ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Value Transaction In Blockchain

Remya Stephen[#1], Aneena Alex[*2]

[#]*PG Scholar*
St. Josephs College of Engineering and Technology, Palai
[1]remyastephen93@gmail.com

[*]*Assistant Professor*
St. Josephs College of Engineering and Technology, Palai
[2]aneenaalex@gmail.com

***Abstract*—Blockchain is a modern technology in industry. Used for secured transaction. Blockchain technology has massive potential, and it has verity of applications. This will offer sever opportunities for different infrastructure. By avoiding third party interaction this technology will provide secured transaction and communication between two parties. Mainly it is done with a peer to peer communication. Trust is increased when conducting financial transaction between two parties. Blockchain technology will reduce the chance of defrauding. This paper focusing on how to make a secured transaction using blockchain. This transaction done based on a value. Simulation should be successfully run based on python language.**

Key words: Blockchain,Hashing,SHA-256, Ledger, Block

I. INTRODUCTION

Most of the banking systems should make money transaction based on different criteria. This transaction is done under some security system. Normally during a money transaction first application should communicate to the gateway by saying its credit card details. Then this gateway submits this information to internet merchant application. Then it will connect to merchant application. After this, merchant application should send back all these information to the applicant. So, this process should take much more time to its processing. There are many chances to hack sensitive data from users.

InsteadofthisBlockchain technology willprovideadvanced security especially for sensitive data. This will deal with a key based transaction. During the transaction value should be encrypted and then there will be a hashing is done using this key. In blockchain network every used have two keys. One private key and one public key. There is more than one block in a blockchain. Every block should have one parent hash and previous hash. This parent hash is pointed to previous hash of the previous block. At the top of the block there will be a nonce. Nonce is nothing but it is a cryptographical number. It only used in one times. This nonce system will help from some attack that is Finney attack. After completing a transaction this block should be added to its blockchain. After making a transaction balance should be updated and updated. After updating value, it will be validated for, if the balance is correct or not, or to check if there is any missing. Then every block should be validated before it adding to a blockchain. Like this it will jumped in to another block. Today all people were using modern technology for communicationthrough internet.Voice and video call,messages,pictures, are travel directly from sender to receiver over the internet. For this transaction we must maintain a trusted third party between these sender and receiver.When it comes in the case of money transaction,people have to trust a third party for complete this, in traditional system. But in the case of blockchain it will give a perfect security in transaction.Blockchain is a decentralized application, or it is one of the layer of the decentralized application.A block is the current part of a blockchain, which records some or all of the recent transactions. Once completed, a block goes into the blockchain as a permanent database [3]. If a block is completed a new block is added with this or a new block is generated.Countless number of blocks are connected to each other in the blockchain.Every block contains a hash of the previous block.

II. RELATED WORK

This section presents how secure blockchain echnolo gy than other security system. Focusing on its different applications, characteristics and its security issues

A. Security Analysis

Blockchain provide better security than other applications. The main advantage blockchain is, it will avoid the third-party interference. Instead of a third party it will appoint a ledger. Ledger is used to

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

store all transaction information.

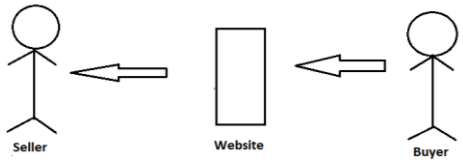

Fig:1 With third party

For example, considering figure 1. From this picture buyer wants to buy a product from the corresponding seller. Which is only possible through this website? Here this website is act like a third party. There is only a possible way, to trust thiswebsite or third party for buying this product. In this case there is a chance to hack this product, or product details. Blockchain gives a finite solution to this problem. That is ledger.

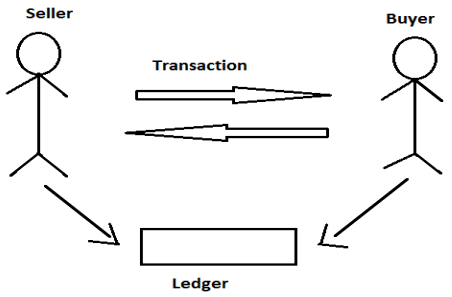

Fig:2 Without third party

From figure 2. This will explain ledger property. For example, there will be a transaction proceed between seller and buyer. This transaction should automatically have recorded in this ledger. This ledger is immutable. Nobody can change the data. This ledger provides much security from third party interaction. So, we can say that blockchain provide better security than other technology.

B. Applications of Blockchain

Blockchain can be used in different types of applications.

1. Blockchain for health care industry:

In the present life tolerant doesn't jump at the chance to uncover their treatment points of interest to untouchable. For this situation patient can utilize this innovation to keep secure all data from others. This blockchain can be utilized as a site, or versatile application. Every last client in a blockchain has two keys. Open key and private key. By utilizing this no one but who can make an exchange. For instance, there two-man Alice and Bob. Alice need to send some protected information to sway. With the goal that Alice sign an advanced mark by utilizing here private key. That implies private key is dependably act like as a secret key. At that point shew will hash the information by utilizing here open key and create an address. At that point sway approve the advanced mark. In the event that it is approved they will make an exchange. So, by utilizing these sort of security techniques, mixtures data can be shielded from others

2. Blockchain to protect personal data

Today there is late increment in announced occurrence of security issue in clients individual information. In view of this there is an outsider control over the information, who will gather all individual data. Blockchain can dispose of this outsider and can exchange specifically between two gatherings. The measure of information as of late expanding in our reality. Facebook, is the biggest online social network, gathered 300 petabytes of individual information. Individual information or delicate information ought not be secure in the hand of outsiders. They are attempted to assault and abuse. Blockchain helps clients that not required to put stock in any outsider. Blockchain perceives the clients as the proprietors of theirown information. Blockchain ought to have its own particular guidelines and control. It is known as brilliant contract. Before beginning an exchange, the door manager ought to make a few standards and will composed as an agreement. It will make a shared correspondence. Bitcoin has exhibited in financial space that is trusted and figuring is conceivable in decentralized system. Blockchain is for the most part proposed to deal with the bitcoin, it is an advanced money.

Electronic medical records

Patients can deal with electronic therapeutic records by utilizing the blockchain innovation. The vast majority of the wellbeing cares establishment ought not enable patient to get to their medicinal information. Patients are getting to be baffled about the security of their therapeutic records. This all can be stayed away from by blockchain. In taking care of electronic medicinal records, blockchain should manage deferent outline work for dealing with the verification, and responsibility. It is for the most part utilized when taking care of the touchy information. Online electronic records in blockchain will worked as decentralized application. In brought

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

together condition all application ought to be done at one area. Be that as it may, in decentralized condition application ought to be done in deferent area. Electronic restorative records ought to act a few difficulties and constraints. That is this by and by controlled records would supplant supplier or doctor's facility records. Some section of the by and by controlled records would be downloaded in to the institutional record to tribute the current information These difficulties can be evaded by blockchain. Since blockchain drives a key trade-based exchange between two gatherings. Their own personality does not delight to any others. Since they are just giving their key personality. Every single client in a blockchain ought to have one open key and one private key.

3. Real Estate

Governments and private companies were tried to reduce land title and fraud by choosing ledger as a way. Real estate business is done with full of paper work. Then there is a chance to enter an attacker. Because these details are not immutable. Real estate business should have several procedures and there is a presence of middle man. So, the customer needs to trust this third party.

To avoid this problem most of the companies were deviated to blockchain technology. It will make real estate as more efficient, flexible and transparent. Blockchain technology will provide the full history of the land. All details should be open to each and every people in this network.

4. Charity

Today people could collect money in name of some charity. But actually, we don't know where this money is going, or if the collected money is reached at correct destination. People are cheated by these types of fraud fund. People were thinking they are doing a favor for the poor people. But The must knowsroute of this money.

Public ledger is an application to use in this situation. Every user in a blockchain should have a public ledger. This ledgershould automatically record all transaction. In the case of charity, people can view the route of money.

III PROPOSED SYSTEM

In proposed system, simply transacting a value between two persons. Before transacting the data, it will be hashed by sha256 algorithm.

- Hashing

Hash is an encrypted form of input data. Applying some algorithm to input data and get another unreadable form of output data is called hashing. Input can be any type of data or any number of bits represent any document, mp3 file, value, money or digital currency. There are different types of algorithm for hashing. In this project SHA-256 is used to hash the input. After hashing the input, it will give fixed length of hashed output. Every simple letter can be hashed. A hash can be generated from a piece of data but cannot generate data from a hash. Simple example for a hash is given in figure 3.

```
In [36]: block_chain[0]

Out[36]: {'contents': {'block_number': 0,
          'parent_hash': None,
          'transaction_count': 1,
          'transactions': [{'Person1': 50, 'Person2': 50}]},
         'hash': 'e349411242acc5fae2b00298ee3fad6af83dfad7a45e09905a7fe5406f3985b0'}
```

Fig:3 Hashing

From the figure it is a python code for value transaction. It denotes the zeroth block. Here block number is represented as zero. Every block should have parent hash and previous hash. Previous hash pointed to hash of the previous block.

A typical utilization for hashes today is to unique finger impression documents, otherwise called check zones. This implies a hash is utilized to confirm that a record has not been messed with or altered in any capacity not expected by the creator. On the off chance that WikiLeaks, for instance, distributes an arrangement of records alongside their MD5 hashes, whoever downloads those documents can confirm that they are really from WikiLeaks by figuring the MD5 hash of the downloaded documents, and if the hash doesn't coordinate what was distributed by WikiLeaks, at that point you realize that the record has been altered some way.

The principal hash is figured for the primary block or the Genesis block utilizing the transaction inside that block. Primary transaction is used to compute a s block hash for the Genesis block. Each new block is generated after a transaction. Its previous hash is additionally used as next blocks parent hash, and also its own particular transaction or input denotes to decide its block hash. This arrangement of hashing ensures that no exchange in the history can be messed with on the grounds that if any single block of the transaction changes, so does the hash of the square to which it has a place, and any after block hashes therefore. It would be genuinely

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

simple to get any altering accordingly on the grounds that you can simply think about the hashes. This is cool in light of the fact that everybody on the blockchain just needs to concur on256 bits to speak to the possibly boundless condition of the blockchain.

❖ SHA-256

SHA represented as Secured Hash Algorithm. It is similar to SHA-1 algorithm. SHA-256 is based on MD5, MD4, and SHA-1. Its function operates in 512 bits message block and 256-bit intermediate hash value. It encrypts the intermediate hash value using message block as a key. This hash function is design by NSA (National Security Agency) [12].

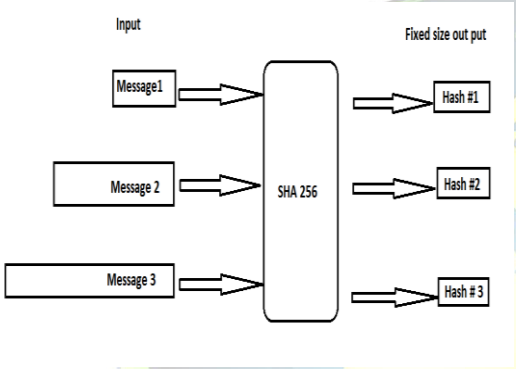

Fig:4 SHA-256

In Blockchain SHA-256 used in many situations especially in mining part. SHA-256 will generate almost fixed size of 32bytes hash value. Shown in fig 4

In this task SHA-256 is utilized as a part of python dialect. It is an inbuilt usefulness in python. So, there is no compelling reason to compose every one of the elements of SHA-256. Rather than this exclusive need to influence a call with the hash to work.

IV PROCESSING METHODS

❖ Transaction Definition

When transacting a value through blockchain, first someone request a transaction. This transaction request should be broadcast into the network via peer to peer communication. The network consists of different nodes. Each and every node should be represented as a computer. Example for transaction definition or how to set a transaction is shown in fig.5

```
In [2]: def make_transaction(mVal = 3):
            sign_bit  = int(random.getrandbits(1))*2 - 1
            tr_amount = random.randint(1,mVal)
            p1_pays   = sign_bit * tr_amount
            p2_pays   = -1 * p1_pays
            return { 'Person1':p1_pays, 'Person2':p2_pays}

        transactions_buffer = [make_transaction() for i in range(30)]
```

Fig: 5 Make Transaction

❖ Validation

Transaction request is broadcasted in to the network. Then the consisting nodes should be validated the transaction and its history. One of the other benefits of blockchain security is it will keep all the history of transaction.

```
def validate_transaction(amount, balance):
    if sum(amount.values()) is not 0:
        return False
    for key in amount.keys():
        if key in balance.keys():
            account_balance = balance[key]
        else:
            account_balance = 0
        if (account_balance + amount[key]) < 0:
            return False
    return True
```

```
balance = {'Person1':5,'Person2':5}

print(validate_transaction({'Person1': -3, 'Person2': 3},balance))
print(validate_transaction({'Person1': -4, 'Person2': 3},balance))
print(validate_transaction({'Person1': -6, 'Person2': 6},balance))
print(validate_transaction({'Person1': -4, 'Person2': 2,'Person3':2},balance))
print(validate_transaction({'Person1': -4, 'Person2': 3,'Person3':2},balance))
```

```
True
False
False
True
False
```

Fig: 6 Validation

After validate a transaction it will proceed to make a transaction. Then it will be added to the older transaction andcreate a new block of data. The new block is added to the blockchain. Then this is permanent and immutable. Like this the network will make another transaction request. Example for transaction validation in python language is shown in fig.6.

❖ Update Balance

After making a transaction, need to update the balance. Because if there is any fault, can be identified through this. Each and every transaction will be recorded in ledger, and it will also have updated

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

❖ Block Validation

The validator nodes of the system get the proposed block and work to approve it through an iterative procedure which requires accord from a lion's share of the system. Diverse blockchain systems utilize unique approval methods. Bitcoin's Block chain utilizes a method called" confirmation of-work", Swell uses" Disseminated Consensus", and Ethereum utilizes" confirmation of-stake". Distinctive advantages and disadvantages there for various technique. The shared factor is that they guarantee that each transaction is substantial and make deceitful transaction unthinkable.

❖ Block Chaining

On the off chance that all transactions are approved, the new block is" anchored" into the blockchain, and the new current condition of the record is broadcast to the network. This entire procedure can be finished in 3-10 seconds.

V SECURITY FEATURES

- Utilize ledger. Ledger should record every single transaction in a blockchain. This record is changeless. Existing information can't be altered or erased. In blockchain innovationtheserecordisdecentralizedapplic ation.Thus, nobody can get to the exchange or even any delicate information from this record. Individuals can just read the data from a record [11].
- Another kind of security include is the chain of block. In blockchain each block ought to contain a hash esteem. These squares are associated by its past hash. Assume an aggressor came to remedy the information, at that point its hash will be changed. It will aect the general chain. In this way, it will expand the assurance of delicate information or data.
- Blockchain innovation is a decentralized application. Essentially it will bolster shared correspondence. In this way, in a system node is considered as PCs. These a huge number of hubs or nodes should to have the duplicate of appropriated record. This is validated the transaction. In theeven that anyofthehubdoes notconcuranexchange, at that point it can't be continuing. In this way, it will be cancelled. This will shield from a misrepresentation exchange [11].

VI CONCLUSION

Blockchain is an astounding subject in late year, it will bolster deferent applications. Blockchain will give Better security amid exchange of any esteem. This innovation is chiefly proposed to dealing with bitcoin transaction. Smart contract, Ethereum and conveyed record are a few utilizations of blockchain, this will likewise give greater security. Most appropriate and for the most part utilized application of blockchain is bitcoin. Blockchain gives quicker and less expensive exchange than some other application. It will

give a superior security particularly to touchy information. Blockchain applications regularly observe extra beets in its straightforwardness and unchanging nature.

REFERENCES

[1] http://www.blockchain4innovation.it/wp/content/uploads/sites/4/2017/05 blockchain

[2] https://www.coindesk.com/information/who/created/ethereum

[3] Iuon-ChangLin1,2 and Tzu-Chun Liao2-ASurveyofblockchain securityissueandchallengesjan-12- 2017

[4] Kenneth D Mandl, PeterSzolovits, Issac S Kohane- Public standards and patients controll:how to keep electronic medical records accessible butprivate3 february 2001

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, Medrec: Using blockchain for medical data access and permission management, in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 2530

[6] G. Zyskind, O. Nathan, and A. Pentland, Decentralizing privacy: Using blockchain to protect personal data, in Security and Privacy Workshops (SPW), 2015 IEEE, May 2015

[7] https://www.researchgate.net/publication/319058582 Blockchain Challenges and Opportunities A Survey

[8] http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf

[9] https://www.dotmagazine.online/issues/innovation-in-digitalcommerce/what-can-blockchain-do/securityand-privacy-in-blockchainenvironments

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

[10] https://www.evry.com/globalassets/insight/bank2020/bank2020blockchain/powering/the/internet/of/value/whitepaper.pdf

[11] https://www.business2community.com/tech-gadgets/issues-blockchainsecurity-02003488

[12] http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf