Credible Data through Distributed Ledger Technology

Karthik B S[1], Shashank S[2]

[1]*Eight Semester, Dept. of Cse, The National Institute of Engineering, Mysore, Karnataka, India*
[2]*Assistant Professor, Dept. of Cse, The National Institute of Engineering, Mysore, Karnataka, India*

---***---

Abstract – *In centralized systems, the results of buying any data online has always been questionable and untrustworthy by customers. This problem has become more prevalent as online shopping has become more common. Most of the existing systems are based on centralized servers where customers must trust the centralized organizing authority for the integrity of the results. This paper proposes a decentralized platform based on Ethereum Blockchain. This idea of adapting decentralized system to make the process of buying and selling data in a cheaper, faster, easier and trustworthy way is a compelling one in the modern society. Distributed systems are a technological improvement in the current world. Distributed ledger technology in integration with Ethereum offers an infinite range of applications that are more flexible.*

***Key Words*: Blockchain, Distributed Ledger Technology, Ethereum, Smart Contracts, dApps, decentralization.**

1. INTRODUCTION

As long as there is choice for customers, all data markets will work on reputation to a large extent. In early days, people used to visit a physical store in order to buy the product. But now people order their desired product online. The item a user wishes to buy will be available at his doorstep. Soon, a hybrid form of shopping will be evolved [1]. People will search the product information online and then go to stores to purchase their products. Around 70% of the consumers read reviews before the purchase of the product. All popular online data marketplaces include a reputation system that facilitates trust in the vendors and the products. However, the reviews and ratings are locked to the data marketplace's own platform, preventing the users/vendors from using the reputation elsewhere. Additionally, the data marketplace selects which reviews to go on top and thereby influences the sales of individual data products. Such activities can be prevented by using block chain. Transparency of data is maintained across the network. Block chain prevents modification of data as per the convenience of the vendors and data holders as a change made in one node reflects in all other nodes. If found improper, changes are roll backed. So, in such a way the integrity of data that is present in the block chain in maintained. In this way users are guaranteed with fair and true data. Malicious activities are hindered with the use of block chain and ledger technologies.

Blockchain is a distributed database of records or a public ledger of digital events or transactions that have been executed and shared among participating parties across a large network of untrusted participants. It stores data in blocks that can verify information and are very difficult to hack [6]. It eliminates the requirement of third-party verification and thus disrupts any sector that leverages it traditionally. Blockchain can replace a third party or middle men whenever the third party or middle men is involved in producing a transaction. Each transaction in the public ledger is supposed to be verified by consensus of the majority of participants in the system and once entered; information will never be erased as it is immutable.

Blockchain data structure is a timestamped list of blocks, which records and aggregates data on transactions that might have ever occurred within the blockchain network. So, blockchain provides an immutable data storage that only allows insertion of transactions and no updating or deletion of existing transactions on blockchain to avoid tampering and any revision. The entire network reaches a point of consensus before a transaction is included into the immutable data storage. The person who is to write the new set of records on the immutable data storage is decided through different mechanisms like Proof-of-work or Proof-of-stake, which are basically the consensus algorithms. Blockchain technology is non-controversial and it has worked flawlessly over the years and is being successfully applied to both financial and non-financial applications. A blockchain-based system is yet to be systematically explored to design it a proper way and there is also a little understanding about the impact of introducing blockchain into software architecture.

2 EXISTING SYSTEM

The existing systems are the usual third-party interfaces which are controlled by a single organization and can act as a single point of failure. When we use third party websites or interfaces, we are required to trust a particular organization.

Traditional databases use client-server network architecture. Here, a user (known as a client) can modify data, which is stored on a centralized server. Control over the database remains within a designated authority, which authenticates the client's credentials before providing access to the database. As this authority is responsible for administration of the database, if the security of the authority is compromised, the data can be altered, or even deleted.

A user with permissions associated with their account can modify entries that are stored on a centralized server. By changing the 'master copy', whenever a user accesses a database using their computer, administrators will get the updated version of the database entry. Control of the database remains with administrators. Access and permissions are restricted to the central authority.

3. BACKGROUND ON DISTRIBUTED LEDGER TECHNOLOGY AND ETHEREUM

To solve this problem, we use the Distributed Ledger Technology which is decentralized, immutable, tamper-proof and uses asymmetric encryption and achieves data privacy. This technology possesses four main features:

a) The ledger is distributed i.e. it does not exist in only one single location but it is distributed. Hence, there is no single point of failure in the maintenance of the distributed ledger.
b) Majority of the network nodes must reach the consensus before a new block with new set of transactions becomes a permanent part of the ledger.
c) One single person cannot take control over the distributed ledger. No middle men.
d) Any proposed "new block" to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.

These technological features operate through the concept of cryptography where the public keys and private keys of the particular accounts are involved, providing a security level equal and/or greater than any previously known database.

Blockchain can be referred to as a public decentralized database with replicates distributed over several nodes simultaneously [7]. In Blockchain there is no authority in charge of managing and maintaining the ledger of transactions. The validity of the ledger's version is established through a consensus mechanism among the validating nodes. The use of Blockchain technology allows a secure validation of transaction's data integrity. Bitcoin, for instance, is the first application developed over Blockchain by Satoshi Nakamoto [8]. On another hand, Ethereum Blockchain [9] is an open-source, distributed and decentralized computing infrastructure that executes programs called smart contracts. It is developed to enable decentralization for applications and not only for digital currency. It is achieved using a virtual machine (Ethereum Virtual Machine, EVM) to execute a complete scripting language. Unlike Bitcoin in which only Boolean evaluation of spending conditions are considered, EVM is somehow similar to a general-purpose computer that simulates what a Turing machine can execute. Changing the state of a contract in the Blockchain requires transaction fees which are priced in Ether. Ether is considered as the fuel for operating the distributed application platform.

3.1 Accounts in Ethereum

There exist 2 types of accounts in Ethereum:

1) Externally Owned Accounts (EOA): An account which is controlled by private keys and has an account address which is determined from the public key. The holder of the private key can transfer ethers to other accounts and can make transactions to the smart contract. EOA's can hold ether as balance in the wallet. It has no associated code with it. Externally Owned Accounts are considered user type accounts and are linked to unique cryptographic keys pair, generated upon account creation. The public key is used to reference the account and also called EOA address whereas the private key on the other hand is used to sign transaction before executing any type of transaction on the network to prove authenticity. EOAs have balances which hold Ether cryptocurrency [10].

2) Smart Contract Accounts: A smart contract is an account which will be generated when a smart contract code is compiled and is deployed to the blockchain. The address of the contract account is determined at the time the contract is created. The smart contract accounts are controlled by code and are created by Externally Owned Account when the smart contracts are deployed. It also has a wallet to store the ether balance. And it has associated code by which it is being controlled by. It is considered as an autonomous agent executed by the EVM and is the core foundation and the main building blocks of any Decentralised Application [10]. Once the code is deployed onto the Blockchain, the Ethereum Virtual Machine will take care of executing the code as long as the conditions apply. It is important to note that smart contracts once deployed to the Blockchain network, they can be visited and viewed via their address with all their associated transactions (to address, from address, timestamp, etc.).

4. LITERATURE REVIEW AND RELATED WORK

We present in this section various solutions that attempt to integrate data market and Blockchain to enable decentralization of marketing of data. We then highlight the added value of our proposed system compared to the others.

Krešimir Mišura; Mario Žagar [11] "Data Marketplace for Internet of Things" published in international conference on smart systems and technologies/IEEE 05 December 2016. In this paper, a P2P-network-based system is proposed, where the data marketplace emerged as a platform to facilitate transparent data transactions between IoT device users and IoT device producers. The data generated by Internet of Things is mostly owned by device owners and is often private in nature. There are however third parties that could benefit from using that data, and the challenge is in allowing them to access it under the conditions that data owners find acceptable. An opportunity presents itself to create a marketplace where device owners could sell that data and data consumers could buy it. Some properties of IoT data make it difficult to trade in traditional data markets.

5. PROPOSED SYSTEM

In this section, we introduce our proposed data marketplace system that aims at solving the existing barriers.

5.1 SYSTEM COMPONENTS

The following are the components that the proposed system consists of:

1) Remix IDE: The main goal of the Remix IDE is to compile the smart contract code using the solc translator and to deploy the smart contract to the blockchain network. After smart contract is deployed on to the blockchain a unique address is generated using which interaction can be done with the smart contract either by making calls or transactions to the smart contract.

2) Web Application: The web application allows the buyer or seller of the data marketplace to authenticate for further processes. The seller when logged into the data marketplace can upload the data and set a desired amount of price to the respective data. If the buyer of the data marketplace wishes to buy the particular data, he can buy it by sending the respective amount of ethers to the seller, after which he can download or view the data and also can validate the data against the hash of the data which will be stored in the ledger.

3) Smart contracts: Here there exists a single smart contract for the data marketplace which handles all the end users of the data marketplace. The selling process includes updating the smart contract ledger with the meta-data of the data uploaded by the seller. The buying process involves updating the smart contract with the flags for the respective buyers of the particular data.

5.2 SELLING THE DATA

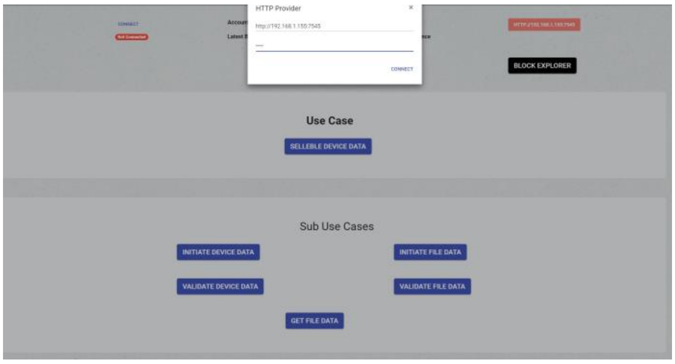
The seller uses the web application to authenticate himself as discussed previously. After the authentication, the seller can sell a particular data on the data marketplace platform by simply uploading the data files and specifying a desired amount of ethers as price and submitting the form accordingly. This process involves a tiny bit of cost which is spent as the gas required for the ethereum virtual machine to execute the smart contract code.

5.3 BUYING THE DATA

The buyer uses the web application to authenticate himself. After the authentication if the buyer wishes to buy specific data, he can just click the buy button and again confirm to buy the data by paying the respective amount of ethers as price which will be sent to the owner of the respective data. The smart contract takes care of the sending the ethers to the owner of the respective data.

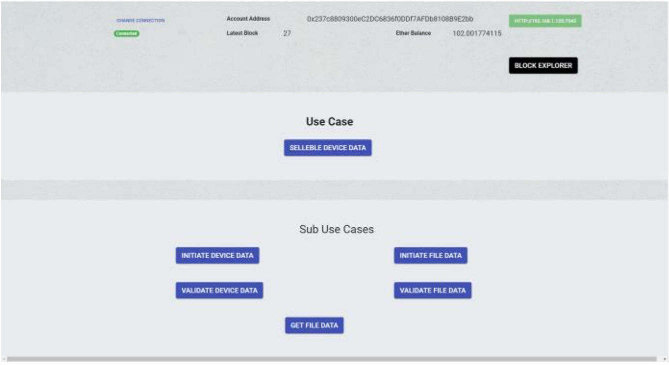
6. IMPLEMENTATION AND RESULTS

To validate the proposed data marketplace system, the following solution has been implemented using various technologies. Django is a web framework for python, which is used to create a user interface which is user friendly. Python is used for the server side scripting. Web3.py a python module is used to interact with the blockchain network. Solidity, a contract oriented programming language which is used for writing smart contracts [12], and HTML, CSS for frontend user interface, JavaScript for the backend interface. A private blockchain network is created using the go-implementation of the ethereum protocol; proof-of-authority is used as a consensus mechanism. And finally, the Django webserver for hosting the decentralized web application.



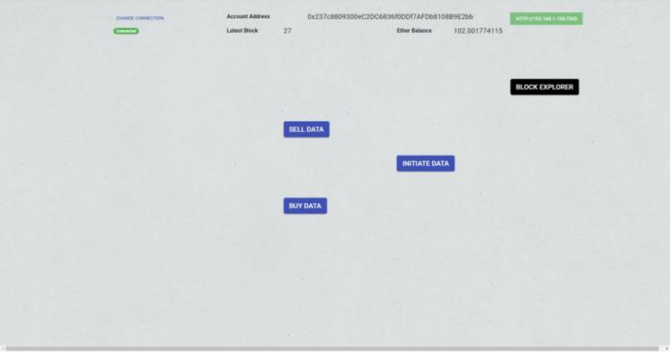
HTTP Provider
http://192.168.1.150:7545

Fig. 1. User login page



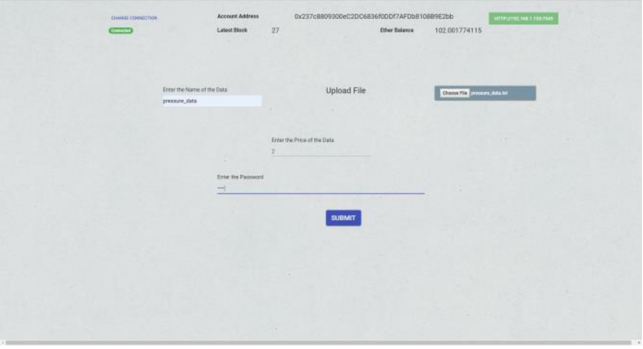
Account Address 0x237c8809300eC2DC6836f0DDf7AFDb8108B9E2bb
Latest Block 27
Ether Balance 102.001774115

Fig. 2. Home page of the web application



Account Address 0x237c8809300eC2DC6836f0DDf7AFDb8108B9E2bb
Latest Block 27
Ether Balance 102.001774115

Fig. 3. Choose to buy or sell the data.



Account Address 0x237c8809300eC2DC6836f0DDf7AFDb8108B9E2bb
Latest Block 27
Ether Balance 102.001774115

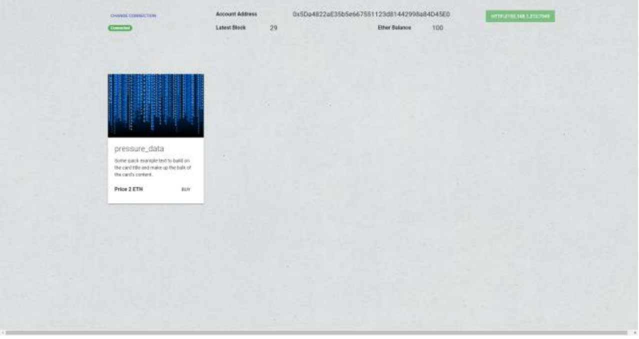
Enter the Name of the Data
pressure_data

pressure_data.txt

Enter the Price of the Data
2

Enter the Password

Fig. 4. Seller selling page



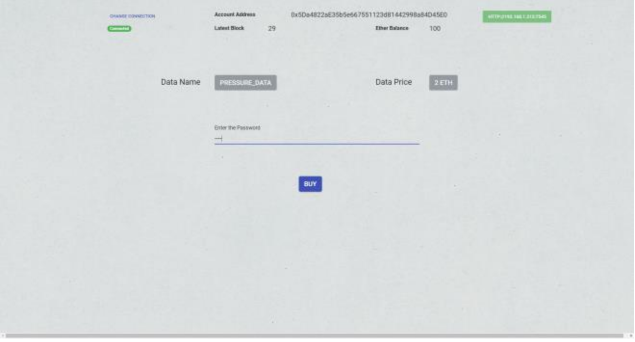
Account Address 0x5Da4822aE35b5e667551123d81442998a84D45E0
Latest Block 29
Ether Balance 100

pressure_data

Some quick example text to build on the card title and make up the bulk of the card's content.

Price 2 ETH

Fig. 5. Buyer home page

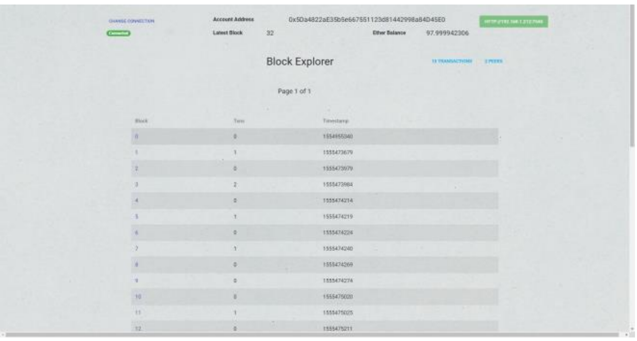


Account Address 0x5Da4822aE35b5e667551123d81442998a84D45E0
Latest Block 29
Ether Balance 100

Data Name PRESSURE_DATA
Data Price 2 ETH

Enter the Password

Fig. 6. Buyer buying page



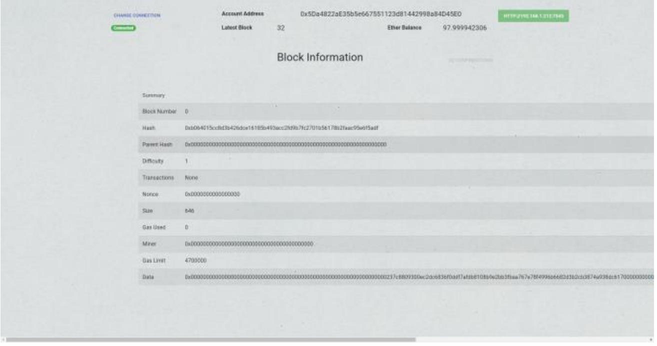
Account Address 0x5Da4822aE35b5e667551123d81442998a84D45E0
Latest Block 32
Ether Balance 97.999942306

Block Explorer

Page 1 of 1

Block	Txns	Timestamp
0	0	1554955340
1	1	1555473679
2	0	1555473979
3	2	1555473984
4	0	1555474214
5	1	1555474219
6	0	1555474224
7	1	1555474240
8	0	1555474269
9	0	1555474274
10	0	1555475020
11	1	1555475025
12	0	1555475211

Fig. 7. Block exploring page



Account Address 0x5Da4822aE35b5e667551123d81442998a84D45E0
Latest Block 32
Ether Balance 97.999942306

Block Information

Summary

Block Number	0
Hash	0xb064015cc8d3b426dce16185b493acc2fd9b7fc2701b5b178b2faac95eb15adf
Parent Hash	0x0000000000000000000000000000000000000000000000000000000000000000
Difficulty	1
Transactions	None
Nonce	0x0000000000000000
Size	646
Gas Used	0
Miner	0x0000000000000000000000000000000000000000
Gas Limit	4700000
Data	[illegible]

Fig. 8. Block information page

6. CONCLUSIONS AND FUTURE WORK

The number of IoT devices used in industries and in day to day life is increasing exponentially. Hence the need to build a trustworthy medium where the data can be shared is also increasing. This project hopes to move towards building a decentralized network of peers using blockchain chain environment. Users can share the data within a network where its integrity will be achieved through the distributed ledger. Ethereum has four development stages, namely, Frontier, Homestead, Metropolis, and Serenity. Even though there is no official roadmap for Ethereum, a lot has been planned for its implementation in the coming years, including a major consensus overhaul from proof-of-work to proof-of-stake.

The next advancement associated with this project will be to add a security feature. The location where data stored can be encrypted and stored in the ledger. When a buyer buys the data, the location of the data will be decrypted and sent to him, which can be achieved through asymmetric key cryptography. Another advancement that can be added is to upgrade the storage of files from local disk to the clouds.

REFERENCES

[1] Farag, S., Schwanen, T., Dijst, M, and Faver, J.2007. Shopping online and/or in-store? A structural equation

model of the realtionships between e-shopping and in-store shopping.
Transportation Research Part A: Policy and Practice. 41, 2 (2007) , 125-141

[2] Andriulo, S., Elia, V. and Gnoni, M.G. 2015. Mobile selfcheckout systems in the FMCG retail sector: A comparison analysis. International Journal of RF *Technologies: Research and Applications. 6, 4 (2015), 207–224.*

[3] Zyskind, G., Nathan, O. and Pentland, A. 2015. Decentralizing privacy: Using blockchain to protect personal data. Proceedings - 2015 IEEE Security and Privacy Workshops. (2015), 180–184.

[4] Zyskind, G., Nathan, O. and Pentland, A. 2015. Enigma: Decentralized Computation Platform with Guaranteed Privacy. arXiv:1506.03471.

[5] Newman, N. 2014. Apple iBeacon technology briefing. Journal of Direct, Data and Digital Marketing Practice. 15, 3 (2014), 222– 225.

[6] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," In P2P, Trento, Italy, 2013

[7] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? a systematic review," PloS one, vol. 11, no. 10, p. e0163477, 2016.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[9] V. Buterin et al., "A next-generation smart contract and decentralized application platform," white paper, 2014.

[10] M. Pilkington, "11 blockchain technology: principles and applications," Research handbook on digital transformations, p. 225, 2016.

[11] Krešimir Mišura ; Mario Žagar_"Data Marketplace for Internet of Things" published in international conference on smart systems and technologies/IEEE 05 December 2016.

[12] C. Dannen, Introducing Ethereum and Solidity. Springer, 2017.

[13] J. Wilson, Node. js 8 the Right Way: Practical, Serverside Javascript that Scales. Pragmatic Bookshelf, 2018.

[14] K. Iyer and C. Dannen, "The ethereum development environment," in Building Games with Ethereum Smart Contracts. Springer, 2018, pp. 19–36.

[15] R. C. Merkle, "Method of providing digital signatures," Jan. 5 1982, uS Patent 4,309,569.

[16] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014. [9] K. Delmolino, M. Arnett,

[17] E. F. Kfoury and D. J. Khoury, "Secure end-to-end voip system based on ethereum blockchain," Journal of Communications, vol. 13, no. 8, pp. 450–455, 2018.

[18] McKnight, D.H., Cummings, L.L., Chervany, N.L., 1998. Initial trust formation in new organizational relationships. Acad. Manage. Rev. 23 (3), 473–490.

[19] Utz, S., Kerkhof, P., van den Bos, J., 2012. Consumers rule: how consumer reviews influence perceived trustworthiness of online stores. Electron. Commer. Res. Appl. 11 (1), 49–58