

# Blockchain Marketplace

Melvin Mathew Johny, Ashlin Biju, Pranjal Tiwari  
SCOPE, Vellore Institute of Technology Chennai, India

**Abstract-** The development of blockchain technology has made it possible to create smart contracts. In other words, it is self-executing code that is stored and executed on the blockchain. This created a decentralized application along with a framework for easy development and deployment. It uses the ethereum framework to implement a decentralized online marketplace, allowing buyers and sellers to participate in ecommerce without a large central entity coordinating the process. Uses the ethereum framework for the marketplace. This makes him one of the most widely used and trusted blockchain technology available on the market today. ethereum extends the application of the blockchain technology used by Bitcoin to provide a Turing complete scripting language. Scripts can be committed to the blockchain via transactions, indefinitely making them publicly accessible. This enables the ability to encode arbitrary state transition functions, and as such the ability to create decentralized blockchain-based applications, otherwise known as Dapps. The application is designed to have a back-end consisting of Solidity smart contracts hosted on the ethereum public blockchain, along with a HTML/CSS/JS front end UI application. The web application will use the web3 API to interact with the smart contracts. While the smart contracts provide all the business logic of a marketplace, using them via an API would not be user friendly and as such a JavaScript web application will be implemented to provide a front-end that can be accessed via a web browser. The market place front end consists of a typical web application. It 5 consists of a JavaScript application that uses Web3 APIs to interact with smart contracts, and an HTML page that provides a graphical user interface.

**Index Terms-** blockchain; smart contracts;

## I. INTRODUCTION

To redeem mobile goods online, users use third-party market places to reduce the risk associated with transactions with anonymous online users to facilitate the completion of financial transactions. Buyers and sellers expect the external market environment to act as a trusted intermediary, providing connectivity and protection services to peers who want to exchange goods and make money, but this will lead to a decline in employment. In addition to these protections, reported cases of payment and delivery failures in the United States resulted in casualty losses totalling more than \$138 million in 2016, and other smaller, anonymous cases. It provides users with better commercial fraud protection than the market, but this makes for a strong mid-sized organization. Contains a large amount of personal information about the user. It can be processed and sold. Recent events have raised the issue of privacy and raised widespread concerns about the collection and use of user data by large companies. Added to this are concerns about the security of sensitive financial information online. Additionally, recent events such as the Quifax data breach have highlighted the dangers of sharing financial information, even for formerly large financial firms. exchanging money online requires the user to provide sensitive personal and banking information,

exposing the data to the risk of a data breach and exposing the user to the risk of her identity being stolen. A large market poses a double threat to users' information security. Because users are required to disclose both personal information, which is important for researching and managing people through big data analytics, and banking information that can be used for their possession. Theft if undisturbed. 7 Recent advances in blockchain technology have created smart contracts (automated contracts that are stored and executed on blockchain nodes), enabling the creation of secure decentralized applications. buterin and the like. proposes a number of smart contract applications, including separate on-chain market places, but does not provide details of such applications. Using smart contracts to create a decentralized on-chain market place would eliminate the need for mid-sized companies to integrate market operations, thus eliminating data integration and user exposure to potential threats

## II. LITERATURE SURVEY

First, confirm that you have the correct template for your paper size. Some literature already exists on the use of blockchain technology as a TTP or arbiter to enable the exchange of digital data. Methods similar to ZKCP employ zero-knowledge, which goes against our efficiency property. Some methods release

specific data and inadvertently breach the privacy of the user. Recent work such as Fair Swap addresses every need for a two-party case.

Work has been done on creating a useful blockchain-based data marketplace. Information can be traded via platforms like IOTA and solutions like DDM and Physical mode. Future projects like Strandr want to offer an extensive range of features associated with data marketplaces.

There is a wealth of literature on data trading, particularly on sensor data and the Internet of Things.

We find from our review that the concept of the Blockchain technology is still in a novel stage. However, the literature points towards central themes and concepts within the technology that has achieved larger success within the literary landscape of Information Systems. We find that several of the identified concepts are of interest to this paper. However, in order to examine each of the concepts in-depth, a categorization approach helps in terms of analysing the identified concepts.

This approach allows us to combine one, or more concepts into a single category from which they can be identified, analysed and synthesized. In addition, we believe that the categorization provides a comprehensive view on the factors underlying the current research body of the topic. In our search, we identify three distinct themes that appear more frequently in the current literature.

### III. PROBLEM STATEMENT

Our project which will be mainly focused on the problems with the Blockchain based distributed marketplace in which we will be implementing a distributed online marketplace using the Ethereum framework where buyers and sellers can engage in e-commerce transactions without the need of a large central entity coordinating the process

#### 1. Existing Solution

Since it is an online digital marketplace where exchange of goods takes place, there is a high chance of vulnerabilities that can take place in the system.

So, there is a high chance of risk that the server accepting the request might get slow down because of service of denial attack where the hackers keep on sending thousands of requests to the server once the website got hacked.

So we have to find the solution in order to avoid DoS attack: 1. Know your network's traffic every organization's infrastructure. 2. Create a Denial of Service Response Plan. 3. Make your network resilient. 4. Practice good cyber hygiene. 5. Scale up your bandwidth. 6. Take advantage of anti-DDoS hardware and software. Capturing these complicated contracts and tracking the flow for fair payout is a challenge. Each seller will have its own restrictions on how the buyer can use this

data, so sufficient work needs to be done in this regard. efficiency: Predicate checking over encrypted data for arbitrary logic is still inefficient. Similarly, Zero-Knowledge.10

Practical homomorphic encryption schemes are only efficient for basic mathematical operations. And this is considered as one of the best schemas so far in this online marketplace website. Data Duplication: Assuring that the buyer is not buying the same data twice is a problem. Today, most digital data bought from online marketplaces are chosen and bought on the basis of the description given by the owner of the data or the platform. Our proposed design suffers from the same problem. Revealing parts of data itself to the buyer to prevent duplicate buys prevents us from delivering fairness. Ensuring data description matches data is a challenge in itself. Moreover, specifying  $\Phi$  in a manner that captures requirements properly without violating any of the marketplace deliverable properties is a tough task. We need to explore tools like Convergent encryption which can provide us a way to avoid duplication without revealing anything about the data.

#### 2. Proposed Solution

As our project is based on the Ethereum Framework. As we all know Ethereum which expands the use of blockchain technology used by Bitcoin. This enables the ability to code regional transformation activities, and the ability to create blockchain-based applications which is known as Dapps. Smart contracts- The Turing-complete scripting language embedded in Ethereum allows for the creation of intelligent contracts. Documents can be included in transactions such as Bitcoin, however contracts also have their own addresses that can send and receive transactions, allowing contract components to be executed upon receipt of the transaction. Ether and Gas Gas, which is directly converted to Ether (ETH) at a real fixed price, is a fuel-efficient unit byte-code calculation within EVM and data storage in the blockchain. The use of the service in the fuel contracts protects the malicious and endless code from being used in the series without the payment of computational costs. Now coming to the details related to our project, as most of the website-related project, it mainly consists of two parts Front-end and back-end.

I will start with the Front-end developers work on what the user can see while back-end developers build the infrastructure that supports it. But as we know both of them are necessary components for a high-functioning application or website. Back End:- First we will be talking about the back end as this is where blockchain technology and the Ethereum framework comes into play. So in our project we have used two smart contracts written in solidity, first is just the basic migrations smart contract. This contract basically ships with any truffle project. Whenever we deploy a new contract to blockchain, truffle framework uses this contract to do that deployment on the blockchain. Second is the main contract where we specified all the conditions and created all functions like create products

and purchase products functions. This contract will provide the business logic which orchestrates the process of listing, browsing and purchasing of items. It will also handle the logistical information exchange between a buyer and a seller required to enable the logistics of a physical exchange. Apart from smart contracts, in the backend the next most important thing is writing tests related to that smart contract. In that we have to write all the basic test cases related to the marketplace smart contract like that the product should have a name, it should have a price etc. Front End:- For the front end part while we know that the smart contracts give the whole business concept of the marketplace, using them via the API will not be easy to use (means interacting with it using a console or terminal window) and as a result the JavaScript web application will be used to provide an accessible conclusion with a web browser.

The marketplace will contain a standard web application. This will include a JavaScript application that uses the Web3 API to integrate both smart contracts and React Js pages to provide user visual imagery. Buy Product:- For this part the buyer can buy any of the listed products of their choice. The Name, Price and owner details of the listed products are all provided there, once the buyer clicks on the buy button and makes the purchase, the ownership of that product gets updated with the buyer's account details. The accounts are all connected to our website using the Metamask extension, in metamask we have to import accounts in it. In our project, we are using Ganache, it's a local blockchain network which provides us with many dummy accounts with 100 ethers in it which we can use for development and testing purposes.

#### IV. IMPLEMENTATION

This project is based on the web3.0 and on the ethereum framework. And the transactions have been made locally on the blockchain local server (i.e Ganache). Now this project is implemented in the two parts:

- Front end
- Back end

In this project, the front end is implemented using reactjs library.

For the backend, we have basically used two smart contracts that have been implemented in solidity. The first file is used for the basic migrations of the smart contract. Thus, whenever we deploy a new contract to the blockchain, the truffle framework is used to deploy the contract in the blockchain. Now, the second contract is the main contract, where we have specified all the necessary conditions of creating the products and also purchasing the products. This contract will provide the business logic which orchestrates the process of listing, browsing and purchasing of items. It will also handle the logistical

information exchange between a buyer and a seller required to enable the logistics of a physical exchange.

Now, all these transactions are being made with the metamask. In our project, we are using Ganache, it's a local blockchain network which provides us with many dummy accounts with 100 ethers in it which we can use for development and testing purposes.

This system design Diagram represents the relationship between the user and the Ethereum network. This is essential for establishing a network between the user and Market place which highlights the entire steps which a user has to take in order to interact with the ethereum framework.

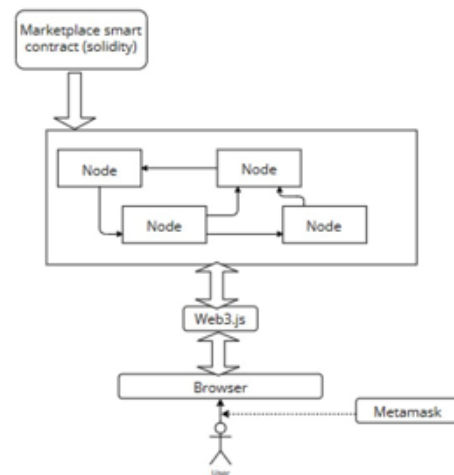


Figure: 1 Marketplace smart contract

Firstly, the user interacts with meta mask. Meta mask is a software currency wallet which is used to interact with the Ethereum blockchain. It allows the user to access their Ethereum wallet through a browser extension or mobile app. Then the user can gain access to the Ethereum Network through the browser where various nodes are interacting with each other simultaneously and buying /selling is being done simultaneously.

In most cases, "Web3.js" refers to a JavaScript library that works with Web3, a collection of protocols and technologies that make it possible to create decentralized apps (DApps) on blockchain systems, particularly Ethereum. Smart contracts and DApps built on the Ethereum platform can be used with Web3.js.

#### V. CONCLUSION

There is no mature application for a decentralized marketplace yet; this is a field that will be very important in the next 1-2 years as a lot of startups are in the first phase of building similar products.

At this stage, it is impossible to predict which segmented market will be the first to reach mass acquisition, but creating a competitive Dapp in place of a promising Ethereum platform with a simple UI promises both knowledge gained and technology capabilities.

However, our Project may be considered successful as:

- By using smart contracts, merchants cannot be discriminated against by the system, as system rules are set in stone smart contracts.
- As an added benefit, we have a publicly guaranteed transparency of system rules. In addition, the fact that transaction data is stored in the blockchain makes it easier to test processes.
- It is shown in the cost analysis of the system that it does not cost the seller to write an item or sell an item, thus cost efficient and beneficial for both buyers and sellers.
- The Ethereum framework maintains user data security, ensuring that no users can get information from another user.

## REFERENCES

1. ETH Gas Station, <https://ethgasstation.info/>, last accessed: 01/05/2018
2. How much does it cost to sell on eBay?, <https://sellercentre.ebay.co.uk/private/what-fees-youll-pay>, [Online] Accessed: 01/05/2018
3. Sell on Amazon - Pricing and Fees, <https://services.amazon.co.uk/services/sell-online/pricing.html>, [Online] Accessed: 01/05/2018
4. Total Retail 2017, <https://www.pwc.com/gx/en/industries/assets/total-retail-2017.pdf>, accessed: 01/05/2018
5. ethersphere/swarm(Dec 2017), <https://github.com/ethersphere/swarm>
6. Benet, J.: IPFS-content addressed, versioned, P2P file system. arXiv preprint arXiv:1407.3561 (2014)
7. Berghel, H.: Equifax and the Latest Round of Identity Theft Roulette. *Computer* 50(12), 72–76 (2017)
8. Buterin, V.: A Next-Generation Smart Contract and Decentralized Application Platform (2013), <https://github.com/ethereum/wiki/wiki/White-Paper>, [Online] Last accessed 02/05/2018; document constantly updated by different people.
9. Buterin, V.: Bootstrapping A Decentralized Autonomous Corporation: Part I. *Bitcoin Magazine* (2013), <https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/>
10. Buterin, V., Griffith, V.: Casper the Friendly Finality Gadget. arXiv preprint arXiv:1710.09437 (2017)