Ilkogretim Online - Elementary Education Online, 2020; Vol 19 (Issue 3): pp. 4591-4599
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2020.03.735612

A Cryptographic Sharding To Achieve Stride Scaling Ability

Sharmila P[1] , Anuratha K[2] , Soshya Joshi[3] , Nandhini J M[4] , Rekha C[5]

[1,2,3,4,5]Department of Information Technology, Sri Sairam Institute of Technology, Chennai, India

Abstract: In all the well developed countries, The salary and the compensation process is digitized, but, still there are issues in the tax processing. Then in few government agencies which are involved with their own ledgers of data, in fact even duplicating data of other agencies. It is more important to ensure the efficiency of tax collection is maintained by government in secures manner. In a decentralized network there is a scarcity in industrial and agency security standards. Service delivery of this kind requires public expenditure. Hence, governments require resources to finance their expenditure system. Where every transactional data will be organized using the technology. A variety of information can be stored using block chain technology and tax related data of the citizens of acountry.

INTRODUCTION

In Recent days all the industrial and business process are digitized to ease the processing and managing of information. In the traditional method, the employers were act like intermediaries they calculate the tax and transmit the tax details and social security payments to the proper agencies, this manual work reduced by enforcing block chain- based smart contract, this problem can be solved. The employers need to provide only the salary figure of an employees with respect to contract terms, the tax and other social security amounts will be auto-calculated. The net salary will be transferred to the employees while the tax details transferred to the respective government agencies.

at the same time accomplish the fragmentation, security and performance measurability. . For current block chain systems, as additional nodes be part of the network, the potency of the system (computation, communication, and storage) stays constant at the best. a number one plan for sanctioning block chains to scale potency is that the notion of sharding: completely different completely

. [4].Sujatha Kumari B A.,et,al, describes “Blockchain based data security for financial transaction system”that Blockchain may be a This process will reduce the time and also save costs and reduces the chances of errors or frauds. The speed, accuracy and transparency of block chains could help to

reduce these burdens for taxpayers by decreasing the risk of fraud. This technology block chain can allow us valuable data to be proceed with accuracy and trust, that they are becoming more commonly immerse in day-to-day business processes.[1]

II. LITRATURESURVEY

Songze Li,et,al stated Coded Sharding Achieves Linearly Scaling potency and Security Simultaneously, that today's blockchain style put up with trilemma assert that no block chain systemwill

different} subsets of nodes handle different parts of the blockchain, thereby reducing the load for every individual node. However, existing sherding proposals deliver the goods potency scaling by compromising on trust - corrupting the nodes in a very given shard can result in the permanent loss of the corresponding portion of knowledge

technology that's booming for a decade and plenty of areas should go underneath improvisation despite its various advancements. The planned system

preponderantly focuses on providing security to the blockchain system exploitation varied mechanisms. the planned model consists of the money transaction-based system that works on the RFID technology. the info obtained from the system is solely accessed by the shoppers World Health Organization ar licensed therefore providing the primary level of security by providing authentication to the valid consumer exploitation M2M authentication. Once the user is documented, he will then have access to the group action system. [8]

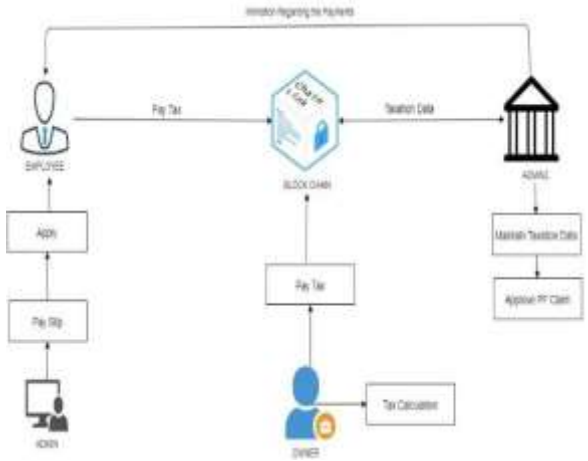
III. EXISTINGSYSTEM

In existing system from the collation, cleansing and verification of data to the preparation, validation and submission of returns, tax processes are largely paper-heavy and labor-intensive. The outsiders include individuals, organizations, and some agencies that needs to get taxpayer information confidentially for the intention of selling the information, to threaten taxpayers or causing political embarrassment, to improve the negotiating position in criminal or civil actions, denying availability, modifying or destroying record. Employees, suppliers, and sellers who are resentful or bribed to gain such information. Taxpayers data processed in a stand-alone systems and stored in a physical magnetic tape.[2][3]

IV. PROPOSEDSYSTEM

The proposed system is designed in which businesses had never ever paid taxes in history were all compelled to stand by the law. The government thereby managed to muss many an industrial feather. According to experts this tax law is great in drafting and aims for maximum benefit to organizations

and users, also increases government revenues. As the system becomes transparent, users will trust the government more and will co-operate in making the whole system viable and compliance will increase. Every entity will pay the tax directly to the tax authority and hence no question of refunds etc. Block chain addresses most of the current issues undergone by the government and the taxpayers. Due to the transparency of block chain the tax payers and the government can able to



check and verify the tax payment details, additionally the application calculates tax for the PF amount and without third party servers, the users can apply and claim the amount. The scalable architecture effect of block chain will provide much more reliability on The stored transactional data. Main advantage in proposed system is One can able to get immediate data about the fundamentals details of the companies like their finances, delivery time, and payment histories. The details will be tamper proof and no one can make any changes.[6]

Fig. 1 System Architecture

WORKING

User get login, that user approval will be provided by admin, then only user get the login. After the approval stage we gathered all information about the users and also salary details to calculate the tax details of the user. In tax calculation module owner and employee has different of tax calculation, that both rules are included in it. By using this rule tax will be calculated automatically and then the deduction details will be provided to the users. [12]This Tax calculation details will be maintained in database for one year. Users can also verify the tax record whenever they needed. In Mailing module paid process, unpaid process and pending amount details will be mailed to the user. User can apply for PF according to their salary, after documentation verification their details will be provided to the government once then approved PF will be generated the user. Then final report will be provided to the user.[7]

The authorization module takes care of the authentication to ownership and employee by verifying the details and to process the transactions and store the records. On the authorization step the pay slip is generated basedon the guidelines provided by the respective organization. All the successful transaction records will be generated and stored in block chain. [13]. This will be available in the entities account which is further can be verified. This will improve the better book keeping and secure the records. User can view the slip apnea view format of data and monitor data from the client and they can order some need medicine they can show only nearest branch of diagnosis agency [8] .The Application owner can fetch the details and it can validate some availability details. Finally, it can have sent the records to Diagnosis. User can maintain a database in MySQL server or SQL server for his/her business requirement.[9][10]

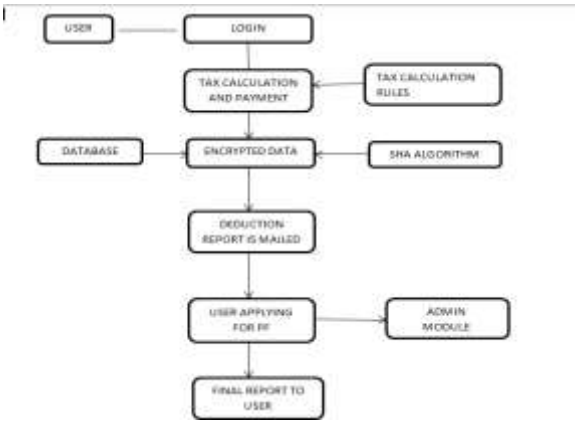


Fig.2 Work Flow

We store the details in the encrypted form by using SHA-512 algorithm. The transaction details will be maintained in their accounts. This module will enable the users to verify their transaction details. The speed, accuracy and transparency of block chains could help to alleviate these burdens for taxpayers by decreasing the risk of fraud. By using this we can easily trace the transaction process and documentation process whenever we needed. processing phase of SHA-512 as the last of these 'intermediate' results. [14]. SHA– 512 algorithm process the message length 2^128 bits and produces a message digest of size 512 bits [11], SHA -512 is more secure and stronger than the hash produce by SHA-256.

V.IMPLEMENTATION AND RESULT

User entering the salary details in pay slip

Fig.3 Pay Slip page

Storing the information in the encrypted form using SHA algorithm

Fig.4 Encrypted data storage

The proof for paying tax will be submitted in this page.

Fig.5 Statement Proof

Table 2 Performance of SHA-512 for different charactersize

SHA-512						
Hash Size (in characters)	**1 ms**	**2 ms**	**3 ms**	**4 ms**	**5 ms**	**Average**
36	**1073**	**1055**	**1050**	**1052**	**1052**	**1056.4**
49	**1834**	**1827**	**1833**	**1836**	**1857**	**1837.4**
72	**1133**	**1131**	**1116**	**1102**	**1110**	**1118.4**
85	**1133**	**1131**	**1116**	**1102**	**1110**	**1118.4**

VI.PERFORMANCE EVALUATION

Performance is measured in terms of the output provided by the appliance. Demand specification plays a very important half within the analysis of a system. only if the need specifications area unit properly given, it's doable to style a system, which is able to match into needed atmosphere. The requirement specification for any system is often loosely expressed as given below:

- The system ought to be ready to interface with the prevailingsystem
- The system ought to becorrect
- The system ought to be higher than the prevailing system

Table 1 Performance of SHA-25 for different charactersize

SHA-256						
Hash Size(in characters)	**1ms**	**2 ms**	**3 ms**	**4 ms**	**5 ms**	**Average**
36	746	724	741	720	758	737.8
49	1505	1496	1507	1498	1516	1504.4
72	1145	1137	1241	1141	1177	1168.2
85	1145	1137	1241	1141	1177	1168.2

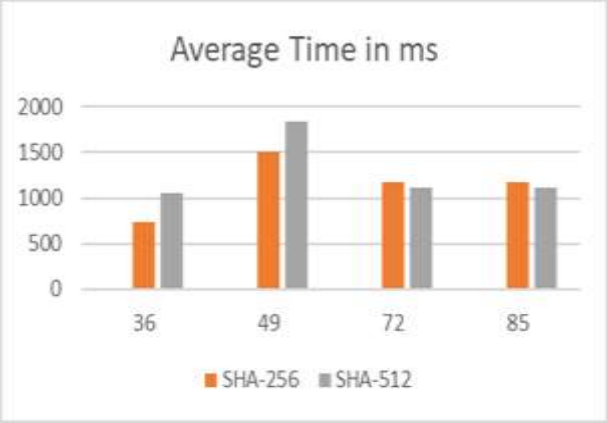


Fig.6 Performance comparison of SHA-12 and SHA-256 based on different Hashsize.

VII .CONCLUSION AND FUTURE WORK

While block chain is not solving all the tax payment issues but it can reduce the manual burden and try to narrow the tax gap. Every government desires minimum leakages in their tax revenues. Block chain holds a lot of promise and governments all over the world are quite excited about implementing block chain in the tax systems. With the current government and its emphasis on digital India, Block chain seems to be the ideal solution for efficient tax collection.

REFERENCES

[1]A. Bahga and V. K. Madisetti, " Blockchain platform for industrial internet of things," Journal of Software Engineering and Applications".

[2] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in IEEE 18th International Conference on e-Health Networking, Applications and Services(Healthcom).

[3] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, et al., "On scaling decentralized blockchains," in International Conference on Financial Cryptography and DataSecurity.

[4]Songze Li, Mingchao Yu, Chien-Sheng Yang, A. Salman Avestimehr, Sreeram Kannan and Pramod Viswanath "PolyShard: Coded Sharding Achieves Linearly Scaling Efficiency and Security Simultaneously" arXiv:1809.10361v2 [cs.CR] 24 Jan 2020.

[5] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and CommunicationsSecurity.

[6] Manisha Nehe, Shitalkumar A.Jain" A Survey on Data Security using Blockchain: Merits, Demerits and Applications", International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC),IEEE XPLORE ,Feb 2020.

[7] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and CommunicationsSecurity.

[8] Sujatha Kumari B A & Sadaf Farheen ," Blockchain based Data Security for Financial Transaction System" 4th International Conference on Intelligent Computing and Control Systems (ICICCS) ,IEEE XPLORE,June2020.

[9] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger.," IACR Cryptology ePrint Archive.

[10] A. E. Gencer, R. van Renesse, and E. G. Sirer, "Short paper: Service oriented sharding for blockchains," in International Conference on Financial Cryptography and DataSecurity

[11] H. Yoo, J. Yim, and S. Kim, "The blockchain for domain based static sharding," in 2018 17th IEEE International Conference on Trust, Security and Privacy In Computing And Communications /12th IEEE International Conference on Big Data Science engineering.

[12] K. Lee, M. Lam, R. Pedarsani, D. Papailiopoulos, and K. Ramchandran, "Speeding up distributed machine learning using codes," IEEE Transactionson InformationTheory.

[13] S. Li, M. A. Maddah-Ali, Q. Yu, and A. S. Avestimehr, "A fundamental tradeoff between computation and communication in distributed computing," IEEE Transactions on Information Theory

[14] Santanu Depnath, Abir Chattopadhyay and Subhamoy Dutt "Brief review on journey of secured hash algorithms" in 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)

[15] A. Gowthaman, Sumanthi Manickam "Performance Study of Enhanced SHA-256 Algorithm" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 4 (2015) pp.10921-10932.