International Journal of Advanced Technology and Engineering Exploration, Vol 6(61)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2019.650071

Research Article

Performance enhancement of the internet of things with the integrated blockchain technology using RSK sidechain

Atiur Rahman[1], Md. Selim Hossain[2*], Ziaur Rahman[3] and SK. A. Shezan[4]

Department of Information and Communication Technology (ICT) at Mawlana Bhashani Science and Technology University (MBSTU) Santosh, Tangail, Bangladesh[1]

Lecturer, Department of Computer Science and Engineering at Khwaja Yunus Ali University, Enayetpur, Sirajganj, Bangladesh[2]

Assistant Professor, Department of Information and Communication Technology (ICT) at Mawlana Bhashani Science and Technology University (MBSTU) Santosh, Tangail, Bangladesh[3]

Department of Electrical and Electronic Engineering, School of Engineering, RMIT University, Melbourne, Australia[4]

Received: 28-October-2019; Revised: 24-December-2019; Accepted: 27-December-2019

©2019 Atiur Rahman et al. This is an open access article distributed under the Creative Commons Attribution (CC BY) License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

In the arrangement of sensor devices, the performance has become a pressing issue with the increase of the enormous network overhead. As IoT has been evolving so rapidly to ease our daily life, communication latency and security can affect its efficient usage, if different aspects of socio-economic issues where IoT is necessarily involved. In line with that, blockchain has been able to show its enormous potentials to equip IoT devices to enhance security and performance. It is so popular because of its self-administering ability through distributed and consensus-driven behavior along with transparency, immutability, and cryptographic security strength. There have been several efforts made to upgrade the network performance besides ensuring safety and privacy concerns. However, the existing approaches such that aligned with publicly available blockchains have come up with certain drawbacks and performance delays. Therefore, it has been raised as a popularly asked question that the existing cryptocurrency driven blockchain technology may not be directly applicable in the areas such as IoT security and privacy. In this work, a two-way peg blockchain system to overcome the performance and overhead issues has been proposed. The proposed approach has been justified after successfully integrating considered IoT networks. It proves that the proposed rootstock (RSK) sidechain based blockchain has a promising ability to work with the IoT networks. The result shows a significant improvement in terms of performance in comparison with its peers, such as Ethereum and Monax, upon different sensor nodes employed.

Keywords

IOT, Blockchain, Sidechain, RSK, Consensus, Transaction.

1.Introduction

Blockchain technology was first built as the framework underlying crypto-currency; it has now shown immense potentials with far-reaching implications in the arena of smart contract-based financial markets, bitcoin integrated artificial intelligence and mostly the distributed ledger-oriented security mechanism of the IoT [1]. The technology lets end-users to communicate and record the value and information called transaction on a peer-to-peer network of computers and smart devices.

The term Internet of Things (IoT), the insightful and smart network of humans, process, data, and things, has been able to hold the principle research trends of recent days, which are fairly a new term to be confused with its peer the Internet of Things (IoT) [2]. In essence, the Internet of Everything (IoE) may further advance the power of the Internet to improve the socio-economic outcome by making life easier to live by adding to the progress of IoT [3, 4]. As smart devices have been getting more connected and accumulating huge information and transaction, similarly the privacy and security has been caught as a fundamental concern with the priority in all aspects of IoT data and information. Most drawbacks have been facing by IoE security is coming from the very architecture of the ecosystem based on a centralized

*Author for correspondence

model [5]. Blockchain is a set of connected blocks are immutable and holds transparent data over the distributed network. A sample blockchain is depicted in *Figure 1*.

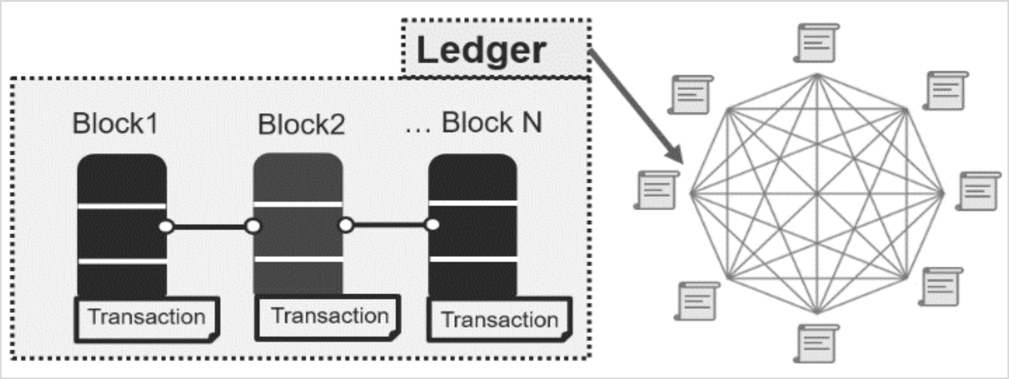

Figure 1 Blockchain blocks and its working procedure on the distributed ledger

The objective of this work is outlined as below-

- Proposing rootstock (RSK) based blockchain which is an improved structure using the concept of sidechain.
- Applying the proposed blockchain for a considered IoT network to monitor its applicability and initial feasibility.
- Evaluating the proposed system in comparison with the existing and more relevant works and concluding the claims that the performance of the proposed approach looks better, indeed.

This article is organized with the following structures-including background, proposed method and materials, evaluation, result discussion, imitations that concluded with a conclusion and future scope section.

2.Backgrounds and related works

IoE data privacy is a research challenge because there stands no enough adjustment in IoT, the heavy rule of IoT systems and central entree replicas for IoT data. There have been so many research contributions that have been made to secure data access on the client server constructed entree control process. IoT service providers also use proprietary sanction procedures, somewhere users of IoE turn as central permitting objects. Though unified IoT data management causes scalability matters in IoT besides vigor the users to faith in central third revelry mediators to accomplish their information, thus they practice data privacy and termination to secure. By way of a result, the research focus is moved to develop a decentralized model for IoE, using RSK sidechains along with peer-to-peer connection mechanisms. For the proven of supporting good safety to bulky scale disseminated networks like as Bitcoin, and further cryptocurrency networks the popularity of blockchains in the IoT domain increased [6]. It is described that blockchains are capable of maintaining an unchallengeable record of data relations and accomplish contact rheostat. The contact regulator element originates after the creation of entree policies round the public key infrastructure (PKI) of blockchain systems [7, 8]. Authors in [9 and 10] highlighted the pros of certifying manipulators' possession of IoT data via a blockchain. It has been discussed the budding of blockchains for smoothing an economy for sensor information and manipulators [11, 12].

3.Proposed method: sidechains for IoT

We can imagine different side chains for different applications of IoT for smart cities. There are various sectors that can be divided for using as sidechains within the IoT architecture. There is a different dimension for IoE applications in smart cities [13, 14]. For smart cities, there may be smart homes, smart parking lots, healthcare, climate and water schemes, transportations and vehicular traffic flow, ecological contamination, shadowing arrangements. There are subcategories cutting-edge each of sectors [15].

3.1Challenges and threats

In this section, the challenges for implementing IoE based smart cities are stated. *Figure 2* illustrates the challenges. They may be security and reliability, heterogeneity, large-scale, big data, in our proposed system we want to deal with the security and reliability using blockchain technology which is called RSK sidechain. Social and legal aspects, sensor networks, DR barriers, etc. [16] are the parts of this technology.

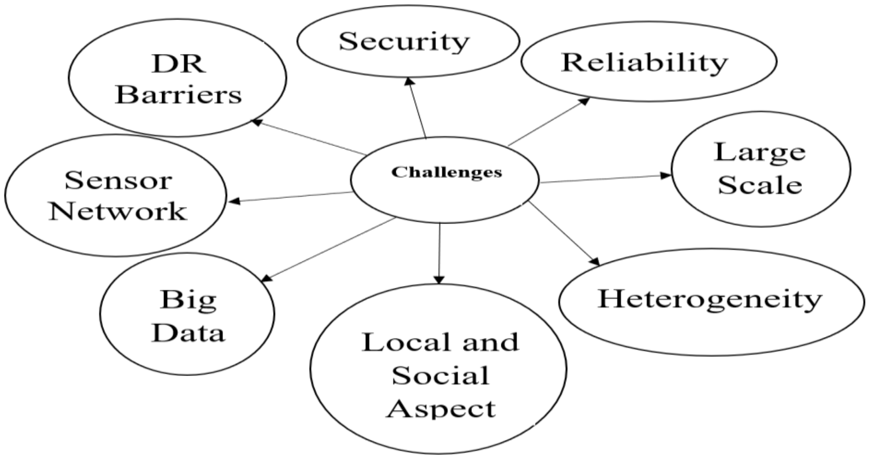

Figure 2 Challenges for implementing of IoT using blockchain technology

3.2Blockchain materials

A sidechain is a separate blockchain that is independent but pegged with bitcoin main net via a two-way peg in the middle. It consents us to handover bitcoins back and forth. By this system we can get two advantages: (1) We can use the security that we have in bitcoin (2) Transfer them or use them in the sidechain with different consensus rules. For example, we can use different block sizes, different block intervals, different mining algorithms [17]. We can also introduce new op-codes such as smart contracts. So, the possibilities of this experiment are quite limitless and we can also utilize the security of bitcoin network generated in the bitcoin main network. The way it will work is a two-way peg. It consists of locked boxes on both the chains. For example, we want to move transfer a bitcoin from a bitcoin network to a sanctioned address our transaction first gets to the locked box in the bitcoin side there will be information in the transaction about the sidechain address [18]. Now once the transaction is received by the locked box the sidechain then releases an equivalent bitcoin called secondary bitcoin (sec BC) which is then sent to the address we indicated in our original transaction in the bitcoin side. If we want to reverse the process, we do exactly the opposite. We send a sec BC to the locked box on the sidechain with information about the recipient bitcoin address. Once that is received the locked box on the bitcoin side releases a bitcoin and that is sent to address, we indicated in our original transaction in the sidechain [19].

3.3Working procedures

To a two-way peg to work these two lockboxes needs to have information about each other and have to be able to release funds simultaneously when the lockbox on the other side was seized. There are a couple of ways for this to work. The simplest way to implement a two-way peg is via central exchanges and in this case, we will have a central party that controls both lockboxes on both sides. The advantage of this is simplicity, but the disadvantage is that we are placing trust in a central party who can if wants to maliciously empty a lockbox in a chain and steal all funds so there is a way to minimize the central trust placed in a central exchange and that is with a federation so we can implement the two-way peg via a federated peg where the lock boxes are now being controlled by a group of entities so to make that transaction across the two chains. Then it require the lock box to have n of m signatures to release funds so on at least n entities of the Federation need to confirm that this is a valid transaction now the advantage of this is similar to what we have before it can be implemented with any two types of chains without specific protocol upgrades or specific all codes but again we have a centralized trust placed in a group of minimum now there is one more type of two-way peg where the two chains can interact with each other without having a middleman and this is via simple payment verification (SPV) proofs.

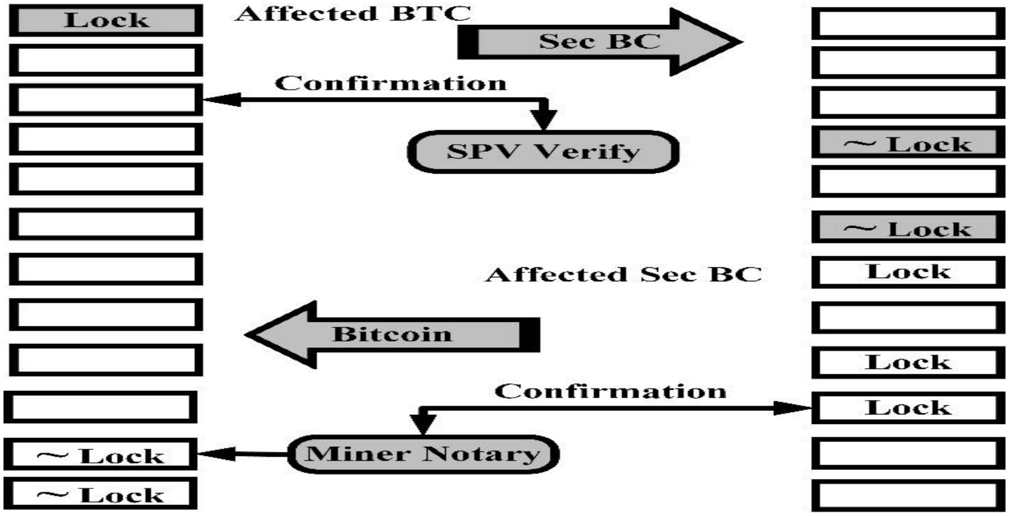

Figure 3 Sample transactions to unlock the BTC with sec BC in using proof of last transaction control for SPV

3.4SPV proof

SPV proof attitudes for abridged compensation confirmation. The SPV proof basically shows that I can prove to you that my transaction is included in a valid block and that miners have created a lot of subsequent blocks on top of it now the SPV proof does not actually say that transaction is consistent with entire blockchain history. It doesn't actually check it across check it to be consistent with all previous transactions from the genesis block onwards instead It's doing a proof indirectly and showing that it's member of a block and a lot of miners trust that the block is correct and therefore they have mined on top of it forming the longest chain. SPV gives the 2 critical factors; a) It ensures the transactions are in a block, and b) It provides attestation (proof of work) that additional blocks are being appended to the chain. By using a two-way peg system with SPV proof we can ensure more security, reliability and efficiency than a system that is using a single chain.

3.5Proof of work

Miners in proof-of-work (POW) chains have the accountability for the growing the chain by repeatedly finding newer blocks. The way of discovering or “mine” for these blocks is by doing the nonstop calculation that requires a lot of processing power. The hash of the block is occupied and affixed a “nonce” to it. It is a random hexadecimal value. The resultant string is then hashed again. That new hashed value cannot be equal to or more than a predetermined value that is called “difficulty.” The miners must be custody on repeatedly altering the value of the nonce until they achieve the required result. If a miner's discovery a block, then they prerequisite to present that newly found block to the network along with the nonce. The network can then simply append the two values and hash it to check the validity of the claim. This is the substance of PoW. It is difficult to solve the possible and finding the exact nonce and It should not be easy to check whether the nonce is correct or not.

4.PeIE: considered IoT system

In our polyethylenimine ethoxylated (PeIE) shaped IoE architecture as shown in *Figure 1* we assume a sidechain called secondary bitcoin (Secoin) running beside the main bitcoin has been demonstrated in *Figure 2.* So, the possibilities of this experiment are quite limitless and we can also utilize the security of bitcoin network beside the main network. The way it will work is considered as the two-way peg. It consists of locked boxes on both the chains. For example, as assumed and drawn in *Figure 3* we want to move transfer a bitcoin from a bitcoin network to a sanctioned address: our transaction first gets to the locked box in the bitcoin side there will be information in the transaction about the sidechain address. Now, once the transaction is received by the locked box the sidechain then releases an equivalent bitcoin called secondary bitcoin which is then sent to the address, we indicated in our original transaction in the bitcoin side. If we want to reverse the process, we do exactly the opposite. We send a secoins to the locked box on the sidechain with information about the recipient bitcoin address. Once that is received the locked box on the bitcoin side releases a bitcoin and that is sent to the address we indicated in our original transaction in the sidechain.

4.1Core components

Infrastructures between local devices or overlay nodes are known as transactions. There are various types of transactions in the RSK sidechain-based overlay block manager (OBM) Access which is a transaction invoked by the smart homeowner to the overlay network. A monitor deal is produced by the proprietor or SPs to periodically monitoring device information. By genesis transaction, an original block is supplementary toward the chain and with remove; a block is withdrawn from the chain. *Figure 4* shows the proposed architecture of service provider and RSK sidechain of OBM access.

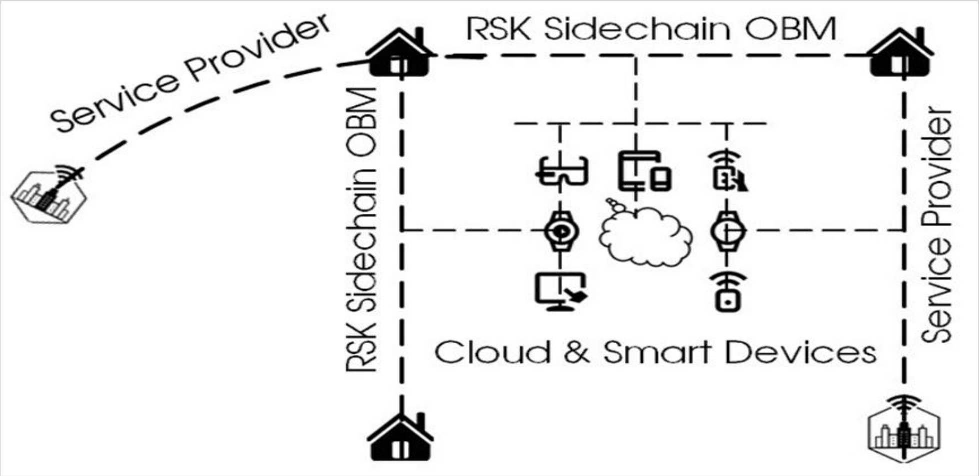

Figure 4 Proposed architecture of service provider and RSK sidechain of OBM access

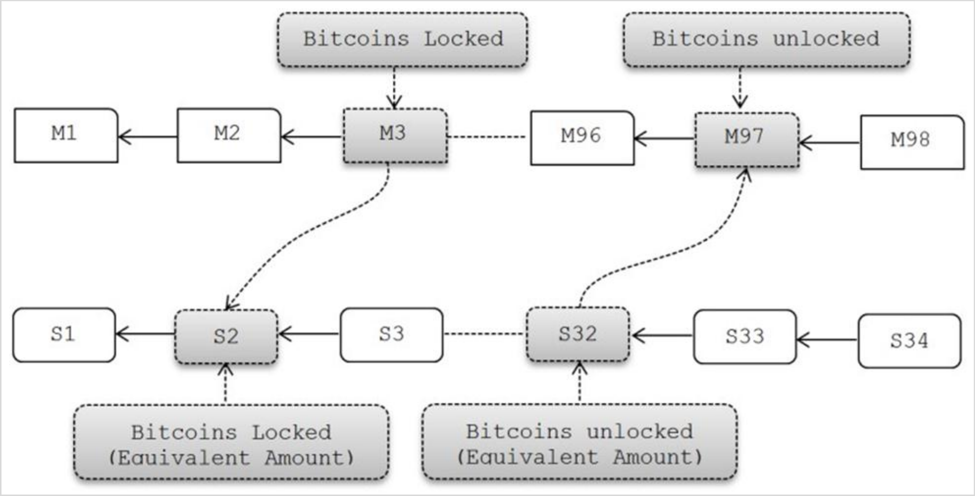
Bitcoins Locked
Bitcoins unlocked
M1
M2
M3
M96
M97
M98
S1
S2
S3
S32
S33
S34
Bitcoins Locked (Equivalent Amount)
Bitcoins unlocked (Equivalent Amount)

Figure 5 Method for creating a two-way peg with BTC and secoins with bitcoin locked and bitcoin unlocked system

4.2Requesters and requesters responsibility

Permitting the followers of the system access to an unchallengeable ledger of completely fruitful and ineffective entree needs delivers responsibility to both requesters and requesters. Deliberate the situation wherever a manipulator vends his sensor information to an advertising corporation. The manipulator approves to consent the corporation entree for one month. If the manipulator cancels admittance privileges on the sidechain neck and neck formerly the month is awake, the corporation's application admittance will be failed; and as indication of delinquency by means of the sidechain proprietor, the corporation can yield times manner history of the aforementioned failed admittance submission. Algorithm displays the process for authenticating a distinct transaction, X that in the public BC all multisig dealings engendered by each requester is systematized in a separate ledger. The output of the multisig transactions generates a standing metric for the supplicant. The connection between consecutive transactions is recognized by the enclosure of the hash of the PK that will be secondhanded by the requester for the next transaction in the third output arena of the present transaction. Thus, the OBM foremost settles this by associating the hash of the requester PK in X with output [8] of the former contract of this requester. Succeeding this, the requester sign, which is controlled within the fourth arena of X, is tested (also called, redeemed) by means of its PK in X. Originally, the requester groups these outputs (constructed on its past of transactions) in the multisig contract. If the request receives the transaction, formerly it would upsurge the yield 0 through unique. Or the requestee augmentations the output 6. To defend the chain in contradiction of nodes those prerogative false standing by incrementing its yields formerly distribution it's to the requestee, in the following stage of deal substantiation, OBM payments which individual one of X's outputs, i.e. whichever the numeral of fruitful contacts (i.e. output 0) or the numeral of banned contacts (i.e. output 6), is enlarged only via individual. Subsequent this, the requestee sign is confirmed with its PK in X. If the steps complete positively, X is confirmed.

```
**Algorithm** Transaction Confirmation.
**Input:** Overlay Transaction (X)
**Output:** True or False Requester Confirmation.
**if** (hash (X.Requester-PK) = X
output 2 **then return** False;
 **else if** (X. requester-PK redeem x.requester-sign)
then **return** False;
**end if**
**end if**
Output Authentication.
**if** (X. output 0 - X. output 0) + (X. output 1 - X
output 1)> 1) **then return** False;
end if
Requestee Confirmation:
 **if** (X.requestee-PK redeem x.requestee-sign) **then**
**return** true;
**end if;**
```

5.Evaluation and analysis

Isolated sidechain preserves kindling of completely IoT information processes and transpire inside an isolated IoT system. The private IoT link contains of IoT strategies as well as individual lawful node consecutively the sidechain. IoT strategies which are prearranged the inimitable pubkeys and prikeys though which it can be customed toward guide encrypted sensor understandings towards the legal node. The legal node acknowledged the information with encryption as data conception proceedings. Legal node enhances innovative blocks in the direction of the sidechain and receipts advanced influences and storing interplanetary. A keen convention can be situated inside the sidechain to achieve the succeeding occupations: Packing a vocabulary by approved canny expedient's pubkey and the hash of the IPFS dossier storage information of smart contract and safeguarding that individual the information incoming from lawful smart devices remain talented to connect through the sidechain validator. The additional is storage a lexicon through pubkeys of petitioners in the system by entree rights and pubkeys of the smart plans whose information the requesters have contact and accomplishment admission regulator on arriving entree request dealings. For meaningful particulars about the viability of the application of the proposed construction and the pertinent placement thoughts, we ensured an act scrutiny of the current block chain submission expansion stages on both the sidechain and association near. We cast off Ethereum in whose cryptocurrency ether is additional individual to Bitcoin. We too rummage-sale Monax, blockchain growth stage for commercial schemes. Ethereum advances consensus by the PoW algorithm. Monax becomes it by means of the Tendermint [15] consensus apparatus [16], which services PoS. We constructed our testbed on an association of five validator nodes, each node we rummage-sale for getting received information from five keen plans. The act metrics we rummage-sale for our investigation remained dispensation overhead, overhead of the network traffic and block dispensation periods.

5.1Processing overhead

We showed a trial on CPU procedure when authenticating new-fangled blocks on the sidechain close. We measured that 5 digital strategies are linked to the way to separate legal node, our plan is to lead trials per variable statistics via external transactions confidential the sidechain system. For completely differences in the arriving transactions, the dispensation overhead endured unaffected with mutually stages. We exhibited the dispensation overhead for the last and the maximum transaction rates that we directed for verified.

5.2Network traffic overhead

The traffic of network traffic above in blockchain technology, which originates beginning the nodes of the nets that contribute hip the consensus step by step process. It is unhurried that traffic above intended for the sidechain since the sidechain solitary includes one legal node. In this research work, the proportion of entree requests, contacts is expected can be less compare to the data formation inside the sidechain. Industrialization of Monax business and it stayed not theoretical on the way to be rummage-sale in a climbable pubnet, the method of risk grid purposes toward. Here, it is restrained that traffic of network taking the variable numbers of nodes to hip the sidechain system, and a fluctuating quantity of entree request transactions arrives for each minute. The explanations have become from this experimentation remain exemplified by *Figures 5 and 6* slighter than the traffic above of Monax. From head to foot network upstairs in Monax is due to the fact the Tendermint agreement train directs ready empty blocks as a rate to square if a peer is awake. Monax was established for business claims and it was not destined to be secondhanded in a climbable pubnet, method of consortium net intentions to be located in the system. By this experimentation, it is unhurried the traffic of network with various numbers of nodes in the consortium network and numerous volumes of contact request dealings inward for every minute. The explanations that have been collected after its trial be situated demonstrated in *Figures 5 and 6.*

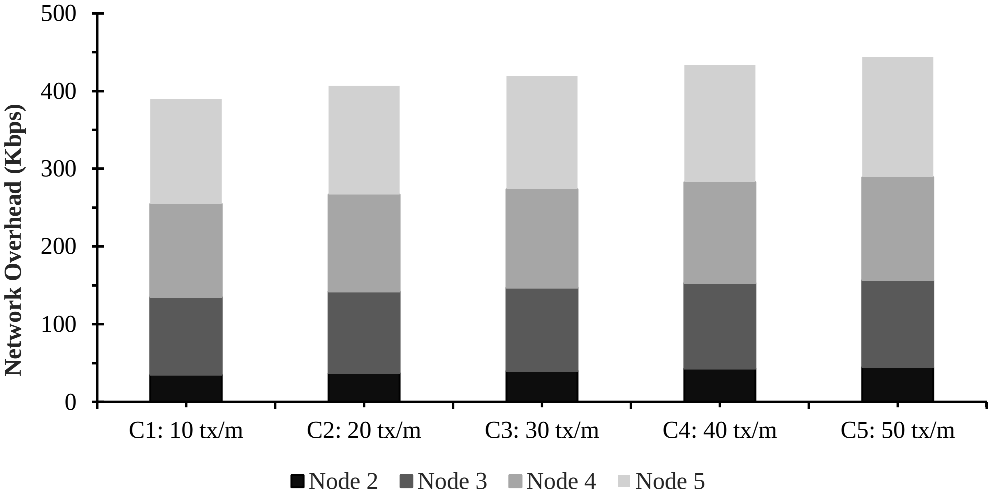

Figure 6 Traffic of network overhead in Monax for different nodes for showing the potential performance

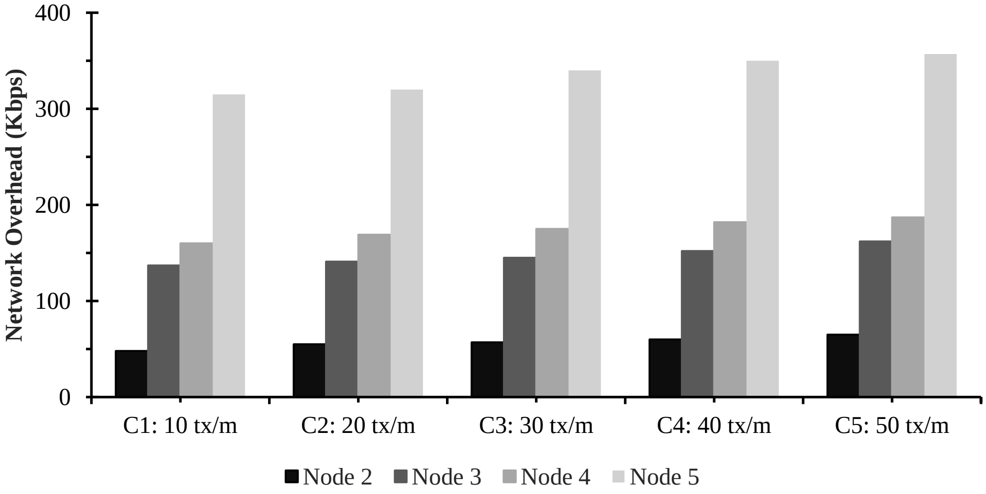

Figure 7 Network traffic overhead in Ethereum blockchain for different nodes showing performance

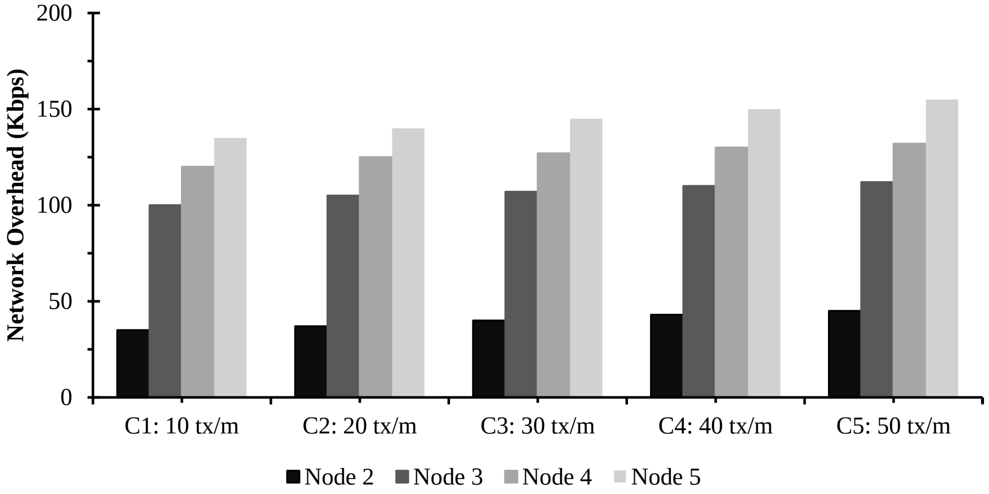

Figure 8 Traffic overhead for the considered sensor network for the proposed blockchain using RSK sidechain

6.Result discussion and limitations

The proposed approach using 2-way peg RSK Sidechain shows significantly improved performance achieved in compare to other existing approach such as Etherum [3] and Monax [7] blockchain. For example, as per the demonstration shown in the *Figure 8*, the performance of the proposed RSK sidechain seems higher than others as it has fewer overheads for different sensor node setup. It also shows that the Etheruem and Monax which are mostly the crypto-currency have similar type of performance on Solidity platform. However, in case of a RSK for example a case 5 for 50 sensor nodes, the simulation shows that less than 200 Kpbs overheads whereas the Ethereum and Monax have approximately 300 kbps. It also shows as per the number of nodes increases the overhead does not increasingly raise proportionately rather, for higher nodes it performs similarly on an average as calculated.

The result achieved is done through Solidity run on MetaMask. For the proposed system evaluation, the initial setup was run on NS2 in to measure the network overhead for five use cases. The result of the small network setup looks promising; however, it could have limitations for heavy network with several thousand sensor nodes. The ongoing work motivates to overcome those challenges such different blockchain integration for the similar IoT test case. *Figure 9* shows the Performance comparisons among the proposed RSK sidechain system, Monax and Ethereum

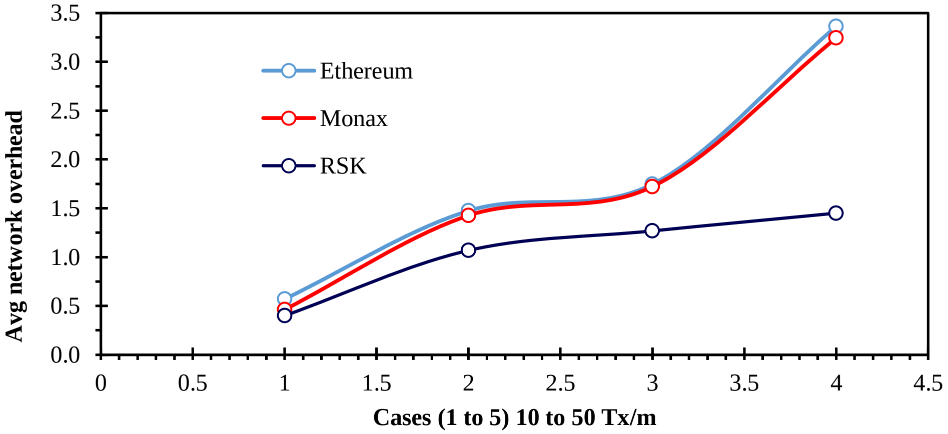

Figure 9 Performance comparisons among the proposed RSK sidechain system, Monax and Ethereum

7.Conclusion and future scope

The IoT will encompass 26 billion devices with 2020. It will create millions of new objects and sensors within a short time interval, all generating real-time data that deserves proper security and privacy concern among the researchers. Applying blockchain Technology to enhance your security is not upfront because of immense challenges such as high resource consumption, scalability, and processing time. Sidechain and RSK integration in the PeIE shaped structure have been proposed. It is helpful in influencing the security of this technology. Its engagements are simple architecture that usages RSK sidechain OBM to reduce the complexity overhead and ensure stronger trust. A performance reputation update strategy is also combined with monitoring and enhancing this trust level. We proposed an IoT fast consensus algorithm that eradicates the requirement of computation by the miners before affixing a block to the blockchain as justified by the respective evaluation section. The consensus technique needs further improvement, which will be included with our future work along with other challenges encountered.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Ferrag MA, Derdour M, Mukherjee M, Derhab A, Maglaras L, Janicke H. Blockchain technologies for the internet of things: research issues and challenges. IEEE Internet of Things Journal. 2018; 6(2):2188-204.

[2] Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing. 2016; 15(5):840-52.

[3] Eckhoff D, Wagner I. Privacy in the smart city—applications, technologies, challenges, and solutions. IEEE Communications Surveys & Tutorials. 2017; 20(1):489-516.

[4] Truong NB, Sun K, Lee GM, Guo Y. GDPR-compliant personal data management: a blockchain-based solution. arXiv preprint arXiv:1904.03038. 2019.

[5] Da Xu L, Viriyasitavat W. Application of blockchain in collaborative internet-of-things services. IEEE Transactions on Computational Social Systems. 2019; 6(6):1295-305.

[6] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2019.

[7] Jones M, Johnson M, Shervey M, Dudley JT, Zimmerman N. Privacy-preserving methods for feature engineering using blockchain: review, evaluation, and proof of concept. Journal of Medical Internet Research. 2019; 21(8):1-18.

[8] Gharakheili HH, Sivanathan A, Hamza A, Sivaraman V. Network-level security for the internet of things: opportunities and challenges. Computer. 2019; 52(8):58-62.

[9] Zyskind G, Nathan O, Pentland A. Enigma: decentralized computation platform with guaranteed privacy. arXiv preprint arXiv:1506.03471. 2015.

[10] Axon LM, Goldsmith M. PB-PKI: a privacy-aware blockchain-based PKI. 14th International joint conference on e-business and telecommunications. 2017(pp. 311-8).

[11] Zhang Y, Wen J. An IoT electric business model based on the protocol of bitcoin. In international conference on intelligence in next generation networks 2015 (pp. 184-91). IEEE.

[12] Zhang Y, Wen J. The IoT electric business model: using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications. 2017; 10(4):983-94.

[13] Shafagh H, Burkhalter L, Hithnawi A, Duquennoy S. Towards blockchain-based auditable storage and sharing of IoT data. In proceedings of the on cloud computing security workshop 2017 (pp. 45-50). ACM.

[14] Zyskind G, Nathan O. Decentralizing privacy: using blockchain to protect personal data. In security and privacy workshops 2015 (pp. 180-4). IEEE.

[15] Ouaddah A, Elkalam AA, Ouahman AA. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In Europe and MENA cooperation advances in information and communication technologies 2017 (pp. 523-33). Springer, Cham.

[16] Barber S, Boyen X, Shi E, Uzun E. Bitter to better—how to make bitcoin a better currency. In international conference on financial cryptography and data security 2012 (pp. 399-414). Springer, Berlin, Heidelberg.

[17] Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for IoT. In proceedings of the second international conference on internet-of-things design and implementation 2017 (pp. 173-8). ACM.

[18] Jacobs IS. Fine particles, thin films and exchange anisotropy. Magnetism. 1963:271-350.

[19] Yorozu T, Hirano M, Oka K, Tagawa Y. Electron spectroscopy studies on magneto-optical media and plastic substrate interface. IEEE Translation Journal on Magnetics in Japan. 1987; 2(8):740-1.

Atiur Rahman is currentlyworkingg as SQA Engineer at Samsung R&D Institute, Bangladesh. He was a student of Department of Information and Communication Technology of Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. He received his Bachelor of Engineering degree in Information and Communication Technology at Department of Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. His research interests are IOT and blockchain.
Email: atiurutchas23@gmail.com

Md. Selim Hossain has been working as a Lecturer in Department of Computer Science and Engineering at Khwaja Yunus Ali University, Sirajganj, Bangladesh. He completed his B.Sc. degree on Telecommunication and Electronic Engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh and M.Sc. (Engg.) on Information and Communication Technology from Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. His main research interest is based on IoT, Blockchain, Cryptography and Network Security, Antenna, Algorithm and Software Engineering.

Ziaur Rahman is currently a PhD Candidate at RMIT University, Melbourne, and an Assistant Professor (currentlyonn study leave) of the Department of ICT, MBSTU, Bangladesh. He was graduated from Shenyang University of Chemical Technology, China, in 2012 and completed Masters from IUT, OIC in 2015. His articles received the best paper award and the nomination at IEEE conferences and published in reputed journals. His research includes Blockchain aligned IoT, Cybersecurity and Software Engineering.

SK. A. Shezan currently pursuing his PhD degree in Electrical and Electronic Engineering from RMIT University, Melbourne, Australia. He was a lecturer of Electrical and Electronic Engineering Department of Uttara University, Dhaka, Bangladesh. He received his Master of Engineering degree from the University of Malaya, in 2016. Moreover, he received his Bachelor of Engineering degree in Electrical Engineering and Automation from Shenyang University of Chemical Technology, China, in 2013. His research interests are Microgrid, HRES, Solar Energy and Wind Energy.