IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

**ISSN: 2454-132X**
**Impact factor: 4.295**
***(Volume 5, Issue 3)***
Available online at: www.ijariit.com

# Peer-to-peer E-transaction system using blockchain

*Abhishek Sundaresan R.*
*abho.sundaresan@gmail.com*
*BMS College of Engineering, Bengaluru, Karnataka*

*Govind K. Rajesh*
*govindkrajesh@gmail.com*
*BMS College of Engineering, Bengaluru, Karnataka*

## ABSTRACT

***We create a simple transaction system with Blockchain as the backbone while making use of Solidity, Node.js, Python and the Kubernetes framework. The resulting system is capable of mining currency, creating wallets and making transactions.***

***Keywords****— Blockchain, Proof of work, double spending, Hyperledger fabric, Proof-of-work*

## 1. INTRODUCTION

Blockchain, the foundation of Bitcoin, has received extensive attention as of late. The blockchain serves as an immutable ledger, which allows transactions to take place in a decentralized manner. Blockchain-based applications are springing up, covering but not limited to financial services, reputation systems, Internet of Things (IoT), and so on. However, there are still many challenges with respect to Blockchain technology such as scalability and security problems.

Development phases for Blockchain applications include the analysis phase, where we collect and analyse the requirements of the Blockchain application to be developed. Identify the entities/parties involved, their roles and relationships. The entities can be physical (assets or users) or virtual (such as concepts). In the design phase, we model the entity attributes as state variables and interactions between them as functions. In addition, we captured the constraints and dependencies. In the implementation phase, we implement the smart contract for the Blockchain applications. The main components of the smart contract are state variables, functions, modifiers, and events in a high-level programming language such as Solidity.

A Decentralized Application (D-App) is an application that uses smart contracts providing a friendly user interface to smart contracts. A typical example of D-App is a crypto currency application that runs on a Blockchain network. A Decentralized application structure is composed of a front-end interface (Web Browser, HTML, and CSS) and a back-end interface (Web3 JavaScript). As described in the figure, the D-App application interacts with the Ethereum node (EVM) using JSON RPC. JSON RPC is a stateless and lightweight remote procedure call (RPC) protocol that is used by Ethereum clients to interact with an Ethereum node.

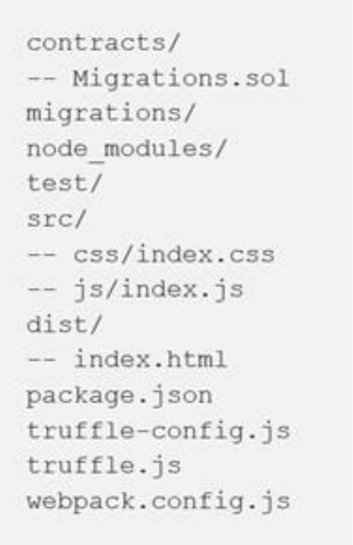
## 2. IMPLEMENTATION

The implementation of this project has the following steps done sequentially in order

(a) Setup the project
(b) Program the Solidity contracts
(c) Create the frontend application
(d) Deploy the application online with IPFS
(e) Use a custom domain for the application, in this case, configurable cloud containers
(f) Run and test the final version of the D-App

Setting up the project as a secure application depends on the contracts ability to generate randomness with Solidity. Different random generation techniques on the blockchain and see what works for the D-App. For this, we used a configurable web pack deployed using truffle under node.js. Then, a folder called Etherium-backend was created in the computer's desktop. Inside, open the terminal or command line using npm -init commands for initiation procedures. We use the ethereal development framework Truffle in this project as a developing dependency (-D) and globally (-g).

Once implemented the resulting folder structure looks like this:



```
contracts/
-- Migrations.sol
migrations/
node_modules/
test/
src/
-- css/index.css
-- js/index.js
dist/
-- index.html
package.json
truffle-config.js
truffle.js
webpack.config.js
```

**Fig. 1: Configuration of web pack**

Our next process was to program the solidity contracts and deploy the front end application using the react framework. We procedurally generated e-wallets and mining services using a default smart contract which is remotely deployed on a test network (Ropsten test network) to create a user simulation environment where wallets and transactions can be made procedurally.

We use configurable cloud containers for deployment and security based on a proxy-HTTP system. The containers are deployed as a docker image using a service called gitKube to each remote server wherein the transaction is cropped to a namespace defined within the server. The contracts are then deployed on a test server using a built-in metamask and money is minded into the faucet defined under that metamask server.

After some ether was reposited and mined into the faucet, our metamask is online and can be used for wallet transactions and hashing. The blockchain deployed is safe behind the proxy setup in the container with the catch that only the user can view the pods in that transaction and see the deployable docker file.

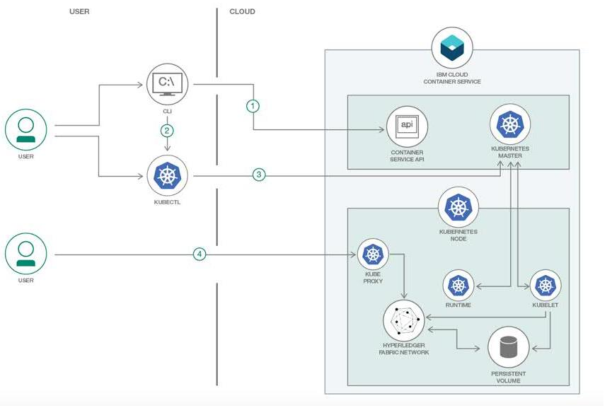


**Fig. 2: Hyperledger fabric in Kubernates**

After the container is initiated as shown in the above diagram, the concurrent transactions are deposited within the dockerfile namespace and deployed on the test server for smart contact forging and referrals as per the user demands.

## 3. RESULT

As we were able to implement our D-App we found Blockchain technology penetrates the construction markets of various services and attracts more and more attention as a result. This is one of the most promising business technologies, which is expected to bring many positive changes to the world of rapid technology and change. Blockchain is most useful when making transactions during the purchase of the real estate, Security etc. Blockchain allows you to fully control and monitor the database of all transactions in the world of currencies and also Bitcoin. You can be sure that money transactions will always be conducted reliably and efficiently. Also, the database will always be 100% protected, so you can be sure that your confidential information will not be stolen or used to your advantage.

One of the most pressing issues was the transparency of transactions. Since it is literally impossible to steal someone else's information from this database, you can be sure that your rights as the owner will not be violated as seen in our implementation whilst current iterations [1] tend to maintain a steadfast approach wherein verifiability meets transparency on various level of inculcation.

With that, we come to reliability. The system is fully equipped [2] with cryptographic algorithms that cannot be forged. Also, these algorithms are programmed in such a way that they will not allow any technical distortion of the data, so they will continue to work even if there is some kind of computer failure. Reliability also works for hand in hand with how safe the user feels with his assets and how verifiable those assets are, out projects gives the user the ability to verify and safeguard transactions to a certain level wherein they can fully understand the safety involved with digital signatures.

The same can be said about smart contracts [3]. These are the deals that are concluded between the parties digitally. They are created by special computer protocols. With the help of such contracts, you will be able to fully monitor the purchase and construction of your house, knowing that the transaction is 100% legal and that it follows all the rules and regulations. Such a smart contract simply cannot be concluded if the established requirements are not met. Smart contacts need oversight from the involved parties and have to be forged in a legitimate plausible way, the transactions made in our system is a hundred per cent legal and preserve their integrity to both users on deployment.

One of the most saving money [4]. Using Blockchain, you will save money on banking transactions and also on waiting time. Transactions have never been so simple and easy. The time spent on a qualitative assessment of assets [5] and getting legal rights within the current regime can be spent on the physical handling of assets and globally verifiable funds whose market price is dependent on profitability rather than government funds and asset shareholders in the current marketplace [6].

As you can see, our approach to Blockchain technology is all about giving its users a smarter way of interacting with the industry as a whole whether it be asset management or legal rights preserved by the integrity of contracts.This system add more transparency to the entire system as a whole.

## 4. CONCLUSION

While Block chain's best-known, most used and highest-impact application is Bitcoin, the potential impact of the technology is much greater and wider than virtual currencies. Indeed, since other applications can 'piggyback' the Bitcoin Blockchain, the biggest impacts of Bitcoin may be found outside the currency domain. Transactions of any kind are usually faster and cheaper for the user when completed via a Blockchain, and they also benefit from the protocol's security. Whereas transactions in Europe are often fast, cheap and secure enough for most purposes, users and proponents of Blockchain applications often see additional benefits in its transparency and immutability. Indeed, there is a growing trend towards less trust in financial and government institutions and greater social expectations of accountability and responsibility.

The popularity of Blockchain technology may also reflect an emerging social trend to prioritise transparency over anonymity. Of course, for each transaction that uses a distributed ledger instead of a traditional centralised system, the intermediaries and mediators are displaced, missing out on their usual source of power and income. For currencies, these are the banks, for patents the patent office, for elections the electoral commissions, for smart contracts the executors, and for public services the state authorities. A significant level of growth in the use of Blockchain technology could see substantial change in the substance and, perhaps, the quantity of' white-collar' work. For example, some of the work of intermediaries and contract lawyers could be replaced by peer-to-peer transactions and smart contracts.

As such, alternative regulatory levers must be developed to uphold the law and maintain the capacity for effective planning and action. Four broad categories of action that governance institutions could mobilise in response to the emergence of Blockchain technology can be identified:

- One option is to respond to ‘the problems to which Blockchain is a solution ‘without using Blockchain at all. For example, if demand for Blockchain is based upon a desire for more transparency in processes, then citizens could be granted more access to government data and processes without using Blockchain systems at all.
- A second option is to actively encourage the development and innovation of Blockchain by the private sector by granting legitimacy to their products. For example, under some conditions, transactions on Blockchain could be given explicit legal recognition as records of executed transactions.
- A third option is to do the reverse of the previous one, i.e. discourage development by refusing to accept the legitimacy of Blockchain-based transactions, for example by overruling and reversing the clauses in smart contracts.
- A fourth option is to adopt a permission Blockchain in existing systems and structures, effectively maintaining the role and power of those responsible as a middleman by providing some of the basic functionality of Blockchain.

To conclude, the fact that the Blockchain protocol provides platforms for both good actions and bad actions does not mean that it is a neutral technology. In its purest form, it promotes are the distribution of power from central actors across wide communities of peers. While the most idealistic and revolutionary visions of Blockchain development will probably remain no more than visions, even moderate implementation of Blockchain may still promote some degree of redistribution and transparency. As Liptinites, Blockchain will not make better people, but it might make some of the precautions necessary in people’s daily lives faster, cheaper, more secure and more transparent.

## 5. REFERENCES

[1] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[2] Nofer, M., Gomber, P., Hinz, O. et al. Bus Inf Syst Eng (2017) 59: 183. https://doi.org/10.1007/s12599-017-0467-3

[3] Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, “A short linearly homomorphism proxy signature scheme,” IEEE Access, vol. 6, pp. 12966–12972, 2018

[4] Miguel Castro, Barbara Liskov, et al. Practical Byzantine fault tolerance. In OSDI, volume 99, pages 173–186, 1999.

[5] Intel. Proof of elapsed time (poet). Available from: http://intelledger.github.io/.

[6] Blockchain -the gateway to trust free cryptographic features https://aisel.aisnet.org/ecis2016_rp/153/