JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Designing Blockchain Enabled Optimized Scalable framework for healthcare systems

[1]Prince Arora, [2]Avinash Bhagat, [3]Yasir Iqbal Mir

[1]Research Scholar, [2]Associate Professor, [3]Assistant Professor
[1]School of Computer Applications,
[1]Lovely Professional University,Phagwara,Punjab

Abstract : The paper deals with the design of the framework with the provision of scalability.To achieve this objective, optimisation operations are performed on the block that ensures the compression in the size of the block .The scalability in blockchain can be achieved by optimising the block and by applying various techniques on it.The paper introduces a technique which allows to develop a scalable blockchain enabled framework that can be used tores olvevariousissuesthatoccursduringtheavailabilityof the data.The framework is based on the design that constructs the block of the blockchain and defines various attributes.The framework also uses a log based optimised model that reduces the size of the block and also promotes scalability.The model also allows to add various healthcare organisations to ensure the availabilityofrecordsateveryend.Thispaperalsofocusesonthe problems that are faced during the scalability of the blockchain network which is highly required in the medical field. A model is also proposed which allows the blockchain model to be highly scalable byenhancingthestructureoftheblock.

IndexTerms **- BlockChain, hash function, medicare, log based model**

I. INTRODUCTION

Blockchain is a decentralised network that stores the data across the network. The easiest way for the transaction to be completed without dealing with online wallets or third party applications is using a blockchain enabled network that allows a peer to peer transaction across the distributed network. The distribution of the data is being made available to various nodes that stores the data in the form of a block and thereplica of the block is also shared across the network.The blockchain is a open-source distributed ledger that allows the transaction to be irreveresible,immutable and non changeable.The data in blockchain starts with a genesis block that initialises the chain of the network.A single block in blockchain consists ofa hash value along with timestamp that uniquely identifies the block across the network.The blockchain allows a trustworthy connection establishment between two various blocks and a smart contract is established between two blocks. The block modelofblockchainisshowninFig1.

Medical is an essential area where the security and scalable of the network is required.Th e e-records of the patients are important for the doctor and the patient as well so a particular technology is required that should provides some features like: immutable,irreversible and also allows the transaction to be decentralised across the network to made it available to theauthentic person.Medical records of the patient can be kept in a way so that the patient can keep track of all the medicines he has taken from various hospitals and health centres ,doctors can also keep an eye on the patient's progress report which helps the doctor to take care of the patient also to save alot of lives by giving the correct medicine to the patients.As per the survey 98,000 people[1] die annually due to mistakes committed by medical professionals .To reduce the number of deaths ,the best thing that can be done is by ensuring the availability of the data at every end and it can be achieved only if the blockchain framework has the potential to be more scalable.

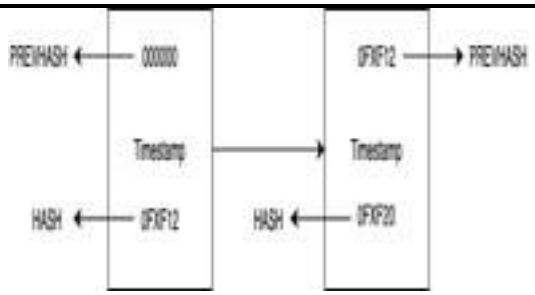

Fig. 1. Block Model of Blockchain

II. LITERATURE REVIEW

To maintain the scalability ,data integrity and hash value ,a particular model named FHIR chain is introduced by changing the size of the reference pointer [1] .The motive of the paper is to convert the arbitrary value to a fixed vale to ensure that the block in blockchain maintains an equality that allows the blockchain enabled network[2] to be highly scalable.The hash value generates a fixed output that takes a random type of values that comes from various resources and using the hash function. The other storage optimization technique[3] is not to pass the data from the original blockchain.The concept of mini-blockchain is introduced to ensure that the mini - blockchain is lightweight and allows a high scalability across the network, due to the lightweight node being used in the model.Separatingthefunctionalitiesoftheblockchain[4]into different systems could improve basic operations. The script system, as well as the traditional interlocked transaction records, are abandoned in this design to cut the block. It is then replaced with a more straightforward understanding of core operations. An account tree was used as the balance sum in this scenario, which included any transactions. The key to these activities is to bundle these functions into transaction groupsthatarestoredinthedatabaseatregularintervals.

Another study introduced the VerSum[5] scheme, which isa novel scheme. It reduces server-side overhead by allowing expensive computations to be distributed among a large number of public logs, such as the Certificate Transparency log, the Namecoin blockchain, and Bitcoin [1]. VerSum clients also double-check the accuracy of the output by comparing it to the outputs of different servers. In another scenario, VerSum creates a dispute resolution procedure to identify anyoutsourcing-relatederrorsandaccuratelyidentifytheappropriateoutput.

The cryptographic approach of zero-knowledge proof (ZKP)[6] is used to validate other entities. It allows the system to disguise the transaction origin, destination, and content while maintaining the immutability of thetransactions. The computational intensity of ZKP, on the other hand, is a disadvantage. It necessitates many rounds of verification betweenthesenderandthereceiver,withthenumberofrounds increasing with each series of processes. In addition, this transaction adds to network latency and limits scalability [7]. Thebitcoinnetwork'smaximumtransactionvalidationrateis7 transactions per second, limiting the throughput of blockchain networks.

There has also been a study towards making blockchain[8] more available to thin clients.All the block data is not stored in the blockchain .Instead of storing the complete data ,it stores only critical elements of the data block.Simpilify Payment Verification(SPF)allows the transaction to store only the important components rather than the complete block. The paper deals with setting the priority to the smart contracts ,it also enhances the chain that is developed by smart contracts.The summarisation and synchronisation of the block is done to ensure the scalability of the blockchain.

Oscar Novo et.al [9] in this paper, the implementation of the framework is done by the genesis block, it scales the connection between the other blocks and chain is created. The security in the blockchain can be achieved by using thegenesis block.

Song[10]proposed the use of blockchain technology which is combined with digital signature to maintain the integrity of the data.Every blockchain transaction is being compared with the verified digital signature to ensure the security of the data. Miller [11] et.al ,in this paper a new decentralized smart contract system is introduced named as Hawk model .In this model a hawk programmer writes a program and a highly effective protocol is generated by the user and transaction is done in blockchain. The model is blockchain based model.The blockchain model of cryptography is formalised and on that basis the smart contract is written.

A minor addition is done in the new model generated byOscar Novo where a special smart contract [12]is created which consists of all the policies that are required for every other smart contract. The access oriented policies are made up of more attributes .To get the access the owner block has to prove the ownership of the data.Once it is matched with the existing block previous hash, the transaction is completed.

Xu et al, proposes a model for the large EHR where an IPFS [13]system is proposed which generates a corresponding hash value.The data is mapped with the IFPS storage where one block of the blockchain can be constructed.This also promotes a key model that a key where the access can be revoked also.The grant and revoke key updates the value of the data.

Azaria et al., defines a model named as MedRec[14] .Basi- cally used to provide secure contracts by creating and adding more attributes to the smart contracts .EHR records are also used to make the records anonymous.But also it comes with various issues like authentication and authorisation fully.

Omar et al,explained the concept of re-encryption[15] key where the doctor allows only updation of data where the re-encryption key is verified by the doctor. The oracles are prepared which can be considered as a repository where the data can be stored and also the data is fetched out from it for the verification purpose.Also the average reputation module can be easily added to it that calculates the average quality of the doctor .It also adds on the formula where the average of the doctor is calculated and if any doctor's average is over par ,in that case they updation is possible which adds on the quality of theresults.

Zhang et al.,developed a model named as FHIR [16]chain model that creates two security smart contracts which consists of various attributes ,the dependency of the quality of the algorithm is based on that.It also comes up with a future work which has the scope for the improvement of medical errors.Although FHIR chain produces a high quality access based mechanism to thesystem.

The paper deals with setting the priority to the smart contracts ,it also enhances the chain that is developed by smart contracts.The summarisation and synchronisation[17] of the block is done to ensure the scalability of the blockchain.

Hardjono explained the design of the model where anonymous entities are given various verifiable entities .Variouskeys are generated to authenticate the various sources of data that comes from variable[18] sources.The public key is generated and to confirm the transaction they key is compared with the public key value.This model majorly focuses on various cryptography techniques to ensure that the data passed from various resources is uniquedata.

Ouddah et al. presented a review not the various previous access control schemes[19] where resources are limited and the feasibility of the model was not possible.The new models will provide various areas and techniques where model access control can be easily implemented .The implementation of the model is highly possible where access control is not an issue thesedays.

III. PROPOSED FRAMEWORK

The paper proposes a framework that supports optimization that can be done during the block construction.Data basically comes from various sources these days like wearables ,gadgets and also the attribute base data updated by variousdoctors.The methodology has an access control scheme which allows the fixed data to be stored and it .To provide a unique hashaddress SHA-256 algorithm is used which provides a unique set of hash value to the system.Due to the data being scatteredacross the network ,the number of address required would be quite higher.The problem is even bigger when the amount of data is small and the hash address is relatively more.To make the model light weight and to ensure the basic block should be low in size .Even if the data is less in the block the size is on the higher size due to address being added to it. Data comes from various sources in the framework and due to the access control mechanism available in the model, the traffic is passed to the next level.The initial block that is called asa genesis block, initiates a smart contract which has previous hash and the hash value.The value of the previous hash is 6 bit long and the hash value is 6 bit in size .Total of 12 bits are required to store the data in a particular block of the hash.The issue become more complex when the number of transactions are more ,accordingly the hash value size needs to be updated and also the address space gets larger.The model constructs associates a hash file which allows the hash value to be stored in the log context.The genesis block address is OFXF12 which is the initial address of the blockchain. Once the data is transmitted the newly constructed block of the blockchain model retains the address of the genesis blockhash .Thenextthingtheblockcandoistocarryalogfile(LF)which is considered as a record file as well.The data that is passed from the block is considered as the initial data along with the log file.The log file is operated on the genesis block hash address .As a result the new hash value is generated .The value generated is equivalent to the new hash value of the new block hash value. To understand this the genesis block has a value OFXF12,this is being moved to all the block based nodes and all nodes i the network can have an easy access to it.The connected block hash value is the value that relates the new blockhashvaluewithacalculativenumberOFXF28whichis+16 more than the initial block of the genesis block.The block usually will require two differentiators other than timestamp and nonce.The two differentiators consists of the value of the initial hash that is stored in the genesis block and also the log file .The data stored in the block is comparatively low in nature.Once the physical data is stored in each of thenodes,the replica is shared across the network .The large size of the block is a matter that allows the network degradation due to high consumption of memory .Not only this the speed of the transaction is also affected .The model will surely reduce the hashvaluepromote scalability of the network.Although,the quality of the block is degraded in many casestolowerdowntheweightoftheblock.

IV. IMPLEMENTATION

The block in the blockchain model consists of two hash set which consists of the hash values of the previous and next block.The hash value depends on the number of blocks in the blockchain.The increase in number of nodes will lead to in- crease in number of digits of the hashing function as well.The proposed model creates a framework[10] that constructs a block with set of calculation model which allows the block to be optimised across the network.The redundancy can be removedbytheproposedmodelandsecurityisalsounchanged in the described model. The two hash function can be replaced by the hash function and a calculative value. The calculative hash function can reduce the block size and enhances the scalability to add more blocks in the blockchain with same power consumption.The value of the hash is converted using the calculation file that ensures the uniqueness and the hash value to be updated with the calculated file.The log file maintains all the records of the changes in the hash value per transaction.The size of the encrypted hash can be reduced and to calculate the value fo the new hash the log file operation is applied to the block .The new hash value can be generated and ensured that the original value meets the value of the blockchain.

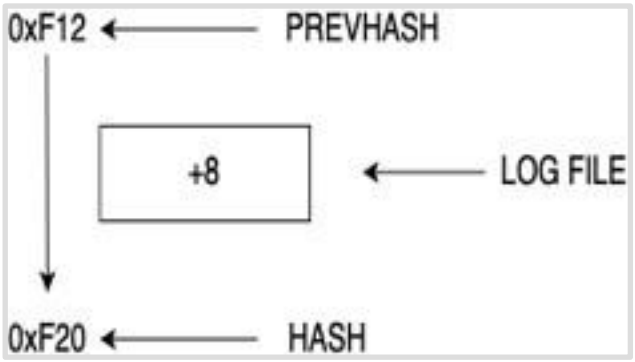

Fig. 2. Log Based Model of Blockchain

The initial block of the blockchain is contains the address and 0xF12 ,the new address is (+8) different with the new hash.Once the block hash is changed with the other hash then the log file maintains the record .The use of the log file will allow to uniquely identify the address of the block .The model compresses the initial hash value with the next hashvalue.The compress model allows the blockchain enabled model to be more scalable.This can be easily used where the hash value is changed upto some extent but when the hash value is changes all the digits ,in that case maintaining the full key value becomes very difficult as the size of the file log value and the actual size of the block consumes same number of digits .Another addition to the model can also be done by creating a mechanism that can be used in the cases where the hash is entire different from other and required an equalspacein the log file.The file will also store the minimum size value that is required to change the next hash value.This will allow the model to lower down the space requirements of the node storage upto some extent.The scalability of the model can be achieved by maintaining the log file and also a mechanismthat ensuresthebestpossiblefitforthecalculationtobestored.The model also promises the security where the same file also checks the hash value by applying the log based on the file as well.The availability of the data at the patient is also a major concern for the development of the model.This model also aims on making it more possible for the patients to ensure thatthedatausavailableattheirend.

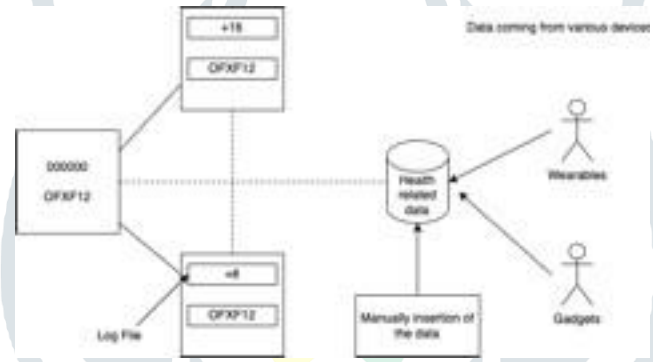

Fig. 3. Systematic framework of flow of data

V. CONCLUSION

Blockchain technology can be widely used because of its decentralised infrastructure and peer-to-peer nature, the blockchain is highly regarded and approved. Bitcoin, on the other hand, protects a lot of blockchain research. However, blockchain could be used in a multitude of sectors other than Bitcoin. Due to various advantages of the blockchain enabled network ,the technology has revolutionised various applications of the blockchain.The issue discussed in the paper related to blockchain is the scalability of the blockchain model that ensures the data to be made available to every end.The compression of the block size is discussed in the paper and also an algorithm is introduced which allows the block size to be reduced.This is one of the most concerned area which lowersdownthescalabilityoftheblockchain.

REFERENCES

[1]Omar, I.A., Jayaraman, R., Salah, K., Simsekler, M.C.E., Yaqoob, I., Ellahham, S., 2020. Ensuring protocol compliance and data transparency in clinical trials using blockchain smart contracts. BMC Med. Res. Methodol. 20 (1), 1–17. http://dx.doi.org/10.1186/s12874-020-01109-5, URL https://link.springer.com/articles/10.1186/s12874-020-01109- 5https://link.springer.com/article/10. 186/ s12874-020-01109-5

[2]U. Nadiya, K. Mutijarsa and C. Y. Rizqi, ”Block Summarization and Compression in Bitcoin Blockchain,” 2018 International Symposium on Electronics and Smart Devices (ISESD), 2018, pp. 1-4, doi: 10.1109/IS- ESD.2018.8605487.

[3]S. Ding, J. Cao, C. Li, K. Fan and H. Li, ”A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT,” in IEEE Access, vol.7,pp.38431-38441,2019,doi:10.1109/ACCESS.2019.2905846.

[4]Zibin Zheng, et al. (2017): An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 6th IEEE International Congress on Big Data, 557-564, available: https://ieeexplore.ieee.org/document/8029379/.

[5]Jelle van den Hooff, M. Frans Kaashoek, and Nickolai Zeldovich. 2014. VerSum: Verifiable Computations over Large

Public Logs. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). ACM, New York, NY, USA,1304- 1316.

[6]Hasan, Jahid. (2019). Overview andApplications of Zero Knowledge Proof (ZKP). 8.5.

[7]Ueno, Taro Hirano, Tomonobu Motohashi, Tomomitsu Okumura, Kosuke Takajo, Kentaro Kuroki, Taiyo Ichikawa, Daisuke Matsuoka, Yutaka Ochi, Eisuke. (2020). Data validation and verification using blockchain in a clinical trial for breast cancer (Preprint). Journal of Medical Internet Research.10.2196/18938.

[8]G. Malik, K. Parasrampuria, S. P. Reddy and S. Shah, "Blockchain Based Identity Verification Model," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019, pp. 1-6, doi:10.1109/ViTECoN.2019.8899569.

[9]O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, April 2018, doi: 10.1109/JIOT.2018.2812239

[10]Dawn Xiaodong Song, "Athena: a new efficient automatic checker for security protocol analysis," Proceedings of the 12th IEEE Com- puter Security Foundations Workshop, 1999, pp. 192-202, doi: 10.1109/CSFW.1999.779773

[11]Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. 839-858. Paper presented at 2016 IEEE Symposium on Security and Privacy (SP).https://doi.org/10.1109/SP.2016.55

[12]Novo, Oscar. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. 5. 1184-1195. 10.1109/JIOT.2018.2812239.

[13]Xu, M., Chen, X. Kou, G. A systematic review of blockchain. Financ Innov 5, 27 (2019).https://doi.org/10.1186/s40854-019-0147-z

[14]A. Azaria, A. Ekblaw, T.Vieira and A. Lippman, "MedRec: Us- ing Blockchain for Medical Data Access and Permission Manage- ment,"20162ndInternationalConferenceonOpenandBigData(OBD), 2016, pp. 25-30, doi:10.1109/OBD.2016.11.

[15]Omar, A.A., Bhuiyan, M.Z.A., Basu, A., Kiyomoto, S., Rahman, M.S., 2019. Privacy- friendly platform for healthcare data in cloud based on blockchain environment. Future Gener. Comput. Syst. 95, 511–521. http://dx.doi.org/10.1016/j.future.2018.12.044.

[16]Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIR- Chain: Applying Blockchain to Securely and Scalably Share Clini- cal Data. Comput Struct Biotechnol J. 2018 Jul 29;16:267-278. doi: 10.1016/j.csbj.2018.07.004. PMID: 30108685; PMCID:PMC6082774.

[17]Nadiya, Ulfah Mutijarsa, Kusprasapta Rizqi, Cahyo. (2018). Block Summarization and Compression in Bitcoin Blockchain. 1-4. 10.1109/ISESD.2018.8605487.

[18]T. Hardjono and A. S. Pentland, "Verifiable anonymous identities and access control in permissioned blockchains," Tech. Rep., 2016

[19]A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "FairAccess: A new Blockchain-based access control framework for the Internet of Things," Secur. Commun. Netw., vol. 9, no. 18, pp. 5943–5964, 2017.