A Distributed Fewer Environment for the Use of Blockchain IoT Device Sharing

K Sundaramoorthy1*, E Thenmozhi2, R Josephineelka3, S Suma Christal Mary4 T. Shanmugapriya5

1Department of Information Technology, Jerusalem College of Engineering, Chennai, Tamil Nadu, India
2,3,4Department of Information Technology, Panimalar Institute of Technology, Chennai, Tamil Nadu, India
5Department of Management Studies, St Peter’s engineering college, Hyderabad, Telangana, India

Email: *ksundaramoorthy1999@gmail.com

Abstract. Due to the fact that the data markets become ubiquitous, it also becomes apparent that Internet of Things (IoT) applications produce data sources that are of benefit for future third party users. We are creating a marketplace for IoT data sources, allowing any pair of data providers and customers to participate in data transactions without any previous dependence on the shared trusts, to unlock those possible utility. We have a marketplace and architecture for the exchanging of streaming data, ranging from data publicity to legally binding exchange deals and payments. We prove that we can give participants an interchange of costs between the transactional data exchange and the possibility of loss of data when trading through unreliable third parties, through the use of blockchained technologies and smart contracts, in particular. On a test platform using Crypto currency Smart Contracts, we analyze these agreements experimentally.

Keywords: Crypto currency, Smart Contracts, Internet of Things, Blockchain

1. Introduction

Data streams from IoT products are increasingly used as market assets of interest not only to product owners but also with a resell value i.e. to consumers from third parties. New types of specialized data markets are emerging to unlock such a value [1], although comparatively less developed than more traditional static data business areas, cf. for such surveys, eg [2], [3] and [4]. In comparison to static information, if not processed in near-real time, the IoT data sources tend to lose their significance and data transmission and supply can be inconsistent.

In the other hand, architectures for data sharing, based on systems like MQTT messaging brokers, enable several parties to receive a single data source, which will certainly enable wide open market spaces for data owners to resell their streams on different instances in real time. While a versatile market place can be sponsored by an IoT network and messaging infrastructure this eventually leads to shared trust problems for the participants, particularly when they are not reputed on the market. In addition, the short-term existence of streams involves effective, automatic processes for the creation and implementation of legally binding trade deals, including payment provisions, during data transmission.

Present blockchain technology that supports smart contracts is the natural way to address both of these requirements, as smart contracts serve as an agent of faith in entering into transactions within an untrusted network of business partners both before, during and after data exchange. In [5] (datum.org) is an example of this method based on the Ethereum network, but is meant to allow everyone to store
the organized knowledge of the blockchain. Compared to that, we plan to have a decentralized, in-
house IoT data marketplace, scalable for the number of respondents and without previous
confidentiality, with specific guarantees on data and cash loss in the case of a participant scam.

New participants (individuals, organizations or companies) should be able to accept the market
flexibly, be resilient to the abandonment of participants as well as tolerate unforeseen partnerships
between them. Anyone with IoT sensors and IoT data sources is then able to monetize and use them as
commercially viable assets. In addition, relative to current deals, for example[6], we aspire for a
marketplace which does not need a centralized trust function, such as a trustworthy network, but rather
relies on reciprocal management mechanisms like blockchains, to impose its own governance
legislation. Figure 1 discusses about broker System Architecture.

![System Architecture](image)

**Figure 1.** System Architecture

We use Ethereum's Smart Contracts to enable contact between a data provider and a customer in
any process. It varies from money transfer interactions to ensure that participants' actions cannot be
reputed and to settle their conflicts which exist in the blockchain network through the interactions that
occur on IT and the core cloud network. This is followed by our earlier IoT-data business proposition,
in which we indicated that Ethereum is able to provide funding without shared confidence for a fully
open marketplace [7].

The solution proposed in [7] is based on the premise that any participant reports on data submitted
and obtained from other participants on a regular basis to a smart contract and the contract will then be
able to use those reports to address conflicts. On the opposite, we recommend a much streamlined and
separate protocol for data vendors, users and a smart contract, backed by blockchain transactions,
which embody the concept of frequent checkpoints during data sharing and guarantees reduced scope
on both sides for fraud. In order to evaluation cost/risk trade-offs which are open, we then use our own
test implementation of the business model in a private Ethereum Network. By setting the frequency of
the checkpoint, the participants are still utilizing the possible external confidence structures where
available.

2. Related Works
The huge number of available IoT data cannot be monetized in terms of optimization and
interoperability. In a centralized or decentralized archive texture there are a range of marketplaces for
IoT data management, including Microsoft Azure BDEX (bdex.com) and Big IoT Marketplace, a
European initiative for allowing IoT Ecosystems to be sold by IoT data providers. The two examples
demonstrate that a single agency controls and regulates communications with the data source and the
information consumer. These are crucial solutions.

Many blockchain networks were used for the sharing of IoT data. Which are private, or allowed,
like Hyperledger (hyperledger.org), Quorum and Corda (marketplace.r3.com). Hyper ledger demonstrates low consensus latency, but does not entirely meet decadal targets, while both J.P.
Morgan's quorum and Corda are aimed at the finance sector through separate methods, which save IoT
data off the chain and maintain consensus among trade parties. The Ethereum blockchain [8], a public
and automated framework for this work provides the communicating parties with smart contracts to
build their DAPPs and makes it a preference platform. This is one of the most relevant blockchain systems.

There are also a number of decentralized IoT markets. ID-MoB [9] is meant to trade in IoT data between IoT suppliers and users in real time and not sensitive IoT data. It works on Ethereum and uses intelligent contracts for business management, market regulation and engagement with the Raid Micropayment Network.

The same is the case with Data broker DOA (databrokerdao.com), a companion to the local IoT sensor data market. The sensor owners placed their data produced by their sensors on the market based on their white papers [10]. They think the online retailers for sensor data will be their business.

Pierre A. Et al [11] derived a smart blockchain marketplace to monetize IoT results. Similar to our model, they use smart agreements for the management and settlement of payments, to send IoT data via MQTT broker. The key difference is that a deposit is required before the subject is subscribed to. This goes against our presumption of no trusts, because the customer is likely to consider leaving a deposit before the reception of the goods as dangerous.

Huang Z. Huang Z. A decentralized IoT data sharing network [12] addresses the problem of the participants' mistrust, and in the same way as we handle, data is shared off-chain and made available to purchasers after the contract has been completed. The data to be accessed is therefore stored, so that this solution cannot be streamed. In addition, there are no promises to ensure that the data is authentic; meaning the advance payment i.e. for data download access is dangerous.

In the field of authentication of data sources, another initiative has appeared on the IoT market. Data pace (datapace.io) is a method of distributed and open data authentication focused on blockchain. The IoT sensors are related to Main flux IoT network that is built into the Data pace device segment known as IoT data platform (Data pace IoT). The distinction between this model and our model is that this model offer authentication of data sources through its own sensing instruments. Our model assumes the honesty of data sources vendors and no special hardware for authentication.

A Ledger (anyledger.io) is also an IoT wallet that connects up the blockchain with the physical world. The blockchain transaction is carried out by any IoT device. It is the first network to allow IoT-Blockchain hardware de-Vice and embedded device applications and finally completes remote system management and blockchain nodes. Any blockchain Ledger system uses their white paper [13] to ensure that tamper proof sensors are carried out quickly and remotely. It uses IPFS for safe data monetization as a decentralized database.

Finally, IOTA (iota.org) declared its support for decentralized markets in late 2017 with the goal of allowing the opening of data silos that currently limit the data to a few entities in a genuinely decentralized data marketplace.” A characteristic aspect of the solution is that, compared to the previously cited ones, the IoT data are currently stored on the tangle [14] on the blockchain (or the variant of the IOTA).

In comparison to IOTA, Streamer (streamr.com) claimed that a brand new blockchain could not be built and the current Ethereum blockchain should conserve money instead. It's an exchange site for real-time data sources. It provides a data creator environment for customers to sell their data. A data manager establishes data sources for their data, as stated in their white paper, and drives it to broksher nodes responsible for supplying it to its data users who buy the data they want by communicating with the Ethereum Smart Management, Data Authorization and Payment contract.

Trust and reputation management is not discussed explicitly in this article, but as part of the markets, a model of trust management should also be developed. On top of our architecture, current faith structures can be used. In [15] examines confidence through the IoT platform layers (physical sensing, network, and application layer), concentrating on a broad range of data quality, power, reliability, usability, and capability characteristics. Their study, however, generally overlooks confidence problems among data market participants in the context of transactions relating to the sharing of data. Roman and Gatti's data sector faith study [16], focused on credit scoring, where clear ties are made through the use of data trading blockchain technologies, is more specifically beneficial in the context in which we operate.
3. Proposed System

We presume that the sharing of streaming data among any pair of participants, e.g. a data provider P and a customer C, is facilitated by any infrastructure transaction-agnostic broker such as the one shown in figure, following normal IOT data streaming practices. The stream is divided into discreet message batches in this data transfer model. The providers mark their messages with topics that define the stream of the provider. A customer is permitted under the terms laid down in a trade agreement, as set out below to subscribe to an issue.

In our previous work [7], we first presumed that the broker was a trustworthy part of a network infrastructure for the construction of a true data exchange port to resolving disputes between producers and consumers (the "Cubs" in Fig. 1). In such a case, the intelligent contract will actually solve these reports. In the same article, we proposed a more confident model, in which each person has the role of reporting. The Smart contract is brought into doubt in this case because the report cannot be counted upon and contradictions cannot be settled by attaching a certain responsibility to one group.

We focus on these issues and we do not need the broker or the participant to create a paper. The broker is just a network feature instead. The marketplace has a double focus. Firstly, the exchanging of streaming data through the broker with assurances on the max damages suffered in the event of adverse behavior. Second, disagreements over the sharing of data should be settled. This means increasing the exchange of data between C and P, which takes place periodically and over the entire time the data stream. The exchange of data between C and P increases. These receipts are traded on the blockchain as part of transactions facilitated by an intelligent contract, denoted SC. At the time of the signing of the trade deal, the duration of the interval, defined as batch size or BS, is fixed. This parameter, as we can see, helps P to monitor the amount of risk to be allowed in C provided the minimal faith.

There are the following elements in the model:

a) The summary of a manufacturer's data;
b) A commercial treaty that contains the facts and procedures of trade to be shared, the market value corrective and additional requirements, such as BS described above;
c) A mechanism to share receipts, which in addition to a neutral smart contract, involves all parties;
d) A credibility model that permits the assigning at the conclusion of each transaction of a reputation score for each pair of participants P and C of participants. Reputational qualities may be used by participants to determine the likelihood of a nontrust individual coming into a contract.

![Figure2. Control flow model](image)

In this paper, we concentrate primarily on the following information. With respect to (4), we can conclude that a credibility model has been placed in place and that every person has a current ranking, regardless of how it performs. Our ongoing analysis is structured to achieve a personalized credibility model and is outside the paper's reach. However there are suggestions for how such a paradigm can be done, see eg. [17].

Each smart contract shall be kept accountable for each (1-3) transaction, in particular for data collection I, (ii) the sharing agreement and (iii) each data reception. Until a trade agreement is in place, C is able to subscribe to P's stream. When the arrangement has been concluded and personally
identifying information is distributed as negotiated, SC shall be informed at TATI Interval C upon termination of the agreement and SC shall have to pay in accordance with the agreement.

However, suppose that C does not alert SC. This could be due to C's inability to actually obtain such data or to its assertion that it has not obtained the data fraudulently. We presume in our model that SC cannot differentiate between these two events, because the data broker does not have to maintain a (verifyably true) record of the transmission of his letter. The only course of action that SC should take in this case is to trust C's argument and therefore refrain from paying P. Therefore, P will be the perpetrator of C's fraud if the broker has limited liability and the participants have no confidence.

For the entire data transmission cycle, checkpoints, both control points are the batch size BS which P will configure in the negotiations with C as part of the agreement. C shall give SC a data receipt at each control unit as part of a transaction blockchain, which will identify that a single batch of data from P is obtained. SC then reports the receipt and alerts P. when the transaction is validated. By the time each batch P stops, its streaming to C has been suspended until it receives SC acceptance. If P doesn't receive a response within a certain time period, the trade deal will be closed and terminated to mitigate damages (in fact, C's Stream subscription will be cancelled). As seen in the Figure 2, data exchange protocols and protocols for receipt data are thus related.

4. Results and Discussions

Our test bed consists of a series of intelligent market and financial arbitration arrangements, distributed over a private test network in Ethereum. In order to write, deploy and connect to the private chain via Remote Product or Calls we have used the Ethereum IDE Remix web (remix.ethereum.org). We used counterfeit accounts with Remix balances as participants in the company.

The costs for each step of the P C relationship by SC are calculated experimentally here. In order to note that the SC and thus gas charges are involved in registering new members, making new deals and establishing a new exchange accordingly. C provides a deposit TP on ETM, as previously suggested, upon the completion of the deal. We calculate RC costs due to the protocol for reception of data, which is significant. For each transaction we've been able to test the gas usage with Remix debugger.

This can also be done by tracking participants' balance sheets and testing discrepancies before and after invoking the intelligent contract process. The rise in some lots obtained would result in the incurrence of more gas for the user. If we believe that a producer would not have a motive to not transmit data as agreed under this arrangement, a trader is not permitted to send receipts or to disclose the exact number of messages sent. If, the receiver is not accurate then the protocol on reception of data is intended to make the market viable by allowing parties to improve their credibility. Since the GUP unit price decides the most relevant the user has a choice of raising the GUP to handle their transactions more rapidly, and thus will have a more timer out of the total TATI to obtain more batches, during transactions in a blockchain to validate by the miners.

In order to understand SC transactions with higher GUP priority in the Ethereum cost and POW model, the miners who verify the transactions are usually searching for transactions with higher GUPs at the next step. The raising of the GUP leads to the reduction of the RT and therewith the interval of the TATI is expanded by the ATM (current total messages) (ethgasstation.info). This is a guide for recognizing the new developments on the gas sector and the existing strategies of network miners. Given the present network condition, petrol prices are recommended from the gas station[18].

5. Conclusion

In the present paper we have suggested a competitive market for the exchange of IoT data with participants' assumptions of minimal confidence. In an attempt to achieve non-Reputability and openness, intelligent contracts on the public Ethereum network are used to mediate all communications between data producers and users. The model distinguishes the exchange from the regu-large control point transfers, and is backed up by message broker's off-blockchain. The model specifically sets the balance between data failure risk, costs, and overall numbers of messages and
allows members, based on their existing credibility, to negotiate equilibrium. We showed experimentally that if it is possible to get a credibility ranking, i.e. from a third-country service which now goes beyond this paper, it is easy to measure trade offset and control the trade risk.

This thesis is still ongoing and seeks to include a personalized model of credibility in which reputation changes rapidly in the history of previous trades on the market. We also want to illustrate that the marketplace supports honest behavior, i.e. members are motivated to improve their credibility in time and (ii) commercially feasible due to exchange costs. We still work on the business scalability with the increase of the amount of participants in the blockchains and how the reputational model is built to ensure less time for players with higher credibility.

References
1. Bejder, E., Mathiasen, A. K., De Donno, M., Dragni, N. & Fafoutis, X., (2020). SHAKE: Mutual Key to Resource-contracted IoT Devices Acceleration. In 2020 IEEE 6th World Forum on Internet of Things.
2. Georgakopoulos, D. (2019, December). Discovery and incorporation of a multinational IoT device. In 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC) (pp. 214-221). IEEE.
3. Lu, D., Han, R., Shen, Y., Dong, X., Ma, J., Du, X. and Guizani, M., (2020). Smart IoT-eHealth Devices: Trustful network sharing scheme xTSeH. IEEE Journal on Selected Areas in Communications.
4. Dawod, A., Georgakopoulos, D., Jayaraman, P. P. & Nirmalathas, A., (2020, November). A service for the exploration, deployment and (re)use of global IoT products. In 2020 IEEE International Conference on Services Computing (SCC), pp. 312-320. IEEE.
5. Refat, R. I., Hannan, M. A. & Hashem, M. M. A. (2020, June). A Secure IoT Data and Sharing Platform on the Blockchain Permits. In 2020 IEEE Region 10 Symposium (TENSYMP), pp. 1312-1316. IEEE.
6. Ayyasamy, S., Eswaran, S., Manikandan, B., Solomon, S. M. & Kumar, S. N., (2020, March). Agri Soil Maintenance based on IoT by means of micro nutrients and crop protection from excess water. In 2020, Fourth International Conference on Computing Methodologies and Communication (ICCMC) pp. 404-409. IEEE.
7. Bonafini, F., Rinaldi, S., Depari, A., Flammini, A., Ferrari, P. & Sisinni, E. (2019, March). Smart Cities IoT Sensor Cluster: effects on computer efficiency of the connectivity infrastructure. In 2019 IEEE Sensors Applications Symposium (SAS), pp. 1-6. IEEE.
8. Bashir, M. R., Gill, A. Q., Beydoun, G., & Mccusker, B. (2020). IoT-enabled intelligent buildings big data management and research metamodel. IEEE Access, 8, pp. 169740-169758.
9. Narayanan, R., Kumar, S. & Murthy, S. R., (2020). MIMO transmited for low power IoT through Cross Technology. IEEE Transactions on Mobile Computing.
10. Li, X., Xiao, R., Pan, M., Jiang, F., Zhao, N. & Wang, X. (2020). Green Traffic Off- Loading over unknown traditional spectrums with a QoS promise End-to-end. IEEE Transactions on Vehicular Technology, 69(9), pp. 9921-9937.
11. Xu, W. and Peng, Y. (2018, September). SharaBLE: A Collaborative Internet BLE Use Program System. In 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) (pp. 381-385). IEEE.
12. Suresh, G. M. & Madhavu, M. L., (2020, July). AI-based intrusion detection system using a software-defined IoT network BAT algorithm. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
13. Bansal, B. & Sharma, M. (2019, June). Offline IoT Architecture Client-Side Verification Platform. In 2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 1044-1050. IEEE.
14. Gupta, B. B. & Narayan, S., (2019, July). Stable Internet of Things platform (IoTs) frameworks focused on card emulation technology. In *2019 International Conference on Communication and Electronics Systems (ICCES)* (pp. 1304-1309). IE.

15. Lardier, W., Varo, Q. and Yan, J., (2020, June). Smart IoT interface dynamic decreased round encryption for energy-efficient wireless communication. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-7). IE.

16. Anand, M. S., M. Balamurugan, R. Shubathra, M. Ragavi, & Priya, R. B. L. (2018). Sugar Level Detection Using Thermal Images. *International Journal of Engineering & Technology* 7(4.39), 637-639.

17. Rubavathy, S. Jaanaa, & P. Murugesan. Experimental investigations on multi-output cyclo-inverter-fed induction heater system. *Australian Journal of Electrical and Electronics Engineering,* 10(4), 2013, 483-489.

18. Nanthini, T., Geetha, M. K., & Arunnehru, J. Occlusion Handling Based on Fractal Texture Analysis in Surveillance Video using Neural Network Classifier.