Journal of
Sensor and Actuator Networks

MDPI

Review

Decentralized Blockchain-Based IoT Data Marketplaces

John Christidis [1], Panagiotis A. Karkazis [2,*], Pericles Papadopoulos [1] and Helen C. (Nelly) Leligou [3]

[1] Department of Electrical and Electronics Engineering, University of West Attica, 250 Thivon Av., 12244 Athens, Greece; mscres-64@uniwa.gr (J.C.); ppapadop@uniwa.gr (P.P.)
[2] Department of Computer Engineering and Computer Engineering, University of West Attica, Agiou Spyridonos Street, 12243 Athens, Greece
[3] Department of Industrial Design and Production Engineering, University of West Attica, 250 Thivon Av., 12244 Athens, Greece; e.leligkou@uniwa.gr
* Correspondence: p.karkazis@uniwa.gr

Abstract: In present times, the largest amount of data is being controlled in a centralized manner. However, as the data are in essence the fuel of any application and service, there is a need to make the data more findable and accessible. Another problem with the data being centralized is the limited storage as well as the uncertainty of their authenticity. In the Internet of Things (IoT) sector specifically, data are the key to develop the most powerful and reliable applications. For these reasons, there is a rise on works that present decentralized marketplaces for IoT data with many of them exploiting blockchain technology to offer security advantages. The main contribution of this work is to review the existing works on decentralized IoT data marketplaces and discuss important design aspects and options so as to guide (a) the prospective user to select the IoT data marketplace that matches their needs and (b) the potential designer of a new marketplace to make insightful decisions.

Keywords: blockchain; decentralized; IoT; marketplace; smart contract; real-time data; internet of things

Citation: Christidis, J.; Karkazis, P.A.; Papadopoulos, P.; Leligou, H.C. Decentralized Blockchain-Based IoT Data Marketplaces. *J. Sens. Actuator Netw.* **2022**, *11*, 39. https://doi.org/10.3390/jsan11030039

Academic Editor: Mingjun Xiao

Received: 16 June 2022
Accepted: 26 July 2022
Published: 29 July 2022

1. Introduction

The data collected by IoT devices play a major role in modern applications. There are many IoT devices deployed that impact plenty of application domains such as manufacturing, healthcare, smart cities, etc. [1]. All these collected data and the devices that generate them are not available for public access [2]. Establishing an IoT data marketplace where data owners could trade their data would unleash the potential of data exploitation to support multiple novel applications and enable revenue creation out of the collected data. The data owners could be either public or private organizations or even citizens that have deployed an IoT infrastructure. Important aspects to take into consideration include: (a) the age of information (which directly affects the value of the information), (b) the issue of "trust" between the data owner and the data consumer and (c) the quality/reliability of the data. In a data transaction, the consumer needs to trust the data owner that the data will be obtained successfully, and the data owner has to be sure he/she will be able to receive their payment. As of now, IoT data marketplaces [3] depend on a third party or middleman to mediate the exchange of the data. This further aggravates the issue of trust mentioned above as the third party could make profit from the data without permission. As a result, there is a need for a "trustless" ecosystem, meaning an ecosystem where trust would be built in a distributed way without any need for the involvement of a third party. This requires a level of secure automation, i.e., the implementation of deterministic processes that are secure by design.

Blockchain technology is a new technology that presents attractive characteristics, primarily data immutability and integrity, which can be exploited to satisfy the previously mentioned needs. In the blockchain approach, Smart Contracts (SC), which are scripts that

are safely stored in the Blockchain, can be used to remove middlemen by replacing them with blockchain validators [4]. Smart contracts are deterministic, which means that if any of the stakeholders do not keep their end of the deal, the transaction will not be committed. The "data" in a blockchain typically consist of transactions. In the case of a blockchain-enabled IoT data marketplace, the "data" that are stored in the blockchain can represent (a) the transaction that refers to data trading, e.g., trading of data sets, and/or (b) the data generated from the IoT devices. Blockchain technology, however, introduces new issues. Since it is transaction based, public blockchains require a fee, in digital cryptocurrency, for each transaction [5]. In the public Ethereum blockchain, for example, the costs are paid in ether for a user to make a transaction in the Ethereum blockchain [6]. Gas costs can amount several euros depending on the transaction's complexity and the current traffic of the network.

Considering the technical aspects of a decentralized IoT Data marketplace, storage of the IoT data is an issue. Thus, the first technical question is whether the IoT data are stored or whether the solutions do not address the data storage at all and instead consider real-time streaming of the IoT data. In the former case, where the solution also addresses the storage of IoT data, the next question to answer is where and how this storage should take place. One could consider storing the data on chain. Public blockchains such as Bitcoin and Ethereum are not able to satisfy the low latency needs of data storing in an IoT data marketplace since blockchains are transaction based and each transaction creates a block that has a limited size. This could result in a significant delay when trying to store the IoT data on a public blockchain. Additionally, while private blockchains can satisfy those needs, they are not fully decentralized. Hybrid or Consortium blockchains also suffer from the same problems, as the benefits of decentralization are not fully achieved with only a few nodes, and should the number of nodes increase significantly, this comes with significant increases in latency. Furthermore, as IoT-generated data increase rapidly with time, keeping the data on chain would challenge the scalability of the blockchain solutions. As a result, researchers considered storing the IoT data off chain, reducing the workload of the blockchain and instead use it for data monetization and for offering access control mechanisms and other services that could benefit from its decentralized and transparent nature, such as rating mechanisms. The next technical decision that needs to be answered is whether the IoT data are stored in a centralized or decentralized manner. In both cases, a hash or another index of the data can be stored in the blockchain. Centralized storage can be easily implemented by using the already existing storages of the data providers or by storing the data in a cloud. In these cases, data integrity becomes an issue since storage owners could alter the data stored, which could result in fraud, such as a trade of altered/invalid data with currency. To ensure the integrity of the data when they are stored in a centralized server outside the blockchain, data verification mechanisms should be employed. Furthermore, there could be some type of trust metric, reputation score or reward/punishment system evaluating the behavior of the actors. In case of implementing decentralized storage such as an IPFS (Interplanetary File System), the integrity of the data can be ensured. However, there could be data accessing issues since the IoT data can be visible. Encryption or other data security protection techniques can be employed in order to deny access to the IoT data from unauthorized users. Referring to the first question, there is the option of not storing the data and instead exchanging them in real time such as IoT data streams. A combination of utilizing storage and providing real-time data streams is also possible. The major technical aspects and the decision process to be followed is depicted in the following Figure 1.

To summarize, a decentralized IoT data marketplace needs to (a) remove the middleman through secure automation of the processes of an exchange of data and currency, (b) support data integrity, (c) support real time data handling and (d) support scalability. In the case of off-chain data storage, there is a need to establish a trust management process among the data owner. There is also a need to consider the cost efficiency for each exchange.

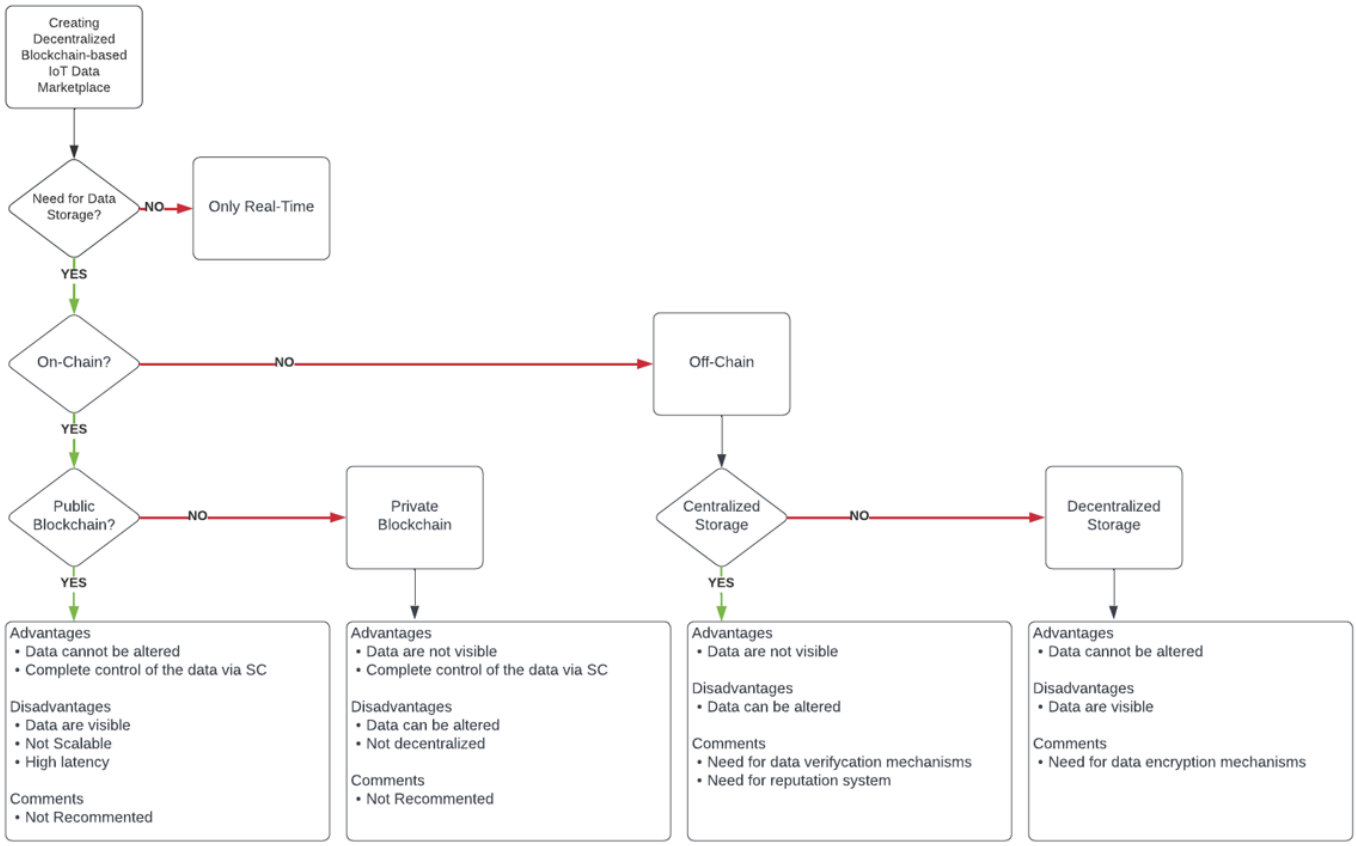

Figure 1. Schematic view of a systematic decision process for the design or selection of an IoT data marketplace solution.

This paper delivers a review of decentralized IoT data marketplaces, evaluating them on the factors mentioned above. The remainder of this paper is organized as follows. Section 2 overviews the works about decentralized data marketplaces using blockchain technology. Section 3 presents the comparison of the works based on the factors mentioned above. Section 4 details the final thoughts and concludes this work.

2. State of the Art

Blockchain-enabled IoT data marketplaces have emerged in the last four years (from 2018). The overview of those works is presented in this section.

2.1. Realization and Evaluation of Marketplace Functionalities Using Ethereum Blockchain

Lars Mikkelsen et al. proposed an architecture of an IoT Marketplace using smart contracts in an Ethereum-based blockchain [7]. They chose to focus on two functionalities of the marketplace, offering creation, which allows data providers to store descriptions of the data they want to offer and offering query, which can be used by consumers to search for data offerings. In their architecture, there are four elements: (a) consumer nodes that can interact with the blockchain by performing actions such as subscriptions or by making queries, (b) end-users of consumer nodes, which are called consumer clients, (c) provider nodes (which create offerings) and (d) provider clients, which can be used by consumer clients to access offerings. For a new offering to be added to the blockchain, a provider client must create a content offering, which is then received by the provider node and creates a transaction against the offering contract. Queries can be performed by consumers to find offerings that fulfill their requirements.

2.2. IDMoB: IoT Data Marketplace on Blockchain

Kazım Rıfat Özyılmaz et al. proposed IDMoB, (IoT Data Marketplace on Blockchain), which is a decentralized and trustless data marketplace [8]. In the marketplace, IoT device vendors and providers of artificial intelligence and machine learning AI/ML solutions are able to collaborate and interact. The data marketplace is deployed as a smart contract in the Ethereum blockchain while the data are stored in a decentralized storage called Swarm. The methods in the smart contacts are created with cost optimization in mind. In this work, there are two main roles: vendors or IoT Manufacturers and customers or AI/ML providers. Vendors are able to register in the application and then register their IoT devices. The devices can then upload data sets into the system from different sensor types. The customers are able to query and request data sets in order to retrieve the data payload. They also implemented an evaluation method in order to evaluate the vendors. The data from the devices are uploaded and stored encrypted in the Swarm. It is noted that the current version of the marketplace does not support real time data, and the data replication is not considered in their paper. They also considered payment channels in order to increase scalability of the marketplace, reducing the number of transactions stored in the blockchain.

2.3. BlendSM-DDM: BLockchain-ENabled Secure Microservices for Decentralized Data Marketplaces

Ronghua Xu, et al. in their work "BlendSM-DDM: BLockchain-ENabled Secure Microservices for Decentralized Data Marketplaces", proposed a microservices-based security mechanism within a permissioned blockchain network to secure data exchange among its participants [9]. It also secures payments of the data exchanges. The microservices are built in smart contracts, which are safely stored in the blockchain. This allows for the microservices to work cooperatively in order to perform tasks such as security enforcement and data analytical missions without decreasing the flexibility or the scalability of the services. The blockchain is managed by the decentralized data marketplace administrators creating a peer-to-peer network. The microservices, built in the smart contracts, are decentralized and expose REST APIs to accept service requests, and their gateway is handled by the administrator of the marketplace or the service providers. In order to access the network, the participants must first register and confirm their identity. Then, their information is broadcasted across the network. Participants can be validators or nodes. The only difference between them is that validators are also miners. The marketplace administrator maintains a global identity profile and authorization policies for the network management. In their proposal, they describe six microservices: the data pub/sub service, which handles the exchange and payment activities; the ID verification, which can be used by the marketplace administrator; the participants rating to evaluate the data provider used by their consumers; data integrity that is used for the confirmation of the data when purchased by consumers; access control which allows the data owners to control their data without third parties; and privacy policies for sensitive data management.

2.4. DMap: A Distributed Blockchain-Based Framework for Online Mapping in Smart City

Fatemeh Mohammadzadeh et al. introduced a blockchain-based platform for anonymous data sharing with data providers along with a marketplace. Their use case is a smart city where vehicles are interconnected with IoT [10]. The architecture consists of nodes that participate in the network, namely the smart vehicles, the city manager, the service providers (SP) and the roadside infrastructures (RSI). SP, RSI, and the city manager manage the blockchain while the smart vehicles connect with the blockchain through the RSI. This improves the scalability of the network. RSI are trusted parties in the blockchain. Vehicle owners are able to decide which data they want to share. To ensure anonymity, vehicles use fresh public key to generate new transactions. Every transaction contains the signature of the smart vehicle and the RSI. The nodes in the RSIs are used as data validators, as they must confirm the validity of the data by multiple sources before creating a new transaction

and store them to a cloud storage. The SPs are able to request data from all the vehicles in a specific area. The vehicles can share their data in real time or data that are already stored. If an SP makes a request, a storage space with all the data requested is created in the cloud storage that is named data directory. The data access control is managed by the blockchain. The connection between the blockchain and the cloud storage is handled by the "rule table" API. The rule table is responsible for confirming if the participants have permission to access the data they requested. For a participant to access the data, an agreement on a price must take place beforehand. For privacy, the identity of the vehicle or the owner of the vehicle cannot be tracked by their public key since it changes after each transaction.

2.5. Enabling on-Demand Decentralized IoT Collectability Marketplace Using Blockchain and Crowdsensing

Duc-Duy Nguyen et al. presented a model of a decentralized IoT data marketplace with operational factors [3]. Data providers can collect data on demand, which means that data collectability is a service where the owners of the devices are able to trade the right to use their sensing power for a specific period of time for a price. This also means that the data can be provided in real time. The marketplace has the following actors: the producer or the sensor that collects and transmits the data, the provider that collects data from producers, the consumer who receives the data and pays for them, the broker that facilitates intermediate transactions, and the operator that facilitates execution of data transactions in the market. The architecture consists of the sensors and their owners/operators layer (which is operated by the producers), the sensing providers layer (which includes the devices that manage, discover and collect data from the sensors, and they are responsible for publishing the collectability of sensors to the market), and the blockchain network and the collectability marketplace layer, which performs transactions and trading activities. While the blockchain is operated by its participants, the market is managed by the market operator and data and sensing consumer layer, which consists of the end users that must register and prove their purchasing power and their identity. If a consumer requests data, then there is a function that identifies providers with relevant data sources. After that, the consumer and the provider agree to a transaction, and a smart contract is deployed in the blockchain, signifying their agreement. Then, the provider can send the data to the consumer. In this work, a reputation system is proposed. However, adding a rewarding system (rewarding the good behavior of the participants) is considered as a future step. They mention that scalability is an issue as well as the authentication and verification of the devices. This approach is cost-effective for data consumers because of the collectability approach of the proposal.

2.6. Toward a Decentralized, Trustless Marketplace for Brokered IoT Data Trading Using Blockchain

Shaimaa Bajoudah et al. envisioned a decentralized IoT data marketplace that does not need any storage for the data while it is trustless and scalable [11]. They proposed the use of smart contracts in an Ethereum-based blockchain for the transactions between data providers and data consumers. The data providers are able to trade IoT data streams. They assumed that the exchange of data streams is handled by a broker infrastructure that is transaction agnostic, while the stream is divided in message batches with each batch having its own topic as a tag filled by the data provider. The consumer can then subscribe to a topic following the conditions set in an agreement with the provider. Smart contracts are used for recording the specification of the data offering published by the data providers, the trade agreement and data receipts of the exchange, which occurs during the duration of the data streams. However, there should be measures for dishonest behavior between the participants such as a reputation model, which is assumed to be in place by the authors. Their system has two layers: the data transfer layer, where the data from the IoT sensors is transferred off-chain to the consumers from the data producers as stated in the agreement in the smart contract, and the blockchain layer where all the smart contracts are stored. In order to participate, a user needs to register in the blockchain. They mention that scalability

will be an issue as long as more participants enter the network. They also considered transaction fees while trying to minimize the number of transactions per exchange.

2.7. Toward Secure and Decentralized Sharing of IoT Data

Hien Thi Thu Truong et al. proposed a framework named Sash that combines IoT platforms with blockchains with the latter used for storing access control policies and taking access control decisions [12]. They also devise a data marketplace by using the advantages provided by blockchain in financial transactions. In their approach, they use hyperledger fabric as their blockchain choice as well as FIWARE [13] as the IoT platform. Instead of public keys, they use prefix encryption, which is a flavor of identity-based encryption. In order to use it, they assume that the key distributor is a trusted authority. The blockchain comprises two entities: data owners, who store their data on a remote storage, and data consumers. Data owners have full control of their data and are able to set a price that consumers need to pay in order to have access to them. Before sharing the data, a transaction is created between data owner and consumer that records the payment of the data. The IoT data is stored off chain and the access control functionality is handled by an IoT broker, which is a centralized entity. Data owners can create offers around their IoT data, while consumers can request access to these data through the smart contract. The contracts also keep trading information between consumers and owners. There is also the storage provider entity, which is a blockchain node and is responsible for the access decision, allowing or denying access to the data. Storage provider is a centralized entity. However, it is possible that the functionality of the storage provider can be distributed among the nodes. The data are encrypted before uploading them to the storage provider. In the smart contract, there are methods for verifying the authenticity of the off-chain data.

2.8. An IoT-Owned Service for Global IoT Device Discovery, Integration and (Re)Use

Anas Dawod et al. proposed the Global IoT Device Discovery and Integration (GIDDI) service [14] in order to facilitate sharing and the reuse of IoT devices that already exist and are owned by different providers. They also state that GIDDY service is scalable and IoT-owned, as it is not owned by specific individuals and is beneficial for IoT providers. The service consists of the GIDDY Blockchain, which is designed for storing and querying the IoT devices' metadata and is the component that ensures that the service is IoT owned, and it is in the GIDDY marketplace. GIDDY ontology has also been proposed in order to provide the IoT devices' description. The GIDDY ontology's characteristics are ownership (used to describe the owner or owners of the device), ID, geo (the location attribute), the discovery-based integration (which contains information for integrating the device such URL, token, Certificate etc.) and the payment conditions, which is the attribute that describes payment options. The GIDDY blockchain, which stores the metadata using GIDDY ontology, prevents the manipulation of the data. Similar to most blockchains do, it has its own nodes and consists of blocks. It also has its own cryptocurrency called SensorCoins. The GIDDY blockchain also supports a device registration and payment service. This is the service that allows the IoT devices to be registered or be updated. The payment services records payments for utilizing the IoT devices, and the currency used for these transactions is the SensorCoins mentioned above. Finally, the GIDDY marketplace provides four services: the registration service, which is using GIDDY ontology to generate the metadata of the IoT device and then sends them to be stored in the blockchain; the query service, which allows IoT applications to search for appropriate IoT devices; the payment services, which create the payment transaction and send it to the blockchain; and the wrappers repository, which can be used for IoT applications to utilize the devices. GIDDY marketplace does not support smart contracts.

2.9. Blockchain Application in Remote Condition Monitoring

Rahma A Alzahrani et al. proposed a framework for the rail industry and considered the factors of scalability, security and decentralization [15]. In their work, they chose to store

data off chain and encrypted, while hash values are stored on chain as proof of ownership and integrity of the data. Sensitive data on chain are also encrypted. The Department for Transport is needed to authorize the participation as a node in the blockchain network. In their proposal, there are three actors: data providers, which could be any stakeholder that funds or operates sensors for remote condition monitoring (RCM) and they are able to create offers that, if accepted, the data are hashed and uploaded on the blockchain. Consumers can request for an offer listed in the network along within time in order to start a new payment process. Consumers could be stakeholders that need data. Smart contracts are the final actors and are used to monitor cost calculations, data delivery and payment processes. Upon new agreement between a data consumer and a provider, the ledgers will be updated with records of the agreement and for the data cost and compensation. A request from the consumer will be checked by the SC for its validity, and if it is valid, a payment process will start. At the end of a successful payment process, the agreement will be generated. The provider then encrypts and uploads the data to an external storage and only the consumer can decrypt them. Data corruption can be checked by the consumer. If the agreement ends, a new agreement must be made. For the payment process, the payments will be kept in the SC until the data have been received or the agreement is cancelled, ensuring no loss on either side. Penalties are also implemented in case of bad behavior.

2.10. Energy-Aware Demand Selection and Allocation for Real-Time IoT Data Trading

Pooja Gupta et al. proposed a trusted and transparent decentralized marketplace for contract compliance for real-time IoT data stream trading generated by battery-operated devices [16] in the Ethereum blockchain. The framework is divided in four layers. The physical layer contains the IoT devices. The off-chain layer performs activities such as battery monitoring of the devices, a demand selection component, the negotiation component that uses contract net protocol for the term negotiation between seller and buyer and the transmission and meeting component, which performs the transferring of the data while keeping track of the count of the data samples. In the blockchain layer, smart contracts are used for the functionalities of the marketplace. Data subscription and registration are used to provide an agreement framework between the actors. Each pair of actors deploys their own data subscription customized as they want. The pricing contract is used to evaluate the pricing of the data to keep the market dynamic and competitive. The rating contract is used for a reputation score for each actor in the market. Finally, the fourth layer is the application layer. There are three main actors, sellers (that post offers of their available resources of the IoT devices), buyers (that make queries for data and rate sellers) and facilitators (that must be a trusted party and oversee a specific service area). They are interconnected in a P2P network. Facilitators receive offerings and queries. They match buyers and sellers depending on their offerings and queries and send a list of possible buyers to the sellers. Then, the sellers send to the desirable buyer a negotiation process request along with data offerings. Finally, the stages of trading and agreement are performed in the smart contacts. The data transfer happens off chain. Before the exchange, the data are encrypted for data integrity. The authors did not consider reselling the data in their work.

2.11. Monetization Using Blockchains for IoT Data Marketplace

Wiem Badreddine et al. proposed a solution for publish/subscribe systems for IoT data marketplaces, which do not provide monetization logic and assume that brokers are trusted entities [17]. They proposed a system that uses distributed ledger technologies and smart contracts. The system along with smart contracts has the broker that handles the connection between the publishers, which are IoT devices and the subscribers or data consumers. Each of them possesses an address in the blockchain. Additionally, device owners are responsible for the devices registered and system manager who owns the smart contract and gives confirmation for the registration of the IoT devices. In their work, they defined a standard pricing in the smart contract based on the number of messages and the volume of data in each transaction. The cost depends on the traceability solution. There

are three solutions depending on the data shared: maximum traceability in which all the participants write detailed information in the blockchain; minimum traceability in which only the broker writes in the blockchain, which is also the cheapest option; and the Bloom Filter [18] option, which decreases the operations on the blockchain while bloom filters maintain data hashes. This also has the best performance among the three options.

2.12. SenShaMart: A Trusted IoT Marketplace for Sensor Sharing

Dimitrios Georgakopoulos et al. proposed Sen Sha Mart [19], which is a trusted IoT marketplace that permits different IoT applications to share sensor readings. They propose an extension of SSN ontology [20] to include metadata for IoT sensors such as ID, location, cost and integration information along with a query language to query these metadata. For the sensor integration, they assume that an IoT platform is already utilized and includes common sensor protocols. Scalability is enabled because it is only the metadata of the sensors that are stored in the blockchain. Shen Sha Mart consists of two blockchains: the provider and the client. They also propose an ontology that consists of sensor ownership, ID, location, endpoints and protocols for each sensor and payment conditions. Shen Sha Mart has the following services:

1. Registration service: this service allows the providers to register their devices using the ontology mentioned in the provider blockchain. This is further supported by the query mechanism they integrated.
2. Integration service: this service allows the selection and activation of sensors by utilizing the ontology's endpoints and protocols attribute. This happens in the client blockchain.
3. Payment Service: This service allows clients to pay the providers for using their sensors by utilizing payment transactions or by submitting payment to a transaction pool. This service is also in the client blockchain.

2.13. Toward a Blockchain Powered IoT Data Marketplace

Pooja Gupta et al. in their work [21] have proposed a three-tiered system architecture. In the first tier, data sellers and buyers as well as the devices of the sellers exist. The second tier consists of geographically distributed facilitators. These facilitators exist in the fog and not in the IoT devices, and they make use of decentralized database systems in order to achieve transparency of the data information. There is also the decentralized marketplace, which they named martchain. This handles the trade related operational transactions. The final tier consists of regulators and auditors. As blockchain is an immutable ledger, there is the issue of not saving privacy-sensitive data in it. Their approach is to create a consortium blockchain network and encode regulation policies in smart contracts. With their approach, only authorized buyers are able to process personal data as well as audit data activities related to cross-regional trades. Pooja Gupta et al. also proposed a two-step demand query mechanism in order to achieve a satisfaction level that will allow the marketplace to sustain through time. The process follows the pattern of matching the buyer's needs with the appropriate seller's metadata and then the seller with the appropriate buyer based on their device's resource availability and the buyer's quantitative demand. This is especially important because IoT devices have limited resource capabilities, which renders them unable to serve multiple consumers at the same time. The marketplace is implemented exploiting the use of smart contracts, which are responsible for the accurate execution of the functionality of the market. They created mechanisms of unauthorized reselling of data, data authenticity and cross exchanging of the data to other marketplaces. They migrated the marketplace contracts on the public Ethereum network, which incurs a specific cost per transaction. The developed smart contracts execute the functionality of data pricing, while every agreement between each different buyer and different seller creates a new smart contract, which makes the application customizable and scalable. In their work, they also employed a digital notary that serves as proof of authenticity in order to enable interoperability across other marketplaces while also being able to track for unauthorized reselling. For the determination of the reselling of data, they implemented a watermarking

technique. Martchain also provides mechanisms for user verification. This architecture automatically manages all the requests and matches between sellers and buyers. In order to keep track of the devices' location in real time (since they used a cluster sharding approach as well as the possibility of an IoT device to change location, which could result in efficiency issues), they developed a handling mechanism for temporary or permanent movement of the device between different areas.

2.14. Cost-Effective Blockchain-Based IoT Data Marketplaces with a Credit Invariant

James Meijers et al. and Andreas Veneris proposed [22] a blockchain-based data trading mechanism that allows the consumers to stay anonymous while data producers are able to sell IoT data streams while they receive their payment accurately. One of their main scopes is to reduce the number of on-chain transactions required for the trade. In their work, they assume (a) that the consumer is able to contact the seller and confirm the validity of the data, (b) that the buyer and the seller are able to keep track of the amount of data sent and (c) that the producer is able to stop the stream at any time. The system can be deployed on any blockchain as long as smart contracts are supported. As privacy is one of their goals, no information about agreement between consumer and producer is stored in the blockchain. The trading process is executed in three stages:

1. Trade setup: At this stage, the data producer deploys a mediator smart contract. The consumer makes an agreement with the data provider on price model for the maximum amount of data that they want to receive. The consumer also sets an amount of data that they will receive without returning a signed receipt to the provider. Then, the consumer sends some funds to the smart contract. Finally, the producer begins to send the data. At this point, the consumer can retrieve the funds but only after notifying the producer in order to receive the amount that they earned.
2. Trade process: At this stage, the producer sends data along with a receipt with the price of the data sent. The consumer may agree on the price and sign the receipt, which is then returned to the producer. With the receipt, the producer is able to retrieve the price mentioned on the receipt.
3. Trade completion: This process continues until any of the parties decides to end the transaction or the starting funds are equal to the amount received.

In this work, they also proposed a credit mechanism that can reduce fees up to 20%. The mechanism works as follows. The producer gives consumer a credit equal of an amount worth of data. The consumer is able to receive data from the producer up to the maximum amount they originally agreed upon plus the credit until the next payment. This results in less overall transactions for the consumer, but the producer risks losing the amount of credit worth of data if the consumer wishes to terminate the deal. In order to determine the best possible credit for each deal, they used a Bayesian model.

The stages mentioned above ensure that neither the consumer nor the data producer will be underprivileged, as the consumer will not pay an amount bigger than the equivalent of the data received and the producer may "lose" the amount of data that was placed in the first stage, which can be set to be small. Since no information other than payments and deposits are stored in the blockchain, there are no privacy issues. Finally, as the number of transactions made during the stages decreases, the total cost for the transaction fees does as well.

2.15. ITrade: A Blockchain-Based, Self-Sovereign, and Scalable Marketplace for IoT Data Streams

S. RafatiNiya et al. proposed in [23] the ITrade, which is a blockchain-based, self-sovereign, and scalable marketplace for IoT data streams. This is a secure and scalable decentralized IoT data marketplace that uses smart contracts for the management of data trading. The design of the proposed work presents the entities of data stream seller, data stream buyer and data stream principal, which is described as a generic entity that can act as seller or buyer. The sensors owned by the sellers have the attributes of type of sensor, status, geolocation, price per data entry and AES private key, which is stored locally by the

seller. The marketplace is a central entity, which has the attributes of owner, registration price for the buyers/sellers, sensor registration price and commission price. The data stream subscription to a data stream is an entity that has an ID (identifier) of the buyer, an ID of the sensor, a timestamp and the number of data entries for each buyer. In order to interact with ITrade, there is a registration process for the buyer/seller or sensor. In order to publish data from a sensor, a validation token is required, and the data are encrypted with the sensor's key. Buyers are capable of subscribing to a certain sensor in order to receive the streaming data, and the payments are managed through smart contracts. When subscribing, the buyer also receives a key to decrypt the data. The proposed work also achieves data sovereignty by the use of the encryption/decryption model. For their streaming system, they used Kafka, which is a distributed event streaming platform.

2.16. An Implementation of a Blockchain-Based Data Marketplace Using Geth

Paulo Valente Klaine et al. suggested [24] a blockchain-based data marketplace that trades data stored into the InterPlanetary File System (IPFS). They suggested a private blockchain, which is smart contract-compatible, and the smart contracts are used to record data information in the marketplace. Record transactions between buyers and sellers allow sellers to whitelist or blacklist buyer's access to the data. The proposed work describes eleven steps that are listed as follows: IoT sensor collects and uploads data to the IPFS; IPFS then returns a hash that acts as the data file's identity and is stored alongside other key information such as the owner of the data, timestamp, etc., in the blockchain; the contract then emits an event with the appropriate information in the blockchain; this information is considered as "topic" and is used for querying in the interface of the marketplace; the buyer is able to make a request by making a payable transaction to the blockchain, which also emits the appropriate event; after the seller receives the payment, he must allow the buyer to have access to the data; the buyer is then able to download the data only if they have permission. This work does not allow for real-time data transfer and, it is possible for the data seller to maliciously impede the buyer from accessing the data, even if they paid the appropriate price.

2.17. FAST DATA: A Fair, Secure and Trusted Decentralized IIoT Data Marketplace Enabled by Blockchain

Akanksha Dixit et al. proposed [25] a platform that ensures fair trading, data storage and delivery in a privacy-preserving manner as well as a trust metric system for the actors of the network. They used hyperledger fabric as the blockchain of their choice. Their model is based on the principle of data sovereignty. Their solution also supports actor's verification. The system actors are the data sellers, clients (which are the data buyers) and storage operators, which are a cluster of peer-to-peer nodes that host the data streams. The system makes use of two decentralized applications. The first one is the marketplace and the second is a security manager decentralized application. The suggested protocol is divided in three stages called phases:

1. Onboarding phase is the phase were the entities, either buyer or seller, create an account and verify their identities. The verification process uses a public and a private key in order to create the decentralized identity. If the decentralized identity and the account match, the actor is officially registered.
2. Data upload phase is the phase where the sellers generate IDs of the streams as well as verification keys for each stream. Then, the data are uploaded, and an identity token of the data is created, which is used by the seller to allow the client to interact securely with the storage layer. The verification is conducted through the security manager. The data are encrypted, and the keys along with the token are recorded in the blockchain.
3. In the last phase, which is the data purchase phase, the client is able to search and select a batch or stream of data and create a payable request. Then, the blockchain verifies that no restriction is placed from the data owner to the seller, and then, the

payment is received. After that, the data transfer is initiated. Then, through an authentication process of the security manager, the client receives the data and they are assured of their integrity.

As a result, Akanksha Dixit et al. stated that fair trade is achieved for the client, as the proposed protocol ensures the full value of the data and for the seller due to the smart contract's payment transactions that cannot be tampered. Storage operators are not able to maliciously use the data because they are encrypted and the operators do not have access to the decryption keys. The mentioned trusted metric system provides ratings and feedbacks of the previous transactions.

2.18. PDS2: A User-Centered Decentralized Marketplace for Privacy-Preserving Data Processing

Lodovico Giaretta et al. proposed [26] PDS2, an architecture of a trustless marketplace. The data processing is performed using encrypted computation techniques in order to achieve exclusive control of the data to their providers as well as exclusive access. The main actors of this work are sellers, buyers and infrastructure. The marketplace must fulfill the following requirements for each actor. Sellers must have full ownership of their data, data privacy and the benefit of receiving value when it is generated from their data. Buyers must have workload confidentiality as well as be sure of the data's authenticity. The platform roles are:

1. Data consumers that prepare and submit workload specifications to the platform. These are binding contracts that specify (a) the input data requirements to be fulfilled, (b) rewards that data providers will receive for submitting valid data, (c) the workload and (d) other conditions.
2. Data providers produce data through their devices, store it in a system and register it with the marketplace. Data providers are notified of the available workloads for which they have eligible data. They can then choose to submit part of their data to that workload.
3. The storage subsystem is responsible for storing the data of the appropriate provider. It matches data against available workloads and gives the executors access to them when authorized by the providers.
4. The executors provide the computational resources on which the workloads are run. Decentralized aggregation methods are used to synchronize the results of all executors participating in the same workload, so that the full output can be computed without sharing the input data.
5. The governance layer keeps track of the available data, the outstanding workloads, the mapping of executors to workloads and the mapping of data to providers and executors. The governance layer is also responsible for distributing rewards and verifying that no actor is behaving maliciously.

The workflow of the proposed work is as follows: the consumer is able to submit a workload to the governance layer and the storage subsystems of the providers verifies if the matching type of data are available. Providers can accept to participate in the workload by submitting their data to executors. They must confirm their participation as well as the executors to the governance layer. The governance layer keeps track of the contribution of all the providers that participate in the workload in order to reward them. Finally, the governance layer instructs the executors to compute the workload in a decentralized manner, and the results are submitted to the governance layer. The consumer is able to retrieve them. The blockchain of their choice is Ethereum, and for the privacy-preserving data processing, the technique of choice is the trusted execution environments. Finally, for decentralized machine learning, they considered federated learning and gossip learning. There are several challenges to overcome with their approach as they noted. The most notable is data authenticity as well as privacy leaks.

2.19. Secure Crowdsensed Data Trading Based on Blockchain

Baoyi An et al. proposed [27] the replacement of the broker with a smart contract stored in an Ethereum-based blockchain for a crowd-sensed data trading system. In order to participate, the users need to offer some ether. The main roles of the system are consumers and sellers. The consumers are able to start the trading of crowd-sensed data by making a transaction on the smart contract, which contains information about the job of data collection. The smart contract then emits an event to notify all registered sellers about the task and its requirements. Sellers are able to submit bids on tasks. The smart contract selects the sellers to conduct the tasks by a blockchain-based reverse auction and determines the payment. The consumer is then able to send the entire reward to the smart contract for safe keeping. Sellers upload the encrypted data to IDDS, which is a distributed data storage based on IPFS. An address is returned from IDDS and is stored in the smart contract. The consumer then receives the corresponding addresses from where they are able to download the data and decrypt using their private key. The consumer then evaluates sellers with a secure truth discovery and reliability rating mechanism powered by blockchain that protects the data from being revealed while determining the validity of the data and the rating scores. The sellers are then able to receive their payments from the smart contract.

2.20. A Decentralized Review System for Data Marketplaces

Anush et al. proposed in [28] a system that provides decentralized reviews and ratings for data marketplaces. The mechanism is deployed in smart contracts to ensure decentralization, transparency and immutability due to the nature of blockchains. In order for the process to begin, sellers provide their product (data) along with a fee and amount for staking. Then, a number of reviewers selected in a double-blind and random manner are given a time limit to review the product by providing an "accept" or "reject" decision. Depending on the majority's decision, the product will either be accepted or rejected, and the majority of the reviewers will receive a reward. The minority of the reviewers will not receive anything. In order to motivate the reviewers to perform a thorough review, pre-determined decision products can be injected randomly to reward the reviewers that answer correctly.

2.21. Fed-DDM: A Federated Ledgers Based Framework for Hierarchical Decentralized Data Marketplaces

Ronghua Xu and Yu Chen suggested in [29] a hierarchical network for their decentralized data marketplace that consists of a public federated network and multiple private and permissioned domain networks. Each intra-ledger domain (domain network) is based on byzantine fault tolerance and the inter-ledger (public ledger) on proof of work. The system is divided into two main parts: the blockchain-enabled microservices and the federated ledger fabric. The microservices have their own API, and each provide different functionality. In order to become a participant in the marketplace, the users must first register and use their blockchain address and ID. Brokers are full nodes that enforce operations in blockchain. The functionalities provided by the microservices are identity verification, rating system, access control and pub-sub payment system while also enforcing privacy policies and providing data integrity. The component of federated ledger fabric connects multiple domain networks within the inter-ledger. In the intra-ledgers, validators are chosen by domain administrators to collect transactions and commit to their private ledger. For the inter-ledger and in order to performed cross-domain operations, the domain networks rely on a set of specific miners to commit the transactions.

2.22. Differential Privacy-Based Double Auction for Data Market in Blockchain-Enhanced Internet of Things

Junhua Zhang et al. introduced [30] a framework that is powered by blockchain for IoT data marketplaces that use mechanisms to match data providers with data consumers and determine the prices for the transactions. They propose a double-auction normal

transaction method, and then, they upgrade it to be based on differential privacy in order to enhance privacy for buyers and sellers. For efficiency and data protection, they use a consortium blockchain with proof of work as consensus protocol. Their architecture consists of the layer of the IoT sensors that collect data and upload them to an edge server layer, and then, the edge servers refine the data and send them to the base station layer. The base station layer is connected to a cloud server. The blockchain is set up in these two layers and is used as storage of data commercials and the transactions. Smart contracts are used in order to define the rules of a trade and are designed to protect the privacy of participants. Finally, the trading platform is set up on the cloud server. Data buyers are able to submit their IoT data requirements in order to match with the appropriate sellers or base stations and directly implement the trading of the IoT data. Then, the blockchain validates the transaction data. In order to protect participant's bid information, the scheme of the data transaction is based on differential privacy considering the rationality of the individual, weak budget balance and truthfulness.

2.23. Toward a Data Marketplace Ecosystem Blueprint for a Community-Driven Data Marketplace

Sebastian Lawrenz et al. proposed [31] an ecosystem for data marketplaces that is controlled and owned by its community. The three main components of this ecosystem are the following:

1. Community system: This system consists of four different communities and each community has specific tasks. First, the provider community defines the rules of the entire ecosystem and keeps it as open as possible. Next, the developer community creates services for the marketplace in order to fulfil user requirements. The user community consists of the data buyers and sellers and finally, the operating community allows the marketplace to function by providing computational resources.
2. Open business architecture platform: In order for the ecosystem to be decentralized, the main services are provided by distributed nodes powered by the operating community. These services have different interfaces: the data interface (which allows the external data to be connected in the marketplace), the money interface (which can be used to connect different payment options), the core foundation interface (which is executed via smart contracts that increase the security and privacy, as smart contracts cannot communicate with external sources). The developing community is able to create smart contracts as long as they follow a set of specific rules called "essential services". Any added functionality is called advanced service.
3. Relationship between the community system and the open business architecture platform.

2.24. Trustworthy IoT Data Streaming Using Blockchain and IPFS

Haya R. Hasan et al. proposed in [32] a solution for resource-constrained IoT streaming devices that utilize the advantages of blockchain technology for the transferring of data chunks. They use re-encryption mechanisms for privacy of the streamed data and IPFS for off-chain decentralized storage for the data chunks. The hashes of the data chunk are stored on a chain that provides high data integrity. Their blockchain of choice is a public Ethereum network. The design of the system relies first on the IoT streaming device with the purpose of sending data chunks to the storage regularly. Next, it is the blockchain that keeps smart contracts for the streaming devices and the rules for the participants. Third are the participants that are represented in the blockchain with their Ethereum address. The IoT streaming devices also have their own address. Owners of the devices are able to create smart contracts for their devices and register interested participants. IoT streaming devices can be sold with an auction that every registered participant can bid on. The ownership is transferred with the smart contract functionality only if the winner of the auction transfers the appropriate amount of ether to the current owner of the device. Next is the decentralized storage that stores all the data chunks. Finally, the option of the re-encryption network proxy is pursued. Authorized users are able to access the data chunks.

For unauthorized users, the data chunks are encrypted. After a certain time that authorized users have access to the data chunks, the data chunks will be re-encrypted.

2.25. dMOBAs: A Data Marketplace on Blockchain with Arbitration Using Side-Contracts Mechanism

Hangyun Tang et al. proposed [33] a highly resilient, trustful and efficient data marketplace that uses blockchain technology with side-contract mechanisms for arbitration. They focus on the data trading procedure, as the main actors of a marketplace are buyers and sellers. In their approach, data are decentralized and held by service providers. They use a distributed storage network (DSN) to provide reliability and durability to the storage service. In order to record and trace transactions between buyers and sellers, they use smart contracts due to their on-chain and automatic execution. In order for a transaction to be successful, data buyers must verify the validity of the data with proof provided by the seller. Service providers are responsible for storing the files of the data and accepting commissions of the data sellers. There are two processes: the data storage process and the data transaction and arbitration process. For the first process, the seller hosts the ciphertexted data in the DSN and next, the DSN assigns a service provider for the hosting. The data's hashed values are also stored as validation proof. Then, data buyers are able to purchase the data. The process transaction between buyer and seller in every step, request, acceptance, data verification, data transmission are handled via smart contracts. In case of no expected verification process, an arbitration request is initiated and proceeds with a side-contract mechanism. The encrypted data are stored in the IPFS DSN.

2.26. TrailChain: Traceability of Data Ownership across Blockchain-Enabled Multiple Marketplaces

Pooja Gupta et al. [34] proposed a solution for tracking the ownership of data across multiple decentralized data marketplaces with the use of watermarking and a blockchain framework. Their blockchain of choice is Ethereum. The main actors are data producers, data buyers and data resellers. The network model consists of the layer of marketplaces where multiple marketplaces can be integrated, the layer of data ownership management, which is based on a consortium blockchain that is used for secure tracking of ownership change, and the token management layer that is responsible for token transferring. There are also three different types of smart contracts. In the first layer, there are the application contracts that provide functionalities for the marketplaces. In the second layer, system contracts are used for tracking and ownership management. In the third layer, payment contracts are used for payments among the participants. There is also the decentralized application layer that serves as the front-end and allows for interaction with the system. In order to track the data's movements, there is watermarking module that allows data producers to embed hidden watermarks within the data.

3. Discussion

From the presentation of the different approaches, it becomes evident that trading IoT generated data is a topic which has attracted interest of the scientific community and that the proposed solutions can differ either on business-relevant aspects (for example, the number and type of the considered actor roles) and/or on the technical implementation aspects (such as on-chain or off-chain IoT data storage). To guide a developer that aspires to implement and make commercially available a blockchain-based IoT data marketplace or the designer of an IoT data marketplace tailored to a specific sector or requirements set, we have tabulated the existing works and their respective characteristics in Table 1 below. The possible values per design element (which are associated with characteristics of the solutions) are: Y if the factor is considered in the relevant work, N if it is not and "n/s" if it is not specified/supported.

Table 1. Design elements implemented in each work.

Design Elements/ Articles	Smart Contracts	Decentralized Storage	Real-Time Data	Data Encryption	Cost Efficiency	Data Integrity	Participants' Rating/Rewards	Scalability
Lars Mikkelsen et al. (2018) [7]	Y	N	n/s	n/s	N	N	N	N
KazımRıfatÖzyılmaz et al. (2018) [8]	Y	Y	N	Y	Y	Y	N	Y
Ronghua Xu et al. (2019) [9]	Y	n/s	n/s	Y	N	Y	Y	n/s
Fatemeh Mohammadzadeh et al. (2019) [10]	Y	n/s	Y	N	N	N	Y	Y
Duc-Duy Nguyen et al. (2019) [3]	Y	N	Y	N	Y	N	Y	N
Shaimaa Bajoudah et al. (2019) [11]	Y	N	Y	N	Y	N	Y	N
Hien Thi Thu Truong et al. (2019) [12]	Y	N	N	Y	N	N	N	Y
Anas Dawod et al. (2020) [14]	N	N	N	n/s	N	N	N	Y
Rahma A Alzahrani et al. (2020) [15]	Y	N	N	Y	N	Y	N	Y
Pooja Gupta et al. (2020) [16]	Y	N	Y	Y	N	Y	Y	Y
Wiem Badreddine et al. (2020) [17]	Y	N	Y	n/s	Y	N	N	N
Dimitrios Georgakopoulos et al. (2020) [19]	n/s*	n/s	n/s	n/s	Y	N	N	Y
Pooja Gupta et al. (2021) [21]	Y	N	Y	n/s	N	n/s	Y	Y
James Meijers et al. (2021) [22]	Y	N	Y	n/s	Y	N	N	n/s
Sina Rafati Niya et al. (2021) [23]	Y	Y	N	Y	N	Y	N	N
Paulo Valente Klaine et al. (2021) [24]	Y	Y	N	n/s	N	Y	N	Y
Akanksha Dixit et al. (2021) [25]	Y	Y	Y	Y	N	Y	Y	Y
Lodovico Giaretta et al. (2021) [26]	Y	n/s	N	Y	N	N	Y	N
Baoyi An et al. (2021) [27]	Y	Y	N	Y	N	Y	Y	n/s
Anusha Avyukt et al. (2021) [28]	Y	N	N	N	N	N	Y	N
Ronghua Xu and Yu Chen (2021) [29]	Y	N	n/s	Y	N	Y	Y	Y
Junhua Zhang et al. (2022) [30]	Y	N	n/s	N	Y	N	N	n/s
Sebastian Lawrenz (2022) [31]	Y	N	n/s	N	Y	N	N	Y
Haya R. Hasan (2022) [32]	Y	Y	N	Y	N	Y	N	N
Hangyun Tang et al. (2022) [33]	Y	Y	N	Y	N	Y	N	Y
Pooja Gupta et al. (2022) [34]	Y	N	n/s	Y	Y	Y	N	Y

From the table above, it is evident that none of the presented works considered all the design factors. Specifically, only in [25] were seven out of the eight design factors considered, missing cost efficiency. In our opinion, this makes [25] the best candidate for consideration when creating a decentralized IoT data marketplace powered by blockchain technology. Most of the presented works use smart contract, and those that do not considered using them in future works [14], except [19] where smart contract usage is not specified. In each approach, smart contracts are used for different purposes as shown in Table 2, which shows the many different functionalities that can be securely automated using blockchain technology. Even though decentralized data storage increases data integrity [8,23–25,27,32,33], in many

solutions, they still prefer to utilize centralized storages or repositories that participants already use. There are works [9,15,16,29] where the encryption and verification mechanisms of the blockchain are exploited to ensure the integrity of the data, which are kept outside the blockchain. In addition, some approaches do not store the data but rather only exchange real-time data (which do not require storage) [3,11,16,17,21,22]. For real-time data, [16] is considered the optimal choice, as it offers richer functionality, missing only the cost efficiency of the transactions. We consider that the "best value for money" options are [3,11], as they employ cost-efficiency mechanisms, i.e., they reduce the number of performed transactions. Data encryption is implemented in almost any work that uses decentralized storage [8,23,25,27,32,33]. Considering pure decentralization [27,32,33] is the best option in our opinion.

Table 2. Smart contract utilization in each work.

Smart Contract Functionality	Articles
Access Control	[8–10,12,15,24,25,29,30,32,33]
Data Offering	[7,11,12,15,25,29,32]
Billing/Receipt	[3,7,9,11,12,15–17,21–25,27,29,32–34]
User Verification	[9,11,25,29,32]
Regulations	[9,21,26,31,33,34]
Rating System	[3,8,9,16,21,24,26–29]
User/Device Registration	[7,8,15–17,23,32]
Data Integrity	[9,15,29,32–34]
Participants' Agreement	[3,11,16,21,32]

4. Conclusions

In this paper, the works on decentralized IoT data marketplaces were reviewed. These marketplaces provide a reliable and trustless way of data exchange. The emphasis of the review was on the design factors such that valuable insights and alternatives are presented to prospective new marketplace designers and/or implementers. However, none of the works address all the topics that have been raised in this sector, which opens the way for the design of a decentralized IoT marketplace considering meeting all the listed needs. Almost all the works considered smart contract-compatible blockchains even though they are used differently. In our future work, we plan to efficiently maximize the use of smart contract while also considering cost efficiency.

Author Contributions: J.C. and P.P. identified and studied the research works. H.C.L. conceptualized the idea and purpose of carrying out this survey and the direction of comparison. P.A.K. was primarily involved in the comparison and in the editing of the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All information and data used in the paper are publicly available.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhariand, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]

2. Ahlgren, B.; Hidell, M.; Ngai, E.C. Internet of things for smart cities: Interoperability and open data. *IEEE Internet Comput.* **2016**, *20*, 52–56. [CrossRef]
3. Nguyen, D.-D.; Ali, M.I. Enabling On-Demand Decentralized IoT Collectability Marketplace using Blockchain and Crowdsensing. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019. [CrossRef]
4. Niya, S.R.; Jha, S.S.; Bocek, T.; Stiller, B. Design and implementation of an automated and decentralized pollution monitoring system with blockchains, smart contracts, and LoRaWAN. In Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS 2018), Taipei, Taiwan, 23–27 April 2018; pp. 1–4.
5. Niya, S.R.; Dordevic, D.; Nabi, A.G.; Mann, T.; Stiller, B. A Platform-independent, Generic-purpose, and Blockchain-based Supply Chain Tracking. In Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2019), Seoul, Korea, 14–17 May 2019; pp. 11–12.
6. Masla, N.; Vyas, V.; Gautam, J.; Shaw, R.N.; Ghosh, A. Reduction in gas cost for blockchain enabled smart contract. In Proceedings of the 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON), Kuala Lumpur, Malaysia, 24–26 September 2021. [CrossRef]
7. Mikkelsen, L.; Mortensen, K.; Rasmussen, H.; Schwefel, H.-P.; Madsen, T. Realization and evaluation of marketplace functionalities using Ethereum blockchain. In Proceedings of the 2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Hamammet, Tunisia, 20–21 December 2018. [CrossRef]
8. Özyılmaz, K.R.; Dogan, M.; Yurdakul, A. IDMoB: IoT Data Marketplace on Blockchain. In Proceedings of the Crypto Valley Conference on Blockchain Technology (CVCBT2018), Zug, Switzerland, 20–22 June 2018.
9. Xu, R.; Ramachandran, G.S.; Chen, Y.; Krishnamachari, B. BlendSM-DDM: BLockchain-ENabled Secure Microservices for Decentralized Data Marketplaces. In Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, 14–17 October 2019.
10. Mohammadzadeh, F.; Mirghasemi, S.A.; Dorri, A.; Ahmadifar, H. DMap: A Distributed Blockchain-based Framework for Online Mapping in Smart City. In Proceedings of the 2019 9th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 24–25 October 2019. [CrossRef]
11. Bajoudah, S.; Dong, C.; Missier, P. Toward a decentralized, trust-less marketplace for Brokered IoT data trading using Blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019. [CrossRef]
12. Truong, H.T.T.; Almeida, M.; Karame, G.; Soriente, C. Towards Secure and Decentralized Sharing of IoT Data. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019.
13. Cirillo, F.; Solmaz, G.; Luís Berz, E.; Bauer, M.; Cheng, B.; Kovacs, E. A Standard-Based Open Source IoT Platform: FIWARE. *IEEE Internet Things Mag.* **2019**, *2*, 12–18. [CrossRef]
14. Dawod, A.; Georgakopoulos, D.; Jayaraman, P.P.; Nirmalathas, A. An IoT-owned Service for Global IoT Device Discovery, Integration and (Re)use. In Proceedings of the 2020 IEEE International Conference on Services Computing (SCC), Beijing, China, 7–11 November 2020.
15. Alzahrani, R.A.; Herko, S.J.; Easton, J.M. Blockchain application in remote condition monitoring. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020. [CrossRef]
16. Gupta, P.; Dedeoglu, V.; Najeebullah, K.; Kanhere, S.S.; Jurdak, R. Energy-aware Demand Selection and Allocation for Real-time IoT Data Trading. In Proceedings of the 2020 IEEE International Conference on Smart Computing (SMARTCOMP), Bologna, Italy, 14–17 September 2020. [CrossRef]
17. Badreddine, W.; Zhang, K.; Talhi, C. Monetization using Blockchains for IoT Data Marketplace. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020.
18. Xie, K.; Wen, J.; Zhang, D.; Xie, G. Bloom Filter Query Algorithm. *J. Softw.* **2009**, *20*, 96–108. [CrossRef]
19. Georgakopoulos, D.; Jayaraman, P.P.; Dawod, A. SenShaMart: A Trusted IoT Marketplace for Sensor Sharing. In Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 1–3 December 2020.
20. Compton, M.; Barnaghi, P.; Bermudez, L.; García-Castro, R.; Corcho, O.; Cox, S.; Graybeal, J.; Hauswirth, M.; Henson, C.; Herzog, A.; et al. The SSN ontology of the W3C semantic sensor network incubator group. *J. Web Semant.* **2012**, *17*, 25–32. [CrossRef]
21. Gupta, P.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Towards a blockchain powered IoT data marketplace. In Proceedings of the 2021 International Conference on COMmunication Systems &NETworkS (COMSNETS), Bangalore, India, 5–9 January 2021.
22. Meijers, J.; Putra, G.D.; Kotsialou, G.; Kanhere, S.; Veneris, A. Cost-Effective Blockchain-based IoT Data Marketplaces with a Credit Invariant. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2021.
23. Niya, S.R.; Dordevic, D.; Stiller, B. ITrade: A Blockchain-based, Self-Sovereign, and Scalable Marketplace for IoT Data Streams. In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 17–21 May 2021.
24. Klaine, P.V.; Zhang, L.; Ali Imran, M. An Implementation of a Blockchain-based Data Marketplace using Geth. In Proceedings of the 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 27–30 September 2021.
25. Dixit, A.; Singh, A.; Rahulamathavan, Y.; Rajarajan, M. FAST DATA: A Fair, Secure and Trusted Decentralized IIoT Data Marketplace enabled by Blockchain. *IEEE Internet Things J.* **2021**, 1. [CrossRef]

26. Giaretta, L.; Savvidis, I.; Marchioro, T.; Girdzijauskas, S.; Pallis, G.; Dikaiakos, M.D.; Markatos, E. PDS^2: A user-centered decentralized marketplace for privacy preserving data processing. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW), Chania, Greece, 19–22 April 2021. [CrossRef]
27. An, B.; Xiao, M.; Liu, A.; Xu, Y.; Zhang, X.; Li, Q. Secure Crowdsensed Data Trading Based on Blockchain. *IEEE Trans. Mob. Comput.* **2021**, 1. [CrossRef]
28. Avyukt, A.; Ramachandran, G.; Krishnamachari, B. A Decentralized Review System for Data Marketplaces. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2021; pp. 1–9. [CrossRef]
29. Xu, R.; Chen, Y. Fed-DDM: A Federated Ledgers based Framework for Hierarchical Decentralized Data Marketplaces. In Proceedings of the 4th International Workshop on Blockchain Enabled Sustainable Smart Cities, Athens, Greece, 19–22 July 2021. [CrossRef]
30. Zhang, J.; Zhong, C. Differential Privacy-Based Double Auction for Data Market in Blockchain-Enhanced Internet of Things. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 8038846. [CrossRef]
31. Lawrenz, S.; Sharma, P.; Rausch, A. Towards A Data Marketplace Ecosystem Blueprint for A Community-Driven Data Marketplace. In Proceedings of the ADAPTIVE 2022: The Fourteenth International Conference on Adaptive and Self-Adaptive Systems and Applications, Barcelona, Spain, 24–28 April 2022.
32. Hasan, H.R.; Salah, K.; Yaqoob, I.; Jayaraman, R.; Pesic, S.; Omar, M. Trustworthy IoT Data Streaming Using Blockchain and IPFS. *IEEE Access* **2022**, *10*, 17707–17721. [CrossRef]
33. Tang, H.; Qiao, Y.; Yang, F.; Cai, B.; Gao, R. dMOBAs: A data marketplace on blockchain with arbitration using side-contracts mechanism. *Comput. Commun.* **2022**, *193*, 10–22. [CrossRef]
34. Gupta, P.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. TrailChain: Traceability of data ownership across blockchain-enabled multiple marketplaces. *J. Netw. Comput. Appl.* **2022**, *203*, 103389. [CrossRef]