable setting. A UI and CLI are the two kinds of ganache. An Ethereum and Filecoin desktop application called Ganache UI is available. For Ethereum development, we offer ganache, a more powerful command-line tool.

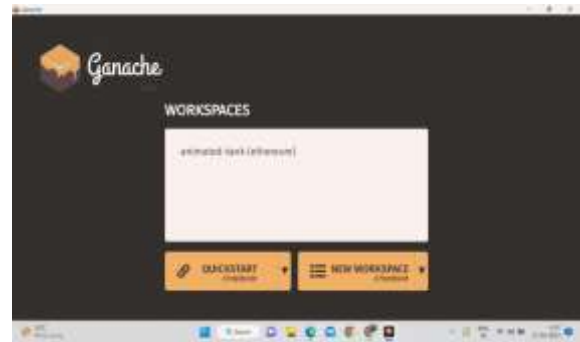


Fig.3: Ganache Interface

2. Metamask

A software cryptocurrency wallet called MetaMask is used to communicate with the Ethereum network. Users can utilize a browser extension or mobile app to access their Ethereum wallet, which can then be used to connect with decentralized applications. ConsenSys Software Inc., a blockchain software firm that specializes in Ethereum-based infrastructure and tools, is the company behind MetaMask. Using Metamask, users may send and receive Ethereum-based cryptocurrencies and tokens, broadcast transactions, store and manage account keys, and securely connect to decentralized applications using a suitable web browser or the built-in browser of the mobile app.

A user's MetaMask wallet (and any other comparable blockchain wallet browser extensions) can be connected to, authenticated, and/or integrated with other smart contract capabilities by websites or other decentralized applications using JavaScript code. This enables the website to send action prompts, signature requests, or transaction requests to the user through MetaMask as an intermediary.

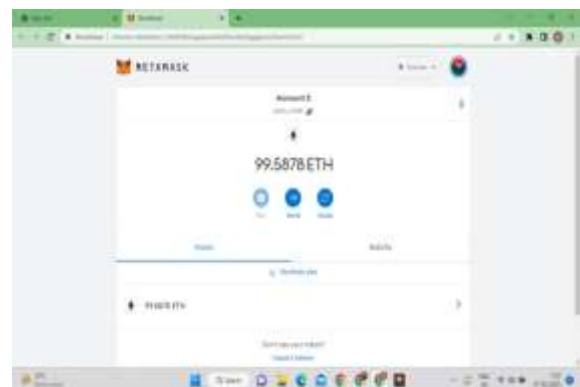


Fig.4: Metamask Interface

3. Algorithms Used

3.1. NFT Smart Contracts

NFTs and smart contracts on the blockchain are the most exciting components (non-fungible tokens). Even yet, the similarities between the two concepts cause confusion for a lot of people. NFTs wouldn't exist without smart contracts, and an NFT smart contract is commonly seen as a single entity with shared goals. These smart contracts can be used in a variety of ways to manage and enhance digital assets. If you want to learn more about them, start by learning how non-fungible tokens interact with smart contracts.

Like cryptocurrencies, NFTs are digital assets that can only be owned by one person at a time. NFTs generally have a supply of just one specific digital token, in contrast to cryptocurrency tokens, which frequently have millions or billions of the same token in circulation. These resources are frequently linked to a link that opens an IPFS file (InterPlanetary File System). The unique token Number and metadata for the asset are provided to the NFT buyer as ownership proof. The ownership of NFTs is distributed through smart contracts, which are also used to create NFTs. Every time a new non-fungible token is issued, the smart contract immediately designates the creator as the owner. NFT smart contracts have the capacity to transfer the token to the new owner after a sale.

Below we can see the solidity code we used to implement NFT Smart Contracts.

```

1  pragma solidity ^0.8.0;
2
3  import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
4  import "@openzeppelin/contracts/access/Ownable.sol";
5
6  contract NFT is ERC721, Ownable {
7      uint256 public totalSupply;
8      string public name;
9      string public symbol;
10     string public baseURI;
11
12     constructor(string memory _name, string memory _symbol, string memory _baseURI) ERC721(_name, _symbol) Ownable(msg.sender) {
13         name = _name;
14         symbol = _symbol;
15         baseURI = _baseURI;
16     }
17
18     function mint(uint256 tokenId) public {
19         require(!exists(tokenId), "Token already exists");
20         _mint(msg.sender, tokenId);
21     }
22
23     function burn(uint256 tokenId) public {
24         require(exists(tokenId), "Token does not exist");
25         _burn(tokenId);
26     }
27
28     function transferFrom(address from, address to, uint256 tokenId) public {
29         require(msg.sender == ownerOf(tokenId), "Not the owner");
30         _transfer(from, to, tokenId);
31     }
32
33     function approve(address operator, uint256 tokenId) public {
34         require(msg.sender == ownerOf(tokenId), "Not the owner");
35         _approve(operator, tokenId);
36     }
37
38     function revokeApprovals() public {
39         _revokeApprovals();
40     }
41 }

```

Fig.5: NFT Smart Contracts

V. RESULTS

Shows the Main Screen, that a user or a service provider may see.



Fig.6: Main Screen

Shows the User interface used for registering details



Fig.7: User signup

The service provider may add any number of products that is shown up here.



Fig 8: Adding new products.

Users may view each and every service provider details.



Fig.9: View Service Providers.

User has an option of adding money to the wallet that is shown up here.



Fig.10: Add money to wallet.

User can search a product that has been added by the service provider.



Fig.11: Search product

Whenever we do a transaction, it is updated here in the form of blocks, and this is done using NFT Smart Contracts.



Fig.12: Ganache Blocks

VI. CONCLUSION

This thesis took a gander at the likely purposes of blockchain innovation in the monetary business and stressed the pertinence and worth of the innovation. The blockchain innovation is pertinent to substantially more than just the virtual cash bitcoin, as this proposition concedes. As a general rule, this theory proposes that bitcoin is a pretty disappointing utilization of this innovation since it permits clients to send and get cash namelessly, which energizes problematic applications. Different purposes for the blockchain innovation have been canvassed in this thesis by referring to recently distributed works. As an addition, we added the data to blockchain wallets. Additionally, we'll employ NFT smart contracts rather than conventional smart contracts to produce hash addresses, and the data will then be successfully delivered to the IPFS server.

REFERENCES

1. Gomathy, V., Janarthanan, K., Al-Turjman, F., Sitharthan, R., Rajesh, M., Vengatesan, K., & Reshma, T. P. (2021). Investigating the spread of coronavirus disease via edge-AI and air pollution correlation. *ACM Transactions on Internet Technology*, 21(4), 1-10.
2. D. Bryans, "Bitcoin and Money Laundering: Mining for an Effective Solution," 89 *Ind. L.J.* 441. Available at SSRN, 2014.
3. V. Buterin, "On Public and Private Blockchains," *Etherum Blog*, 2015.
4. R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, Technology, and Governance," *The Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213-238, 2015.
5. D.W. Diamond, and P. H. Dybvig, "Bank runs, deposit insurance, and liquidity," *The Journal of Political Economy*, vol. 91, no. 3, pp. 401-419, 1983.
6. Dhanabalan, S. S., Sitharthan, R., Madurakavi, K., Thirumurugan, A., Rajesh, M., Avaniathan, S. R., & Carrasco, M. F. (2022). Flexible compact system for wearable health monitoring applications. *Computers and Electrical Engineering*, 102, 108130.
7. M. Jakšič, and M. Marinč, M., "The Future of Banking: The Role of Information Technology", 2015.

8. Bančinvestnik, K. Malinova, and A. "Market Design for Trading with Blockchain Technology," 2016, Available at SSRN.
9. S. Murray, "Blockchain can create financial sector jobs as well as kill them," *The Financial Times*, 2016.
10. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. Manuscript. Narayanan, A., 2008.
11. J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies," Princeton University Press, 2016.
12. G. W. Peters, and E. Panayi, "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," Available at SSRN, 2015.
13. M. Pilkington, "Blockchain technology: principles and applications. Research Handbook on Digital Transformations," edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2015.
14. A. Pinna, and W. Ruttenberg, "Distributed Ledger Technologies in Securities Post-Trading Revolution or Evolution?" *ECB Occasional Paper*, p. 172, 2016.
15. PWC, "The future shape of banking: Time for reformation of banking and banks?" 2014.
16. P. Stafford, "Blockchain for banks still at the 'gluten' stage. *The Financial Times*," 2015.
17. L. J. Trautman, "Is Disruptive Blockchain Technology the Future of Financial Services?" *The Consumer Finance Law Quarterly Report* (forthcoming), 2016.
18. L. J., Trautman, and A. C. Harrell, "Bitcoin vs. Regulated Payment Systems: What Gives?," *Cardozo Law Review* (forthcoming), 2016.