Truth discovery Mechanism: A decentralized blockchain approach

A.VishnuSiddhan[1], A. AzhaguJothi[2],S. PriyaDarshine[3],B. Sarathpriya[4],V.D Sri Hari[5]
UG Scholar [1, 2, 3, 4], Assistant Professor [5]
Department of CSE, Sree Sakthi Engineering College, Coimbatore.

Abstract

In the period of big data, the data about a similar article gathered from various sources is definitely gets conflict. This wonder inspires the need of truth disclosure, which expects to naturally locate the genuine case among numerous clashing cases. Truth discovery is point of botch as the nodes in the network functions independently. As the block-chain lacks support for on-chain data confidentiality, we utilize the privacy-preserving solution and incorporate it with blockchain for privacy protection. We implement the framework with the Ethereum blockchain and demonstrate it`s performance in which the process of extracting accurate data from the large data sets that are combined from the crowd-sourcing applications. Most of existing publicly supporting frameworks depend on central servers, which are dependent upon the powerless nesses of conventional trust-based model. They are also vulnerable to distributed denial of service stacks due to malicious users involvement. The decentralized model along with block chain ensures data privacy and reliable truth discovery process and overcomes single

Index Terms—*Block chain, Truth discovery, secure crowd sourcing, ethereum*

I. INTRODUCTION

Truth discovery is the way toward amassing dependable and exact information from numerous clashing assets. A fact revelation task is finished by communicating the assignment and the laborers require the undertaking by getting a prize. The diggers at that point total the outcome and send it to the requester.

In the modern time data is being generated from various conflicting sources [1].Thereforethere is a need to find which data is reliable and accurate. In this framework, the crowdsourcing application is used to collect data from different sources and the data is aggregated by the miners to identify the accurate result from the conflict data

Crowdsourcing is used in complex problem solving methods and provide an open call to the workers to complete the task as defined in the smart contract[2][3].

The existing models work on the basis of centralized server model which has many overheads in the implementation.

In this model, there is a centralized server in which the data is processed and stored. The clients only collects the data from the workers and doesn`t stores or process any data. The client totally depend on the server for it`s operations and cannot function on it`s own.

In the current models, the unified model has concerns, for example, single purpose of disappointment and powerless against Denial of Service [DOS] assaults. The brought together model depends on the ace slave relationship wherein the customer legitimately relies upon the server for it's functionalities. At the point when the server execution corrupts the general execution of the framework is influenced

Blockchain is a digital ledger in a decentralized manner in every node in the system. Each node in the system is independent in nature and it doesn`t depend on each other.

The blockchain eliminates the need of the central server to process and store the data. Each node act as a server and a

client that processes the data itself and store the data in it. There is no master-slave relationship in the de-centralized model therefore there if a node fails or any fault occurs it doesn`t affect the whole system. There is no single point of failure.

Every block possess the hash value of the preceding blockby forming a hash chain called blockchain which is public, immutable and ordered distributed ledger[4]. The blocks can be never interfered or changed. The miners derive the final results and uses the existing block hash to add new blocks to the blockchain.

The blockchains are used to store the smart contract details and user`s credentials. The Ethereum blockchain is used here which is an open source blockchain that preserves the data in a confidential and efficient manner. The transactions in blockchain are recorded in chronological order[5]. Thus, all the chunks in the blockchain are time marked.

The smart agreements contain the exceptional location, reward balance ahead of time and content that characterizes the depiction of the assignment. The brilliant agreement is changeless. When the substance in the shrewd agreement is refreshed in the blockchain even the requester of the undertaking can't change it.

When the workers submit the task and presents the information to the blockchain the knowledge contract is denied and the prize is sent to the client. After the excavators total the outcome and add it to the new squares in the blockchain they will be compensated as characterized in the sharp agreement.

The Ɛ- local differential privacy is used to provide privacy to the data that is submitted by the workers and it prevents the miners and requesters from accessing the original input data given by the user[6].

II. PROBLEM FORMULATION

A. Architectural model

In the structure the design is isolated into three layers, Application layer, Blockchain layer and Storage layer. Application layer gives UI to the publicly supporting task[7][8]. The program is sent to the blockchain layer in the wake of being assembled, at that point they are composed to the blockchain in the wake of being confirmed by data diggers. The storage layer is the most reduced level, which is essentially used to store the real information estimations of assignments and arrangements.

The structure comprises of four significant entities[9]. They are requesters, labourers, blockchain and miners. The requester module characterizes the shrewd agreements that characterize the conglomerating procedure for the assignment, the quantity of required specialists, rewards data, the errand, and the prize/punishment rules. The laborers guarantee the assignment that is mentioned by the requester and presents the information to the blockchain[10][11]. Once there are answers submitted from various labourers, the miners execute the tasks archived in the brilliant agreement and make obstructs on the blockchain.

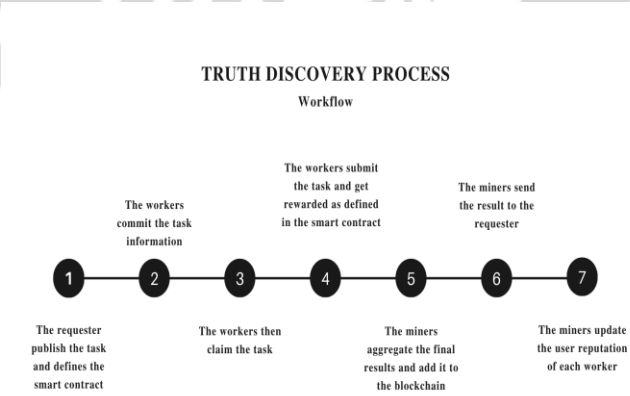


Fig. 1.ArchitecturalModel and Work Flow

B. Threat model

The workers are considered as the trusted entities and they are independent entities in the system. The workers and requesters can access the all the data in the system. The requester only obtain the aggregated results from the miners.

C. Design goals

1. Privacy Preserving

The workers information might contain the sensitive data that must be secured[12][13]. The third party access to the data in the blockchain and the aggregated results must be denied.

2. Soundness

The final result from the miners should be accurate and the requester should not request to verify the results.
There should be no third party verification for identifying the reliability of the final results

3. Other issues

The workers and the miners should receive the rewards for the quality of data they provide to the system.
The malicious users should be identified based on the user reputation they score at the end of each crowdsourcing task.

III. RELATED WORKS

Accessible motivating mechanism basically thinks about the honesty of the system, yet for the most part overlook the issues of security and protection brought about by a trustful focus. A protection saving blockchain motivating force component in publicly supporting applications, in which a cryptographic money based on blockchains is utilized as a safe impetus way[26][27].

Most of existing publicly supporting frameworks depend on focal servers, which are dependent upon the shortcomings of customary trust-based model, for example, single purpose of disappointment. They are additionally defenseless against conveyed disavowal of administration (DDoS) and Sybil assaults because of malignant clients involvement[28]. Truth disclosure alludes to the system to evaluate the obscure client unwavering quality from gathered tangible information while deducing honest data by means of value mindful information conglomeration. We will likely form a safe square chain swarm detecting framework that guarantees information privacy, information trustworthiness, exact conclusive outcomes and strength.

Information classification is a significant concern square chain application [29]. The Ɛ-neighborhood differential protection guarantees security of the information in the square chain. The laborers information may contain touchy data like wellbeing records and other private information so these information must be made sure about before they are put away in the square chain [30].

IV. CONSTRUCTION

The framework has four phases namely publish, submit, aggregate and update.

In the publish phase, the activist publish the task to the workers and provide a reward based on the task. In the submit phase, the worker commit the task and obtain the reward by submitted the data. In the aggregate phase the miners derive the final results. In the update phase, the miners update the user reputation based on the quality of the data they provide.

A. Publish

The requester defines the number of workers required to complete the task, penalty and reward information for the workers and miners as a smart contract through the blockchain[14][15].

The contract is defined as the ‘recruiting process for workers’ so that the workers commit the data to the blockchain. When the minimum criteria of the smart contract are met, the status is changed to ‘in progresses and the miners will aggregate the final results to the requester.

The meta data of each user will be updated to the blockchain when they join the task to submit the data[16].

B. Submit

The document in the collection is assigned with a switch value, r. The switch is a vector value which is a multiple of L and E, where is the no of groups the document collection has been divided and E is the no of times the document has been copied[17].

C. Aggregate

The miners aggregate the final reliable and accurate results from the input data[18]. The miners create new blocks in the blockchain as defined in the smart contract. A key value map $<a_{q,i}, r_{q,i}>$ is used to store the aggregated result and actual input data in the blockchain. $a_{q,i}$is the i-th value of the question.$r_{q,I}$ is the aggregated value of the question. The aggregated value of all questions is initialized to zero. After successful mining of each data the aggregated value is updated as follows,

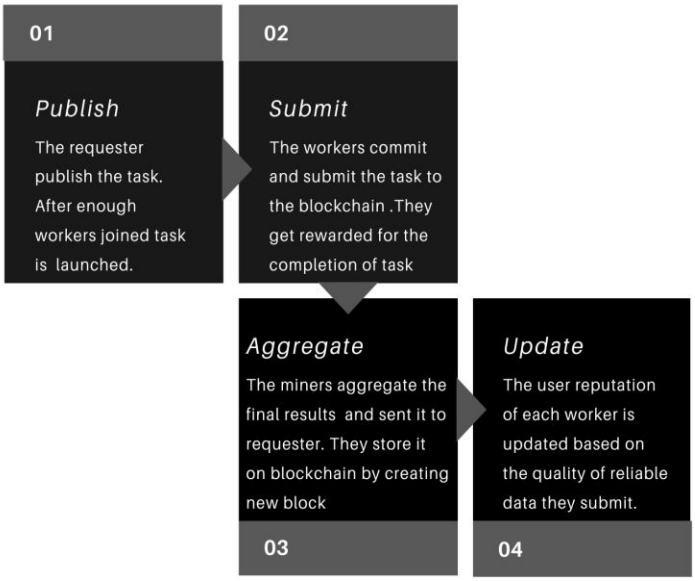
$r_{q,i} = \Sigma_{w \in Wsub} x_w . 1(a_{q,i}, a^{\wedge}{}_w{}^q) + r^{old}{}_{q,i}$

The final aggregated result of the crowdsourcing task is obtained as follows,
aq= aq,i, with rq,i= max(rq,i, $1 \leq i \leq |Aq|$)
After each data is aggregated and added to the blockchain the miners will be paid automatically based upon the smart contract. The miners cannot access the original data that is submitted by the user and doesn`t access the metadata of the every worker in the task.

D. Update

In the update phase, the user reputation is updated by the miners based upon the quality of relevant data they provide to the blockchain. The user reputation is represented as x_w,

$x_w = x_w + \Delta x_w$



V. PERFORMANCE ANALYSIS

In this section, two parameters are analyzed first the outcome of the framework and then we analyze theperformance of our framework.

A. Privacy protection

The local differential privacy is used to disturb two input values and if the untrusted miners access the data they cannot return back to the unique answer submitted by the worker[19][20].

The miners and asker cannot access the original data that is submitted by the user due to the e- local differential privacy.

The decentralized model alongside block chain guarantees information protection and dependable truth disclosure process that defeats single purpose of disappointment as the hubs in the system capacities freely[21][22].

Once the data is stored in the blocks of the ethereumblockchain it cannot be changed or tampered. The transactions in blockchain are recorded or stored in chronological order. Thus, all the blocks in the blockchain are time stamped.

B. Fairness

In the brilliant agreement the requester initially characterizes the prize or punishment to the diggers and the laborers. The smart contract works in self-propelled way and the specialist will get the prize once they complete the errand. At the point when the excavators total the conclusive outcomes and add the solid information to the squares of the blockchain they will be compensated as characterized in the savvy contract by the requester. In the event that the laborers don't finish the undertaking, the prize will be declined [23]

C. Soundness

The soundness of the framework is achieved when the smart contract has been executed as all the operations are pre-defined in the smart contract. The miners aggregate the result on the same set of answers[24][25].

VI. CONCLUSION

In this paper we principally center around the deployment model of truth discovery framework that jelly client and information security in the publicly supporting errand. The keen agreements characterize the activities expected to complete the activities of the assignment. After the each effective fruition of the errand and information is submitted to the blockchain the excavators and the laborers will be compensated for their undertaking.

The native differential security is utilized to give protection to the information that is presented by the laborers and it keeps the diggers and requesters from getting to the first info information given by the client and we forestall the information being gotten to by the malignant clients.

The system dispenses with the issue of single purpose of disappointment in light of the fact that nature is arrangement in a decentralized way.

The exhibition investigation show that the structure gives security and the decency of the block chain

VII. REFERENCES

[1] X. Zhang, G. Xue, R. Yu, D. Yang, and J. Tang, "Keep your promise: Mechanism design against free-riding and false-reporting in crowdsourcing," IEEE Internet of Things Journal, vol. 2, no. 6, pp. 562–572, 2015

[2] G. Zhuo, Q. Jia, L. Guo, M. Li, and P. Li, "Privacy-preserving verifiable set operation in big data for cloud-assisted mobile crowdsourcing," IEEE Internet of Things Journal, vol. 4, no. 2, pp. 572–582, 2017.

[3] S. Melanie, Blockchain: Blueprint for a new economy. "O'Reilly Media, Inc.", 2015

[4] J. R. Kan Yang, Kuan Zhang, "Security and privacy in mobile crowdsourcing networks: challenges and opportunities," IEEE Communications Magazine, vol. 53, no. 8, pp. 75–81, 2015.

[5] M. v. d. S. Yu Zhang, "Reputation-based incentive protocols in crowdsourcing applications," in 2012 Proceedings IEEE INFOCOM, Florida, USC, 2012, pp. 2140–2148

[6] C. Miao, W. Jiang, L. Su, Y. Li, S. Guo, Z. Qin, H. Xiao, J. Gao, and K. Ren, "Cloud-enabled privacy-preserving truth discovery in crowd sensing systems," in Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems. ACM, 2015, pp. 183–196.

[7] G. C. Dan Peng, Fan Wu, "Pay as how well you do: A quality based incentive mechanism for crowdsensing," in Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2015, Hangzhou, China, 2015, pp. 177–186

[8] H. Z. B. Y. Z. Gang Wang, Tianyi Wang, "Man vs. machine: Practical adversarial detection of malicious crowdsourcing workers," in Proceedings of the 23rd USENIX Security Symposium. Usenix Security 2014, vol. 14, San Diego, CA, 2014

[9] S. Zhang, J. Wu, and S. Lu, "Minimum makespan workload dissemination in dtns: Making full utilization of computational surplus around," in Proceedings of the fourteenth ACM international symposium on Mobile ad hoc networking and computing. ACM, 2013, pp. 293–296.

[10] Y. Kan, Z. Kuan, R. Ju, and S. Xuemin, "Security and privacy in mobile crowdsourcing networks: challenges and opportunities," IEEE Communications Magazine, vol. 53, no. 8, pp. 75–81, 2015.

[11] A. S. Federico Ast, "The crowdjury, a crowdsourced justice system for the collaboration era," 2015.

[12] Y. Kan, Z. Kuan, R. Ju, and S. Xuemin, "Security and privacy in mobile crowdsourcing networks: challenges and opportunities," IEEE Communications Magazine, vol. 53, no. 8, pp. 75–81, 2015.

[13] T. Ruffing, A. Kate, and D. Schroder, "Liar, liar, coins on fire!: Penalizing ¨ equivocation by loss of bitcoins," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015, pp. 219–230.

[14] . S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009

[15] R. Kumaresan and I. Bentov, "How to use bitcoin to incentivize correct computations," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014, pp. 30–41

[16] H. To, G. Ghinita, L. Fan, and C. Shahabi, "Differentially private location protection for worker datasets in spatial crowdsourcing," IEEE Transactions on Mobile Computing, vol. 16, no. 4, pp. 934–949, 2017

[17] W. Gavin, "Ethereum: A secure decentralisedgeneralised transaction ledger," Ethereum Project Yellow Paper, vol. 151, 2014

[18] B. Halder, "Evolution of crowdsourcing: potential data protection, privacy and security concerns under the new media age," RevistaDemocracia Digital e GovernoEletronico ˆ , vol. 1, no. 10, pp. 377–393, 2014

[19] J. Benet, "Ipfs-content addressed, versioned, p2p file system," arXiv preprint arXiv:1407.3561, 2014

[20] X. F. J. T. Dejun Yang, GuoliangXue, "Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing," in Proceedings of the 18th annual international conference on Mobile computing and networking, Mobicom 2012, Istanbul, Turkey, 2012, pp. 173–184

[21] X. Z. Depeng Dang, Ying Liu, "A crowdsourcing worker quality evaluation algorithm on mapreduce for big data applications," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 7, pp. 1879–1888, July 2016.

[22] E. Toch, "Crowdsourcing privacy preferences in context-aware applications," Personal and ubiquitous computing, vol. 18, no. 1, pp. 129–141, 2014

[23] M. H. Cheung, R. Southwell, F. Hou, and J. Huang, "Distributed timesensitive task selection in mobile crowdsensing," in Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing. ACM, 2015, pp. 157–166

[24] D. M. MarcinAndrychowicz, Stefan Dziembowski, "Secure multiparty computations on bitcoin," in IEEE Symposium on Security and Privacy, S&P 2014, San Jose, CA, 2014, pp. 443–458.

[25] X. Yu, M. T. Shiwen, Y. Li, and R. D. Huijie, "Fair deposits against double-spending for bitcoin transactions," in Dependable and Secure Computing, 2017 IEEE Conference on. IEEE, 2017, pp. 44–51.

[26] I. Bentov and R. Kumaresan, "How to use bitcoin to design fair protocols," in International Cryptology Conference. Springer, 2014, pp. 421–439.

[27] J. Howe, "The rise of crowdsourcing," Wired magazine, vol. 53, no. 10, pp. 1–4, Oct. 2006

[28] J. C. A. N. J. A. K. E. W. F. Joseph Bonneau, Andrew Miller, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies,"

[29] "Elance and odesk hit by ddos," "https://gigaom.com/2014/03/18/ elance-hit-by-major-ddos-attack-downing-service-for-many-freelancers/", [Online].