Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 7, July 2021, pg.68 – 75

An Operative Application of Distributed Ledger Technology for Banking Domain

Sharmila S P[1]; Harsha Pandit Moger[2]

[1]Assistant Professor, Department of Information Science and Engineering, Siddaganga Institute of Technology, Tumakuru
[2]Associate Engineer, PriceWaterhouseCoopers SDC, Bengaluru
sharmila@sit.ac.in [1]; harshapm91@gmail.com [2]

DOI: 10.47760/ijcsmc.2021.v10i07.010

Abstract— Banking systems have been using a centralised network over several years. Any attack on the centralised unit would risk a whole lot of banking data. To avoid this, Blockchain is an approach, which is more appropriate to hold the large data in a safe manner as it is a decentralised network. The purpose of this paper is to provide better understanding about using blockchain for the banking sector by outlining the opportunities, benefits and challenges of this technology. We propose a technique of banking using blockchain which would make things simpler, safer and transparent. Also, at some point in time, we can even put restrictions to limit the transaction amount, day limit, credit limit or other restrictions depending upon the banking rules. Through these restrictions, attempts towards hacking or misuse could be prevented. This work would benefit the banking sectors and modify the direction of Finance.

Keywords — Blockchain, Ethereum, Smart Contract, Meta-mask

I. INTRODUCTION

Millions of transactions happen every second in the world. The use of digital innovative technologies, like mobile and online banking offers new experiences. More than 59% of the global population have access to internet facilities [1]. In this regard, speed, availability, efficiency, convenience, effectiveness and transparency of banking and financial processes are empowered. This contributed to confront some of the challenges encountered with expediting transactions across numerous sectors. The advent of blockchain technology has been foreshadowed as the subsequent revolution that will alter the size and shape of the banking and finance industry and the mode of conduction of business transactions.

1.1 Blockchain

Blockchain can be demarcated as a chain of blocks that embraces some information. Block is a data structure that comprises transaction data. The technique is envisioned to timestamp digital documents so that it is impossible to backdate them or tamper them [2]. The blockchain can be used for securing transfer of items like money, property, contracts, etc. without requiring a third-party intermediary like a bank or government. Once a data is verified and validated inside a blockchain, it is very difficult for further modification.

The blockchain is a software protocol. However, it is not possible to run Block chains without the Internet. It can also be termed meta-technology as it is made up of several technologies and also capable of affecting many other technologies like big data, Machine learning, Artificial Intelligence and many more [2,3]. It is comprised of: a database, software application, some connected computers, etc.

There is a disguised potentiality hidden in the blockchain technology that can bring a big revolution in the financial industry. This technology can be effectively applied in innumerable financial technology applications. A competitive landscape has been generated in financial technology which has energised the FinTech revolution. A great platform has been set up for banks and nonbanks that is based on blockchain in order to facilitate cross network transfers and payment services. Blockchain technology has found its applications not only in the field of finance and economics but also in the field of health, and education. It also provides a technical and secured platform for record keeping, stock trading, smart contracts and even digital currency such as Bitcoin. It is really a misconception that Blockchain is meant for cryptocurrencies. Bitcoin is a peer-to-peer currency which may be based on the decentralised digital-payment system that uses Blockchain network technology but it is not the same as Blockchain.
Transactions are a source for a country's economy, this would decide the position worldwide. Thus, security to these transactions to a wider extent is very important. Blockchain would help here in banking with its decentralised characteristic.

A study on fundamental characteristics of cloud computing is made in Diao Zhe that analyses acual risks associated with cloud storage for storing and transmitting data via cloud terminal [3].
Yinghui Zhang [4] et al has projected a technique for outsourcing services where no third party interferes for the completion of the transaction and still transactions are executed in a secure and fair fashion.

Bpay, which uses block chain in cloud computing, is one of the outsourcing services with a fair payment framework. In the proposed system we made an attempt to analyse soundness in terms of security and compatibility in order to ensure the robust fairness for the financial transactions.

We have also reviewed the work of Ilya Sukhodolskiy, Sergey Zapechnikov [5]. Here they have proposed a prototype where multiple users may access the datasets of an untrusted cloud environment in a controlled manner. The access control mechanism used in the system is ciphertext policy, which is based on dynamic attributes. But the system has a distributed ledger to provide log details, peculiarity of this is that records are mutable and it contains a set of security events like generation of key, requisition for access, assignment of access policy and change or revocation of access policy.

We propose a distributed ledger to be maintained to secure the bank transactions possessing immutability characteristic feasible with Ethereum framework.

Every transaction will be encapsulated in a block, which in turn would encompass many other transactions. Thousands of these blocks will be developed each second to protect the transaction data from foreign attacks or hacking. This property would give banking its utmost protection. Implementing blockchain technology in banking would bring a revolution in the world of finance. Our approach is a small effort for this insurgency.

The remainder of the paper is organized as follows:

Section II provides an acquaintance of terms related to our work. Section III describes background information and related work about micropayment systems. Section IV describes the issues in the current banking system and Section V presents a model that depicts how blockchain resolves these issues. Section VI presents the choice of the platform for implementation followed by the proposed model and prototype of the system design; Section VII concludes the paper by highlighting the insights on future directions

II. KNOWLEDGE ON INDEX TERMS

It is important to have information on the terms we would be using in the rest of the paper. These terms are vast, each one of these would constitute a mega-chapter. However, fundamental knowledge would be acquired with the discussion of the following sub-chapters.

2.1 Ethereum Blockchain

There is an open source blockchain based on a distributed computing platform featured and best performed with smart contract, which is Ethereum blockchain. Paper reference in Ethereum 'ether' is the token/digital currency that powers the Ethereum blockchain and is needed to pay for blockchain transactions. Another advantage is that Ethereum provides smart contracts, the agreements/financial contracts transcribed in automatically executable computer code on meeting certain specific conditions [6].

2.2 Smart Contract

There is an agreement between two parties with some agreeable terms included which is called smart contract in the context of blockchain technology [7]. The major difference identified between Ethereum and other types of digital currencies is mainly concerned with the smart contract. Smart contract is usually a piece of code in digital format but not a physical entity. It includes a series of instructions which is programmed in solidity, which is a high-level language specifically designed for writing smart contracts. This functions on the basis of IFTTT logic which means if-this-then-that. The first set of instructions are always executed and followed by the next function and after that the process endures until the end of the contract.

For a banking application like this each and every step is a progression to execute the succeeding step.
Step 1: Initial requirement is creation of a prerequisite number of accounts.
Step 2: Further transaction is initiated by entering the amount to be sent to the recipient's account.
Step 3: During the execution of the transaction there is a need for continuous monitoring of the transaction.
Point to observe here is that any of the above steps will not be executed if at least one of the previous step/s is not executed. This is the vital fragment of the smart contracts that one can perceive which is exclusively existing between the bank server and the individual executing the transaction may it be, requesting or transferring a sum of amount.

2.3 Meta-mask:

Meta-mask is a Gateway for Blockchain and is a crypto wallet. With the help of this gateway demonstration of blockchain can be done in an effective and easy manner. Meta-mask will also help us through local networks or international networks.
We use meta-masks for the demonstration of Ethereum. Fake ethers can be added in many ways using which an illusion to real time transactions can be found. However, the fake ethers will have no value for making transactions.

2.4 Ether:

There is major fuel for this distributed application framework (Ethereum) and it is termed as Ether. It is a form of payment. The chief purpose of Ether is to give developers an incentive with the intention of encouragement in order to develop applications of a better and still higher quality, since wasteful code is always more expensive.

It is the cryptocurrency generated by the Ethereum platform and is the only currency that can be accepted in the form of payment as a transaction fee. It is granted as the mode of payment for the miners who perform the computation.

2.5 Mining:

The process of adding a block to the blockchain, and verifying computation involved in every transaction on the Ethereum blockchain is entitled as mining. One who is involved in the mining process is a miner. Miners produce new blocks each time, which is checked and validated by other miners for validity. Presently blocks are validated by inspecting whether or not they encompass a Proof of Work of a specified difficulty or the concerned effort. The Proof of Work system has the potential to modify the Proof of Stake system. Anyone can participate and contribute the effort in the process of mining, but the probability of discovering a legal, valid, effective and operative block intensifies the power consumption of the device that is performing the computations.

2.6 Gas:

Another energy behind the execution of transactions on the Ethereum platform is designated as gas. This gas is purely consumed internally and is remunerated with Ether. The gas price keeps varied by developers, so that the cost of execution of the code is maintained constant with the fluctuation of the price of an ether.

It measures how much "work" an action or set of actions takes to perform. It is commonly referred to as the fee for the transaction.

Ether = gas limit * gas price

(Where, gas limit refers to amount of gas use for the computation)

2.7 Token:

Ethereum is also established on the custom usage of tokens, which can be sold, bought or traded for every transaction. One of the most significant tokens is ERC-20, which has emerged and materialized as the technical standard for all smart contracts on the Ethereum blockchain for the implementation of token.

2.8 Transaction:

A signed bundle of data or package that is equipped with a message to be transferred from a regular account is referred to as a transaction. A transaction comprises the following evidences:

- A signature that identifies the actual sender.
- The recipient details, to whom the message must be actually sent.
- Amount of Ether to be transferred.
- Initial value of STARTGAS that represents the maximum number of computational steps the transaction is allowed to consume.
- GASPRICE value - the fee the sender must be paid per computational step.
- Data field which is optional.

III. BACKGROUND

There are some limitations of the blockchain technique and respective solutions for smart contracts among Secure identities. [8] Highlights the solution for this limitation by integrating Public Digital Identity with Ethereum via Identity-Based-Encryption (IBE). The author deliberated about background information of Public Digital Identity. Also discussed how operations are carried out in an Identity Based Encryption (IBE). IBE is completely based on cryptography techniques like public key Infrastructure and Certification authority. The main goal of the author is to allow the association of a digital identity with a blockchain transaction. Smart contract is proposed by using Distributed

ledger. IBE is used for the authentication process for the user to receive their own private key from the Private key Generator and portrayal is carried out by considering two Ethereum users.

Focussing on the decentralized digital currencies and uses in the real-world applications [9] elucidated about Ethereum notions in the blockchain. Bitcoin has its own ledger format and transaction system. transaction system works in the Bitcoin and some information about the structure of the system. Proof-of-work is nothing but a hashing scheme for the blockchain technique and for the crypto transaction in Bitcoin and Ethereum.

IV. CURRENT BANKING SYSTEM AND CONCERNS

This section provides knowledge about banking and the payment system used nowadays. We discuss here the impact of blockchain technology in overcoming drawbacks of the current bank system. Current banking system/s is dependent on some of the third-party applications which makes banking less secure and may sometimes provide false information. Following are few issues with this type of banking:

High operation charges/transaction fees: Most of the current banking systems depend on the third-party application, hence a transaction fee is deducted from the amount that is to be transferred. For small transactions this doesn't seem to be a big factor but when large transactions are performed the amount deducted as the transaction fee emanates to be a major factor.

Double spending: Double spending is the process where a currency is spent twice. This issue doesn't arise in Physical currencies as there is no duplication of currencies. In digital transactions or currency while exchanging a token, the holder may make a copy of the token by retaining the original token.

Financial crashes: This is the situation where a token gets lost through its journey by some technical problems like sudden shut down of a bank server.
These types of situations put the investment into risk and reprocessing them would be time consuming too.

V. UNRAVELLING THE CONCERNS

Following are properties of Blockchain which are enough to solve the issues of the current banking system.
Decentralized: This is a type of storage where the files are stored in multiple computers on a decentralized network thereby protecting data at one particular point of time. In current applications centralization of the data is entrained in large numbers and it's the major issue. So, if there is a data breach or any kind of failure in the centralized server then the entire data is lost and the recovery is difficult or impossible. Thus, Decentralization is important and Blockchain, Ethereum, makes its complete use. use of the third-party payment platforms like PayPal or JusPay which complicates their development and makes them dependent and are prone to foreign attacks.

Transparency: Another feature of the blockchain technology is transparency; it means that whatever you store in the blockchain is visible to everyone. Application of zero knowledge proof can preserve the user's privacy [6].
Built-in payment system: This is a type of payment where the transaction occurs directly between two nodes without any involvement of third-party application. Most of the current applications make

Public ledgers: The ledger which holds the details of all the transactions that happen on the block chain network and is transparent to everyone, associated with the system.

Verification of each and every transaction: Each and every transaction is verified by cross-checking the ledger and the validation signal. By doing so, the issue of double spending is eliminated.

Less transaction fee: Current application of the banking makes use of the third-party application, which takes a certain amount as transaction fee. The blockchain system does not make use of the third-party application hence lesser transaction fees.

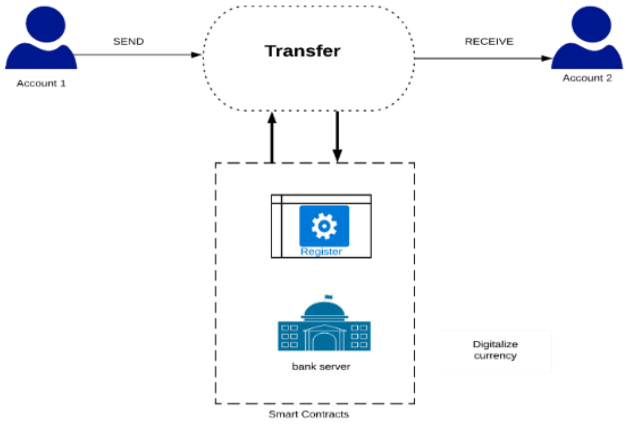

Fig : Smart Contract unravelling the concern

VI. CHOICE OF THE PLATFORM FOR IMPLEMENTATION

Hyperledger is another platform for using Blockchain. We elucidate the purpose for choosing Ethereum over Hyperledger is due to some advantages of Ethereum. [10] We relate these two platforms in the following parameters for the implementation of blockchain network in the table given below.

Characteristics	Ethereum	Hyperledger
Platform	Under generic blockchain platform	Under modular blockchain platform
Mode of operation	Public or private	Private
Governance	From Ethereum developers	From Linux foundation
Consensus	Mining process is based on the Proof-Of-Work and Ledger level	Mining process is based on Proof-Of-Work but transaction level
Smart Contract	Smart contract code is written in Solidity language	Smart Contract code is written in Java and Go Programming language
Currency	Uses ether and tokens via Smart contract	No currencies and tokens via chain code

VII. PROPOSED MODEL

We intend to propose the block chain monitoring system. It consists of a collection agent, web server for monitoring transactions, and a node interface. Initially the data is gathered by the collection agent. The collection agent gathers blocks, transactions and account information. In the case of the Ethereum network several transactions are being performed every day. The data is collected and is transmitted

to the web server through the node interface. Meta-mask is the node interface. Finally, the data being collected can be viewed using the web server ether scan. In ethers can an individual will come to know the balance remaining in the account, amount of ether transacted from one account to another and the block number. Figure shows the configuration of the proposed system. After the setup of Ethereum and Meta-mask, the transactions are carried out through Meta-mask and the analysis engine analyses the data being transferred and is provided through the webserver.

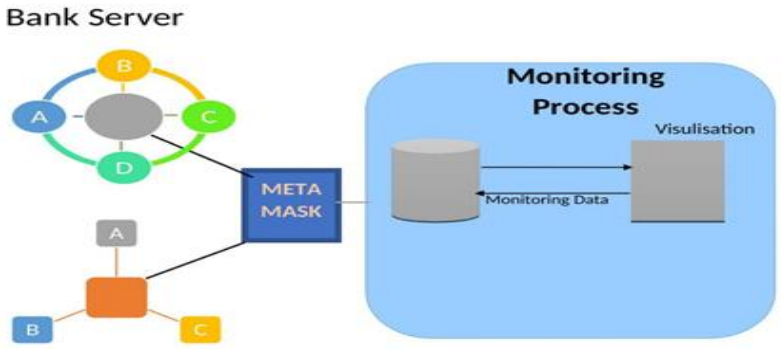

Fig 3: Proposed System

7.1 Blockchain mining and transactions

This section explains how the transaction is confirmed and is added to the blockchain. When the user wants to send the ether from one account to another through Ethereum and then the transaction takes place through the blockchain. When the user wants to send the ether, the transaction that needs to be performed is then broadcasted in "the pool of unconfirmed transactions" waiting for the miner to be picked up[11]. The unconfirmed transactions are not stored in a single pool but are subdivided into local pools. Miners on the network select the transactions from these pools and formulate them into a "block" based on the gas fee. More than one miner can select multiple transactions into a single block. By selecting transactions miners can create a block of transactions. For the miner to transfer the block, the miner first needs to solve a complex mathematical problem also referred to as "proof of work". Every block has a unique mathematical problem. This process is called mining. In the pool of unconfirmed transactions, each transaction is prioritized based on gas fee, higher the gas fee faster the transaction. After the mining process, the block is added to the blockchain and it is then distributed to the other nodes in the network. when the block is added to the chain other blocks added on top of it provides the confirmation for that block. More the addition of blocks, the higher the difficulty for the attacker to alter.

Average percent of work, which miner lose due to that reason, described by the relation

$$\mathrm{PW} = \frac{T_{cycle}}{T_{block}}$$

Where,

T_{cycle} - execution time of one cycle of the calculation.

T_{block} - average time of finding a new block in the Ethereum cryptocurrency.

ERC20 Token: It is the standard token[6] used in Ethereum and consists of the following functions.


```
contract ERC20Interface {
function totalSupply()
     public constant returns (uint);
function balanceOf(address tokenOwner)
     public constant returns (uint balance);
function allowance(address tokenOwner, address spender)
     public constant returns (uint remaining);
function transfer(address to, uint tokens)
     public returns (bool success);
function approve(address spender, uint tokens)
     public returns (bool success);
function transferFrom(address from, address to, uint tokens)
     public returns (bool success);
event Transfer(address indexed from, address indexed to, uint tokens);
event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
```

VIII. CONCLUSION

The proposed work will bring a change in banking sectors by providing a newer mode of transactions. Also, the approach would make banking independent from third party application, which consumes approximate processing charges for each transaction, on the other hand Blockchain uses gas fee which will be used for prioritising a transaction and/or discarding the transaction. Using this gas fee, we can also set restrictions to the accounts or the credits.

Since Blockchain uses distributed ledger, every transaction is transparent and a miner can handle it completely, thus privacy in banking is restricted. Owing to distributed ledger, transactions don't get discarded due to server issues. Each transaction will be handled separately.

Some of the challenges of Ethereum Implementation are in terms of time and power consumption. The transaction time of Ethereum Blockchain is around 20 seconds and it is not fast enough for some conditions that require immediate responses. Therefore, it may be difficult for time-sensitive conditions. The proposed system needs to use a high processing power computer.

REFERENCES

[1]. (2018). *Global Internet Usage*. Accessed: Apr. 11, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Global_Internet_usage

[2]. S Narang, P Chandra, S Jain, Y Narahari, "Foundations of blockchain technology for industrial and societal applications" Adv. Comput. Commun 2, 32-51 2018

[3]. Bozic, Nikla, Guy Pujolle, and Stefano Secci. "A tutorial on blockchain and applications to secure network control-planes." 3rd Smart Cloud Networks & Systems (SCNS). IEEE, 2016.

[4]. Yinghui Zhang[4] Yinghui Zhang, Robert H. Deng, Ximeng Liu, and Dong Zheng, Outsourcing Service Fair Payment based on Blockchain and its Applications in Cloud Computing, IEEE Transactions On Services Computing.

[5]. Ilya Ilya Sukhodolskiy, Sergey Zapechnikov, A blockchain-based access control system for cloud storage, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) Moscow, Russia.

[6]. Vujičić, Dejan, Dijana Jagodić, and Siniša Ranđić. "Blockchain technology, bitcoin, and Ethereum: A brief overview." *2018 17th international symposium infoteh-jahorina (infoteh)*. IEEE, 2018

[7]. Bozic, Nikola, Guy Pujolle, and Stefano Secci. "A tutorial on blockchain and applications to secure network control-planes." 3rd Smart Cloud Networks & Systems. IEEE, 2016

[8]. Francesco Buccafurri, Gianluca Lax, Lorenzo Musarella, and Antonia Russo 'Ethereum Transactions and Smart Contracts among Secure Identities', 2019.

[9]. Dejan Vujicic, Dijana Jagodic, Sinisa Randic "Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview" 17th International Symposium, March 2018.

[10]. Sajana, P., M. Sindhu, and M. Sethumadhavan. "On blockchain applications: hyperledger fabric and ethereum." *International Journal of Pure and Applied Mathematics* 118.18 2018.

[11]. Y. Heinze, "How long do Ethereum transaction take?" 2017. [Online] Available: https://support.metalpay.com/hc/enus/articles/115000373814-How-long-do-Ethereum-transactions-take-

