International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

CROWDBC: A Blockchain-Base Decentralized Framework for Crowdsourcing

J. Jayashree, Ch. J. V. S. Snehith, K. Venkat, P. Chaitanya, J. Vijayashree

Abstract: ***Due to lack of server reliability and user data privacy encryption of data is required before the cloud is outsourced. We have found a compromised method within the blockchain in order to perform a keyword search which is secured on data that is encrypted against malicious service providers and users in cloud. SSE: Privately offers the cloud storage used in symmetric search encryption (SSE) systems, which cannot be regarded as a true cloud. The cloud service is also known to be credible. Let us start by emphasizing the importance of data storage within a public chain. The client is allowed by system to upload them in form which is encrypted, data content is distributed to the nodes of cloud and make sure that the data is available through encryption techniques. Presentation of a blockchain based system for providing the keyword search service with secure storage of distributed data. TKSE performs verifiability on server side so that true cloud servers are protected from being posed by owners of malicious data in the data storage process. Furthermore, technology of blockchain and hash functions are used to allow payment which is fair without third parties involvement for research fees, although if cloud or user is harmful. Our review of security and evaluation of performance show that TKSE is efficient and safe and be suited for cloud computing.***

Keywords: ***blockchain, encryption, CrowdBC, crowdsourcing, cloud***

I. INTRODUCTION

Crowdsourcing has gained considerable interest and acceptance in recent years since it was invented in 2006 by Jeff How through an open call for solutions, a collaborative form of troubleshooting. Today crowdsourcing is considered as a method of problem-solving by many Companies, starting from web and mobile design creation. There are various common applications for crowdsourcing such as Turkish mechanic, Azure, and UBER. We expect this will change the way people function significantly in this sector. Human intelligence-based crowdsourcing is composed of the following roles: candidates, workers and the centralized crowdsourcing system (fig.1).

Revised Manuscript Received on February 05, 2020.
* Correspondence Author
J.Jayashree*, Assistant Professor, Department of Computer Science and Engineering, VIT, Vellore, Tamilnadu, India.
Ch.J.V.S.Snehith, Department of Computer Science and Engineering, VIT, Vellore, Tamilnadu, India.
K.Venkat, Department of Computer Science and Engineering, VIT, Vellore, Tamilnadu, India.
P.Chaitanya, Department of Computer Science and Engineering, VIT, Vellore, Tamilnadu, India.
J.Vijayashree, Assistant Professor, Department of Computer Science and Engineering, VIT, Vellore, Tamilnadu, India. vijayashree.j@vit.ac.in

Candidates pose complicated machine tasks but the crowdsourcing method is easy for humans. A group of workers involved in this role that competes and proposes solutions for crowdsourcing method, while candidates can pick a suitable solution (usually the best solution to solve the problem) and award the correspondent Employee, Hiring the world's biggest freelancer on the marketplace today,

considering Upwork, It allows "customers" (candidates) to deposit a significant payment in "Customers" may then interview or recruit "self-employed" (workers) to design or write. The "self-employed" who focuses in the specialization area compete for the job and the winners will be awarded accordingly. Despite the prosperity of crowdsourcing systems, however, they are subject to traditional trust model weaknesses, which involve some unavoidable challenges. Current crowdsourcing networks were previously vulnerable to DDoS attacks, remote kidnappings and prank attacks, making resources inaccessible. Elance and oDesk, currently managed by Upwork, are cutting services for most workers because they were affected by Distributed DoS attacks during 2014. Secondly, most crowdsourcing systems run the company on a centralized platform from which only the point of failure is necessarily affected. A services outage born because of a hardware issue in Uber in April 2015, which lead to Passengers being unable to interrupt the order after the service was terminated. Third, confidential user credentials (e.g. email address, name and telephone number) and activity solutions are stored in the crowdsourcing system database that is at risk of privacy breach and data exposure. A device freelancer allegedly violates the privacy law to find out the true identity of a user who holds the Australia Information Commissioner's Office (OAIC) IP addresses, active account, and fake accounts for December 2015. Third, in cases of conflict between applicants and staff, they need the support of the crowdsourcing network to provide arbitrary arbitration, which can lead to behaviors known as "fake reports." Finally, crowdsourcing companies are inclined in increasing their own profits and requiring applicants to pay for services, which would raise usage costs. In present scenario, most crowdsourcing systems may require a 5 percent to 20 percent mobile service rate[2]. A lot of work has been done to fix some of the above mentioned problems in crowdsourcing systems. Differential Encryption and Privacy (DP) are used for data privacy protection. It proposes reputational mechanisms to deal with "false relationships" and "free driving" behaviour. Distributed architectures are created to avoid a single failure point and bottleneck issue. Nevertheless, most of these inquiries are based on traditional crowdsourcing models based on triangles, which crumble in trust.

So far none of the existing works have simultaneously provided solutions to all of the previous problems. This work is therefore inspired by the following: can we build a decentralized crowdsourcing network with transparency, resources, protection and low rates of service? To answer that question, we are proposing a decentralized crowdsourcing system based on blockchain.

The framework has many advantages, such as enhancing user security and service availability, enhancing flexibility in crowdsourcing with the full language of Turing programming and reducing costs. Our framework therefore has the potential to break the multitude of traditional models.

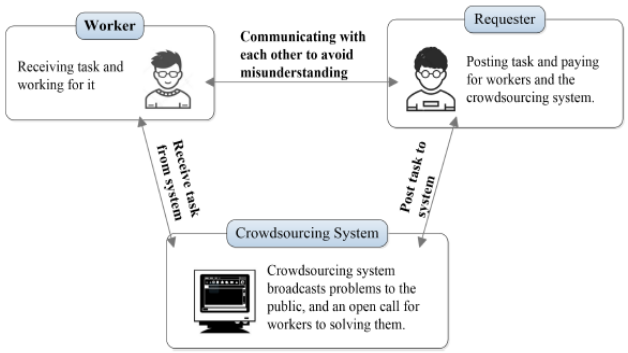

Figure1. The system model of traditional crowdsourcing.

We conceptualize a decentralized crowdsourcing blockchain framework called CrowdBC that doesn't rely on central third parties to achieve the crowdsourcing. Our framework guarantees user privacy Allow users to register in distributed archives encrypted without real identity and archive solutions. -identity requires a security deposit before involvement which can effectively counter attacks such as attacks on DDoS, Sybil and "False News." Plus, users don't have to pay multiple platform fee for the expensive conventional crowdsourcing service, just a little amount of transaction fee needed. CrowdBC also increases the flexibility of crowdsourcing through the Turing-complete programming language to logically represent complex crowdsourcing.

We propose a specific solution based on the proposal frame of reference The smart contract is utilized to do all the crowdsourcing processes that includes activity registration, reception at home, awarding of prizes, etc. In the system, we present three Standard Smart Contracts: Users Registration Contract (URC), Users Summary Agreement (USC), Applicants Employment Contract (RWRC), through which crowdsourcing features such as publishing can be obtained and an activity received without relying on any central authority. In particular, the most useful feature in comparison with traditional systems is the evaluation of the activities under process through a smart contract instead of a subjective third party. Ideally this scheme can prove surprising enough and useful in practice.

Using a software prototype based on an Ethereum audience test network with real world data sets, we implemented this scheme to check the feasibility.

The experiment results show how usable and scalable our proposed crowdsourcing system is. We also illustrate a discussion of Future enhancements to this scheme.

II. RELATED WORK

The Internet and mobile devices explosively increasing, crowdsourcing work has become an emerging trend. We primarily discuss several art works in three main parts: the centralized , the distributed and blockchain based crowdsourcing system. Centralized framework for crowdsourcing. Different crowdsourcing Systems are centrally developed[2],[3],[19],[20]. Such crowdsourcing frameworks provide the crowdsourcing tools, such as worker selection, reward mechanism and the discovery of reality. Upwork and WAZE, are two well known crowdsourcing platforms, allows candidates to hire employees/workers efficiently to find answers to tasks (e.g., accidents, traffic jams at WAZE). Also they requested detailed user information (e.g. Freelancer and WAZE) and user information was stored, centralized platform activity data that may be subject to confidentiality escape[7], Distributed DoS / Sybil attacks[5], and bankruptcy single-point issue[6]. proposed mechanisms based on auctions EFT and DFT [14] proposed a reputation-based incentive mechanism to address fake and free crowdsourcing attacks reports, but traditional three-parity model based methods that does not apply to our idea. In addition, there are a variety of incentive systems for saving money reward activity based on the crowdsourcing system, which inevitably raises the possibility of failure[21]. Distributed framework for the crowdsourcing. The creation of distributed crowdsourcing framework also involves many studies. 18] D2 protocol for the design of distributed crowdsourcing network delay tolerance (DTN) systems was introduced. The writers wanted to collaboratively complete a computational task and carry out The Lesser Makepan. [22] suggested a work assignment scheme in the crowdsourcing method using social relations. They focused on load balancing in the distributed model. [23] introduced a selection of asynchronous and distributed human mobile activities. While[18], [22] and [23] concentrated on spreading the operation, they actually had a centralized service delivery structure that is incompatible with our idea of building the crowdsourcing system centrally. Crowdsourcing system based on blockchain. [24] CrowdJury proposed to be a blockchain-based crowdsourcing framework for the award's judicial process. This is more relevant to our approach but there are no guidelines for the specifics on crowdsourcing architecture. [25] and [26] introduced crowdfunding focused on blockchain, A different form of crowdsourcing. [27] introduced an alternative and similar kind of protocol that uses blockchain to target Small value crowdsourcing transactions problem. Additionally, crowdsourcing research based on blockchain recently gained interest in the sector, such as Gems[29], microworking. The above given works are limited by your specification requests (e.g. crowd jury with court judgment), while conceptualizing a decentralized blockchain

framework with much extent broader goals, as providing directions to system designers ,who are about to design a class of decentralized crowdsourcing protocols.

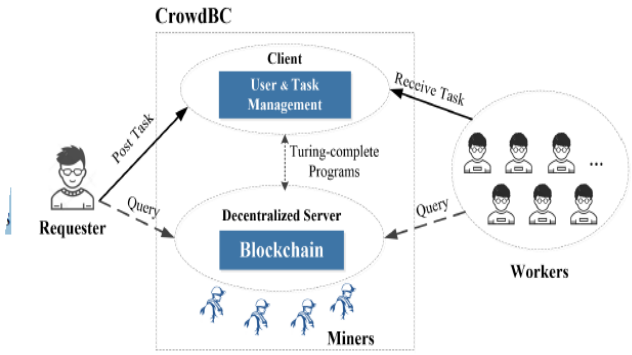

Fig. 2: The system model of CrowdBC.

III. EXISTING SYSTEM

Additionally, cryptographic hash functions and blockchain technologies are used in enabling fair payment of research fees without introducing third parties, even the user or cloud are harmful. The digitally signed encrypted data index in TKSE allows the user to search for encrypted data which is outsourced and verify the search result returned from the cloud whether satisfies the predefined search conditions or not. Our safety review and performance assessment indicate that TKSE is stable, efficient and suitable for cloud computing, first suggested a user-side verification SSE scheme. Verifiability at the user side was also carried out in SSE. Fair payment is also made using blockchain technology and hash function without the introduction of TTP.

Disadvantages

- Less Security
- It is not having any data content
- Identity privacy is neglected

IV. PROPOSED SYSTEM

To retain search functionality, technologies of search encryption were built in two representative configurations including the symmetric key configuration. The concept could not combine explicitly with blockchain technologies where user and the CSP have to define the requirement for redeeming the search speeds needed by the server of the secret key MAC encryption feature as a fundamental component of information security. It is used in numerous security applications and protocols, such as building signature schemes to generate digital and random MAC numbers to guarantee data integrity and the data source authentication.

Advantages

- Saving data management cost
- User privacy protection and data security
- integrity protection
- message authentication code[MAC]

SYSTEM ARCHITECTURE:

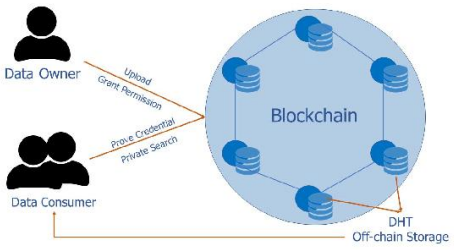

Figure3. BlockDs system model

V. RESULTS AND DISCUSSION

In this article, we present architecture of CrowdBC, a Decentralized Blockchain-based crowdsourcing platform. We observed that the conventional centralized crowdsourcing mechanism is suffering with privacy leakage, single point failure and high service levels. CrowdBC is formalized to deal with these centralized issues. In-between we are improvising crowdsourcing versatility through a smart contract to reflect crowdsourcing dynamic logics. A number of smart contract-based design algorithms had been proposed within the framework to build a concrete scheme.

In addition, we assess our attention to Ethereum with implementation of components that provide decentralized crowdsourcing services. Since We are in early stages of blockchain technology and considering some important works for the future.

VI. CONCLUSION AND FUTURE WORK

First, we are only implementing today's basic crowdsourcing process, but there are more complex far scenes to manage. Second, an efficient assessment mechanism designing is fundamental. We believe an evaluation function the can provided by applicant while task is being published. Nonetheless, we must also recognize that the applicant does not know the solution and therefore, it is becoming difficult to provide an accurate evaluation of the task.

REFERENCES

1. J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, 2015
2. X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015
3. H. Li, F. Zhang, J. He, and H. Tian, "A searchable symmetric encryption schemeusingblockchain,"arXivpreprint,2017.[Online].Available:https : //arxiv.org/pdf/1711.01030.pdf
4. H.G.DoandW.K.Ng,"Blockchainbasedsystemforsecuredatastoragewit hprivatekeywordsearch,"inServices(SERVICES),2017IEEEWorld Congress on. IEEE, 2017, pp. 90–93.
5. R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 776, no. 99, pp. 1–12, 2018.

6. J. Howe, “The rise of crowdsourcing,” Wired magazine, vol. 53, no. 10, pp. 1–4, Oct. 2006.
7. 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.
8. B. Halder, “Evolution of crowdsourcing: potential data protection, privacy and security concerns under the new media age,” Revista Democracia Digital e Governo Eletr˜onico, vol. 1, no. 10, pp. 377–393, 2014.
9. E. Toch, “Crowdsourcing privacy preferences in context-aware applications,” Personal and ubiquitous computing, vol. 18, no. 1, pp. 129–141, 2014.
10. M. v. d. S. Yu Zhang, “Reputation-based incentive protocols in crowdsourcing applications,” in 2012 Proceedings IEEE INFOCOM, Florida, USC, 2012, pp. 2140–2148.

AUTHORS PROFILE

J. Jayashree, received UG degree from Anna University, Tamilnadu and received PG degree from VIT University, Tamilnadu and PhD from VIT University. She is working as Assistant Professor Senior at VIT University, Vellore, Tamilnadu, India. Her research interests include Data Mining, Machine Learning. She had published a good number of papers in reputed Scopus Indexed Journals.

Ch.J.V.S.Snehith, I am a student pursuing my B.Tech at VIT Vellore and I am doing my B.Tech in Computer Science Engineering.

K.Venkat, I finished my secondary Schooling at Sri Chaitanya Jr. College and I am pursuing my B.Tech at VIT Vellore and I am doing my B.Tech in Computer Science Engineering.

P.Chaitanya, I finished my schooling in Narayana school and my secondary Schooling at srichaitanya Junior College and I am pursuing my B.Tech at VIT Vellore and I am doing my B.Tech in Computer Science Engineering.

J. Vijayashree, received PG degree and PhD from VIT University,Tamilnadu. She is working as Assistant Professor Senior at VIT University, Vellore, Tamilnadu, India. Her research interests include Data Mining, Machine Learning. She had published a good number of papers in reputed Scopus Indexed Journals.