March- April 2020
ISSN: 0193-4120 Page No. 3375 - 3381

Novel Architecture Design to Improve Security for Block Chain Technology in Crypto Economic Market using IOT

M.KavithaMargret[1], Dr.A.Balamurugan[2], D.Vijayanandh[3]
[1]Assistant Professor, Sri Krishna College of Technology, INDIA, 9994282327, 1kavithamargret@gmail.com
[2] Professor & Head Sri Krishna College of Technology, INDIA, 6383436117, a.balamurugan@skct.edu.in
[3]Assistant Professor, Hindusthan College of Engineering and Technology, 9894514401, INDIA,
[3]*dvanandh@gmail.com*

Article Info
Volume 83
Page Number: 3375 - 3381
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 22 March 2020*

Abstract:
IoT is one of the most popular and ubiquitous technology in this decade .IoT is everywhere now. Cryptoeconomics is an area of applied cryptography and it is not a subfield of economics rather it is technology of economic incentives and economic theory into elucidation. Bitcoin, ethereum are some of the example for block chains and are yields of cryptoeconomics. Another name for blockchain technology is a Distributed Ledger Technology that will influence the aspects of digital business .Combining blockchain technology and IoT results in increasing economic growth of the business environment. Merging of the above two technology and security issues are the focus of this paper .In concern with the security of the block chain technology 15% of the attack is handled by SHA algorithms. Public- private key algorithms are proposed to protect block chain architecture. To improved security in block chain set of mechanism will be focused in this paper for decentralized prediction market, auction system, block chain computation and storage.

Keywords: *Internet of Things , Block Chain, Security*

I INTRODUCTION

Block chain is a distributed ledger based computation and information sharing platform, distributed nodes connected together to form a Block chain technology. It is an open digital ledger with many blocks connected one after another each record has immutable timestamp within chain.

Block chain forms a data structure where nodes are linked to one another in linear order. Each link has pointer reference to refer next block in the connected chain network. Characteristics of block chain technology is Immutability, Decentralization, Security, Increased Capacity, Anonymity

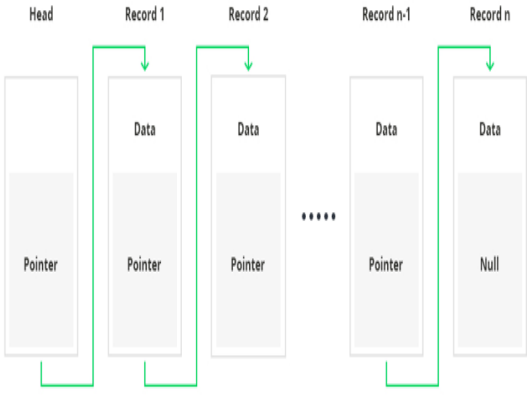

Figure 1. Structure of Block chain

- Each block in Block chain has two parts a header and a data payload. payload is used to store a trans-actions in a crypto economic market

- The header has the information of blockchainlength and content.
- 32-bit SHA256 hash value is calculated to give information about the previous block

II INTERNET OF THINGS

Internet connect devices and enable machine to machine communication over the internet medium. Here we listed some implementation of IoT

Smart wearables

Wearable devices are mainly used for measuring parameters like sleep anea, bloodpressure, diabetes, bloodpressure, obesity, etc. As the population increases with increase in chronic illness, health care system is needed to recognize the stress and strain in people in general.Serious issues in health monitoring can be done by wearable devices only if its accurate else it will cause big problems for the patient if proper alarming is not done at emergency time.Many complex algorithms are developed and in developing stages to measure the parameters of the human body with good accuracy.Many patches are body worn and could measure skin temperature, monitor ECG of the patient, etc by using the Near Field Communication [1].

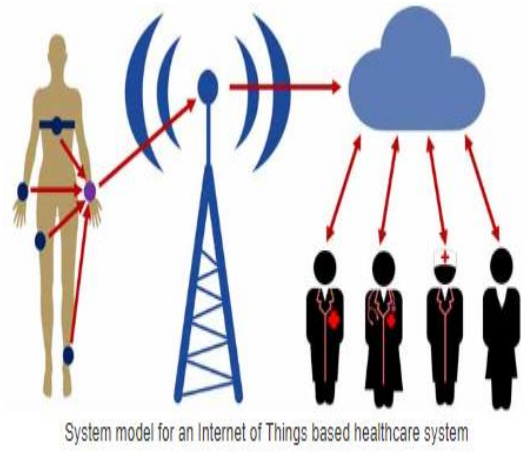

Figure 2. IOT based Health Care

Sensors monitoring focus on the various parameters in body by both long range communications and short range communication.Collection of data is done by using machine to macine communication through collection of networking devices.Wearable devices not only easy to monitor the patients various parameters but also reduces the resources needed in hospitals such as rooms, caretakers, bed, etc.This smart wearables are mainly used for elderly people who can't be treated in hospitals as they are resistant to hospital zones at elderly age.E ven joint movement can be tracked therapy with smart devices.Sensor nodes in smart wearable devices collect the data likeblood-glucose, joint angle sensors, blood oxygen sensors, falldetection[8], etc and send to central node where the information is processed and sent to an external environment.However, patients sensitive data should be strongly maintained with full security.While choosing short range and long range communication should include error detection and correction mechanism with less delay.Delay in delivery of data should not be present as critical sitation in patients may appear at any time.Machine learning algorithms are proposed for the continuous monitoring of the progress of patient to determine whether there in steady increase in the improvement of the health of the patient by wearing the smart devices.In general if blood pressure are to be monitored, the smart devices takes the information from various locations of the body at regular and irregular intervals and

Send the information to central node which is the worn device to measure blood pressure.A average record of the patient's blood pressure system could be build.It uses different algorithms to analyse the data and informs the patient regarding the highest and lowest blood pressure level within 15 days or 30 days as per the predefined settings in the smart devices which is subject to change.

Blood oxygen can be measured by PPG signals [9] using pulse oximeters which holds PPG sensors.Thehaemoglobin in the blood absorbs the light from the LED which is kept along with

March- April 2020
ISSN: 0193-4120 Page No. 3375 - 3381

photodiode beneath the skin along the figure.Photodiodes measure the the quantity of light that is not absorbed and the variations in the absorbed and non-absorbed light calculate the blood oxygen[2].

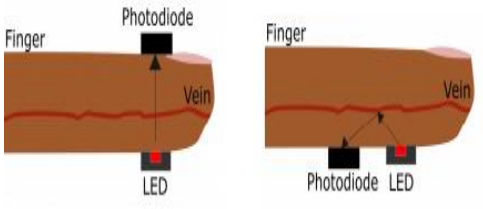

Figure 3.absorbance mode Vs reflectivemode PPG sensors for pulse oximetry

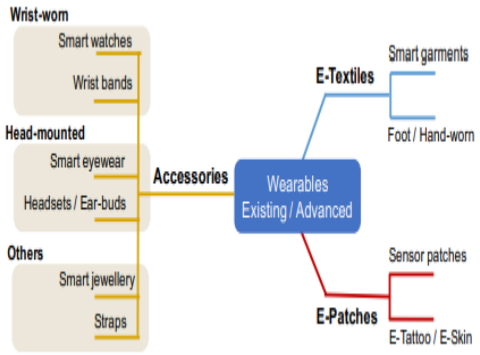

Figure 4. classification of wearable devices

Smart eyewears are special type of smart wears which is a type of contact lenses with wireless communication along with sensing mechanism for monitoring eyes.Smartjewellery like smart rings, clips, neckweareteare used for health monitoring.Armbands, belts monitors physiological signals of human[4].To identify the stress, skin conductance parameter is very important in which sweatness is measured which is controlled by sympathicneroussystem.Heartrate, skin temperature [14] can also be used to monitor the system.Basic voltage divider mechanism is used where sweatness decreases th resistance in the skin and increases the conductivity which can be measured with output voltage which will be very high.By using filters, higher frequency can be filtered out[3]

e-health

- Sensor networks and smart devices are required for various analysis of the patient in e-health monitoring system. It also promotes continuous monitoring of the patient from remote areas. Complete details of the patient is stored in centralised server and it is made available to doctors through smart devices. Cloud storage is used for the continuous storage of data from the patient. High speed internet is also required to closely monitor the patients by the doctors and caregivers. All the medial reports are generated and stored as soft copy within the cloud for easy accessible. Patients who are very old and can't be hospitalised can be monitored easily from their home through smart gadgets like smart phone. Wireless sensor networks plays major role in monitoring the patients as it collects the parameters from the patient and store it in the server.

Illustration of e-health monitoring system

The architecture of the e-health monitoring system includes various sensors at patient level and also to monitor environmental conditions.The data gets processed and stored in the cloud which is then made accessible by the doctors and caregivers at the hospital.Each patient medical history will be recorder with unique access to id and if any serious issues occurs to th4e patient who are at remote or in hospital based on the parameter values doctors advise the emergency unit for the patients.Many alarms are placed to monitor the patients by the caregivers.

Realtime health advice and action is activated when the patient emergency condition is not attended by any doctors or caregivers.The smart devices try to match the parameters obtained from the patient to the previous history and if any match is found they try to provide the medication done previously by enabling the emergency alarm again to the caretakers[1].The security of the system plays major role as some loop holes if present might

change the history of the patients which may cause the patient to fatal death.

Since e-health deals with patients' lives, atmost care in designing the smart devices with proper security enabled mechanism to be done. Apart from hospitals, many devices like fitness devices, activitytrackers, sleep monitoring devices also present with utmost care[5].These devices in general show the rate of sleep/day, activity or workout's efficiency to measure the burning of calories in the body, footsteps made per day with text message if footsteps are beyond 10, 000, monitoring the stress, bloodpressure, etc. Smart devices became quite widespreadnowdays with affordable cost even for middle class users.

III LITERATURE SURVEY

An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3

The author proposed HyperledgerFabric utilization of consensus algorithm to handle up to 1/3 malicious byzantine replicas

Tareq Ahram1, Arman Sargolzaei2, Saman Sargolzaei3, 4, Jeff Daniels5, and Be Amaba6

Author proposed agile value chains, closer customer relationships, faster product innovations, , and quicker integration with the IoT and cloud technology.

Francesco Restuccia, Member, IEEE, Salvatore D'Oro, Member, IEEE, Salil S. Kanhere, Senior Member, IEEE, TommasoMelodia, Fellow, IEEE, and Sajal K. Das, Fellow, IEEE

- Author proposed clustering algorithms to address scalability issues to reduce communication and computation overheads
- Author proposed DAG way for representing each node of representing

BlockChain for IoT Security and Management: Current Prospects, Challenges and Future Directions

Shanto Roy, Md. Ashaduzzamany, Mehedi Hassan z, and Arnab Rahman Chowdhury

Author proposed Consensus Algorithms -Proof of Work (PoW), Proof of Stake (PoS) in addition to that he introduced a new consensus system named proof of concept (PoC) that substitutes traditional algorithms.

IV IOT AND BLOCKCHAIN INTEGRATION

We proposes novel protocol that will meet the security issues when merging block chain technology with IoT in crypto economic market that will reduce block chain alteration , peer to peer node security , standards and authentication. Performance and analysis of Cryptographic public –private algorithms will be taken into consideration to propose a novel architecture design. Extrinsic factor for the existing security algorithm will be analyzed and solution for block chain security will be meet by this new architecture. The architecture in this paper solves an existing difficulties like Transparency and anonymity, Consensus problems, Problems with smart contracts and increases improved security, scalability, less cost, increased efficiency, improved traceability and speed of transaction.

BIOT (Block chain with IoT)

To get better optimized framework merging of these two Techniques in an arena such as edge computing, fog and cloud computing is encouraged

Trials and prospects In BIOT

Challenges are Security weaknesses and threats, best selection of security Algorithms , scalability in machine to machine communication , plasticity and elasticity of devices , data privacy , authentication and confidentiality of data , Legal issues , Consensus mechanism

March- April 2020
ISSN: 0193-4120 Page No. 3375 - 3381

Proposed system

Proposed system Ensure the following aspect

- Intrusion detection and prevention techniques
- Cryptographic approaches
- Network design
- Consensus Algorithms

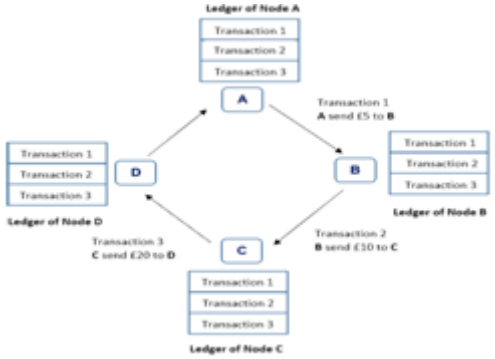

Figure 5. Layered transaction in distributed ledger

Platforms and applications

Blockchain platforms for creating blockchain applications.

Platform	Blockchain	Consensus	Crypto currency	Smart contracts
Ethereum	Public and permission-based	PoS	Ether (ETH)	yes
Hyperledger Fabric	Permission-based	PBTF/SIEVE	None	yes
Multichain	Permission-based	PBTF	Multi-currency	yes
Litecoin	Public	Scrypt	litecoins (LTC)	no
Lisk	Public and permission-based	DPoS	LSK	yes
Quorum	Permission-based	Multiple	ETH	yes
HDAC	Permission-based	ePoW,Trust-based	Multiasset	yes

Figure 6. Block chain platform and applications

Intrusion detection and prevention techniques

When combining IoT with Blockchain the network design should detectt and prevent unauthorized access to network devices, dynamic changes in network path and scanning of traffic is an major issue in BIOT. Network defence system with high security algorithms need to handle the above issue

Multilayered Security and Privacy Model

Block chain architecture may be private, public, and hybrid.

First layer of proposed architecture ensures strong access control mechanism for firewall and used to authenticate data.

Second layer provides intrusion prevention provides high level of intrusion detection and prevention with ACM to the File.

Third layer provide top level security policy with encryption algorithms, Data Layer (DL), and Access Control layer

Cryptographic approaches

Public and private key cryptographic algorithms provides confidentiality and integrity, secure hash algorithms provides authentication

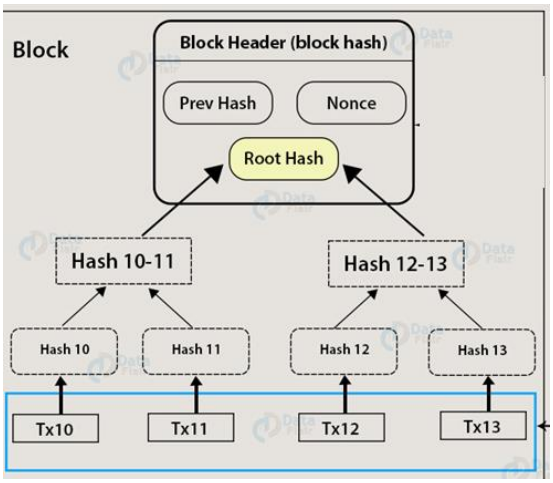

Figure 6.Level of encryption in distributed ledger

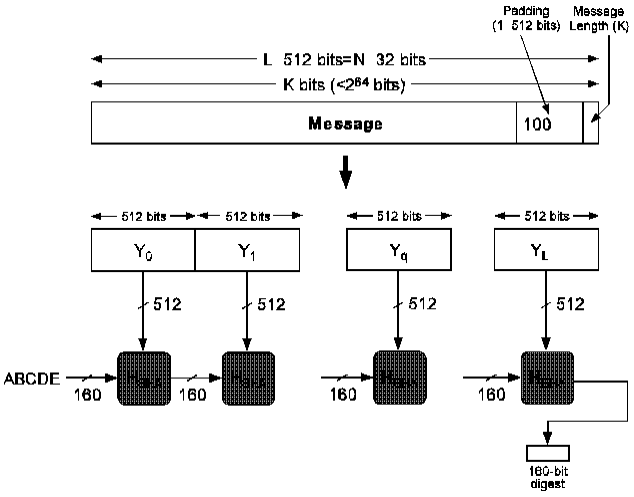

Figure 7. SHA 512 algorithm

March- April 2020
ISSN: 0193-4120 Page No. 3375 - 3381

Network design

DAG : Directed acyclic graph is used to obtain information about network .The priority based on their position in the DAG graph a model to calculate threats based on a weighted on DAG is proposed .

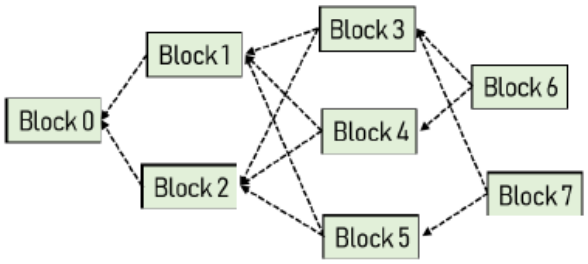

Figure 8. DAG

Specifically, this is a dynamic proactive multipurpose threat response model designed to minimize threats and costs.

Other optimization methods such as genetic algorithms could be implemented to respond optimally and quickly to threats in the future

Consensus Algorithms

50% of the attacks are controlled by consensus algorithm. Here we propose

Proof-of-Work (PoW): is used to validate the honesty of the data by finding solution of puzzles

Proof of Stake (PoS):

Proof-of-Stake is a consensus mechanism in block chain the actors who have a stake could add the blocks.

We propose authenticated delegated proof of stake and access control fault tolerance system which is slightly different from PoS and Pow .

Authenticated delegated proof of stake and access control fault tolerance system authenticate all block in the node and validate each node for miners

V SECURITY IN BC BASED IOT ECOSYSTEMPRIVACY OR CONFIDENTIALITY

Symmetric AES algorithm is used to provide privacy issues and asymmetric (ECC, RSA) cryptographic systems used to provide confidentiality

Integrity:

In BIOT each block is maintains data integrity with digital signature field by means of Elliptic curve Digital signature algorithm). To ensure integrity Nonce can be added in each block if any alteration is done that will be monitored by miners in the BC

VI AUTHENTICATION

DDoS attack in a BC is impossiblebecause almostall thenodes in the BC network is authenticated so it is evade from masquerading

VII CONCLUSION

BIOT by nature has wider scope in crypto economic market. To increase authentication and confidentiality of participants in a decentralized approach we propose different layer of security

The BC model that needs to be adapted with IoT, needs modification in the verifying process as the traditional consensus algorithms seem costly compared to the proposed consensus algorithm.

Design of a standard integration of different systems require further research attentions [14].

VIII REFERENCES

[1]. A. Whitmore, A. Agarwal, and L. Da Xu, “The Internet of Things –A survey of topics and trends, ” Information Systems Frontiers, vol. 17, no. 2, pp. 261–274, 2015.

[2]. Glen Martin (Forbes), “How The Internet Of Things IsMore Like The Industrial Revolution Than TheDigitalRevolution, ”

https://www.forbes.com/sites/oreillymedia/2014/02/10/more-1876-than-1995/#674c4e0b66d2.

[3]. L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey, "IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[4]. O. Bello and S. Zeadally, "Communication issues in the internet ofthings (iot), " in Next-Generation Wireless Technologies. Springer, 2013, pp. 189–219.

[5]. S. Tayeb, S. Latifi, and Y. Kim, "A survey on iot communication andcomputation frameworks: An industrial perspective, " in Computing andCommunication Workshop and Conference (CCWC), 2017 IEEE 7thAnnual. IEEE, 2017, pp. 1–6.

[6]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet ofthings (iot): A vision, architectural elements, and future directions, "Future generation computer systems, vol. 29, no. 7, pp. 1645–1660

[7]. Poornaselvan K.J., Gireesh Kumar T., VijayanV.P.Agent based ground flight control using type-2 fuzzy logic and hybrid ant colony optimization to a dynamic environment

[8]. Selvy P.T., Palanisamy V., PurusothamanT.Performance analysis of clustering algorithms in brain tumor detection of MR images

[9]. T. M. Fern´andez-Caram´es and P. Fraga-Lamas, "A review on the use ofblockchain for the internet of things, " IEEE Access, 2018.

[10]. J. C. Song, M. A. Demir, J. J. Prevost, and P. Rad, "Blockchaindesignfor trusted decentralized iot networks, " in 2018 13th Annual Conferenceon System of Systems Engineering (SoSE). IEEE, 2018, pp. 169–174.

[11]. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: Alightweight scalable blockchain for iot security and privacy, " arXivpreprint arXiv:1712.02969, 2017.

[12]. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: Adistributed solution to automotive security and privacy, " IEEE CommunicationsMagazine, vol. 55, no. 12, pp. 119–125, 2017.

[13]. A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust& authentication fordecentralized sensor networks, " arXiv preprintarXiv:1706.01730, 2017.

[14]. Sreeja N.K., Sankar A. "Pattern matching based classification using Ant Colony Optimization based feature selection", 31, 2818, 91, 102, Soft Computing Journal, 2015.

[15]. Kotapuri Mercy Rosalina and Kommoju C Sravanthi "Simulation of Load Redistribution Attack using YALMIP software in Electrical Energy Market", Journal of Green Engineering, vol.9, issue. 4, pp.526–539, 2019

[16]. Kurian, J., Christoday, R.J. and Uvais, N.A., 2018. Psychosocial factors associated with repeated hospitalisation in men with alcohol dependence: A hospital based cross sectional study. *International Journal of Psychosocial Rehabilitation. Vol 22 (2) 84, 92*.

[17]. Melnichuk, M., 2018. Psychosocial Adaptation of International Students: Advanced Screening. *International Journal of Psychosocial Rehabilitation. Vol 22 (1) 101, 113*.

[18]. Daly, A., Arnavut, F., Bohorun, D., Daly, A., Arnavut, F. and Bohorun, D., The Step-Down Challenge. *International Journal of Psychosocial Rehabilitation, Vol 22*(1) 76, 83.