Inducing Trust in Blockchain-enabled IoT Marketplaces Through Reputation and Dispute Resolution

Panagiotis Michalopoulos, Srisht Fateh Singh and Andreas Veneris
The Edward S. Rogers Sr. Department of Electrical & Computer Engineering
University of Toronto, Toronto, Canada
{*p.michalopoulos, srishtfateh.singh*}*@mail.utoronto.ca, veneris@eecg.toronto.edu*

***Abstract*—In order for the metaverse to achieve its full potential, access to data from the physical world is required. The Internet of Things can be such a provider of data, but a widely adopted marketplace to enable monetization and trade between interested parties does not yet exist. One of the reasons is the level of trust between the participants regarding the integrity of the exchanged data. In this paper, a reputation system is proposed that aims to alleviate this problem by providing a mechanism to ensure the validity of the traded data. Under this system, every seller is assigned a score, which buyers can use later to make informed decisions while ensuring it is economically disadvantageous for illicit actors to manipulate the scores. A dispute resolution scheme is also presented that acts as a fail-safe mechanism to further establish trust in this system, along with a proof-of-concept prototype of the proposed reputation system. Empirical results in this paper show the feasibility of the proposed system and provide insight in its behaviour with respect to its parameters.**

***Index Terms*—blockchain, IoT, reputation, trust, data, marketplace, dispute resolution**

1. Introduction

The metaverse envisions a new virtual world in which the existing physical world and its social structures are incorporated through the use of technologies, such as Augmented/Virtual Reality and digital twins. It promises to enable next generation applications impacting many aspects of people's lives, such as social interactions and commerce [1], [2]. A critical prerequisite of this vision is the ability of the metaverse to acquire a wide variety of real-world data, ranging from a user's physical attributes to traffic conditions and weather information [1], [2].

One of the possible streams for data acquisition, which we consider in this paper is the Internet of Things (IoT). IoT has seen, in recent years, an increased adoption [3] leading to the production of a vast amount of data: the International Data Corporation estimates for 55.7 billion connected IoT devices by 2025 that will be generating almost 80 billion zettabytes of data [4]. As such, an IoT data marketplace is needed in order to provide appropriate economic incentives for sharing all these data with applications in the metaverse. However, among others, designing such a marketplace faces two crucial challenges caused by the lack of *trust* between the participants in the market regarding (i) the fulfillment of the payment by the buyer and (ii) the integrity of the data being offered by the seller.

These challenges can be addressed using blockchain technology, which enables payments over the web, while its smart contract functionality can enable programmable reputation and trust. Most of the existing blockchain-based IoT marketplace designs [5]–[8] address the first challenge by focusing on implementing payment channels that specify how the payment and the data transfer should be done. However, the second challenge of ensuring seller integrity for their data remains largely unaddressed. In particular, and to the best of our knowledge, prior art that touches upon it [9]–[11], does it as a by-product of the core premise behind their work without providing an extensive analysis or evaluation of the underlying proposals.

In contrast, the primary goal of this paper is to induce trust in blockchain-based data marketplaces by focusing on data integrity. To achieve this we adopt a component-based view of IoT marketplaces, in line with the analysis found in [11]. As such, we introduce *reputation* and *dispute resolution* components that complement the underlying payment system, which is not the focus of this work. The first component establishes a reputation system in which sellers accrue a reputation score through their interactions with buyers, which the latter can use to make informed choices by choosing sellers with a reputation above a specific threshold. The second component provides a dispute resolution mechanism and serves as a *fail-safe* mechanism when the reputation system is unsuccessful in preventing a seller from not honoring their agreement with the buyer (*e.g.,* by sending faulty data).

Our proposed design adopts a blockchain-based approach that leverages the accountability, security, and transparency of the blockchain. At the same time, it eliminates the need for a trusted party and any single point(s) of failure present in traditional centralized marketplaces.

In summary, the contributions of this work are:

- A reputation system based on the trading volume of a seller to assist buyers in selecting the most suitable seller, capable of resisting ballot stuffing and badmouthing attacks. The proposed system has minimal requirements and it can extend an existing IoT marketplace as long as it provides public access to the trading volume of each seller.
- A dispute fail-safe resolution mechanism when the reputation cannot fulfil its purpose. This mechanism leverages decentralized oracles to ensure the fair reimbursement of the participants.
- A proof-of-concept implementation of the reputation system in the form of a reputation aggregator smart contract that buyers can query in order to find the seller with the higher reputation.
- An evaluation of the reputation system through simulation and experiments to profile the aggregator contract with respect to its associated costs.

The rest of the paper is organized as follows: Section 2 presents the related work in the field. Section 3 presents the proposed reputation system and its mathematical formulation. Section 4 describes the proposed dispute resolution mechanism and Section 5 discusses the implementation details of the reputation aggregation contract. Section 6 describes our evaluation procedure and the obtained results and Section 7 concludes the paper.

2. Background

2.1. Related Work

Existing literature examines both *centralized* and blockchain-based *decentralized* solutions to IoT data trading. These works can be further divided into those that consider the reputation aspect in their design and those that do not. With respect to centralized marketplaces, solutions like [12]–[14] provide a wide array of services, such as brokerage and payment settlement by leveraging centralized Software-as-a-Service architectures.

Out of these, [12] includes the provision for a data quality service in their design, but leaves its implementation as future work. In [13], the basic requirements and design for a reputation and trust component are laid out (*e.g.,* input types, sources of trust), without a specific instantiation.

In contrast, designs proposed in [5]–[11], [15] adopt a decentralized approach, where no central entity controls the platform offering increased transparency and accountability. Proposals in [5]–[7], [11] deal with the mechanics of data transfer and payment execution to ensure a fair settlement.

On the other hand, the authors in [15] present a data trading system for the MQTT protocol, that includes a reputation component for which the mathematical formulation is presented. However, the throughput of the system is limited as the blockchain is used for the on-chain storage of the data. In [9] the authors use a reputation system by modifying the one proposed in [16], but without providing further analysis. Finally, in [10] the authors propose a payment mechanism, which they enhance through a dispute resolution mechanism, for which they propose an initial design. In contrast, in this paper we provide an extensive analysis of the reputation system accompanied by simulation results and a feasibility study. Further, our system is not limited by an underlying architecture and it is capable of interfacing with various payment mechanisms. With respect to dispute resolution we provide a detailed proposal.

Reputation systems in the literature are not only limited to data marketplaces, but cover a wide array of applications, such as Vehicular Networks [17] and securing communication between IoT devices [18]. The key difference between these systems and our proposal is that the latter was specifically designed to build upon and take advantage of existing payment solutions for IoT marketplaces, such as the one described in the next section.

2.2. Underlying Payment Channel Protocol

This paper designs a reputation and dispute resolution mechanism on top of the payment channel proposed in [7]. The authors propose a data trading system that enables a seller and a buyer to exchange data off-chain in batches, while they use the blockchain as a trusted intermediary tasked with keeping track of the payments. In particular, every pair of seller and buyer uses a separate smart contract that functions as an escrow and verifies the different stages of the payment process. To achieve this, it uses various counters, such as the amount of data transmitted and the cumulative payment received by the seller. Following is a detailed explanation of the protocol.

1) The buyer deposits d worth of money in the contract.
2) The seller sends an ε amount of data.
3) Upon receipt of the data, the buyer denotes their approval by creating and sending a receipt to the seller
4) The seller can now send another batch ε of data beginning a new cycle and withdraw the payment at any time by submitting the most recent receipt.

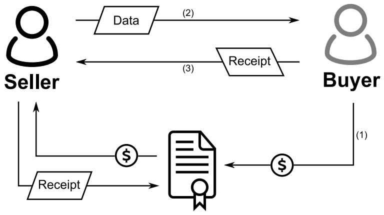


Figure 1. The basic procedures of the payment channel

Figure 1 presents a diagram of the aforementioned procedure. The bottom half depicts the on-chain transactions, while the top, the off-chain transactions.

3. Reputation

Given the large number of stakeholders involved in a marketplace, it is important to ensure that they behave honestly. To this end, a common solution is the employment of a *reputation system* [9], [15], which rewards participants when they follow a set of predefined rules and punishes them otherwise. Following, we propose such a system, by presenting its properties, its mathematical formulation, and an analysis of its parameters.

3.1. Mechanism Objectives & Notation

The aim of the reputation system is to provide data buyers with a means to estimate the integrity of the data they will receive and to select the most appropriate seller to buy from. To achieve this the reputation system should exhibit the following properties:

- *Badmouthing resistance:* a seller should not be able to tamper with the reputation of its competitors by maliciously giving negative reviews.
- *Ballot stuffing resistance:* as a seller's trading volume increases and they assume a dominant role in the market, it should be increasingly difficult to artificially inflate their reputation (*e.g.,* by buying from themselves).
- A *reputation recovery mechanism* should be available to sellers so they can recuperate from reputation losses and avoid permanent exclusion from the market (*i.e.,* no buyer is buying from them). This is important as low reputation is not always a sign of malicious behaviour.
- New sellers in the market with low trading volume are able to eventually obtain a high reputation and they are not obstructed by established sellers.
- Buyers are free to set their own acceptance thresholds and make a trade-off between data quality and the chance for lower prices.

Following is the notation used throughout this paper. Let $\mathcal{M} = (\mathcal{S}, \mathcal{B}, \mathcal{P}, \mathcal{SC})$ be an IoT data marketplace, where *sellers* $s_i \in \mathcal{S}$ can make their data available to *buyers* $b_j \in \mathcal{B}$ through various ad-hoc blockchain-based *payment channels* $p_{i,j} \in \mathcal{P}$, between seller s_i and buyer b_j. Every $p_{i,j}$ is implemented through a *smart contract* $sc_{i,j} \in \mathcal{SC}$ that follows the design of [7].

3.2. Badmouthing Resistance

To achieve resistance to badmouthing we take advantage of the *trading volume* $v_{i,j}$ of each $p_{i,j}$ of a seller following the assumption that it reflects the acceptance of their data by the buyers. In other words, data from a seller with high trading volumes can be trusted to be more accurate and useful and vice versa. Therefore, high volumes represent positive evaluations and low ones negative. Further, to better capture the association between trading volume and seller reliability, only the trading volume of the last w days is taken into account by the reputation calculation process, so as to not penalize previous sub-optimal behaviour or not allow sellers to compensate for future sub-optimal behaviour with their historical performance.

Formally, let $v_{i,j,d}$ be the trading volume of $p_{i,j}$ at the end of day d. Then after day $d = D$, we will have:

$$v_{i,j}[D] = \frac{1}{w} \sum_{D-w+1}^{D} v_{i,j,d}$$

Using the trading volume, which is part of the state of the system, eliminates the need for a separate evaluation process by the buyers (*i.e.,* rating). This reduces the complexity of the system and, more importantly, makes malicious negative evaluations (badmouthing) impossible, since only a decline in the trading volume can signify this.

3.3. Ballot Stuffing Resistance

To achieve resistance against ballot stuffing, the reputation is derived in such a way that it is economically expensive, and therefore inefficient, for a malicious seller with a high trading volume (and by extension high reputation) to manipulate it. In more detail, $v_{i,j}$ is bounded by a sigmoid function $f(x)$, which means that further gains in the trading volume of a high reputation seller (*i.e.,* the volume is on the concave part of $f(x)$) will result only in a small increase in reputation. As such, the seller is forced to spend an amount of money that is comparable to their current trading volume should they wish to increase their reputation. At the same time new sellers that enter the market are not limited and are allowed to acquire an initial reputation with low volume.

Let $V_{i,j}[D]$ be the bounded trading volume of $p_{i,j}$:

$$V_{i,j}[D] = f\left(v_{i,j}[D]\right)$$

where $f(x)$ is the logistic function. Quantity $V_{i,j}[D]$ can also be thought of as the reputation of a single channel. Then the reputation r_i of s_i after day D across all of their payment channels is:

$$r_i[D] = \sum_j V_{i,j}[D] \tag{1}$$

A buyer, on the other hand, can set their own personalized threshold τ_j above which they consider a certain seller as providing reliable data. Therefore, more flexibility is introduced in the market allowing buyers to trade data quality (by reducing their threshold) for cost, as low-reputation sellers can sell their data at a lower price.

3.4. System Parametrization

An important aspect of the proposed reputation system is the parameters that govern its behaviour (*e.g.,* the rate of increase of the reputation). These are the minimum r_{min} value of the reputation, its respective trading volume $x_{r_{min}}$, and $x_{0.5}$. By fixing $x_{r_{min}} = 0$ and $r_{min} = 0$, we determine the initial conditions for any new seller.

The point $x_{0.5}$ is set to reflect the point where $\dfrac{d^2 f}{dx^2} = 0$ and denotes the trading volume for which $V_{i,j}[D] = 0.5$. Changing this point controls the rate of growth of the reputation of a seller with respect to their trading volume. $x_{0.5}$ is therefore set to be the median of all $v_{i,j}$ in the marketplace. This requires a seller to exceed the median trading volume of the marketplace in order to reach a channel reputation of 0.5. Larger values for $x_{0.5}$ increase the difficulty of obtaining reputation in the marketplace, while smaller decrease it.

4. Dispute Resolution

The reputation system might not be always guaranteed to produce the desired results, especially when the market is still new and the reputation is in an early, transitory phase (*i.e.,* not enough evaluations have been gathered). For these cases, a fail-safe *dispute resolution* mechanism is proposed that will resolve potential disputes arising from bad quality data produced either maliciously or due to sensor malfunction. The basic requirements for such a mechanism are: (i) *dispute detection*, a way to securely verify that an event of fraud happened and (ii) *reimbursement distribution*, a way to fairly collect and distribute funds for the reimbursement.

For the first, a distributed oracle, as presented in [19] is used to detect and verify the occurrence of a dispute. The common element in these oracle designs is the existence of two groups of people: *submitters* SB and *voters* V. The former can submit a question q_i, accompanied by a bounty B_i, to a list of questions Q. This list is considered and voted on by the voters. In our case, a submitter is a buyer b_j with the question q_i asking whether the disputed data is faulty, and hence of no use to them. Voters, on the other hand, stake an amount of money on whether q_i is true or false. The largest stake determines the outcome of q_i and the respective voters are rewarded a fraction of the bounty B_i while the rest are penalized.

Regarding the collection and distribution of the reimbursement there are two possible sources for the funds. Either a small percentage of the fees from every $p_{i,j}$ goes to a central pool from which reimbursements are payed or a part of the offending seller's trading volume is given to the buyer provided that the seller has not yet retrieved their money. To this end, $p_{i,j}$ can incorporate an asset freezing mechanism, whereby withdrawals from the channel are halted, but the data transfer is allowed to continue.

5. Implementation

To demonstrate our reputation system and verify its feasibility we implement a proof-of-concept *reputation aggregator* in the form of a smart contract, along with a helper *seller contract*. The aggregator computes the reputation of sellers based on their trading volumes across all of their payment channels. The seller contract keeps track of all the channels of a seller and produces their median trading volume. We write both software modules in the Solidity[1] language. To compute mathematical exponents and logarithms we use the Solidity ABDK[2] Library.

The aggregator contract maintains one dynamic array of ranked reputations, in which the first element has the highest reputation and the last one, the lowest. It also maintains one dynamic array with the median volume of each seller. Lastly, it has one mapping from addresses to indices, so the positions of a seller in the reputations and medians arrays can be found efficiently. All of them are initialized empty.

The contract's public functions are `registerSeller`, `updateReputation` and `query`. The first one is called once by any seller willing to be listed. It informs the aggregator of the seller's median volume and initializes the seller's reputation to r_{min}. In order to update the dynamic

[1] https://docs.soliditylang.org/en/latest/
[2] https://github.com/abdk-consulting/abdk-libraries-solidity

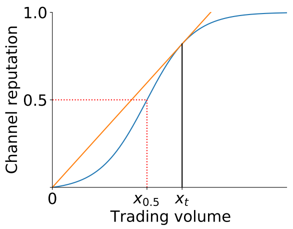


Figure 2. The main quantities involved in manipulation resistance

arrays of the aggregator contract, first it is determined whether the element (*i.e.,* reputation or median volume) needs to move up or down in the rank. Then, it is iteratively swapped with its neighbours until it reaches its new location.

The second function is called periodically by the seller contract in order to update the seller's median volume. The aggregator will use it to approximate the median trading volume of the entire market in order to compute the value of $x_{0.5}$ and recalculate $f(x)$ before updating the reputation.

The `query` function of the contract is called by interested buyers and will return the addresses of the sellers that have a higher reputation than the buyers threshold. Then the buyer can choose one to establish a new payment channel.

The seller contract has a similar structure to the aggregator contract and exposes the `registerChannel` and `updateVolume` public functions. The first registers the various channels of the seller, while the second is called by $p_{i,j}$ every time a receipt is submitted by the seller and notifies the aggregator of the seller's new median volume.

6. Evaluation

6.1. Theoretical Evaluation

We demonstrate how the design of the system makes it difficult for an attacker to manipulate their reputation by buying from themselves in order to increase their trading volume – and by extension, their reputation. We assume a rational attacker who adopts an optimal strategy that allows them to achieve the maximum reputation gains with respect to the capital they use. We propose the following lemma:

Lemma 6.1. *An increase in the median trading volume of the marketplace will cause an increase in the lower bound of the capital needed to execute the attacker's optimal strategy.*

Proof. To prove this we will argue in terms of a single channel, as once an attacker achieves an optimal strategy, they can replicate it across multiple channels.

Based on the construction of the system to execute an optimal strategy an attacker has to provide x_t amount of capital, where x_t is the x coordinate of the intersection of $f(x)$ and its tangent crossing $(0, 0)$ as depicted in Figure 2. x_t is optimal because this point gives the maximum possible reputation per unit of capital spent. In parallel, the attack capital is always bounded from below by the median volume *i.e.,* $x_t \geq x_{0.5}$. Therefore, as the marketplace experiences higher trading volume, the median volume increases. This increases the lower bound on x_t. Therefore, a more established market incurs a higher cost for reputation manipulation. □

6.2. Empirical Results

We compute the evolution of the reputation of a single seller over time to investigate the influence of w on the rate with which a significant decline in data quality after a time instant t_0 will get reflected in the reputation. To achieve this we simulate one seller with k buyers. Each buyer will buy data worth a different amount of money at regular intervals selected uniformly. Further, every buyer has a *tolerance* level, which decreases with every low quality data batch received. When their tolerance is depleted, the buyer stops transacting with the seller.

TABLE 1. CONTRACT DEPLOYMENT & INVOCATION GAS CONSUMPTION

Contract	Gas	Ether	USD
Aggregator deployment	1879681	0.069548197	113.12
Seller deployment	1100691	0.040725567	66.24
Aggregator:register (10)	154832	0.005728784	9.32
Aggregator:update (10)	306142	0.011327254	18.42
Seller:register (10)	178686	0.006611382	10.75
Seller:update (10)	99178	0.003669586	5.97

In Figure 3 we present the reputation of a seller with respect to time. We denote t_0 with a dotted red line. We observe that a smaller window provides more responsiveness to the system by achieving a faster convergence to zero. For the case where $w = 3$, the system needs 5 time units (when k=5), whereas for $w = 10$ and $w = 15$, it needs 7 time units. Regarding k, we see that as its value grows, the convergence point moves further to the right. This is especially prominent between $k = 5$ and $k = 10$, suggesting an an upper bound after a specific number of sellers is reached.

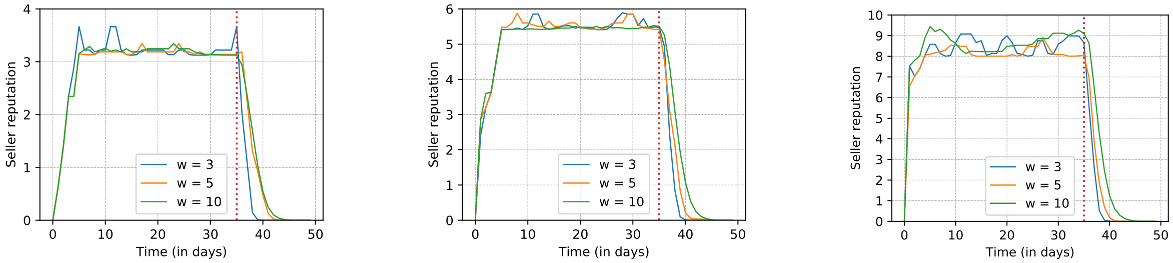
To study the feasibility of our solution we implement the reputation aggregator and seller contracts as described in Section 5 and we measure the gas consumption and cost of the `registerSeller`, `updateReputation`, `registerChannel`, and `updateVolume` functions. We also measure the deployment cost of the contracts.

In Figures 4a and 4b we present the gas consumption of the most important smart contract functions with respect to the number of sellers and channels already registered in the smart contract state. It should be noted that `updateReputation` and `updateVolume` cannot be invoked when no registered entities exist. As such, no measurements were obtained for 0 entities. We observe that the `register` functions present an almost linear increase in their consumption. A possible explanation could be that the reputation/volume of new sellers and channels is based only on one data point resulting in a temporary increase of their rank until w observations are obtained. Therefore, more swaps are required. Further investigation is needed for conclusive results. On the other hand, the cost of the more frequently called `update` functions remains more stable as the rank of a seller/channel does not change drastically between calls and swapping occurs only between immediate neighbours in the ranked list. Out of the two, `updateReputation` is more expensive, since it has to consider all the channels of a seller and performs more complex calculations for computing the reputation score.

Finally, in Table 1 we present the gas required by a selection of the functions in Figures 4a and 4b and by the deployment of the two contracts in terms of Ether and USD. Conversions were based on the average gas price over the last year and the price of one Ether as of February 6, 2023, namely 37 Gwei and $1,626.53 respectively.

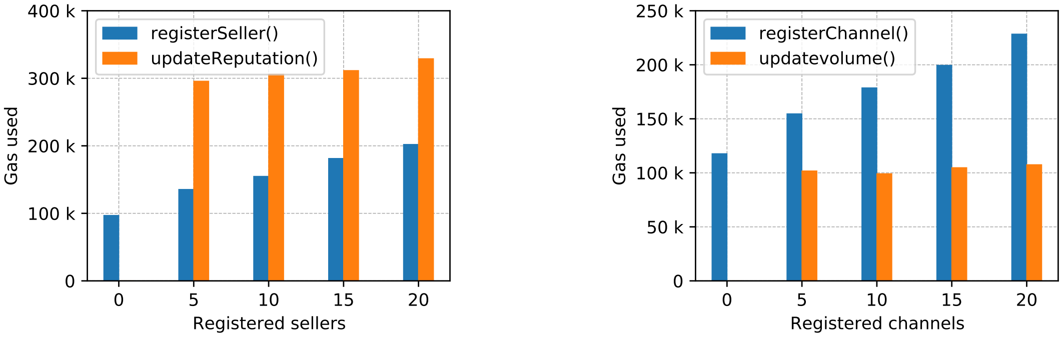
7. Conclusion

IoT data marketplaces can help the metaverse gain access to physical world data, but the lack of trust between a market's participants can lead to a reduced adoption. In this paper we present two possible mechanisms which can be used to induce trust in existing IoT data marketplace designs. We show how reputation can help the buyers in



(a) $k = 5$ (b) $k = 10$ (c) $k = 15$

Figure 3. r_i for different values of w and k



(a) Reputation aggregator contract (b) Seller contract

Figure 4. Contract gas usage

choosing good quality data and how a dispute resolution scheme can complement it as a fail-safe mechanism. We experimentally study the behaviour of the reputation system and demonstrate the feasibility of the proposed proof-of-concept implementation.

References

[1] R. D. Pietro and S. Cresci, “Metaverse: Security and privacy issues,” in *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, dec 2021.

[2] T. R. Gadekallu, T. Huynh-The, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. B. da Costa, and M. Liyanage, “Blockchain for the metaverse: A review,” 2022.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[4] IDC. (2021) Future of industry ecosystems: Shared data and insights. [Online]. Available: https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/

[5] S. Bajoudah, C. Dong, and P. Missier, “Toward a decentralized, trustless marketplace for brokered IoT data trading using blockchain,” in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, jul 2019.

[6] S. Delgado-Segura, C. Pérez-Solà, G. Navarro-Arribas, and J. Herrera-Joancomartí, “A fair protocol for data trading based on bitcoin transactions,” *Future Generation Computer Systems*, vol. 107, pp. 832–840, jun 2020.

[7] J. Meijers, G. D. Putra, G. Kotsialou, S. S. Kanhere, and A. Veneris, “Cost-effective blockchain-based IoT data marketplaces with a credit invariant,” in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, may 2021.

[8] R. Radhakrishnan, G. S. Ramachandran, and B. Krishnamachari, “SDPP: Streaming data payment protocol for data economy,” in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, may 2019.

[9] A. Dixit, A. Singh, Y. Rahulamathavan, and M. Rajarajan, “FAST DATA: A fair, secure and trusted decentralized IIoT data marketplace enabled by blockchain,” *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[10] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, “Mind my value,” in *Proceedings of the Seventh International Conference on the Internet of Things*. ACM, oct 2017.

[11] G. S. Ramachandran, R. Radhakrishnan, and B. Krishnamachari, “Towards a decentralized data marketplace for smart cities,” in *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, sep 2018.

[12] T.-D. Cao, T.-V. Pham, Q.-H. Vu, H.-L. Truong, D.-H. Le, and S. Dustdar, “MARSA: A marketplace for realtime human sensing data,” *ACM Transactions on Internet Technology*, vol. 16, no. 3, pp. 1–21, may 2016.

[13] B. Krishnamachari, J. Power, S. Cyrus, and S. H. Kim, “Iot marketplace: a data and API market for iot devices,” 2017. [Online]. Available: https://msbfile03.usc.edu/digitalmeasures/gerardpo/intellcont/USCIoTMarketplace_Jan152017-1.pdf

[14] K. Misura and M. Zagar, “Data marketplace for internet of things,” in *2016 International Conference on Smart Systems and Technologies (SST)*. IEEE, oct 2016.

[15] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, “Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems,” *IEEE Access*, vol. 6, pp. 12 295–12 303, 2018.

[16] L. Xiong and L. Liu, “PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 07, pp. 843–857, jul 2004.

[17] C. P. Fernandes, C. Montez, D. D. Adriano, A. Boukerche, and M. S. Wangham, “A blockchain-based reputation system for trusted VANET nodes,” *Ad Hoc Networks*, vol. 140, p. 103071, mar 2023.

[18] Z. Tu, H. Zhou, K. Li, H. Song, and Y. Yang, “A blockchain-based trust and reputation model with dynamic evaluation mechanism for IoT,” *Computer Networks*, vol. 218, p. 109404, dec 2022.

[19] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, “Astraea: A decentralized blockchain oracle,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, jul 2018.