Decentralized Blockchain-Based IoT Data Marketplaces

Subjects: Computer Science, Information Systems

Contributor: John Christidis, Panagiotis A. Karkazis, Pericles Papadopoulos, Helen C. (Nelly) Leligou

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.

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

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**.

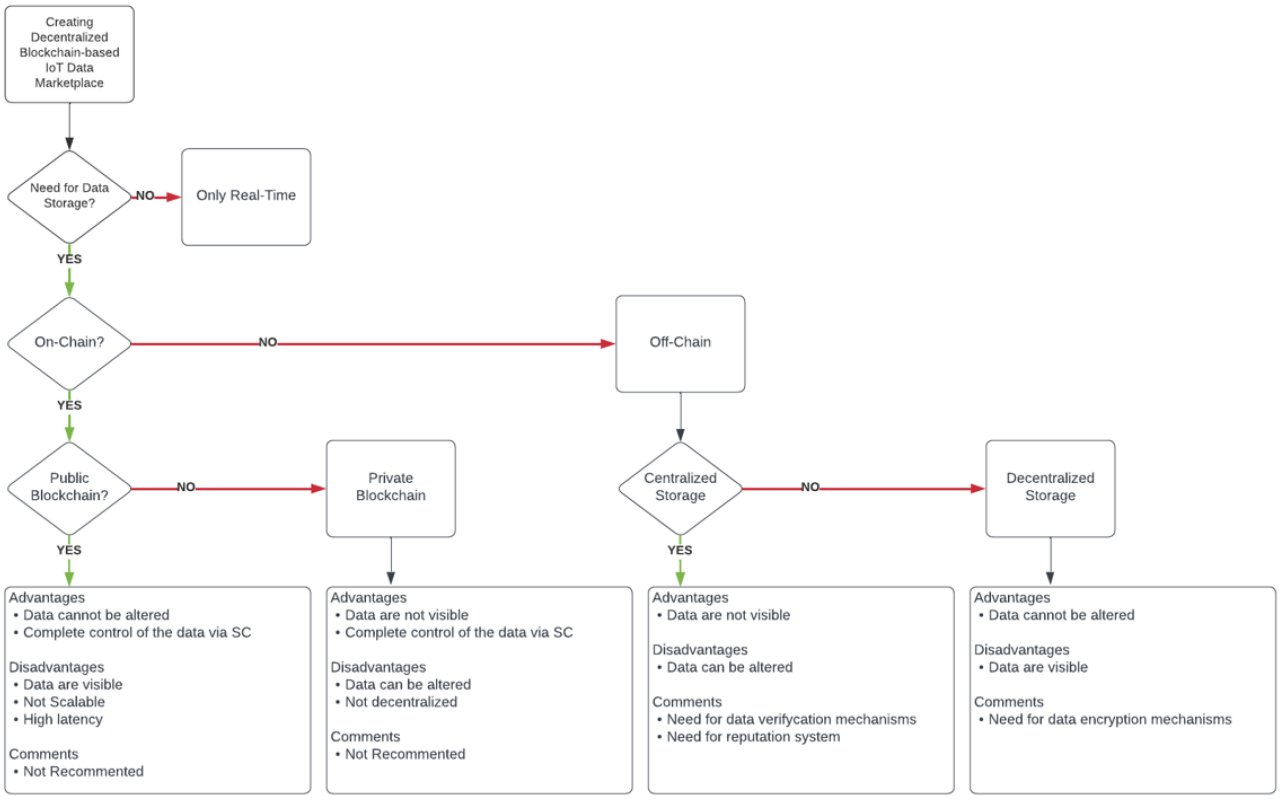

Figure 1. Schematic view of a systematic decision process for the design or selection of an IoT data marketplace solution.

2. Decentralized Blockchain-Based IoT Data Marketplaces

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:

- 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.
- 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.
- 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.

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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
