Asian Journal of Research in Computer Science

8(4): 12-20, 2021; Article no.AJRCOS.68126
ISSN: 2581-8260

BPS: Blockchain Based Decentralized Secure and Versatile Light Payment System

Shahed Ahamed[1*], Moontaha Siddika[1], Saiful Islam[1], Sadia Saima Anika[1], Anika Anjum[1] and Milon Biswas[1]

[1]Computer Science and Engineering, Bangladesh University of Business and Technology, Dhaka, Bangladesh.

Authors' contributions

The word has done by all of our team members hard work. Each and every of team members did this work with a lot of responsibilities. In one word it would be impossible without the collaboration of all team members. In specifically Author SA maintain the all responsibilities of each and every team members besides he did some works in coding section and he drew all the figure related work. Author SI who maintain the most of the coding part. Author AA did really hard work in maining the latex for designing the paper. Authors MS and SS help in some writing part. Author MB was the supervisor throughout the work. After completing the paper all the members read and approved the final manuscript by our supervisor.

Article Information

DOI: 10.9734/AJRCOS/2021/v8i430206
Editor(s):
(1) Dr. Manish Mahajan, CGC College of Engineering, India.
Reviewers:
(1) Jasvant Mandloi, Government Polytechnic Daman, India.
(2) Pratik Patel, GTU, India.
Complete Peer review History: http://www.sdiarticle4.com/review-history/68126

Original Research Article

Received 27 February 2021
Accepted 03 May 20211
Published 14 May 2021

ABSTRACT

In the present age, online payment system is a very simple practice. But many people use this system to manipulate people's money. Many are trying for finding a variety of solutions. But there is no way to stop that crime. Blockchain's yoke is a blessing. Using blockchain is a very easy way to complete a payment without making any mistakes. Hacker will never find a way to do their work in this kind of system. Our System is full worked with Blockchain. Basically, we choose blockchain as our project because it is the most secure way to do a transaction in every online system. The central business model is based on a database management system. Once accomplished the security of the transaction can no longer be guaranteed. On the other hand, it is really expensive to resolve possible fraud transactions by a middle man. Aiming at solving issues concerning security and worthlessness, there is a proposal of a model which is completely made of blockchain system. In Our system there are many blocks of information of each and every transaction. We have

*Corresponding author: E-mail: 16172103157@cse.bubt.edu.bd;

proposed an algorithm. The algorithm will make consumers able to transact through cryptocurrency in blockchain networks. It is totally different from the fiat system where consumers will be able to transact without the help of third parties and vendors can also be relieved with their transaction. This type of transaction will be very comfortable for both consumers and vendors. Consumers along with vendors can see the whole transaction date, time and everything that they dealt with when the transaction was held.

Keywords: Blockchain; secure transaction; electronic payment; cryptocurrency; bitcoin.

1. INTRODUCTION

Promoting the throughput of blockchain systems like bitcoin and cryptocurrency has been an important research problem. Again, in this era off-chain systems of payment are the most pledging technologies to accept this challenge. Considering the overall situations of payment system blockchain has made a tremendous change. Once cash was the primary way of transaction. People would buy and sell everything using hard cash. Then debit and credit cards became popular. People can easily buy and sell their products using debit or credit card but for this consumer along with vendors need to pay an amount of fees to the bank. Sometimes the address can be changed from unauthorized threats. That is a risk of payment transaction. There has been a massive change in the payment system for a few years. Now the most common and the most impressive part of the payments system is the cryptocurrency. It brings a massive change in this site. Day by day people are very interested in this system. This can store payment transaction. But though the most common using site is debit or credit card system to transfer money for education site and others. Our propose model is all about blockchain related works. Our main aim is to make a secure payment system where one can easily transact their usual transaction. We have developed the system. The system will fully be managed by some minors who validates the transaction. The transaction is built into a block. And the transaction is broadcasted across the whole network. And then the block is added to the chain. Each block is added through a process POW (proof Of Work) which acquires permission on blockchain network for confirming the transaction or adding new block into the chain. There is a hash function which is conducted in this model. And the hash function is used which takes a transaction input and returns it into the output of the fixed length. Using this hash function to transact the data, that is the process of hashing. The transactional output of the given hash function which is called hash. Hashing uses SHA-256 algorithm. That is the process of completing the transaction. Then our system enforces to secure this that is actually reliable for the user. At first Certificate Authority will generate two types of keys-public key and private key. They are used for encryption and decryption. And the private key is used to generate the digital signature that makes the transaction more secure. And the miner validates the transaction. Actually Blockchain technology is an innovation idea for payment transaction. It can prevent the transaction from an unauthorized access and can store the whole transaction securely.

Every user will get their personal signature and miner will check the signatures if there any problem then the minor could stop the transaction. by these key minors make users signature. The Enacting empiric outcomes via the well-known digital wallet and bitcoin has make our system much secure.

2. EXISTING WORK AND LIMITATION

Nowadays technology has enriched each and every sector in many ways. In this recent world everything is automated like E-voting [1,2], supply chain management [3], robotics [4], vehicle registration [5], national identity card management [6], sentiment analysis [7], applications for own security [8] and so more. Many researchers have been conducted on blockchain and its application. There is a secure and efficient payment solution for MOOC environment in blockchain technology. MOOC is actually an online education platform. It is based on the database management system [9]. There is a distributed payment system based on payments token. It can protect the consumer from identity theft [10]. Thing-to- thing payments are a central facilitator in the IOT. It offers the devices to pay each other without any human interaction [11]. When a transaction is done by an IOT device, it takes a long time to verify when transactions are done in two places using the same blockchain wallet transaction. To resolve this problem, they have made a prototype which is FastPay where it takes only 9 second to solve

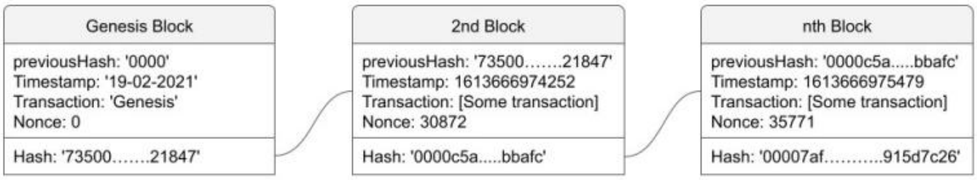


Fig. 1. Securely hashing data flow in blocks of blockchain

it. In FastPay prototype, there is a special user named Broker who works in the middle between payer and payee. To do a transaction using FastPay prototype, 4 steps should be done [12]. In this paper they have promoted a solution which is designed to solve the problem of latency in Blockchain networks in relation with the ability of running real-time services monetized through cryptocurrency. They have raised a solution that runs off- chain which facilitates agreements between the vendors and the customers. It manages late payments. A transaction represents a cryptocurrency transfer between two nodes that is executed within the main network. In this paper they develop LATENT TRANSACTION ALGORITHM. It performs all the latent transactions which is recorded on the ledger until that time [13]. There is a cost saving approach which minimizes the transaction time and storage for small amount of time. Electronic coin is presented by the chain of digital signature [14]. Each block records a set of transaction and the associated metadata. Satoshi Nakamota first perceive the blockchain as a peer to peer money exchange process. Nakamota refer a transactional token as bitcoin [15]. A peer-to-peer version of electronic cash system offers online payments to transact directly one client to another client without the favour of a trusted third party. There is a solution to the double spending problem using a peer-to-peer network. Transactions which are ineffective to inverse would defend sellers from deception. Electronic coin is identified as a chain of digital signature. Each owner transfers the coin to the next by signing a hash of the previous transaction and the public key of the next owner. Payee can verify the signature to verify the chain of the ownership [16]. In order to set up a concrete DCAP system, we first planned a Condition Anonymous Payment (CAP) scheme (based on our proposed signature of knowledge), whose security can be exhibited under the defined formal semantic and security models. The conditional anonymous payment scheme is required to provide the traceability of the transaction in order to identify the long-term address of the sender of a envious transaction. The current value-added tax (VAT) administration system performs as a centralized server, which consists of high risk attacks by hackers. Only a few countries use the digital technology to calculate and manage VAT. By combining Decentralized Storage Network (DSN) with Smart Compact (SC), a new model is offered based on blockchain technology for authentication of the transaction, calculate and approve VAT [17]. Embedded secure bitcoin payment module is designed to realize the automatic payment. There is crypto chip in the module can provide crypto algorithm to protect the transaction and there is security protocol which deals with transaction process. Data deduplication is one of the important technologies to decrease the storage cost of cloud storage system. In a cloud storage system with deduplication technology, the client can outsource the data files to the cloud storage server and pay for them [18]. There is a paper of improving Banking Transactions Using Blockchain Tech- nology. The majority of banks offer various online services to their customers that focuses especially on domestic and international banking transactions. Banks use enough time to perform bank transactions from one bank account to another, some of which take more than a week [19]. In paper [20] there is a payment system DCAP. DCAP is decentralized conditional anonymous payment. Since all bitcoin transaction are publicly attainable so the real identity of the user attack the network analysis, address clustering and transaction graph. The transaction anonymity of CAP scheme is integrated into the DCAP system for preventing the users' real identities from being disclosed. Exchanges chained within the DCAP framework allude to a SPK verification, which is created by the mysterious private key (comparing to the sender's mysterious address). Confirmation of these exchanges as it were includes the mysterious addresses of sender and collector, instead of their long-term address. But in this paper, there are some limitations like they do not provide users digital signature which can ensure their security. Users and administrators on this system will not be able to see the balance from users accounts by which they can ensure whether attackers are trying to hack the system or not.

In the existing system, the system sends a request to the sender before the receiver. The sender then verifies the request with the certificate authority. The certificate authority executes all the work. In this, the system blocks his account when he unknowingly makes a transaction. The existing system immediately blocks the user and cancels the transaction in case of any suspicious transaction. This is the limitation of the existing system. In our system, we have tried to solve this problem.

3. FUNDAMENTAL OF TRANSACTION PROCESS

A. Blockchain

Blockchain could be a system of recording data in a way that produces it difficult or inconceivable to deflect, hack, or cheat the framework. It could be a particular sort of database. Distinctive sorts of data can be put away on a blockchain but the paramount common utilize so distant has been as a record for exchanges. Every single transaction is stored in a public list that is regarded as a blockchain.

B. Bitcoin

Bitcoin may be a decentralized computerized money, with- out a central bank or single director, that can be sent from client to client on the peer-to-peer bitcoin arrange without the requirement for intermediary. Bitcoins are made as a remunerate for a handle known as mining. Each bitcoin is a computer record which is stored in a digital wallet on a computer.It is an online form of cash.

C. Cryptocurrency

The word “cryptocurrency” is inferred from the encryption procedures which are set to secure the arrange. Cryptocurrency may be a frame of installment that can be traded online for products and administrations. Numerous companies have issued their possess monetary forms, frequently called tokens, and these can be exchanged particularly for the great or service that the company gives. Cryptocurrencies work employing a innovation called blockchain.

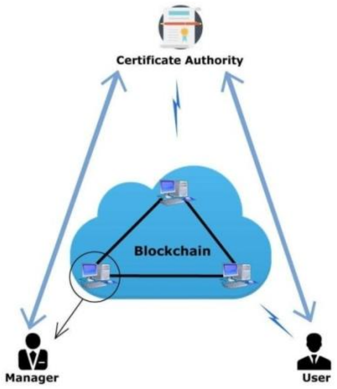


Fig. 2. Blockchain

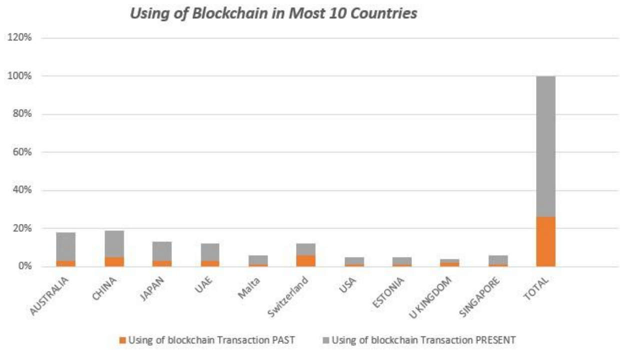


Fig. 3. Statistics of using blockchain system in most 10 countries around the world

4. SECURE TRANSACTION PROCESS

Definition of Algorithms: Here we present the transactions of payment system. S and R are the sender and receiver of the transaction. Additionally there are miner who actually validates the transaction.

Keygen: 1exp φ Taking input that is a security parameter and the algorithm returns a pair of public key (Pk) and private key (Pr). Sign (Pr, m): It takes a private key Pr as input and m. This algorithm returns a signature γ on m.

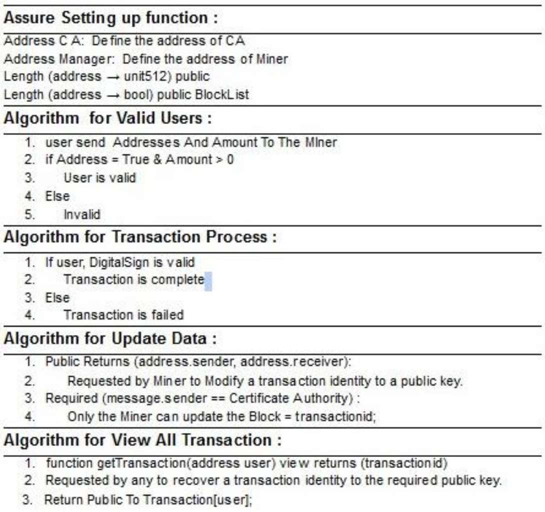
Verify (γ, Pk): It takes a input signature & public key pk. The algorithm returns true or false. This algorithm is called to verify the transaction.

BlockchainGen (b, Pk, Pr, n): Taking input bitcoin b, public key Pk, private key Pr, n chain. Algorithm returns a chain of n chains. Then the blockchain is created. And then bitcoin is altered into a chain of n chains.

The whole transaction Process is completed in 5 phases. The phases are given bellow:

Phase 1 Setting up function: CA is regarded as a trusted third party who is accountable for managing the certificate of users. In this model, their task is to generate the public key for the user. Here the public key can address 512 unit of length and then store them to a block.

Phase 2 Valid users: In this phase miner verifies the users by their address and amount. If the amount is greater than 0 then the user is valid.



```
Assure Setting up function :
Address C A:  De fine the address of CA
Address Manager:  Define the address of Miner
Length (address → unit512) public
Length (address → bool) public BlockList

Algorithm  for Valid Users :
user send  Addresses And Amount To The MIner
if Address = True & Amount > 0
    User is valid
Else
    Invalid

Algorithm for Transaction Process :
If user, DigitalSign is valid
    Transaction is complete
Else
    Transaction is failed

Algorithm for Update Data :
Public Returns (address.sender, address.receiver):
    Requested by Miner to Modify a transaction identity to a public key.
Required (message.sender == Certificate Authority) :
    Only the Miner can update the Block = transactionid;

Algorithm for View All Transaction :
function getTransaction(address user) view returns (transactionid)
Requested by any to recover a transaction identity to the required public key.
Return Public To Transaction[user];
```

Fig. 4. System Algorithm

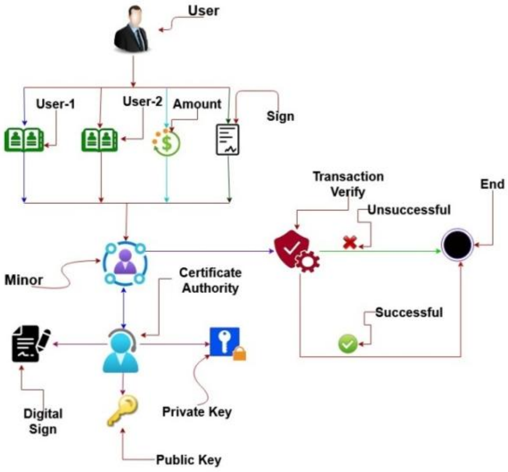


Fig. 5. Secure transaction process using blockchain technology

Phase 3 Transaction process: UDS (User digital signature) is a term which is used to validate the authenticity and integrity of the transaction. It is created for users. There are miners for checking the digital signatures. If digital signature is valid then the transaction happens otherwise it cancels the transaction.

Phase 4 Update data: If the users need to update some data, they send request to miner to update the data. Then miner does the task with the help of certificate authority and update the block with updated information.

Phase 5 View all transactions: All blockchain transaction must be checked by miners. It will be checked if there is any transaction without public key. Miner can store the transaction securely and can view all the transactions.

5. IMPLEMENTATION

We have implemented the transaction process that is secure and reliable.Here is a JSON file that is used to represent the structured data.

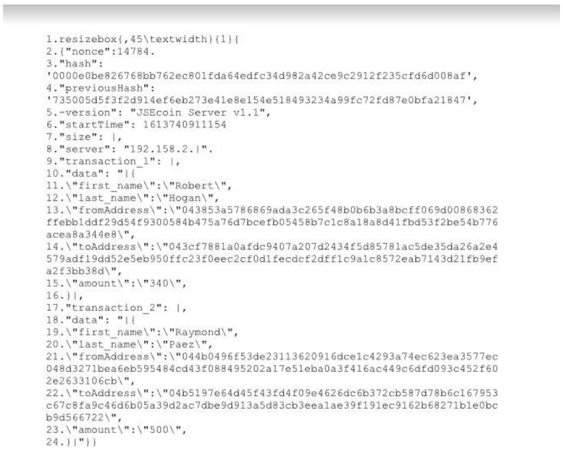
6. RESULTS AND ANALYSIS

An application is developed on the basis of secure transaction system using blockchain. The simulation results showed that the blockchain based proposed transaction system would bring the following benefits:

1. In our proposed architecture, the sender gives all the information to the minor. Then the miner verifies all the information. But in the older system, receiver sends a indictment to the sender and sender then transmits all the information to the Certificate Authority (CA) for the verification and it’s a time consuming process. So our system is comparatively much faster.

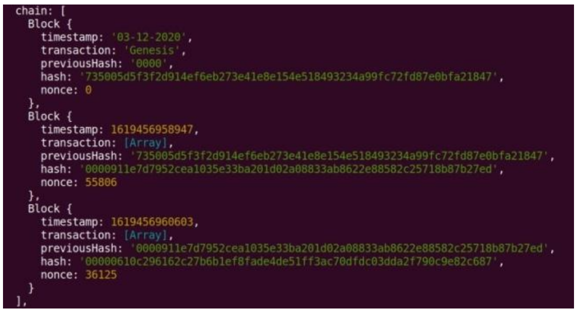
We have proposed the comparison between the existing system and proposed system in Table 1.

2. In our proposed system the work of the Certificate Authority (CA) has been divided with the miner so that it can perform more requests comparatively the older system. In the older system, the Certificate Authority (CA) executes all the work so it takes much time to complete the requests than our proposed system.



```
resizebox{,45\textwidth}{1}{
{"nonce":14784.
"hash":
'0000e0be826768bb762ec801fda64edfc34d982a42ce9c2912f235cfd6d008af',
"previousHash":
'735005d5f3f2d914ef6eb273e41e8e154e518493234a99fc72fd87e0bfa21847',
-version": "JSEcoin Server v1.1",
"startTime": 1613740911154
"size": |,
"server": "192.158.2.|".
"transaction_1": |,
"data": "|{
\"first_name\":\"Robert\",
\"last_name\":\"Hogan\",
\"fromAddress\":\"043853a5786869ada3c265f48b0b6b3a8bcff069d00868362
ffebb1ddf29d54f9300584b475a76d7bcefb05458b7c1c8a18a8d41fbd53f2be54b776
acea8a344e8\",
\"toAddress\":\"043cf7881a0afdc9407a207d2434f5d85781ac5de35da26a2e4
579adf19dd52e5eb950ffc23f0eec2cf0d1fecdcf2dff1c9a1c8572eab7143d21fb9ef
a2f3bb38d\",
\"amount\":\"340\",
}|,
"transaction_2": |,
"data": "|{
\"first_name\":\"Raymond\",
\"last_name\":\"Paez\",
\"fromAddress\":\"044b0496f53de23113620916dce1c4293a74ec623ea3577ec
048d3271bea6eb595484cd43f088495202a17e51eba0a3f416ac449c6dfd093c452f60
2e2633106cb\",
\"toAddress\":\"04b5197e64d45f43fd4f09e4626dc6b372cb587d78b6c167953
c67c8fa9c46d6b05a39d2ac7dbe9d913a5d83cb3eea1ae39f191ec9162b68271b1e0bc
b9d566722\",
\"amount\":\"500\",
}|"}}
```

Fig. 6. Implementation of the system model



```
chain: [
  Block {
    timestamp: '03-12-2020',
    transaction: 'Genesis',
    previousHash: '0000',
    hash: '735005d5f3f2d914ef6eb273e41e8e154e518493234a99fc72fd87e0bfa21847',
    nonce: 0
  },
  Block {
    timestamp: 1619456958947,
    transaction: [Array],
    previousHash: '735005d5f3f2d914ef6eb273e41e8e154e518493234a99fc72fd87e0bfa21847',
    hash: '0000911e7d7952cea1035e33ba201d02a08833ab8622e88582c25718b87b27ed',
    nonce: 55806
  },
  Block {
    timestamp: 1619456960603,
    transaction: [Array],
    previousHash: '0000911e7d7952cea1035e33ba201d02a08833ab8622e88582c25718b87b27ed',
    hash: '00000610c296162c27b6b1ef8fade4de51ff3ac70dfdc03dda2f790c9e82c687',
    nonce: 36125
  }
],
```

Fig. 7. Implementation result of the system

Table 1. Comparison between the existing system and the proposed system

Classify	Existing system	Proposed system
Verification	In existing system the verification is weak.	In proposed system the verification is very strong.
Task Manager	In existing system task is managed by CA.	In proposed system CA has been divided with the miner to manage the tasks.
Unauthorized Access	Existing system blocks the unauthorized access.	Proposed system records the unauthorized access and store it for further investigation.
Time Consuming	Existing sys- tem is more time consuming.	Proposed system is less time consuming.

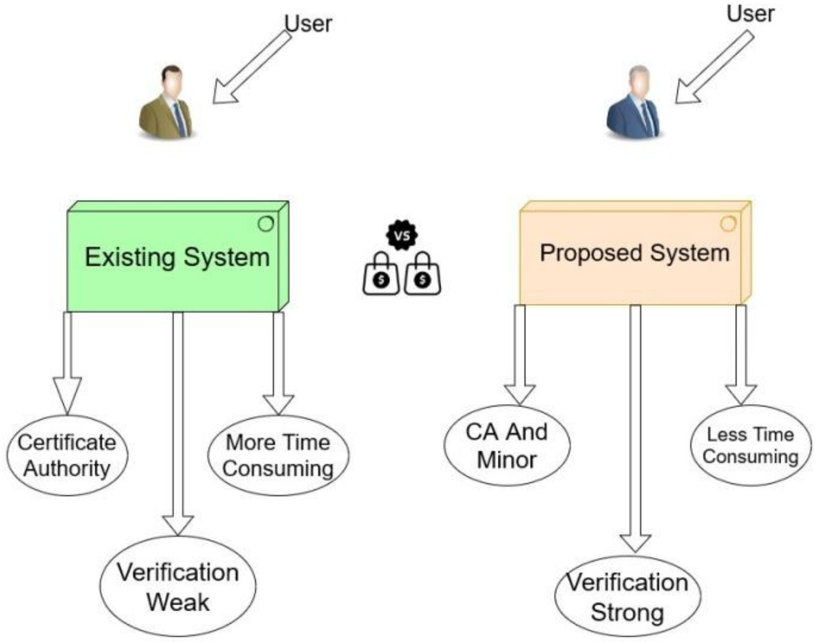


Fig. 8. Comparison between existing system and our system

3. If our system finds that someone is trying to make an uninformed transaction, it immediately cancels the transaction, puts it on hold instead of blocking the account. But in this type of case, the older system immediately blocks the user and cancels the transaction.

7. LIMITATION OF OUR SYSTEM

There are some limitations which we have faced in the system.

1. Blockchain needs a large network of users. For that sometimes this causes problem.
2. Having a server of our certificate authority takes a little comparative time to create private keys, public keys and digital signs.
3. The structure of blockchain is relatively difficult to under- stand.

8. CONCLUSION

From the experiments , we have tried to secure the payment transaction that is easy and more flexible. Blockchain has the potential to help someone or some organization that use it to ensure transactions as well as safety. We have already developed a secure return system. The main objective of our work was to secure the payment system .We also introduce some advance services. In doing so, we have faced many difficulties and overcame them. We discuss about the reliability of a secure transaction system. In our model, anyone can maketheir personal or business transactions through a beautiful payment system that is actually secure, easy and a very low amount of time .We have developed a simple and secure system by reviewing many statistics. Since all the information in the system will be through on block so no one has the opportunity to hide or change the information.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Biswas M, Mahi M, Nayeen J, Hossen R, Acharjee UK, Md W. BUVOTS: A blockchain based unmanipulated voting scheme. Rakib and Acharjee, Uzzal Kumar and Md, Whaiduzzaman, BUVOTS: A Blockchain Based Unmanipulated Voting Scheme; 2020.
2. Mukherjee PP, Boshra AA, Ashraf MM, Biswas M. A Hyper-ledger fabric framework as a service for improved quality e-voting system. In2020 IEEE Region 10 Symposium (TENSYMP) IEEE. 2020;394-397.
3. Al-Amin S, Sharkar SR, Kaiser MS, Biswas M. Towards a blockchain- based supply chain management for e-agro business system. InPro- ceedings of International Conference on Trends in Computational and Cognitive Engineering Springer, Singapore. 2021;329-339.
4. Akib AA, Ferdous MF, Biswas M, Khondokar HM. Artificial Intelli- gence Humanoid BONGO Robot in Bangladesh. In 2019 1st Interna- tional Conference on Advances in Science, Engineering and Robotics Technology (ICASERT) IEEE. 2019;1-6.
5. Hossain MP, Khaled M, Saju SA, Roy S, Biswas M. Vehicle registra-tion and information management using blockchain based dis- tributed ledger frombangladesh perspective. In: IEEE Region 10 Symposium (TENSYMP). IEEE; 2020.
6. Datta P, Bhowmik A, Shome A, Biswas M. A secured smart national identity card management design using blockchain. In2020 2nd In- ternational Conference on Advanced Information and Communication Technology (ICAICT) IEEE. 2020;291-296.
7. Mahi MJ, Hossain KM, Biswas M, Whaiduzzaman M. SENTRAC: A novel real time sentiment analysis approach through twitter cloud environment. InAdvances in Electrical and Computer Technologies. Springer, Singapore. 2020;21-32.
8. Khatun S, Sarkar S, Biswas M. SecureIT– A weapon to protect you. Available at SSRN 3568797; 2020.
9. Lu L, Chen J, Tian Z, He Q, Huang B, Xiang Y, Liu Z. Educoin: A secure and efficient payment solution for mooc environment. In 2019 IEEE International Conference on Blockchain (Blockchain) IEEE. 2019;490-495.
10. Zouina M, Outtai B. Towards a distributed token based payment system using blockchain technology. In 2019 International Conference on Advanced Communication Technologies and Networking (CommNet) IEEE. 2019;1-10.
11. Lundqvist T, de Blanche A, Andersson HRH. Thing-to-thing electricity micro payments using blockchain technology. In 2017 Global Internet of Things Summit (GIoTS) IEEE. 2017;1-6.
12. Hao Z, Ji R, Li Q. Fastpay: A secure fast payment method for edge-IoT platforms using blockchain. In 2018 IEEE/ACM Symposium on Edge Computing (SEC). IEEE. 2018;410-415.
13. Popa AB, Stan IM, Rughinis¸ R. Instant payment and latent transactions on the Ethereum Blockchain. In 2018 17th RoEduNet Conference: Networking in Education and Research(RoEduNet) IEEE. 2018;1-4.
14. Rezaeibagha F, Mu Y. Efficient micropayment of cryptocur- rency from Blockchains. The Computer Journal. 2019;62(4):507-517.
15. Sakr S, Zomaya AY eds. Encyclopedia of big data technologies. Springer International Publishing; 2019.
16. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system; 2009.
    Cryptography Mailing list.
    Available:https://metzdowd. com
17. Nguyen VC, Hoai-Luan PHAM, Thi-Hong TRAN, Huynh HT, Nakashima Y. Digitizing invoice and managing VAT payment using blockchain smart contract. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) IEEE. 2019;74-77.
18. Kaid D, Eljazzar MM. Applying blockchain to automate installments payment between supply chain parties. In 2018 14th International Computer Engineering Conference (ICENCO) IEEE. 2018;231-235.

19. Li C, Hu F, Xu D. RPDT: An architecture for IP traceback in partial deployment scenario. In 2019 IEEE 5th= International Conference on Computer= and Communications (ICCC) IEEE. 2019;1602-1608.

20. Lin C, He D, Huang X, Khan MK, Choo KKR. DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain. IEEE Transactions on Information Forensics and Security. 2020;15:2440-2452.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/68126