Blockchain With Crypto Coin Transaction By Nodes With Flask And Smart Contract

Nitiwit Kuldiloke(2K19/CO/263)
nitiwitkuldiloke_2k19co263@dtu.ac.in
Pooja Jaiswal(2K19/CO/275)
poojajaiswal_2k19co275@dtu.ac.in

***Abstract*— The cryptocurrency have been developing by the blockchain and the transaction process is occurred via the smart contract which is 2nd layer(cryptocurrency transaction) and 3rd layer(smart contract) of the blockchain. In the ending 201 decades, the first decentralized cryptocurrency, Bitcoin, was developed by Mr. Nakamoto Satoshi and some ideas of the protocol named as Bitcoin have still been confused since then. We developed the blockchain which is feasibility for blockchain starter and explain the protocol of its in this paper and implement Smart Contract along with user friendly using Flask as web node to decentralized our blockchain with Python and create smart contract with Truffle Grenache provided by Ethereum protocol of Crypto.**

Keywords—Blockchain, Smart Contract, Cryptocurrency, Peer to Peer(P2P), Decentralization, SHA256, Block Mining, Consensus Protocol.

I. INTRODUCTION

With $786.32 Billion market capability, Bitcoin is familiarized other cryptocurrency to world-wide. The blockchain is the Technology which each block connecting to each other like a chain which using timestamp, nonce, and Hash(SHA256) as the identifier to access the block (The cryptography part has been used in hash) which the blockchain will be decentralized by the Genesis-Block and will distribute the hash of each block to the other by Peer-To-Peer Network(P2P) which using Consensus Protocol to authenticate each blockchain. Thus, Genesis-Block will connect to other node(Miner or Other PC or MemPool). In order to explain the step of implementing the blockchain we used Flask as the decentralization web for user friendly and feasibility.

Every blockchain contain the different hash and nonce which identify themselves from each other. If there is the intruder who want to change a single bit of data in blockchain the SHA256(Hash cryptography) will change the entire document of hash and ditch the fraud blockchain out of the chain by Consensus Protocol.

The transaction of cryptocurrency keep happening in every day. The data of transaction have been made by the blockchain technology which will be explained later in this paper. The transaction are running on the smart contract which is blockchain's program which help managing the transaction of cryptocurrency and the token also.

II. BACKGROUND STUDY AND RELATED WORK

A.) A smart-contract is nothing but a program of blockchain that self-verifies, self-executes, and is immune to tampering. Nick Szabo proposed the smart contract concept in 1994 [5]. It enables the execution programming code with no involvement of third parties. The list below is component of creation of smart contract: address, state, function and value Taking input of transaction, executes the related code, and causes the output events to occur. The logic implementation states fluctuate depending on the function. Since 2008, when the Bitcoin cryptocurrency introduced blockchain technology. The mandatory of integration of blockchain in smart-contract has been a focus as area of development since it provides P2P transactions along with databases that could be kept openly in secure system in a trustworthy system. Tatsuya Sato and Yosuke Himura's design work. Mostly, the information of transaction will be held in smart contract, and automatically perform itself . The smart contract is implemented in several blockchain platforms using the computer language Solidity.

The smart-contract has the following characteristics:

• A smart-contract is a machine-readable code that is running on a computer blockchain platform.

• Smart-contracts are a component of a single software application.

• Smart-contracts are programs that are triggered by an event.

• Once developed, smart contracts are self-contained and do not require monitoring.

• The availability of smart contracts is made available.

Solidity is a high-level programming language that is used to construct smart systems.

contracts. Creating a blockchain platform of solidity

Ethereum, Zeppelin, Eris DB, and Counterparty
Smart contracts can be tracked and are irreversible.

B.) A blockchain is a provided data storage which is shared among nodes which each computer connected to each other. Likely database, blockchain collect data by electrically

form. As critical function in ecosystem of cryptocurrency, Bitcoin are famous ,E.g., Bitcoin, in term of keeping a decentralized and secured record of transactions. The blockchain's imaginative thought is to guarantee the precision and security of an information record and produces believe without the necessity for a trusted third party.

The structuring process of data is built differently significance from an old-fashioned style database and blockchain. It accumulated information within the network which known as blocks, which holding data in set. As the storage of block become full, it is enclosed then connect to the block which is filled before this one.

A database typically organizes inputted data into tables, which a blockchain, as the name suggests, organizes its data becoming to pieces (blocks) that are merged together. When developed in the manner of decentralized, this data structure creates an irreversible data chronology. Due a block is completed; it is etched in the stone and becomes parts of this chronological history. As addition of block into the chain completed, it is provided a specific time stamp. Each and every block contain SHA256 or cryptography protocol

C.) Secure Hashing Method (SHA) 256 is the hash function of Bitcoin Protocol and algorithm in order to mining, referring to the cryptographic hash function that outputs a 256-bit long result. The address generating and administration is regulated by 256- Hash. It is used for verification of transaction too. Hash function are used twice in Bitcoin which mean that SHA-256

The algorithm is a variation of the National Security Agency's SHA-2 (Secure Hash Algorithm 2). (NSA). SHA-256 is used in prominent encryption protocols too like SSH,SSL, and TLS, as well as operating system which allow people to use as open source such as Linux. The algorithm of Hash is incredibly secure, and its inner workings are not known to the general public. One change in Block, Entire hash will change.

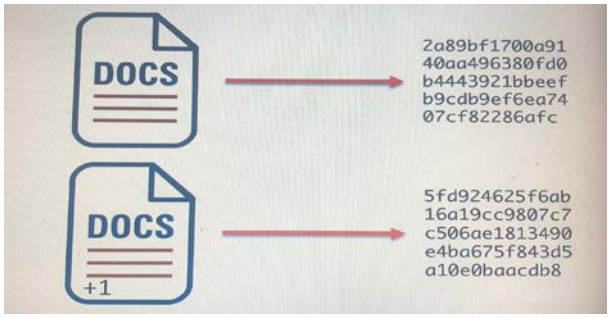

Figure 1: Change in Hash if one bit change in Block

D.) Mining Blockchain is transaction adding process to the blockchain which is already existed there ledger of transactions distributed among all blockchain users. Whereas most people associate mining of bitcoin, also it is employed by other blockchain-based systems. Mining involves creating a hash of a block of transactions that cannot be readily manipulated, hence, without a centralized mechanism method, guaranteeing the integrity of all block in blockchain will be proceeded. That is why some hackers utilize workstations they have broken into to mine bitcoins, causing an unsuspecting victim to pay for the costs of mining while reaping no advantages. Thus, the protocol to confirm whether the block in the chain is authentic is used; the protocol is Consensus Protocol.

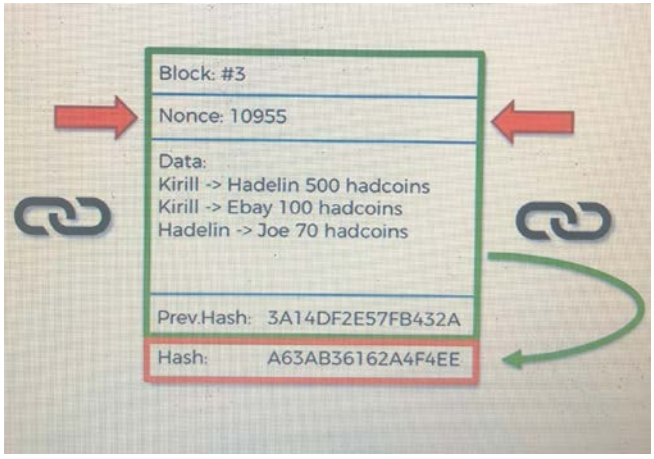

Figure 2: Example of Blockchain which have been mined

E.) The Consensus Protocol serves as the blockchain's foundation, allowing every participating node simultaneously verify transactions. The Bitcoins Consensus Protocol is implemented on Proof of Work (Pow), that consumes both time and resources. When comparison to Visa and MasterCard, Bitcoin's transaction verification rate is relatively slow, prompting the development of alternative consensus mechanisms..

All or any other blockchain apps, also known as decentralized applications (dApps), differ in terms of how networks reach consensus. Instead of using centralized nodes or servers, dApps use peer-to-peer (P2P) computer networks. Another feature of decentralized applications is the lack of centralized power. Most of the standard programs we use today are managed by a group of individuals or businesses that define the terms of use of dApps as the process of building a decentralized system of scale.Types of consensus protocols

Before we go into the consensus protocols, let's have a look at a statistical fact about them.
In theory, the blockchain is considered hacked if a hacker ga ins access to 51 percent or more of the network.
Different types of consensus procedures address the 51 perc ent attack problem in different ways.

Work Evidence

One of the first consensus protocols utilised in blockchain a pplications was Proof of Work.
It works by computing hash values and validating transactio ns until a certain number of trailing zeros are detected in the hash value. In the hash function, a nonce is defined as a random number that creates the required number of trailing zeros.

Properties Proof of Work is intended for permissionless public ledgers and relies on the computational power of the node's systems to achieve consensus.
A linear structure is used to represent the blocks. Each block is a collection of transactions.
The mining part of bitcoins is concerned with solving the cryptographic puzzle of locating a random integer, which leads to hashes with a certain amount of leading zeros.

Using the public and private keys issued to each user, each transaction is validated and signed.
Consensus methods serve as the foundation of blockchain by assisting all nodes in the network in verifying transactions. Bitcoin's consensus protocol is proof of work (PoW), which is both energy and time-consuming. In comparison to Visa and MasterCard, the rate of transaction verification in Bitcoin is relatively slow. As a result, other consensus protocols have been proposed.

All crypto-currencies and other blockchain apps, also known as decentralized applications (dApps), differ in terms of how the network achieves consensus. Instead of a centralized node or server, dApps use a peer-to-peer (P2P) network of computers. Another feature of decentralized applications is the lack of centralized authority. The majority of the standard programs we use today are managed by a group of people or businesses who determine the conditions of usage.

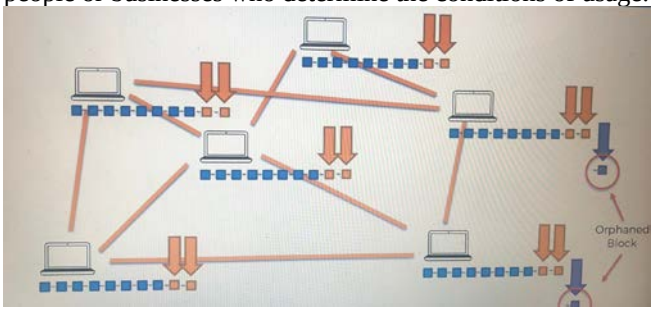

Figure 3: Process of Proof of Work of Consensus Protocol

Proof Of Stake(Ethereum)

Ethereum was one of the first major cryptocurrencies to adopt proof-of-stake consensus. Let's take a closer look at this case. Assume we are miners who are validating the transactions. A person who validates transactions in bitcoin by computing the hash value with a particular number of leading zeros receives the allocated quantity of bitcoins.

A validator is chosen and assigned a block as proof of stake consensus. To begin validating, the miner must assign a portion of his cryptocurrency. If the miner is successful in invalidating the transaction, the prize is the stake they initially committed, plus specified transaction costs. This is a method of penalizing bad behavior and incentivizing good behavior.

Properties

The validators are chosen based on their financial investment in the network.
The goal is to avoid the centralization of mining centers and to give all miners the opportunity to validate.
It is eco-friendly because there is no computational challenge to solve.
Mining does not necessitate the use of specialized gear. Which will protect the transaction of cryptocurrency

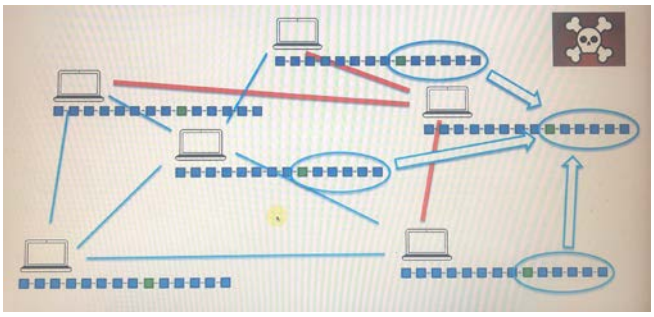
Figure 4: Identify Malicious attack by Consensus Protocol

F.) Cryptocurrency transactions It is a digital payment system that does not rely on banks to verify transactions. It is a peer-to-peer payment system that allows anyone to send and receive money anywhere. It is simply a digital record in an online database to verify the validity of a specific transaction. Instead of tangible money being moved and exchanged in the real world. Currency transactions, including bitcoin, are recorded in a publicly accessible ledger. Cryptocurrency is stored in digital wallets. Bitcoin was the very first cryptocurrency and remains the most famous one to this day. Most of the investment in cryptocurrencies is speculative, with investors sometimes driving prices sky high..

The term "cryptocurrency" refers to the use of encryption to verify transactions. This means that sophisticated encryption is used to store and transmit bitcoin between wallets and to public ledgers. The goal of encryption is security and safety. Each of transaction will to process after the next block of the chain have been mined. One who would mine it will get the reward from that block as they help provider find the hash of block which will process up to thousand transactions request from other node to be process. All of these transaction request will be stored in MemPool and then allocated by algorithm in the block to process such a transaction request.

G.)UTXO is The amount of digital currency that remains after a bitcoin transaction is referred to as an unspent transaction output (UTXO). It is similar to the change you receive after purchasing an item, but it is not a lesser denomination of currency—it is a transaction output in the database generated by the network to allow for non-exact change transactions. As an accounting measure, the portion of the total bitcoin that is not spent in a transaction is used. Each transaction, like double-entry bookkeeping, has an input and an output. Consider 1 BTC to be a bucket full of coins. A UTXO is represented by each coin. If you pay.5 BTC for something from Bob, the network will give Bob the entire bucket of coins and return the.5 BTC you owe in "change." You now have a.5 BTC UTXO that cannot be divided into smaller amounts.

H.) MemPool is where all legitimate transactions are held while the network of Bitcoin confirms them. A huge mempool size suggests increased traffic of network, as a result of which the average confirmation time is longer and the priority expenses are greater. The capacity of Mempool chart informs us the time consuming of the congestion would remain, The transaction of Mempool Count graphic, on the other hand, displays how Transactions are frequently clogged. For us to verify,

transactions from the mempool must be included in the block. The block cannot include more than 4 million weight units (1 million vbytes), and each transaction has its own weight dependent on the type of UTXO transaction utilised (input) and the address delivered to (output).
Each Bitcoin node produces its own version of the mempool by joining the Bitcoin network. The mempool material is compiled from some instances of the engineering team's current Bitcoin node. Blockchain.com; This enables us to collect as much data as possible in order to create a trustworthy meme pool.

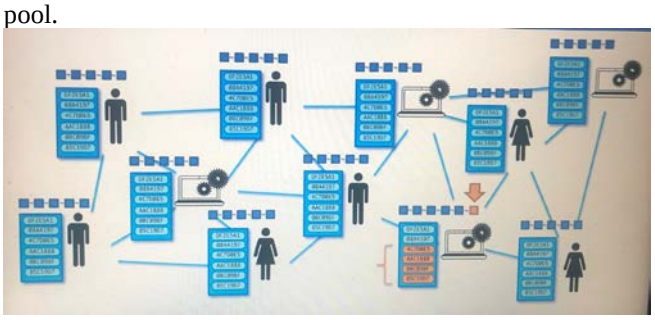

Figure 5: Transaction Process with MemPool

III. PROBLEM DESCRIPTION

Blockchain implementation will make the insight of protocol how each other protocol work and show how is it actually work and how can each node connect to each other by the specific HTTP which will be implemented.

Initially, we use Python and Flask to create site to decentralize the Genesis block or the initial block which will connect to each other nodes by connection via Flask site by HTTP format. The OSI Model which is the concept of Computer Network will be performed as node connection via Subnet http://127.0.0.1:5000/. After connection each node we will create smart contract by Grenache Ethereum Framework.

IV. ALGORITHM

START-> create block -> proof_of_work Consensus Protocol create -> check_if_chain_valid -> connect to Flask -> Get_mine_block ->Get_chain ->add_node ->add_transaction -> replace_chain

A.) Building Blockchain
Building blockchain with the algorithm which is required to be perform; create_block, get_previous_block, proof_of_work, hash, is_chain_valid, add_transaction, add_node, replace_chain which all these functions contain the algorithm of building Blockchain will be provided.

B.) Request Decentralization from Server
Deploy the Genesis blockchain which will be the initial block which will be chain if the next block is mined and chain to it.

C.) Connect Node
Pull request to HTTP server to connect the node with other node with different device which will mine the blockchain
D.) Start Mining
The algorithm which have been included will run and will mine the block itself

V. IMPLEMENTATION

Languages:-
Python, Solidity

Operating System:-
Windows

Library Packages or APIs Used:-

- Flask : To set up HTTP framework server environment
- Requests: To perform function request from Post man server environment
- Uuid : To show HTTP format message
- urllib.parse : To relate the HTTP message
- hashlib : To perform SHA256 algorithm
- datetime: To make a timestamp to Blockchain
- JSON : To get the json file for framework server environment

Framework:
Flask Framework server Environment

Software used:-
Ganache , Postman, Spyder(Python IDE),Solidity compiler

A. Decentralize Blockchain

Deploy the blockchain which have been create by compile the Spyder which will connect the node to Postman http://127.0.0.1:5000/ location and generate the Genesis Block which will be connected by other block later.

The block which will be mined and connect to the the chain will contain the data of the last blockchain too.

After running the program, the transaction would be performed too. The data of each transaction will be store in blockchain which will be mined after the request have been sent to MemPool and when there is exist the block to connect to the chain the transaction will occur in that block

B. Create Smart Contract

With Ganache software and solidity and MyEtherWallet We create the smart contract Server location which will provide you a Hash256 address as your address for wallet and with MyEtherWallet perform with the address from Ganache we could create the wallet with will contain the data as the solidity languages which have been developed by C++ languages

VI. RESULTS AND OBSERVATION

Given screenshots , provide the results that we have obtained.

A. Generate Genesis Block and connect node

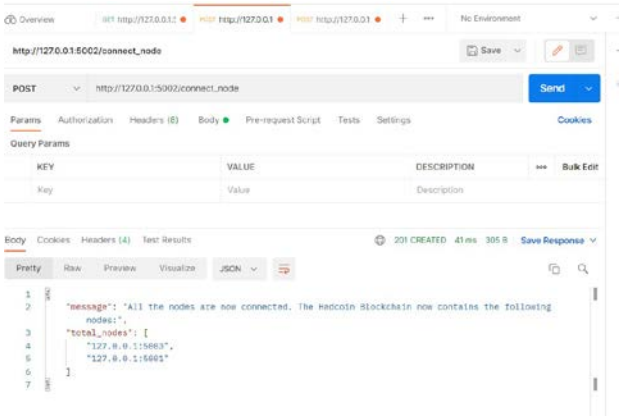

Figure 6: Connect Node

B. Mine the block

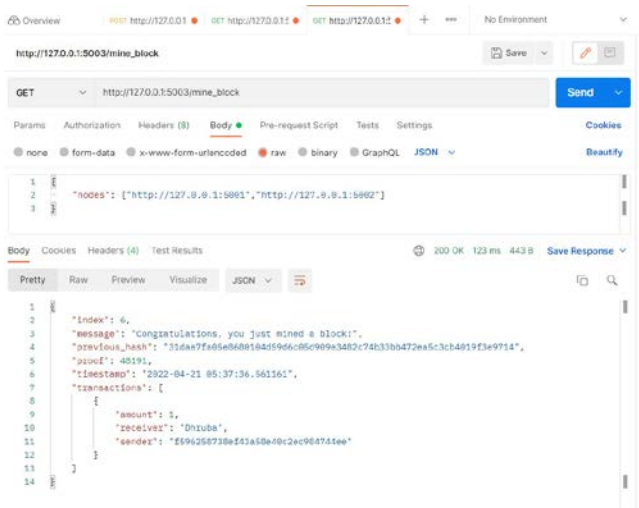

Figure 7: Mine the Blockchain

C. Longest Chain win the chain

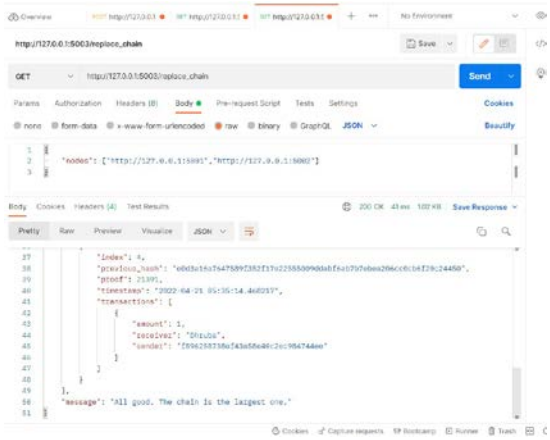

Figure 8: Longest Node win the chain

D. Make Transaction

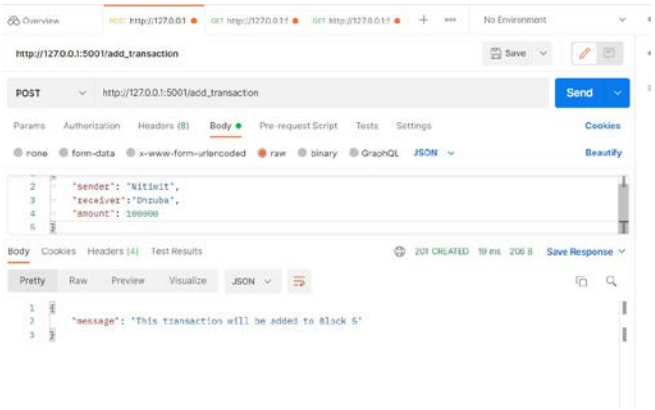

Figure 9: Make Transaction from port 5001 Nitiwit to 5003 Dhruba

E. Mine Block with Transaction

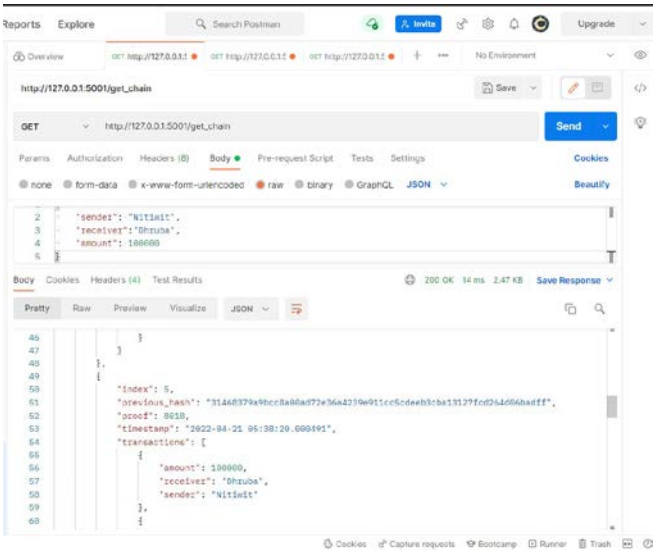

Figure 10: The blockchain with the transaction

F. Create Smart Contract

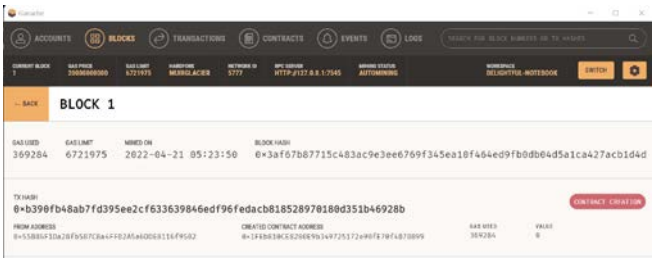

Figure 11: Smart Contract

H. Transaction with Smart Contract (Buy Had coin)

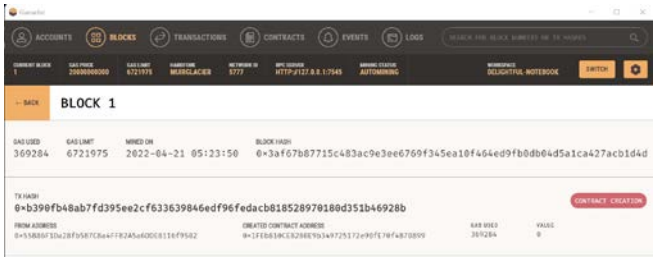

Figure 12: Ganache first transaction

I. Check value of Had coin

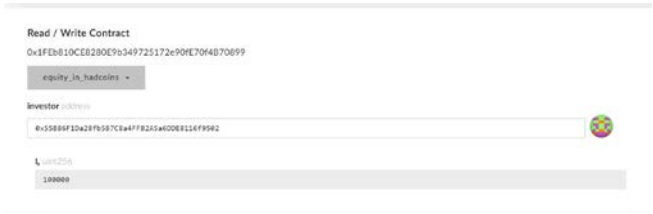

Figure 13: Value of Had coin in USD

J. Sell had Coin via Smart Contract

Figure 14: Sold had coin

K. Had coin Transaction in smart Contract

Figure 15: List of total transaction of Had Coin in our Etherwallet

VII. CONCLUSION

The blockchain is the new choice of transaction. There are thousands of transactions made in a minute via blockchain and smart contract even E-wallet.

We provided every detailed including for fundamental understanding of blockchain and cryptocurrency and smart contract which are very useful in the future of blockchain as it is easy to understand.

The implementation and application of smart contract and blockchain would be various in the future thus, provide the fundamental idea here is the aim of our project which related to computer network in term of Peer-to-Peer protocol.

In the conclusion, the idea of the topic might be developed into another Bitcoin in the nearer full as or be used as the currency itself as Ethereum nowadays is considered as the money for transaction too.

VIII. REFERENCE

[1] E. Agichtein, C. Castillo, D. Donato, A. Gionis, and G. Mishne. Finding high-quality content in social media. In Proceedings of the First ACM International Conference on Web Search and Data Mining (WSDM '08), 2008.

2] J. Allan, editor. Topic Detection and Tracking: Event-based Information Organization. Kluwer Academic Publisher, 2002

[3] Matches the Skype Network Traffic Forensics. 3 Internet Criminal Procedures and Trusted Computer Workshop, October 29-30, IEEE Xplore Press, Ballarat, pages: 19-27. Segment: 10.1109/CTC.2012.14 Bardis, N.G. furthermore, K. Ntaikos, 2008.

[4] H. Becker, F. Chen, D. Iter, M. Naaman, and L. Gravano. Automatic identification and presentation of Twitter content for planned events. In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media (ICWSM '11), 2011

[5] Al-Riyami, SS and K.G. Paterson, 2003. Uncertified public key cryptography. Methods for the Ninth World Theoretical Conference furthermore, Use of Cryptology and Information Security, November 30- Dec. 4, Springer Berlin Heidelberg, Taiwan, pages: 452-473. DOI: 10.1007/978-3-540-40061-5_29 Azab, A., P. Watters and R. Layton, 2012.

[6] Building security AES cryptographic-based visit application calculation and key administration. Methodology for tenth World WSEAS Conference on Mathematics Methods, Numeracy Methods and Intelligent Systems, (TIS '08), ACM, USA, pages: 486-49

[7] D. Sheiko, “Persistent Full Duplex Client-Server Connec-tion via WebSocket,”2010. http://dsheiko.com/weblog/persistent-full-duplex-client-ser-ver-conne ction-via-web-socket

[8] Makoto, “Living on the Edge of the WebSocket Proto-col,” 2010. http://blog.new-bamboo.co.uk/2010/6/7/living-on-the-edgeof-the-web socket-protocol