Journal of
Sensor and Actuator Networks

MDPI

Review

Blockchain as IoT Economy Enabler: A Review of Architectural Aspects

Diego Pennino [1], Maurizio Pizzonia [1], Andrea Vitaletti [2] and Marco Zecchini [2]

[1] Dipartimento di Ingegneria, Sezione Informatica e Automazione, Università degli Studi Roma Tre, Via della Vasca Navale 79, 00146 Rome, Italy; pennino@ing.uniroma3.it (D.P.); pizzonia@ing.uniroma3.it (M.P.)
[2] Dipartimento di Ingegneria Informatica, Automatica e Gestionale, Sapienza Università di Roma, Via Ariosto 25, 00185 Rome, Italy; vitaletti@diag.uniroma1.it
* Correspondence: zecchini@diag.uniroma1.it

Abstract: In the IoT-based economy, a large number of subjects (companies, public bodies, or private citizens) are willing to buy data or services offered by subjects that provide, operate, or host IoT devices. To support economic transactions in this setting, and to pave the way for the implementation of decentralized algorithmic governance powered by smart contracts, the adoption of the blockchain has been proposed both in scientific literature and in actual projects. The blockchain technology promises a decentralized payment system independent of (and possibly cheaper than) conventional electronic payment systems. However, there are a number of aspects that need to be considered for an effective IoT–blockchain integration. In this review paper, we start from a number of real IoT projects and applications that (may) take advantage of blockchain technology to support economic transactions. We provide a reasoned review of several architectural choices in light of typical requirements of those applications and discuss their impact on transaction throughput, latency, costs, limits on ecosystem growth, and so on. We also provide a survey of additional financial tools that a blockchain can potentially bring to an IoT ecosystem, with their architectural impact. In the end, we observe that there are very few examples of IoT projects that fully exploit the potential of the blockchain. We conclude with a discussion of open problems and future research directions to make blockchain adoption easier and more effective for supporting an IoT economy.

Keywords: Internet of Things (IoT); blockchain; payment; economy; tokens; applications of IoT and blockchain; smart contracts; scalability

Citation: Pennino, D.; Pizzonia, M.; Vitaletti, A.; Zecchini, M. Blockchain as IoT Economy Enabler: A Review of Architectural Aspects. *J. Sens. Actuator Netw.* **2022**, *11*, 20. https://doi.org/10.3390/jsan11020020

Academic Editor: Lei Shu

Received: 27 January 2022
Accepted: 24 March 2022
Published: 29 March 2022

1. Introduction

The Internet of Things (IoT) is a network of tiny devices connected over the Internet to observe the physical world, gather data, and consciously act on it in a useful way. Billions of connected IoT devices are expected to bring a substantial added value for communities and for individuals, also in view of the fact that IoT is tightly connected with several well-known trends, such as Big Data, smart cities, and Industry 4.0, which promise to deeply change many aspects of our lives in the future. As an example, the unprecedented amount of data gathered by billions of IoT sensors will bring us the ability to get new insights and actionable intelligence regarding our world [1,2]. The pervasive presence of smart connected devices will enable the development of innovative services to improve our lives [3] and to face new and unexpected challenges, such as the COVID-19 outbreak [4], and private and public objects (i.e., things) will be available to anyone for renting, even for a short time, to support a new form of shared economy [5].

The general problem of giving a reward to subjects that contribute to this novel added value ecosystem is not only an economic or business-related question. Many IoT applications are peculiar regarding the amount of involved users, the volume and diversity of generated data, the frequency of economic transactions and their latency constraints,

as well as security requirements. Hence, related technical and architectural aspects are by themselves an interesting cross-cutting dimension for many IoT applications.

This is even more compelling if we observe that decentralization is going to be a fundamental aspect of evolved IoT ecosystems. In fact, a single organization handling a vast amount of heterogeneous and pervasive IoT devices is not simply unrealistic, but also unfeasible. We expect that in the more complex scenarios, many organizations will contribute to a single IoT ecosystem. Furthermore, the pervasive nature of IoT deployments usually requires the involvement of end-users that buy, deploy, and contribute their devices to an ecosystem on the basis of some kind of future advantage. Ecosystems of this kind grow as more people are willing to contribute, and not (only) under the pressure of centralized investments.

This decentralized nature of the IoT is a natural contact point with blockchain technology, and in particular, the usually open participation of users to IoT deployments suggests the employment of public/permissionless blockchains. For this reason, in this paper we will focus on the integration of IoT with that kind of blockchain, citing permissioned approaches only occasionally. This will provide the highest guarantees in terms of decentralization and security, but leave open significant challenges in terms of scalability, a key property for IoT.

In essence, we will consider the reference scenario depicted in Figure 1. Thing providers are individuals or organizations that make things, and/or the data generated by those things, accessible to others. Examples of thing providers range from citizens running smart sensors for the collection of data on pollution in their houses to organizations renting scooters in cities (see Section 4 for a list of interesting use cases). On the other side, thing consumers use things and/or their generated data. Examples are citizens renting a scooter, or environmental protection agencies using data gathered by private citizens.

In general, the participation of thing providers to an IoT ecosystem is motivated by a benefit. While in some cases, this might simply come from a community sharing the same purpose (e.g., environmental monitoring to improve the safety of a shared place), in general, an appropriate and automated economic reward is a natural incentive leading to an IoT-based economy.

Renting a thing (e.g., a scooter) is likely the most straightforward case of IoT-based economy, but many other models are possible, such as selling data or getting a reward for participating in a network of interconnected things to serve as a data packet router.

All the above considerations immediately suggest the use of blockchain technologies to support an IoT-based economy. In fact, blockchains are well known to be able to support the exchange of economic values (embodied by cryptocurrencies, or more precisely, tokens) in a decentralized manner and with a high level of security, without the need for the involved subjects to trust each other. In this setting, where the blockchain is primarily employed to exchange tokens, the employment of public/permissionless blockchains provides the highest guarantees and allows the exploitation of the tokens in a wider ecosystem. For example, we can envision an ecosystem in which the tokens gained to support the collection of environmental pollution data are employed for renting a scooter. The employment of blockchain brings many advantages in terms of flexibility because it allows us to implement an algorithmic governance capable of autonomously handling all the important aspects of the reward process, such as when to pay the reward, how its amount is calculated, who is charged and when, and so on. It also provides new financial tools to sustain the whole ecosystem, like Initial Coin Offering (ICO) and market-driven prices. These financial tools can be adopted as mechanisms to reward all the thing providers that want to participate in an ecosystem. A token that can be exchanged with many others, or that can be accepted as payment in many contexts, is more valuable (an economist may say more liquid) than one that is accepted as payment in only a few situations; this strengthens our previous choice to focus this work on the integration of IoT with public/permissionless blockchains. However, the employment of a blockchain has some drawbacks. Beside the obvious increase in architectural complexity, it forces one to make some architectural choices that have a significant impact, for example, on the scalability and on the resiliency of the whole system.

In this paper, we provide a review of architectural aspects of the integration of IoT and public/permissionless blockchain, to support the IoT-based economy. In our review, we start from some selected relevant projects and scientific papers in which the blockchain-based IoT economy is central, and we analyze the technical aspects of this integration, providing a reasoned survey of blockchain technologies and of architectural choices and showing their strengths and weaknesses. We deliberately neglect the financial, economical, ethical, and social analysis (see, for example, [5–7]) of the implications behind the considered scenarios, focusing only on the technologies that enable them. For example, we do not investigate what the economic drivers behind the adoption and sustainability of the business models leveraging cryptocurrencies or tokens are. However, we focus on the technical ingredients (e.g., smart contracts, payment channels, etc.) and architectures to enable those models. Other works [8–13] have analyzed this economic benefit, citing payments as a reason to adopt BC with IoT, only from a scientific point of view. Because a scientific solution can sometimes be tricky to apply in a real scenario, in this work, we started from real use cases. Finally, we remark that this paper focuses on techniques and strategies enabling a blockchain-based economy for IoT applications, but we invite readers interested in works showing how IoT benefits from the integration with blockchain to read [14,15].

Structure of the Paper

In Section 2, we provide some background on IoT and blockchains. In Section 3, we review some blockchain technologies that are particularly suited for use in IoT ecosystems. In Section 4, we consider a set of applications that either take advantage of the reference scenario for the IoT economy depicted in Figure 1 or propose a setting in which that scenario is a natural evolution. In Section 7, we analyze the main technical ingredients and architectural choices to enable the IoT economy, also referring to choices actually made by the considered projects. In Section 6, we go beyond simple payments, discussing some financial tools enabled by blockchain adoption, their relation with IoT, and their architectural impact. Finally, in Section 8, we provide some conclusions and discuss some open problems.

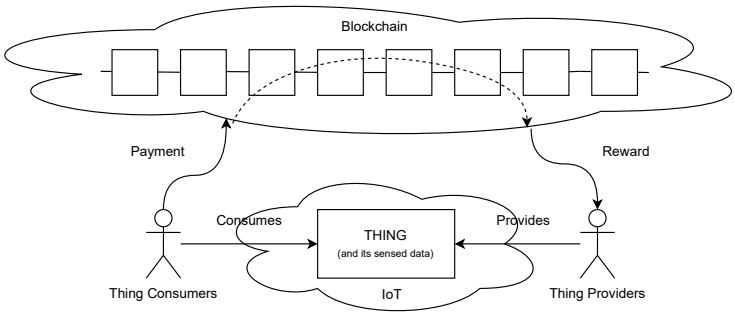

Figure 1. A schematic representation of the reference scenario. Thing consumers pay to use things or the data they gather. They are entitled to do that only if their payment was recorded in the blockchain. Thing providers get a reward to make their things or data available. The reward is autonomously dispensed by a transaction on the blockchain. Payment and reward might be two sides of the same transaction; however, this is not always the case.

2. Background

The two main technical components in the reference scenario in Figure 1 are the IoT and the blockchain. In this section, we introduce some background on these technologies, with a particular focus on the main aspects affecting the interaction between them.

2.1. Internet of Things Background

The Internet of Things (IoT) is a network of physical objects—things—that are equipped with sensors, actuators, and computation and communication capabilities for the purpose

of observing a physical phenomenon, delivering the monitored data over the Internet, and acting in the environment, either according to local autonomous decisions or implementing remote commands [16].

The amount of IoT devices is rapidly increasing. By 2025, forecasts suggest that there will be more than 75 billion IoT-connected devices in use, which is three times those deployed in 2019 (https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, (accessed on 28 March 2022)). The unprecedented amount of data collected by the IoT on the physical world, combined with cloud computing, promotes the development of new services, affecting many aspects of human daily life and with great market potential. Typical areas of application include manufacturing, smart city, supply chain, transportation, agriculture, energy management, environmental monitoring, and many others [16].

Lately, IoT devices have not only been exchanging data; an emerging trend is to enable Machine-to-Machine (M2M) payments, turning each connected device into a platform for selling and purchasing. By 2022, 451 Research's IoT Market Monitor expects that USD 7.5 billion in new transactions will be driven, in the US, through IoT payments (https://www.forbes.com/sites/jordanmckee/2019/10/09/the-internet-of-payments-has-arrived/?sh=6faa22da3e69, (accessed on 28 March 2022)).

A typical IoT architecture consists of things, gateways, and the cloud platform (see Figure 2) [17]. Usually, things support power-efficient wireless technologies (e.g., LoRaWAN [18], Sigfox [19]) that, in order to limit the energy consumption and prolong the network lifetime, do not allow direct connection to the Internet. In this scenario, gateways are more powerful devices, usually not bounded by energy constraints, in charge of receiving the wireless communications from the things and delivering the messages to the cloud platform over the Internet. In some cases, the things can be directly connected to the Internet, either because they exploit power-efficient wireless technologies (e.g., NB-IoT), or because, in some specific scenarios, they can be connected to external and/or renewable power sources that allow the exploitation of more energy-demanding wireless technologies [20]. The trade-off between energy consumption, expected network lifetime, and connection quality (in terms of bandwidth, latency, and coverage) are application-specific.

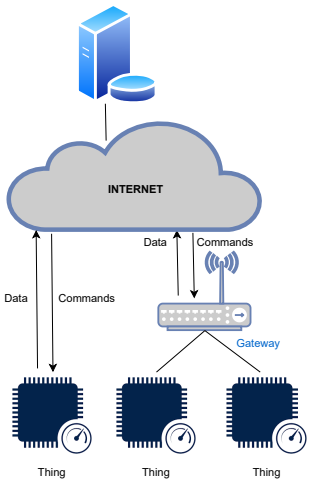

Figure 2. A schematic representation of a typical IoT architecture.

The things (or sensor nodes) are end nodes with sensors/actuators that are usually programmed for a specific application purpose. As already discussed, things can be deployed in a variety of application domains, and consequently, they feature very heterogeneous characteristics [17]. However, when compared even to low-end notebooks, they are usually devices with very limited resources, as shown in Table 1. This is extremely important, since most current blockchain technologies have requirements that cannot be easily satisfied even by low-end notebooks.

Table 1. A comparison of low-end notebook components with typical things.

	Low-End Notebooks	**Things**
Processing Power	AMD's Athlon are considered cheap CPUs and feature from 2 to 4 cores and a frequency of more than 3 GHz (https://www.amd.com/en/processors/athlon-desktop, accessed on 28 March 2022).	Typical microcontrollers used in sensor nodes are single-core and reach a maximum clock speed in the order of MHz (https://www.st.com/content/st_com/en/arm-32-bit-microcontrollers/arm-cortex-m7.html, accessed on 28 March 2022).
Data and code memory	Even very inexpensive notebooks have at least 4 GB of RAM, and at least 128 GB if SSD or more than 500 Gb if HDD	An IETF report from 2014 claims that the most powerful class of sensor nodes commercially available in the market features around 50 KB of data memory (e.g., RAM) and around 250 KB of code memory (e.g., flash memory) [21]. In the last years, however, these specifications have increased, reaching the maximum of 2 GB for code memory and 1 GB for RAM memory (1). The size of persistent data memory, such as EEPROM, in sensor nodes is in the order of KBs [22].
Energetic Power	Notebooks can be connected to power plugs, providing all the necessary energy, and can run for a few hours on batteries that can usually be easily recharged. This is unacceptable for most IoT applications.	Most of the things in IoT networks are battery-powered, and their deployments can make them difficult to recharge. As a consequence, things have limited available energy. Especially when wireless transmission is used, the radio often consumes a big portion of the total energy consumed by the device [21]. A common technique to reduce power consumption and increase the device lifetime is duty-cycling. Duty cycle is the ratio of time a component (e.g., communication, sensing, computation) is on compared to the time it is off. Obviously, this technique prolongs the lifetime of operations at the cost of decreased performance.

Table 1. *Cont.*

	Low-End Notebooks	Things
Wireless Connectivity	The availability of power and the facility in recharging the battery allows the employment of relatively long-range and high-bandwidth wireless technologies. Wi-Fi is available in all notebooks and allows hundreds of Mbps.	Typically sensor nodes communicate via low-power wireless protocols with low data rate, such as BLE, 802.15.4 (e.g., 6LoWPAN, Zigbee, Thread, WirelessHART etc), or LPWAN (e.g., LoRa [18]). For instance, short-range protocols, like BLE and Zigbee, reach a maximum data rate of 1Mbps [23] and 250 kbps [24], respectively, while long-range wireless protocol, such as LoRa, allows a maximum data rate in the order of only tens of kbps [25].

The massive production of data foreseen in the IoT impacts on network performances and on data congestion to the cloud servers. For this reason, additional computing layers, such as edge and fog computing, can be added between the things and the cloud to carry out the computation closest to the sources of data with the purpose of (a) filtering data to limit the traffic to the cloud and (b) improving the responsiveness to handle local events, and in general, enhancing the thing's computational and storage capacity [26]. Edge computing is data computation that happens at the network's edge, in proximity to the things, while fog computing acts as a mediator between the edge and the cloud for various purposes, such as data filtering or a localized learning model [17].

Section 7.2 discusses the main issues in accessing a blockchain from the things, and Figure 3 summarizes the possible roles of things and gateways with respect to blockchain integration. For the sake of simplicity, in this paper we limit our attention to gateways, but they actually represent any edge computing device capable of enhancing things' limited resources to support more advanced blockchain functionalities.

2.2. Blockchain and DLT Background

A Distributed Ledger Technology (DLT) is a decentralized log of records, the ledger, managed by multiple, usually autonomous, participants (also called users or subjects), across multiple nodes (for more details, see [27]). At each instant of time, the ledger represents a unique state that is updated by atomic transaction; this update is essentially the appending of a new record to the ledger. Unlike a centralized database, a distributed ledger is decentralized; there is no need for a central authority or intermediary for processing, validating, and/or authenticating transactions.

A blockchain is a type of DLT where transactions are recorded according to an immutable order obtained by means of cryptographic hash functions that chain the blocks in which transactions are recorded. Since DLT gained attention through the diffusion of the blockchain, it is common practice to use the term blockchain even when talking about other types of DLT. For this reason, in the rest of the paper we will adopt the same common practice. The most common blockchains can be abstracted as key-value stores. For example, in a blockchain implementing a cryptocurrency, keys are *addresses* (also called *accounts*), while values are the balances of their *wallets*. In this scenario, a transaction is an operation that transfers cryptocurrency from one wallet to another. We call *pending* transactions those that are generated by users but are not (yet) processed by the blockchain. A *confirmed* transaction is an immutable transaction that was successfully processed by the blockchain. The state of the blockchain is a totally ordered sequence of confirmed transactions. For efficiency reasons, transactions are not confirmed one-by-one but aggregated into *blocks*. Pending transactions are confirmed when a new block is hl*created* (or hl*mined*). The mining of a new block requires:

(1) selecting a subset of pending transactions;
(2) ordering them;
(3) verifying that all transactions of the block, considered in the chosen order, comply with certain *consensus rules* (which depends also on the application domain).

The process of verification of consensus rules is called *validation*, and a transaction that passes this check is *valid*. The *consensus* (see [28–30]) is the decentralized process by which a block is finally stored in the ledger.

For the sake of simplicity, in the blockchain, we can assume that a block b is composed of two parts: the *body* that contains all the valid transactions, and the *header*. In the body, transactions are usually ordered and stored using an *Authenticated Data Structure* (ADS) [31–33], which efficiently links their content with a cryptographic hash r_{body}. For the sake of simplicity, the header can be summarized as a tuple $\langle r_p, r_{\text{body}}, sec \rangle$, where r_p is the hash of the header of the previous block p (this cryptographically links all blocks to obtain a chain), and *sec* is security information that provides proof that the block is the result of a consensus among many nodes. Hash r_{body} is employed to efficiently prove the presence of a transaction in the block exploiting cryptographic proofs obtained by ADSes (e.g., Merkle proofs).

A blockchain is typically managed by a set of autonomous *nodes* that collectively create a peer-to-peer (p2p) network adhering to a protocol for inter-node communication and validating new blocks. Nodes do not trust each other, and malicious nodes are tolerated within certain limits, which depend on the consensus algorithm.

It is possible to distinguish three main types of blockchain nodes.

- A *full* node verifies and relays the transactions and the blocks to the network. To check the validity of pending transactions, it has to independently validate the complete copy of the blockchain.
- A *light* node connects to full nodes to interact with the blockchain. Namely, it uses full nodes as intermediaries. It needs only the chain of the block headers to operate. It can ask selected content of block bodies (i.e., the transactions) to full nodees when needed. Light nodes do no need to trust a specific full node, since full nodes provide the required information equipped with Merkle proofs. The amount of resources and storage needed is several orders of magnitude lower than that of a full node, while achieving a very high level of security. It currently takes about an hour and 100 MB to synchronize the entire Ethereum mainnet blockchain with a light node.
- A *client* node relays on 3rd-party hosted nodes providing API to access blockchain services (e.g., Infura). These clients connect to a remote node and completely trust its responses in a non-cryptographically-proven manner.

Both full and light nodes suffer the problem concerning the first synchronization with the network, since they must download a huge amount of information. For example, nowadays, a full node of Ethereum, must download $\approx$ 1200 GB of data (Sources: https://ycharts.com/indicators/reports/ethereum_statistics, https://etherscan.io/chartsync/chaindefault, (accessed on 28 March 2022)). Since this is a change of 90% from one year ago, it is easy to highlight the first synchronization as a big problem in the blockchain scenario, and a huge one if we also consider the limitations of the IoT devices. To mitigate this problem, some solutions (such as [34–36]) have been proposed. The main concept of those solutions is the acceptance of a trade-off between the amount of stored information and the amount of data that a node can verify.

Blockchains can be categorized according to who can write or read the content of the ledger and to who can participate in the consensus. In *public* blockchains, anyone can read the content of the ledger and propose a new transaction that, if successfully validated by the consensus, will be eventually stored in the ledger. In contrast, in *private* blockchains, users are authenticated, and access control allows or denies each user operation, as occurs for access control of regular information systems. Similarly, in a *permissionless* blockchain, every user can participate in the consensus (in this paper we also use the term *unpermis-*

sioned), while in a *permissioned* one, the participation in the consensus is allowed only for specific users.

While initially, blockchain was primarily conceived to implement cryptocurrencies, the most intriguing functionality of more recent technologies (e.g., Ethereum [37], EOS [38]) is *smart contracts*. These consist of pieces of code that are executed as part of a transaction. In simple terms, in these cases, the blockchain implements a global decentralized computer, and smart contracts are the programs running on it.

Smart contracts can act only on data that are stored in the blockchain. However, in the IoT use cases that we consider in this paper, there is a need to access off-chain data. This is addressed by an architectural solution that is called *oracle* (for more details, see [39]). A detailed discussion of oracles and their role in the IoT context is provided in Section 7.3.

The growing need for better performance compared to the speed of transaction management pushed the blockchain community to reuse a structure from the field of graph theory, the *Direct Acyclic Graph* (*DAG*). The DAG substitutes the chain, and each vertex of this graph represents a transaction of the system. Using a DAG instead of a normal chain brings the following advantages:

(1) suited for microtransactions and high volumes of transactions;
(2) eliminates the need for mining (each node can create and validate a transaction independently);
(3) fees may be reduced significantly;
(4) lower energy consumption.

On the other hand, it brings the following disadvantages:

(1) has not yet sustained high levels of decentralization;
(2) is more vulnerable to attacks due to its parallelization.

Currently, the DAG structure is used by EthereumII (in its new mining algorithm Ethash [40]), IOTA [41], Obyte [42], and Nano [43].

On a permissioned blockchain, peers are part of a well-known community that share a common goal, and consequently, there is usually no need of an explicit reward to incentivize participation. On the contrary, in permissionless blockchain, anyone can participate in the consensus, so a natural approach is to reward—usually in the native token of the system—whoever is working for the advantage of the network. For instance, in Bitcoin and Ethereum, a peer receives Bitcoin and Ether tokens, respectively, for solving the PoW; on Algorand, the peers of the elected committee reaching consensus are rewarded with Algos. New tokens with specific features, beyond the ones provides by native tokens, can also be created by smart contracts in compliance with standards (e.g., [44,45]). Alternatively, some technologies have specific support for the streamlined creation of new tokens, such as, for example, Algorand [46]. Tokens can be of two types:

- *Fungible tokens*, if each token represents a value in the application. If two users exchange among themselves the same amount of fungible tokens, they will end up in the same initial state. For instance, fungible tokens may be used to represent an internal cash system, a voucher, and so on.
- *Non-fungible tokens* (NFT), if each token is a digital twin of an off-chain object. If two users exchange among themselves their NFTs, they will not end up in the same initial state. For instance, NFTs can be used to represent an object of the physical world (such as a car, real estate, etc.) or an object of the digital world (such as images, audio files, etc.) in-chain.

In conclusion, for this blockchain overview, if the reader is interested, we also want to suggest [47,48], which summarize the current challenges faced in the blockchain field.

2.3. Decentralization and Scalability: The Blockchain Scalability Trilemma

As we stated in Section 2.1, an IoT ecosystem may produce a big amount of data and transactions, and therefore, using solutions that can handle and process such an

amount of data is a key property that should be guaranteed. However, scalability and high transaction throughput are still open issues for blockchain technologies. Introduced by Vitalik Buterin [49], the *scalability trilemma* states that it is challenging to create a system that is scalable, decentralized, and secure. Essentially, Buterin conjects that a system cannot excel in all three aspects but has to express a trade-off. We now describe the three aspects.

- A blockchain is *decentralized* if no single entity controls the consensus, meaning that no one can control or censor the data that transacts through it. When consensus is governed by a limited number of entities, decentralization is limited. In this respect, permissionless blockchains guarantee the highest level of decentralization (anyone can contribute to consensus), while permissioned ones are more centralized.
- A blockchain is *secure* if, to alter its correct behavior, or status, for example to perform a double-spending attack, an attacker has to control a large number of the nodes participating in the consensus, usually more than half or more than 1/3, depending on the consensus algorithm adopted. Typically, blockchain systems provide a high level of security, without any compromise.
- A blockchain is *scalable* if it can support high transaction throughput and future growth. Current blockchain technologies have severe limitations regarding scalability. One aspect is that adding more nodes to the blockchain does not increase the maximum transaction throughput (more nodes just perform the same operations). It may be interesting to note that, since transactions have to be executed sequentially, throughput and latency are not independent. Algorand, which is considered one of the best performers among the permissionless blockchains, can reach more than 1200 transactions per second, producing a block every 5 s. An example of a citizen-oriented Algorand-based application can be found in [50], where performances are also discussed. Some proposals of blockchains that increase their maximum transaction throughput when the number of nodes increases are available in the scientific literature [51,52]. See also Section 3 for IoT-targeted solutions.

In general, permissioned blockchains can provide higher transaction throughput and low latency, since only a limited amount of known nodes participate in the consensus, thus limiting the overall complexity—at the cost of a greatly reduced decentralization. In this work, we mostly focus on permissionless blockchains.

Proof-of-Work (PoW), the most consolidated consensus mechanism, provides limited transaction throughput scalability, but guarantees high decentralization and security. However, in recent years, the concentration of miners in very few geographical areas with low energy costs has brought into question the true decentralization of PoW.

IOTA [41] is a distributed ledger with unprecedented performance in terms of scalability, but at least in its original implementation, it relies on *coordinators*, which greatly reduce decentralization. Indeed, the main IOTA network is governed by "the coordinator", a centralized node run by the IOTA Foundation. The coordinator states which transactions and data are included in the ledger. The IOTA Foundation plans to ditch the coordinator in version 2.0 of the IOTA protocol.

Can we extend the Buterin trilemma to the Internt of Things (IoT)?

The IoT is:

- decentralized, if the network is made by devices managed by autonomous organizations and/or the data produced by the IoT are handled by autonomous organizations,
- secure, if to alter the correct behavior/status of the network, an attacker would need control of the majority of the nodes. Device security is only as good as the weakest link in the infrastructure. As Brody said, "So if I have a very sophisticated hack-resilient blockchain network, but the operating system that my device runs on is poorly patched or isn't maintained or isn't updated, I've rendered all of that pointless and my device is easily hacked at the edge.",
- scalable, if nodes can be added to the network while still guaranteeing suitable SLA.

3. IoT-Targeted Blockchain Technologies

Table 2 summarizes some DLT technologies that are declared to be suitable for use in IoT solutions. They can be categorized into two categories:

(1) those that aim to provide better performances in terms of scalability and reducing transaction fees;
(2) those also aiming to guarantee blockchain verifiability for IoT devices, enhancing the security of the overall system.

Scalable technologies. In Section 2.3, we described how current blockchain technologies are affected by scalability problems. This limits their adoption with IoT due to the large amount of produced data and transactions. Research has attempted to design new solutions, attempting to solve this problem at different layers and with various approaches.

A first approach is at the consensus layer, through Proof-of-Stake (PoS) consensus algorithms, which are more efficient and guarantee a higher transaction throughput with respect to PoW. Algorand [53] is an example of PoS blockchain, and it guarantees around 1200 transactions per second [54]. Despite its limited decentralization, delegated Proof-of-Stake consensus also reaches good performance in terms of scalability (see, for example, EOS.IO [38]).

Another approach is the one based on the adoption of a Directed Acyclic Graph (DAG) instead of a blockchain. IOTA [41] is among the leaders in this field. In IOTA, for each new transaction, every node participates in the consensus by validating two other transactions that are on the border of the DAG, and therefore, there is no need to pay fees. This is a relevant aspect considering the large amount of transactions necessary to store IoT data on-chain. However, as we mentioned in Section 2.3, IOTA currently relies on a centralized coordinator.

Finally, the last approach to enhance scalability is through three techniques at layer-2, as summarized in [55].

(a) *State/payment channels* are communication channels transporting transactions that could occur on the blockchain, but instead get conducted off of the blockchain, without significantly increasing the risk of any participant. On the mainnet, we can find only the "opening" and the "closing" of the channel (representing the initial and final general-purpose state or balance). Lightning Network [56] for Bitcoin and Raiden Network [57] for Ethereum are examples of layer-2 channels.
(b) *Sidechain* is a separate blockchain attached to its parent blockchain through a two-way peg. It is a technique enabling one to move assets of the parent blockchain to the sidechain, and vice versa. Polygon foundation [58] has released a sidechain attached to the Ethereum mainnet.
(c) *Rollups* is a technique where a number of off-chain transactions are validated on-chain, either by default, leaving the possibility open to network users to dispute in case of an invalid update, or with a single cryptographic proof (e.g., zk-SNARK [59]). The first case is known as *optimistic rollup*, the second one as *zk-rollup*. The Polygon foundation has also released Hermez [60], a system to realize zk-rollups, while Optimism [61] and Arbitrum [62] are well-known implementations of optimistic rollups.

Highly verifiable technologies. Things are resource-constrained devices (see Section 2.1). They usually have limited processing power, with a clock in the order of MHz, a RAM smaller than 1 GB (usually hundreds of MB), and a communication bandwidth of at most 1 Mbps (usually hundreds of Kbps). Furthermore, in many cases, things are battery powered, and to extend the device lifetime, duty-cycling techniques are commonly employed, which further limit the overall throughput of the node. These limited resources are in contrast with some typical requirements of most blockchain technologies. As an example, a full node requires hundreds of GB and a throughput of hundreds of MBps (speed of SSD) to copy the blockchain in a fair amount of time (tens of hours). This applies primarily to public/permissionless blockchains, since private/permissioned ones usually deal with

lower amounts of data. In this work, we focus on public/permissionless blockchains, as already stated in the introduction.

IoT devices are able to host neither a full node nor (in many cases) a light node. Therefore, to connect to the blockchain, they need to rely on an external full node that has to be trusted. INCUBED [63] is a protocol that aims to solve this problem. In INCUBED, small devices rely on any untrusted node of a specialized decentralized network.

The Mina protocol [64] aims to be a lightweight blockchain that maintains a constant size of just 22 kB, regardless of how many transactions are committed to the network. This size should allow anyone to operate a node and help secure its network without needing sophisticated computer hardware. The key to the Mina protocol is the incorporation of zk-SNARKs. In Mina's case, this means that the nodes in the network do not verify all transactions in all blocks. Instead, the blockchain is represented with an easily verifiable cryptographic proof (the zk-SNARK). This proof is much smaller than the size of most other blockchains and represents the state of the whole chain (and not only the latest block). Combined with a Proof-of-Stake consensus mechanism, Mina claims their implementation of zk-SNARKs significantly cuts down on the resources needed to process and record transactions.

Table 2. DLT technologies adaptable with IoT solutions.

Approach		Technology	Reference	Why Useful for IoT?
DAG		IOTA	[41]	Scalability, feeless
PoS Technology		Algorand	[53]	Scalability
DPoS Technology		EOS	[38]	Scalability
Layer-2 scaling techniques	Sidechain	Polygon	[58]	Scalability
	Rollups	Polygon, Optimism, Arbitrum	[58,61,62]	Scalability
	Payment/State Channel	Lightning Network	[56]	Scalability
Blockchain secure access		INCUBED protocol	[63]	Verifiability
Lightweight verifiable blockchain		Mina protocol	[64]	Verifiability

4. Blockchain-Supported IoT-Economies Use-Cases

In this section, we describe the process used to select the projects and applications that represent our use-cases to motivate and support the illustration of the technical components in the rest of the paper.

4.1. Methodology

In our investigation, we looked for projects and applications with the following *eligibility criteria*:

- Projects/applications should have the goal to manage an ecosystem of IoT devices that, even if currently limited in size, has the potential to scale up both in terms of devices and involved people.
- Projects/applications should entail economic transactions among subjects and/or IoT devices within the ecosystem and represent values by means of blockchain tokens. Transactions should be automatically triggered by IoT devices, or this possibility should at least be a future valuable direction of development.
- Projects/applications should potentially involve a conspicuous community and/or involve one or more companies.
- Projects/applications should be realized or realizable by using unpermissioned blockchains. The reasons for this choice were discussed in Sections 1 and 2.3. As an

exception, we may also consider projects based on permissioned blockchains when they represent interesting use-cases, and when they might potentially be implemented on unpermissioned blockchain.

To achieve our goal, we considered (1) works taken from the scientific literature and (2) projects that are not scientifically documented, but that have published enough details regarding their goals, the economic relations between actors, their architecture, and their integration of IoT and blockchain technologies.

For surveying relevant scientific works (see Section 4.3), we adopted an approach inspired by the PRISMA methodology [65]. PRISMA is based on four main phases: identification, screening, eligibility, inclusion. We refer the reader to [65] for the details regarding each phase. This methodology provided us with a reproducible process of scientific paper selection starting from well-established research databases.

Concerning the projects that are not scientifically documented, namely those that did not publish a paper in renowned journals or proceedings, there are unfortunately no reference databases to search on. We stress that the habit to publish a white or yellow paper outside the usual scientific venues is quite common in the blockchain community, as also witnessed by the original paper by Sathoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", published in 2008. This is due to the aim and necessity of making these papers available to a wider audience.

Furthermore, web search engines provide results that vary over time. For these reasons, it is almost impossible to apply a procedure that can be easily reproduced, like PRISMA; hence, for the selection of the projects, we reverted to an informal web search.

We are conscious of the fact that, with this approach, we obtain a non-formally-defined sample of the current relevant projects for blockchain-based IoT economy. However, considering real-life projects is very important to understand the current state of the art of blockchain-enabled IoT economy, since, from the beginning of our search, we recognized that real projects, promoted by companies, startups, or communities, have to face challenges that are hardly encountered by scientific research projects. In particular, they have to face scalability problems, real users' interaction, and oddities of unpermissioned blockchains, such as market-dependent transaction fees, just to mention a few. Further, real-life projects often provide complete implementations (or at least plans) for many architectural aspects, which in scientific works may be overlooked. For these reasons, we consider fundamental the inclusion in our survey of real-life projects, even if, in their selection, we cannot follow a formal reproducible procedure.

4.2. Selection of Real-Life Projects and Applications

For searching out real-life projects and applications, we informally used web search (by the Google search engine), web navigation, and projects mentioned in the scientific literature, selecting elements that match the eligibility criteria discussed above and that provide a representative set of projects and applications relevant for the blockchain-enabled IoT economy. The results of our survey are shown in Table 3.

Table 3. A list of some prominent examples of applications or projects involving an IoT economy. For each mentioned application, the table indicates whether it is based on a public (Pub) or private (Priv) and permissioned (Perm) or unpermissioned (Unperm) blockchain. In the column "simplified flow", we emphasize the thing (T), the producer (P), the consumer (C), and the reward (R).

Reference	Short Description	Simplified Flow
Helium [66,67] (Pub, Unperm)	The Helium network is a decentralized wireless network that enables devices anywhere in the world to wirelessly connect to the Internet. Powering the Helium network is a blockchain with a token incentivizing a two-sided marketplace between coverage providers and coverage consumers. It employs the unique proof-of-coverage consensus.	Coverage providers (P) get a reward in HNT native tokens (R) to host gateways (T) in their premises to offer wireless connectivity—mostly LoRA—to coverage consumers (C) connecting their devices to the Helium network.
PlanetWatch [68,69] (Pub, Unperm)	PlanetWatch leverages advanced technologies and the engagement of local communities to raise the standards of environmental monitoring. It encourages citizens to operate sensors and consequently earn token rewards for their data streams, thus having the potential of a wide coverage.	A citizen (P) gets a reward in Planet native tokens (R) to host environmental sensors (T)—mostly for air pollution—in their premises. The data produced by those sensors are of interest for service providers or government agencies (C).
Fishcoin [70] (Pub, Unperm)	Fishcoin, with its trace protocol, provides a platform to trace, in-chain, all the steps of the fishing supply chain. Digital tokens are used as a means to incentive data sharing in a proportional way: the more you share, the more you earn.	Stakeholders in the fishing supply chain (P) host sensors (T) collecting data on fishing and fish trading all along the supply chain and get rewarded in Fish native token (R) from government agencies and decision makers (C) that currently have little data for 90% of seafood.
SingleEarth [71]	Instead of linking carbon and biodiversity credits to the sale of raw materials such as forests, which cause CO_2, Single.Earth proposes the "tokenize nature" concept. CO_2-producing materials that are kept in the ground are linked to tokens that can be bought by whoever want to contribute to keeping CO_2 low (for example, by regulation constraints).	Landowners (P) earn Merit native token (R) through nature conservation (T). Companies, organizations, and eventually individuals (C) will be able to purchase tokens and own fractional amounts of natural resources, rewarded with carbon and biodiversity offsets.

Table 3. *Cont.*

Reference	Short Description	Simplified Flow
SavePlanetEarth [72] (Pub, Unperm)	SavePlanetEarth (SPE) is a global initiative dedicated to developing an array of different programs to combat global warming and climate change.	SavePlanetEarth cryptocurrency (R) is offered to investors (C). A carbon credit market opens SPE as an investment for companies and individuals (P) to offset their carbon footprint (T). They can accomplish this by purchasing carbon credits and redeeming them on the blockchain, making everything transparent and verifiable.
Medicalchain [73] (Priv, Perm)	Medicalchain enables the user to give healthcare professionals access to their personal health data. Medicalchain then records interactions with this data in an auditable, transparent, and secure way on Medicalchain's distributed ledger, built using a dual-blockchain structure.	The Marketplace enables Medicalchain users or patients (P) to negotiate commercial terms, in MedTokens native tokens (R), with third parties and healthcare professionals (C) for the use of their personal and health records (T).
SolarCoin [74] (Pub, Perm)	Solar energy is now the cheapest fuel in over 150 countries. SolarCoin is a cryptocurrency that incentivizes a solar-powered planet distributing SolarCoin as a reward for solar installations.	Owners (P) of solar installations (T) get a reward in SolarCoin native tokens (R) from citizens or institutions (C) willing to give an incentive for the adoption of solar energy. SolarCoin can be traded for government currencies on cryptocurrency exchanges, or spent at businesses that accept them.
Smart car applications [75] (Pub, Unperm)	Data collection on cars and drivers experimented by Jaguar and Land Rover relying upon the IOTA infrastructure.	Drivers (P) install sensors in their car (T) to collect data on their driving habits, which are delivered to service providers and city authorities (C). Producers are rewarded in tokens (R) that can be used for paying, for instance, toll roads, electric charges, and parking fees.

Table 3. *Cont.*

Reference	Short Description	Simplified Flow
ElaadNL [76] (Pub, Unperm)	ElaadNL is a smart charging infrastructure lab founded by Dutch grid operators. It develops an autonomous self-balancing power grid using IOTA for Machine-to-Machine (M2M) communication, where machines pay each other in tokens as incentive to cooperate to balance energy consumption in the grid.	Nodes that charge batteries (P) are rewarded in IOTA cryptocurrency (R) when they help in balancing the grid (e.g., charging slowly), providing an advantage to owners (C) of Power Grid nodes (T) that produce electricity.
Power Ledger [77] (Priv, Perm)	In the era of Distributed Energy Resources (DER), Power Ledger is a trading platform, namely a network that allows consumers to sell energy to their peers in a trustless environment. The Power Ledger Platform provides a transparent governance framework that allows the ecosystem to seamlessly interface with energy markets around the globe.	Energy producers (P) realize the value of their investment in DER and POWR native token (R) by monetizing their excess energy (T) in much the same way as Uber and Airbnb allow people to monetize their cars and spare rooms by selling them to other people (C).
Industry Marketplace [78] (Pub, Unperm)	The Industry Marketplace is a vendor- and industry-neutral platform, based on IOTA, automating the trading of physical and digital goods and services. The initiative is targeted to support Industry 4.0 projects with Machine-to-Machine (M2M) economy.	Industry 4.0 machine components (T) act as independent service providers (P) and consumers (C). Transactions are performed in IOTA cryptocurrency (R).
Vehicles rental [79,80]	Scooter/car/bike rental in cities.	Veichles (T) are rent by renting companies (P) to people moving in the city (C) who pay the service using a cryptocurrency (R).

4.3. Selection of Scientific Works

We performed the identification phase of PRISMA, selecting Scopus [81] as our reference research article database. Scopus is the Elsevier's abstract and citation database, launched in 2004. It covers nearly 36,377 titles from approximately 11,678 publishers, of which 34,346 are peer-reviewed journals in top-level subject fields.

We used the search tool of Scopus to focus on papers related to blockchain as an IoT economy enabler. A query is always in the form TITLE-ABS-KEY (search keys in AND), which means retrieving documents that have in the title, abstracts, and keywords all the

specified search terms. Furthermore, we limited our analysis to the years between 2018 and 2021. As an example, the query for searching all documents with terms "iot AND blockchain AND economy" in the time range 2018–2021 is the following:

TITLE-ABS-KEY (iot AND blockchain AND economy) AND (LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018))

Table 4 reports the amount of documents retrieved by several relevant queries, where we only specify the search terms, for simplicity. We focus on the results of the queries "iot AND blockchain AND economy" (query *E*) and "iot AND blockchain AND payment" (query *P*).

Table 4. Queries and corresponding retrieved documents for our identification phase.

Search Terms	Documents Result
iot	75,704
blockchain	25,944
iot AND blockchain	4287
iot AND blockchain AND economy	141
iot AND blockchain AND payment	159

In the screening phase, we considered the 141 papers resulting from query *E* and the 159 papers from query *P*. We further restricted our attention to the ones with at least five citations. We obtained 38 papers for query *E* and 59 papers for query *P*, with an overlap of 6 papers.

In the eligibility phase, we analyzed the 91 papers resulting form the screening phase. Many of those works are reviews (with a different focus with respect to this paper), papers about economics, or highly focused on using the blockchain to provide security guarantees for IoT devices and communications, beyond the rewards transactions. We considered only those papers that propose new architectures, tools, projects, or applications strongly related to our reference scenario depicted in Figure 1. Further, we noted that, in many of the considered papers, the ability of implementing payments by blockchain infrastructures is simply mentioned as a key enabler, but architectural aspects (like those described in Section 7) are either not detailed or only partially described, and the specific financial tools (see Section 6) are not analyzed in depth. In fact, scientific papers usually have the objective of proposing new approaches, the validation of which is rarely performed by setting up a fully-fledged ecosystem. The final outcomes of this process, in view of the eligibility criteria listed in Section 4.1, are the 32 included papers [9,10,82–111].

Finally, in Table 5, we relate the content of the selected scientific works with the real-life projects listed in Table 3. This table shows that most of the main concepts, ideas, and tools presented in the scientific works are actually implemented in the selected real-life projects and applications, which furthermore have to face the technical challenges of a real deployment on the market—a key aspect for solutions aimed at exploiting the blockchain as IoT economy enabler. For this reason, we mostly rely on projects and applications listed in Table 3 as references for the survey of architectural aspects provided in Section 7 and of blockchain-based financial tools provided in Section 6.

Table 5. Projects and related scientific papers identified by the PRISMA methodology.

Project	Related Research Work, with Short Motivation
Helium [66,67]	As in Helium's proof of coverage, [98,107] devise new kinds of proofs for consensus related to the distribution of new software/firmware upgrades. In [108], a local 5G network is shared among several operators, as in Helium the network is shared by a multiplicity of devices. Newtork usage is paid in both works. In [111], an ad-hoc blockchain is proposed, as in Helium.
PlanetWatch [68,69]	PlanetWatch is an example of incentivizing green consumption behaviour. Green behavior is also addressed in [101] for dams and [84] for Industry 4.0.
Fishcoin [70]	Fishcoin proposes a data marketplace about fishery. Design and realization problems are quite similar to those considered in [85,96,103,111]. Fishcoin promotes the value of data with respect to their quality, a concept that is also discussed in [110], where they propose a reputation system for IoT data using a blockchain.
SingleEarth [71]	Green behavior is also addressed in [84].
SavePlanetEarth [72]	Green behavior is also addressed in [84].
Medicalchain [73]	Medicalchain proposes a data marketplace about personal health data, similar to the one devised in [95]. Moreover, design and realization problems are quite similar to those considered in [85] for smart cities and in [94,97] for a general-purpose sensor.
SolarCoin [74]	SolarCoin is an example of "consume less, consume locally" and green behaviour (as in [84]). This approach can be applied in other application contexts as well: for instance, the system in [99] encourages good behavior at home.
Smart car applications [75]	Smart car applications may involve the collection of data (e.g., related to driving habits). Design and realization problems for systems that are able to create a data marketplace are similar to those described in [85]. It is an example of the advanced and cyber-resilient automotive industry discussed in [83].
ElaadNL [76]	It is an example of the advanced and cyber-resilient automotive industry discussed in [83].
Power Ledger [77]	In [91], they describe a proof of concept where trading and payment of solar energy is managed on a blockchain.
Industry Marketplace [78]	The Industry Marketplace is a vendor- and industry-neutral platform, based on IOTA, that automates the trading of physical and digital goods and services. The authors of [88] present a distributed data marketplace allowing different actors to purchase and monitor data streams coming from the smart city thanks to the use of IOTA technology. In [90], IoT devices (e.g., smart locks, light bulbs, air conditioning, fans) are rented from a service provider. An industry market place can also support Industry 4.0 projects with Machine-to-Machine (M2M) economy, as proposed in [105], and Vehicle-to-Everything (V2X) economy, as proposed in [106].
Vehicles rental [79,80]	This is an example of the advanced and cyber-resilient automotive industry discussed in [83]. In [89], they show how digital technologies can support the appropriate and circular management of EEE (electrical and electronic equipment) products and WEEE (waste from electrical and electronic equipment). In [90], IoT devices (e.g. smart locks, light bulbs, air conditioning, fans) are rented from a service provider. The authors of [109] propose an architecture for a marketplace to (re)use an IoT device registered on the network by a provider. In [100], IoT devices are adopted by insurance companies to detect events in the real world and trigger transactions unlocking payment. The authors of [102] propose optimizing the rental operation using a multi-blockchain architecture. The concept of rental, involving interaction with an IoT device using a smart contract, is also addressed in [104].

5. Applications Classification According to Performance Requirements

In this Section, we introduce a classification of the IoT sample applications presented in Table 3 according to the performances that they require from the blockchain. Performance requirements impact certain design choices, which we describe in Section 7. The

classification provided in this section helps us to understand the most important aspects to consider when choosing a blockchain technology for an IoT ecosystem.

The evaluation of the performance of blockchain is a complex task that requires one to compare technologies with fairly different approaches (e.g., permissionless vs. permissioned blockchain) in search of appropriate trade-offs, the most important of which are well captured in the blockchain trilemma (see Section 2.3). As an example, it is possible to gain fairly good scalability in permissioned blockchain where a limited number of nodes can participate in the consensus, thus limiting the complexity of permissionless blockchain where every node can participate. However, this improvement in performance is clearly paid in terms of decentralization.

Recent works such as [112,113] are first attempts to provide a systematic survey of the performance of different blockchain approaches. While a number of performance metrics could potentially be considered in our discussion, we focus on two of the most relevant here: latency and transactions throughput.

The *latency* of a blockchain network is the time between the submission of a transaction to the network and the first confirmation of acceptance by the network in the blockchain. In certain technologies based on proof-of-work, after the first confirmation, the transaction becomes "more final" as more blocks are added beyond the initial confirmation. However, in the IoT case, the first confirmation is usually enough. In particular, when the IoT application involves micropayments, the cost of undoing on confirmation is much higher than the obtained advantage. For example, vehicle rental applications [79,80] may be based on micropayments, as well as the Helium [66] ecosystem.

The *transactions throughput* of a blockchain is the number of transactions handled per second, usually denoted by TPS. Table 6 in [112] shows that regardless of the adopted technology, in fairly limited evaluation environments that can only provide an upper bound on the performance, the latency is between about 0.1 s and 361 s, and the transactions throughput is between about 5 TPS and 6000 TPS. These numbers are in line with some other available performance evaluations [114] where Bitcoin performs 7 TPS, Ethereum 20, and Visa roughly 24,000 TPS.

Latency requirements are clearly application dependent. However, many applications require some sort of interaction with a human (e.g., a payment should be confirmed before the scooter is unlocked), which provides a guideline for latency. In the following, we consider a latency comparable to the one necessary to perform a payment by a credit/debit card, which involves the authorization of the card issuer, to be *low latency*. In processing credit cards transactions, 5 s is considered an upper bound; however, 10 is still tolerable. Similarly, we consider the current throughput of credit card circuits, namely an order of tens of thousands of TPS, to be a high transactions throughput. In this case, we also relax this constraint, considering a high throughput of the order of thousands of TPS to be satisfactory.

According to the above considerations, the applications considered in Table 3 can be classified as shown in Table 6. Note that applications with low (bounded) throughput are rare, since IoT technology is pervasive and tends to scale to a large number of IoT devices, unless there is some intrinsic limit in the application domain. We were not able to find any relevant application that requires low latency and is not throughput demanding.

Table 6. Classification of the applications in shown Table 3.

	Low Transactions Throughput	**High Transactions Throughput**
Low Transaction Latency	*We did not find any relevant examples in this class.*	This class is the most demanding in terms of blockchain technology. It includes applications in which a potentially unbounded number of IoT devices and/or human subjects transact and need a transaction receipt in an interactive manner. Examples in this class are Medicalchain [73], smart car applications [75], ElaadNL [76], Power Ledger [77], Industry Marketplace [78], and vehicle rentals [79,80].
High Transaction Latency	This class is the less demanding in terms of blockchain technology. It comprises applications in which the number of subjects and devices is intrinsically bounded (e.g., landowners) and payments are not interactive. An example of this class is Single.Earth [71].	The applications in this class are characterized by a potentially unbounded number of IoT devices and subjects. However, they do not need real-time payment. Examples in this class are Helium [66,67], PlanetWatch [68,69], Fishcoin [70], SavePlanetEarth [72], and SolarCoin [74].

6. Blockchain-Based Financial Tools for the IoT

Blockchain technology has had a close connection with finance since the beginning. It is well known that one of the main success story for blockchain is Bitcoin, the first cryptocurrency. Beside the original novelty of implementing transactions in a decentralized setting, it is now clear that blockchains enable a wide range of novel financial instruments, many of which are specific of blockchain-based economic systems.

In this section, we discuss some of them that we believe are of special interest for an IoT-based economy and focus on the technical and architectural aspects to enable them.

6.1. Guaranteed Payments and Funds Unlocking

Blockchain-enabled payments can be made arbitrarily complex. In simple cases, spending or transferring funds is allowed after proving their possession. However, in general, blockchain technologies support the adoption of a wide variety of conditions, such as the following examples:

(1) having the consent of m out of n other users ($1 \leq m \leq n$);
(2) checking the expiration of a deadline;
(3) checking that some other transaction has actually occurred.

Further, any logical combination of the above is possible, and since in IoT a device can signal the occurrence of a physical event in blockchain (by a suitable transaction [115,116]), this can be part of the condition as well. For example, this enables automated escrow systems [115,116], in which funds are unlocked when an actor executes some physical action. For blockchains that support smart contracts, any user that is entitled to create a smart contract can create his/her own custom conditions. For ad hoc blockchains with no smart contract support, this flexibility is also available, but decisions regarding which kind of conditions to adopt have to be made by the system designer in advance.

Sophisticated payments between parties are used in many use-cases: in SavePlanetEarth [72], individuals exchanges SPE tokens with NFTs representing carbon credits; in MedicalChain [73], medical researchers buy access to a relevant patient's health data in a marketplace, paying in cryptos. Escrow payments are adopted in [79], where a user who is willing to rent a vehicle directly buys an unlock token from a smart contract to activate the vehicle.

6.2. Tokens

Tokens are digital assets whose ownership is recorded in a blockchain. Almost all unpermissioned blockchain networks have a *native* token (more properly called *coins* or

cryptocurrencies). However, many technologies provide easy means to create new kinds of *non-native* tokens for specific purposes (see Section 2.2). Each kind of token (native or not) has specific rules according to which token units are created (we also say *minted* or *mined*), transferred, and destroyed (we also say *burned*). These rules are designed to fit the purpose of the token and can vary greatly among tokens. Some reasons to have custom tokens are the following:

- They can be given to a thing provider, owning a thing, as a reward for allowing other users to use that thing.
- They can be used as money to buy a service or data within the ecosystem.
- They can represent a specific real thing so that ownership of the thing is represented in blockchain by the ownership of the token. This is the case of *non-fungible tokens* (NFTs), also called *asset tokens*.
- They can be sold to investors and enthusiasts in the initial phase of a project for the purpose of raising fiat money funds by means of an Initial Coin Offer (see below). In turn, token holders get some rights within the newborn ecosystem, such as, for example, having access to an offered service at a lower price, getting a small share of the income, or expressing a vote for the governance of the project.
- They can be used as a security to represent a share of the value of the ecosystem that can be traded and exchanged on a market (see below).

The first three cases are realized by standard blockchain features, possibly integrated with capabilities of IoT devices to coordinate transactions with physical events. The last two cases require relying on exchange services, which might be completely independent of the IoT ecosystem or might be integrated with it.

In addition, approaches are possible where multiple tokens are used in a single ecosystem, where, for example, one token has the objective of representing the value of the ecosystem as a whole and is traded on the markets, and another serves as a cryptocurrency to buy and sell services in the ecosystem. The value of the second kind of token might be artificially anchored (*pegged*) to a fiat currency to keep the price of services within the ecosystem stable. This approach usually requires an oracle to observe the current exchange ratio of the first token with a fiat currency and an automatic way to transform the first kind of tokens into the second one, on demand. PlanetWatch [68] adopts two tokens with this perspective: Planet tokens are used as a mean to reward citizens for their provided measurements, and they are traded on the market; Earth Credits can be used to obtain services or products within the PlanetWatch ecosystem, and they can be exchanged either with euros, at a fixed price, or with Planet, at a price depending on its quotation. In Helium [66] and Powerledger [77], two tokens are similarly used.

It is worth mentioning that, since different sets of rules result in different "economic behavior", the new field of study called tokenomics (heavily based on game theory; see, for example, [6,117–120]) aims at understanding and foreseeing the effect of a certain set of rules.

Further information about the wide variety of possible tokens, their purposes, and their rules can be found in several works (see, for example, [121,122]).

6.3. Incentives

Incentives are an important part of any unpermissioned decentralized architecture. They are usually provided as tokens that reward a positive behavior and that can be converted into something valuable (e.g., fiat money or services) for whoever expressed that behavior. In general, in a blockchain, the reward is given for processing transactions and participating in the creation of new blocks. Integrating IoT with blockchain, we can provide incentives to motivate general positive behaviors, such as keeping some device active or hosting sensors. This may be not directly linked to a certain service or object to be actually used by anyone. In fact, there is some value just in having a part of the system be available for its use. This may motivate thing providers to join a project even in the very beginning phase, when end users are unlikely to buy any service. The possibility to reward service

availability with freshly created tokens is clearly a value added of the blockchain adoption, in which the token creation strategy can be decided as part of the design of the system. From an architectural point of view, the only critical point is to assess that the condition for the reward holds. Related information may either be directly obtained from smart devices or assessed by an oracle (see Section 7.3). Incentive mechanisms are present in all projects that are listed in Section 4. For example, in PlanetWatch [68], citizens are rewarded when their measurements are uploaded to the blockchain, and in Helium [66], rewards are given when thing providers contribute to prove-of-coverage and to route data.

6.4. Exchanges and Offsetting of Exchange Rates

Exchanges allow one to buy/sell tokens, either for other tokens or for fiat currency. They are fundamental services that allow people to buy tokens to be used in an ecosystem or to convert tokens earned in an ecosystem into fiat or other cryptocurrencies. They are normally centralized, but there are examples of blockchain-based decentralized exchanges [123,124], which can possibly be integrated into user applications [125]. Certain IoT ecosystems may have among their goals the purpose to create or facilitate a market. In this case, some form of decentralized market management may be part of the ecosystem. The Power Ledger project [77] is a prominent example of this approach for smart grids. A token that is traded in an exchange varies its *price* (or *exchange rate*) over time. This feature is considered good if the token is meant to represent the value of the ecosystem, since it allows the token owners to gain if the project is successful. On the other side, if the token is meant to be used to buy services or data in an ecosystem, excessive price inflation may have a catastrophic effect, possibly making the actual price of services or data offered in the ecosystem no longer competitive. It is possible to offset the latter problem by pure technological means. In fact, by means of an oracle, it is possible to record in the blockchain the exchange rate of a token with respect to a fiat currency. Clearly, transactions on a blockchain must be performed using a token; however, using the last exchange rate, it is possible to dynamically adjust service/data prices expressed with the token so that they are stable when expressed in fiat currency. In the vehicle-renting system devised in [79], at the time of renting, the client application exchanges money with a cryptocurrency (ETH in their case) in the background to maintain a constant rental cost. Similar approaches are realized by Helium [66] and Power Ledger [77].

6.5. Staking

As written above, using a blockchain, it can be possible to realize mechanisms that lock tokens and unlock them only when certain conditions hold. Imposing users to lock tokens before allowing them to do certain actions is called *staking*. Using blockchain, the realization of staking is easy. In fact, funds can be locked for a period of time, and it is enough to programmatically check the presence of the stake in blockchain before allowing the execution of the specific action. There are several reasons to adopt staking.

- A first use of staking is to guarantee that a user has correctly fulfilled a certain task. Clearly, there should be a way to assess the correct execution of the task. In the IoT world, this may encompass taking data from a device or from an oracle. If the task is executed correctly, the user can get the benefit of their work and continue their job (or stop and get staked tokens back). If the user is recognized to cheat, the user is deprived of their staked tokens. This approach is used in escrow systems and in proof-of-stake consensus algorithms. In IoT systems, for example, a user can promise to keep a device up and running and can guarantee his/her honesty by staking some tokens.
- Staking can be useful to avoid denial of service attacks and Sybil attacks [126]. In fact, an attacker can emulate a large number of users, nodes, or devices, essentially for free. In this way, the attacker can subvert certain systems (e.g., voting, blockchain consensus, or reputation systems). Forcing each user to stake some tokens makes the cost of the attack proportional to the amount of users, nodes, or devices being emulated. Note that this also impacts the IoT world, since cheap devices are usually

easy to clone maliciously. On the other hand, it is possible to create hard-to-clone devices by wiring private keys and having a public key infrastructure that signs corresponding certificates. However, this approach centralizes the trust in one, or a few, certification authorities, which is undesirable in a decentralized architecture. An example of a decentralized certification approach based on blockchain is described in [127].

- For projects that are valued using the price of a token, forcing users or thing providers to stake some tokens helps to reduce the amount of tokens in circulation. The more users or thing providers want to put tokens at stake, the higher is the demand for the token, and hence, according to the law of supply and demand, the higher is the price of the token. In other words, it is possible to obtain a non-speculative growth of the value of the token (i.e., a growth that matches the growth of the user base) by carefully designing the rules and adopting the blockchain to enforce them [128]. This approach is used in non-IoT blockchain-based services (e.g., [129,130]). Clearly, this is a general approach that can be fruitfully applied also in the context of blockchain-based IoT ecosystems.

For example, Helium [66] requires providers of validator nodes to put some Helium native tokens (HNT) at stake. In this case, staking increases the price of HNT. A complex system of penalties is not applied on staking, but rather, the amount of work reward is limited.

6.6. Burn-and-Mint Equilibrium

This approach was pioneered by the Factom blockchain-based data integrity service [131] and has now been adopted also in the IoT context by the Helium [66] network. In this model, the tokens paid by a consumer are not earned by anyone but simply burnt. This approach decouples the amount paid for data or services from the amount of tokens earned by the thing provider. Now, suppose one fixes the price p paid by the consumer in fiat currency and charges the consumer by the amount of tokens t that corresponds to p at the current exchange rate. To do that, the architecture has to include an oracle that regularly acquires the last exchange rate of the token and provides it to the blockchain to be used to compute the amount of tokens to be charged for each payment. Let B be the amount of burnt tokens in a certain unit of time. Let M be an amount of new tokens that is periodically minted and distributed among all nodes or thing providers proportionally to the job they have done in that period [128,132,133]. Let us assume M to be constant, and suppose we start from an equilibrium state in which $B = M$, and hence the amount of circulating tokens is constant over time. An increase in demand increases the burning rate B with respect to the constant token-minting rate M. Token scarcity makes the token price increase. In turn, a higher token price limits the demand, forcing B to stop increasing. Intuitively, the system is expected to settle into a new equilibrium at a higher price [128,132,133]. The opposite is true if demand decreases. Further, nothing prevents one from changing M artificially to achieve different objectives. A formal analysis of these kinds of blockchain-based economic systems can be found in [134].

7. Architectural Aspects of Blockchain-Based IoT Economy

When an IoT ecosystem is equipped with a blockchain, many aspects regarding the blockchain itself and how it is integrated with the rest of the ecosystem have to be carefully considered. The adoption of a blockchain is not free, but it raises problems (e.g., regarding scalability) that have to be addressed to allow a project to develop and work correctly and profitably. On the other hand, it is possible to recognize some blockchain design opportunities that become available when a blockchain is used in an IoT ecosystem.

In this section, we discuss the design problems and opportunities for an IoT–blockchain integration when the blockchain is primarily a payment enabler. Throughout this section, we refer to the projects and applications identified in Section 4 to provide practical examples of the discussed choices and problems. We also refer to the classification shown in Section 5

when dealing with performances. In the rest of this section, we first discuss problems and possible approaches and/or solutions to address them (Sections 7.1–7.5). Section 7.1 focus on high-level technology and deployment choices. Sections 7.2 and 7.3 focus on interfacing the blockchain with the rest of the ecosystem. Sections 7.6 and 7.7 focus on supporting high transactions throughput with low costs. Then, we address opportunities rising from the blockchain–IoT integration (Sections 7.6 and 7.7).

7.1. Blockchain Nodes: Technology and Deployment Choices

When adopting blockchain for an IoT application, we have three main options:

1. leverage an existing general-purpose public blockchain network;
2. leverage an existing blockchain technology while creating a distinct dedicated network;
3. create a new ad-hoc blockchain technology and a new corresponding network.

In order to reduce production costs and leverage the reputation and reliability of already deployed solutions, the first option is usually considered the most appropriate, and it is easy to find examples of this approach (see, for example, [75,76,78]). As already discussed, public permissionless blockchains also have the advantage of providing the highest guarantee in terms of security—a crucial requirement for the IoT economy—and to facilitate the employment of the obtained incentives in a wider ecosystem of heterogeneous applications and services. In Section 4, the reader can find many examples of projects adopting general-purpose unpermissioned blockchains. The main drawback of this approach is that the IoT application is going to depend on the fluctuations of the public blockchain, and in particular on its network load. Public networks may be congested by usage spikes due to speculations [135] or other applications [136], just to mention two relevant examples. Further, communities governing a general-purpose public blockchain may make choices (e.g., regarding architecture evolution or required node power) that may be in contrast with the needs or the design of the considered IoT application. For these reasons, in some scenarios a dedicated blockchain network may be preferred. In other words, a well-known blockchain technology can be adopted only for a specific application with a dedicated network. In this case, all the issues related to fluctuations can be more easily handled. MedicalChain [73] is an example of this approach implemented as a permissioned blockchain. However, permissioned blockchains have limited decentralization, as already discussed in Sections 1 and 2.3. The most ambitious multivendor IoT ecosystems would probably rely on unpermissioned blockchains.

The third approach is to develop an ad hoc blockchain technology to be deployed as a dedicated blockchain, typically on IoT gateways. This is more costly, but allows greater flexibility. For example, in the Helium [67] network, a specific blockchain is proposed that leverages the physical presence of devices on a territory, and their scarcity, to realize a new proof-of-coverage consensus algorithm. The work done by devices to achieve consensus is not wasted (as occurs in Bitcoin and in all blockchains based on regular proof-of-work), but is reused within the Helium ecosystem, realizing an elegant and efficient use of resources.

Regarding this third approach, a possible criticism is that an ad hoc dedicated blockchain may be considered less reliable than a general purpose public blockchain. In fact, we can expect a smaller community working on the codebase, and hence governance, bug fixing, and software updates are expected to be less effective. On the other side, an ad hoc technology is expected to be simpler and more focused on the needs of the specific IoT application.

In general, the trade-off between the possible greater efficiency of ad hoc solutions and the time necessary to acquire a satisfactory reputation with the wider public—key ingrediente for the success of an IoT economy—should be carefully evaluated.

7.2. Accessing a Blockchain from Resource-Constrained Devices

Since things and thing providers are often large in number, it is natural to consider hosting the nodes of the blockchain in the very same IoT devices. However, as remarked in Section 2.1, IoT devices are very often resource constrained and thus cannot always satisfy the requirements highlighted in Section 4. Figure 3 summarizes the possible roles of things

and gateways with respect to blockchain integration. Things are hardly suited to directly speak to the blockchain due to their limits, and usually, with current technology, they just rely on a distinct (trusted) device or service to submit blockchain transactions on their behalf. If they are attached to the blockchain, they can at most play the role of a light node.

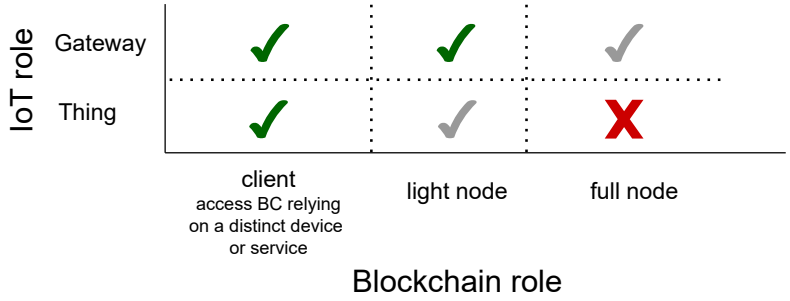

Figure 3. Summary of the possible blockchain roles that IoT devices can have.

If the IoT architecture encompasses a nearby gateway or a server of a fog computing layer (see Section 2.1 for more details), these can be directly exploited to interface the blockchain, surely in the role of a light node and, in certain cases, even as a regular full node. In this case, a gateway or a server can be used by its nearby things not only for connecting to the Internet but also to submit blockchain transactions.

In view of Figure 1, there are at least two fundamental use-cases to be supported regarding the interaction between IoT devices and the blockchain: a device should be able to interact with the blockchain (1) to perform payments and (2) to assess that a payment has been performed. Ideally, any device that has to perform these tasks should have access to the whole blockchain status (or history, depending on the technology). This is clearly unfeasible even for moderately powerful devices, such as, for example, mobile phones. To overcome this problem, light nodes adopt *simplified payment verification*, where Merkle proofs [31] are used as a means of verification of the information collected from untrusted nodes.

However, even simply collecting and storing these proofs is still well above the power of many IoT devices. The work in [137] analyzes this problem and surveys results about different SPV implementations in the context of healthcare applications. It is worth mentioning a new technology, Mina [64], which offers an elegant solution using advanced cryptography and recursive zk-SNARKs to reduce the size of the blockchain to tens of KB (instead of hundreds of GB). Instead of verifying the entire chain from the beginning of time (full node), participants fully verify the network and transactions using recursive zero-knowledge proofs (or zk-SNARKs). Nodes can then store the small proof (of constant size), as opposed to the entire chain. While very promising, the Mina protocol can be considered still in its infancy.

A more drastic solution that eases the adoption of very small IoT devices is to avoid having them store any proof. This means relying on an external centralized service to access the blockchain, which has to be considered trusted. An example of this approach is given by Helium [66]. While this may be considered secure enough for many applications, the introduction of a centralized element in the architecture has been regarded us unsatisfactory by some authors. For example, the INCUBED protocol [138] and other competing solutions [139,140] have the objective to provide very small devices with access to a blockchain without relying on a trusted third party.

Figure 4 summarizes the possible relations between things and a blockchain.

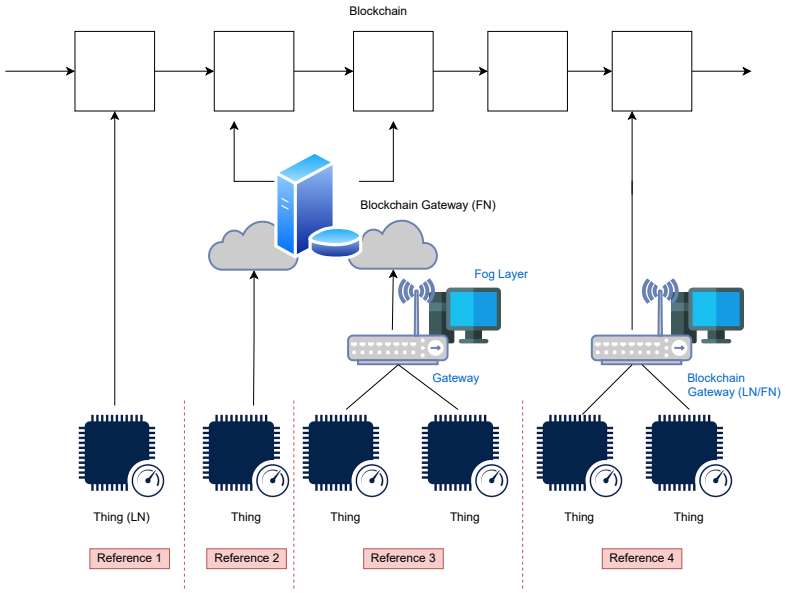

Figure 4. There are four main types of reference scenarios. In Reference 1, things have sufficient resources to operate autonomously as light nodes (LN). In Reference 2, things can autonomously be connected to the Internet, but their limited resources require them to rely upon third-party blockchain services to interact with the blockchain. In Reference 3, things need to rely on a gateway to access the Internet, but also in this case, the gateway or a server of a fog computing layer does not have sufficient resources to interact with the blockchain, and thus it relays on a third party. In Reference 4, things still need a gateway or an intermediate fog computing layer, but in this case, the gateway or the server has sufficient resources to run a light (LN) or full (FN) blockchain node.

7.3. Oracles: Interfacing the Blockchain with Off-Chain Data and Devices

Blockchains and smart contracts can only access data stored within the blockchain itself; on the contrary, IoT applications are ultimately designed to provide access to the physical world. This occurs, for example, in vehicle rentals [79,80], smart cars [75], and Industry Marketplace [78]. Blockchain technologies are designed to be deterministic, that is, when the whole transaction history is replayed it always ends up with the same results. Determinism is important so that blockchain nodes can come to a consensus [141]. If a smart contract requires accessing the measure of a smart meter, the value could differ from time to time, or even from place to place, causing nodes in the future, or without access to a certain site, to reach different conclusions about the state of the network, thus breaking the consensus. *Oracles* are components that allow a blockchain, or a smart contract, to get inputs from outside the blockchain. They inject data coming from outside the blockchain into regular blockchain transactions. In this way, they become part of the blockchain history and can be handled deterministically by all blockchain nodes.

There are several oracle services providing APIs to allow smart contracts to access external data. Examples include Chainlink [142], Provable [143], BandChain [144], and Tellor [145]. Oracle functionalities can even be part of an IoT ecosystem. For example, in Helium [66], certain nodes of the network are in charge of providing information about the exchange ratio of the Helium native token to keep the service price constant (see Section 6). This is a form of special-purpose oracle included in an IoT ecosystem.

Oracles can be classified according to the following aspects.

Origin of off-chain data. There are *software oracles* and *hardware oracles*. A software oracle handles information data that originates from online sources, like the prices of commodities and goods, flight or train delays, and so on. Therefore, it extracts the needed information from an online resource and pushes it into the smart contract. Hardware oracles allow smart contracts to gather information directly from the physical world, for example, a car crossing a barrier where movement sensors must

detect the vehicle and send the data to a smart contract [75], or RFID sensors in the supply chain industry [78].

Inbound/outbound oracles. *Inbound oracles* pull in-chain data from the external world. *Outbound oracles* provide smart contracts with the ability to send data to the outside world. An example would be a smart lock in the physical world, which receives payment on its blockchain address and needs to unlock automatically.

Degree of decentralization. Oracles can be centralized entities getting data from the off-chain world. However, using only one source of information could be risky and unreliable. For further security, a combination of different oracles may be used, where, for example, three out of five oracles could determine the outcome of an event. This combination of multiple oracles is called *consensus-based oracles*. ChainLink [142] and Tellor [145] are two examples of decentralized oracles. The special-purpose oracle of Helium mentioned above is consensus-based but has limited decentralization, since currently, only 11 fixed members can submit exchange ratio data (nine of them are anonymous for security reasons).

Figure 5 summarizes two methods of interaction of an IoT device with the blockchain. The thing can autonomously initiate the interaction with a smart contract. In this case, it acts as the source of a "standard" transaction invoking the smart contract; consequently, oracles are not necessary. If the thing is queried by the smart contract, oracles are required to guarantee the determinism and provide a consistent data view of the observed thing.

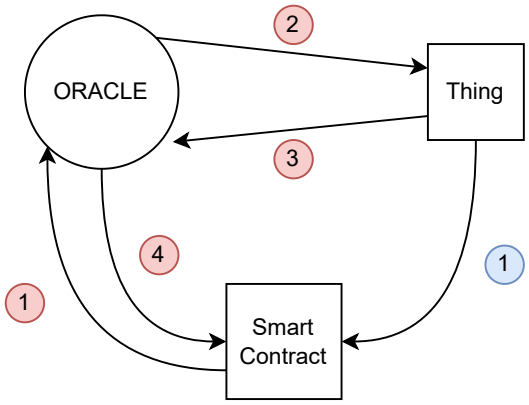

Figure 5. Methods of interaction of an IoT device with the blockchain. When the thing pushes data into the blockchain, it can autonomously start a transaction (1). In all the cases where a smart contract needs to access data available on a thing, it has to make a request to an oracle (1) that collects the data from the thing (2 and 3) and makes them available for any subsequent request (4), guaranteeing consistency.

7.4. Transactions Throughput, Fees, and Sidechains

As already observed, scalability (i.e., supported transactions per second) is a major issue when blockchain is applied to the IoT. It easy to observe that most of the sample applications shown in Section 4 can scale to a huge number of devices and require very high transaction throughput. Bitcoin, the first blockchain, is able to sustain only a small number of transactions per second (about 7). A vast amount of literature is available on blockchain scalability [34,35,146]. Newer technologies may sustain even several thousands transactions per second. However, since in many applications we expect a large number of micropayments, depending on the application and on the size of the network, even the faster blockchain technology might represent a bottleneck that imposes a strong limit on the expansion of an IoT ecosystem.

When resorting to a general-purpose public blockchain network, this problem is exacerbated by the fact that the blockchain is shared with a plethora of users that are unrelated

with our IoT application. For optimal functioning of the blockchain, they collectively have to generate a frequency of transactions below the maximum blockchain throughput.

Since resources of a publicly shared blockchain are scarce, and they are paid by users, the price users (or things) pay for their transactions is governed by the law of supply and demand. When the demand of transactions is close to the maximum transaction throughput, the nodes of the blockchain start picking transactions to be included in the next block, favoring those that pay more. For the most successful blockchains, this has led to very high transaction fees [147].

Further, the actual transaction cost depends on the exchange rate of the blockchain native token with respect to fiat currency, which may greatly vary over time. Certain unpermissioned blockchains have overcome this problem by proposing an approach in which transactions are feeless. Some of them are EOS [38], Nano [43], and IOTA [41]. They achieve this result by different approaches: moving the cost onto developers (EOS), asking for the users to participate in transaction confirmation (IOTA), and assuming operators of nodes have other interests beyond fees (Nano). Other approaches achieve low fees for most transactions (e.g., NEO [148]). However, even in those cases, scalability limits remain.

One solution to this problem is the adoption of *sidechains*, namely secondary blockchains connected to the main one, with a mechanism that allows bidirectional transfer of assets between the two chains. Sidechains may have their own consensus protocols specifically designed to improve scalability and interact programmatically [149] with the *mainchain* to provide the highest security guarantees and take advantage of well-reputed tokens and technologies.

Communication between the sidechain and mainchain are governed by a protocol that has to be realized with smart contracts and off-chain devices. A large number of proposals of protocols and technologies are available in the literature and as open projects [150–154]. Some IoT-specific contributions regarding sidechains are also present in literature [155–158].

In any case, it is important to note that, at the time of writing, current blockchain technologies do not provide higher transactions throughput when the number of nodes increases. This means that any blockchain imposes an upper bound on the frequency of transactions that can be processed; hence, it is important to choose the blockchain technology in accordance with the growth plans of the IoT network.

In certain cases, it is possible to adopt special high-transactions-throughput solutions for payment transactions based on payment channels (see Section 7.5).

7.5. State and Payment Channels

In certain IoT applications, the problem of limited maximum transactions throughput of blockchain technologies (see Section 7.4) can be effectively tackled with the adoption of the so-called payment channels. A typical problem is charging for the use of a service on the basis of how much it is used and doing that continuously while the service is running.

This was initially considered for incremental payment of video streaming, but the problem is relevant in typical IoT applications, such as vehicle renting [79,80].

Payment channels are one of the main ideas behind micropayment off-chain solutions, such as the Lightning Network [56]. In a *payment channel*, two entities (nodes or IoT devices), which are supposed to make a large number of small payments, agree to stake an amount of tokens to guarantee that they behave correctly in managing all micropayments off-chain. The blockchain is used when the channel is opened and the two parties stake their funds, and when the channel is closed and actual settlement is performed. Each micropayment is executed off-chain by exchanging partially signed transactions that commit each party to the new value of the settlement. These transactions are supposed not to be submitted for acceptance in the blockchain unless one of the two parties misbehaves and the channel has to be closed unilaterally, freezing the current balance. The complete technical details of this approach are very clearly explained in [159], and the performance of the Lighting Network in terms of efficiency and fee reduction are optimized for the IoT ecosystem in [9].

The technique can be extended to any kind of state change, and in this case, channels are more properly called *state channels*.

Payment channels are extremely convenient since transactions are not limited by the maximum throughput of the blockchain but only by network and hardware limits. Fees are not paid for each economic transaction, but only for opening and closing transactions, which makes the adoption of a general-purpose unpermissioned blockchain much safer. In any case, the same technique can be used also in dedicated blockchains. This is the approach of Helium [66], in which payments of the Helium packet-forwarding service are performed using payment channels where the corresponding open and closing transactions are submitted on the Helium dedicated chain.

7.6. Smart Contracts

One of the fundamental aspects of the blockchain is that it allows the realization of automatic behavior, which usually bring some financial effect, without relying on a trusted centralized third party. This has opened the possibility of realizing automatic versions of well-known economic mechanisms or creating new ones that can exist only in a blockchain-based economic environment. Some of the most relevant, for the IoT contexts, are discussed in Section 6.

All blockchains provide a consensus mechanism to accept and order transactions (see Section 2.2). In principle, transactions may be limited to the simple creation and transfer of tokens. However, the need for more complex transactions was quickly recognized (see Section 6). In general, when designing a blockchain, there is great flexibility in the kind of transaction that can be realized. However, at least for general-purpose blockchains, the spectrum of possible useful kinds of transactions is so wide that it is impossible to realize, natively, all possible kinds of transactions.

For this reason, almost all general-purpose blockchains (starting from Bitcoin) have some form of scripting language that allows the user to adapt the rules to accept transactions according to his/her needs. In general, we define a *smart contract* as software that runs in a decentralized manner on a blockchain, allowing the developer to customize the rules according to which the transaction should be accepted. With the introduction of Ethereum [37], smart contracts acquired enough power and flexibility to allow very general applications: transactions can invoke smart contracts, smart contracts can record data to be used in subsequent invocations (i.e., they have a state), and the application logic can manage funds that are under the control of the smart contract (see, for example, Solidity [160]).

While this flexibility is very appealing, it is worth noting that it has a significant cost. In fact, smart contracts require a very controlled execution environment (a so-called *virtual machine* (e.g., see [161])) that impacts on the efficiency of their execution. Further, the development of smart contracts has been recognized to be quite critical from the security point of view [162], in the sense that it is hard to code safe smart contracts.

Given this difficulty and the fact that smart contracts may control large amounts of tokens (i.e., money), they are among the preferred targets of hacking activities.

As an example, the Helium project encompasses an ad hoc blockchain that does not support smart contracts. Its very specific functionalities are hardcoded in the helium software.

7.7. Consensus Mechanisms Based on Physical Properties

While this paper is mostly focused on the advantages that blockchain can provide to IoT ecosystems, there is also an interesting advantage in the opposite direction. In fact, in an unpermissioned blockchain, the way in which the consensus on the next block is achieved is extremely critical for the security of the whole system. The main problem is that a simple vote-based approach is insecure. In fact, for an attacker, it is easy to emulate a large number of nodes (an approach known as *Sybil attack*) to obtain the majority in a decision. For this reason, it has to require some effort to participate in the consensus. In regular blockchains, the most famous approaches to this problem are the so-called *proof-of-work*, in which participants have to prove that they have solved a cryptographic puzzle, and

proof-of-stake, in which participants have to prove that have staked (i.e., frozen for a certain amount of time) a certain amount of tokens (see also Section 6).

A special-pupose blockchain in an IoT ecosystem can take advantage of the physical existence of IoT devices to obtain a high level of security while asking participants to perform some work that is useful for the ecosystem. For example, in Helium [67], consensus security is based on a so-called *proof-of-coverage*. In this approach, participants regularly challenge *hot-spots* to assess their coverage of a certain area. This kind of work cannot be easily scaled programmatically, since physical presence near the hot-spot is required. At the same time, this monitoring activity is reported to the users as valuable information about areas covered by the Helium network [163].

Certain constraints or tasks that are available in an IoT ecosystem can be used to create special-purpose consensus mechanisms. In our opinion, this is an aspect that is underutilized. For example, SolarCoin [74] encompasses the concept of *verified energy production*; however, this concept is not exploited for consensus.

Other approaches based on physical properties were proposed in the literature and are candidates to be used in IoT ecosystems; see, for example, [164,165] and the surveys [166,167].

8. Conclusions and Open Problems

We surveyed the relevant architectural aspects of blockchain–IoT integration for the IoT-based economy. In particular, we focused on the adoption of unpermissioned blockchains that enable decentralized architectures.

Our analysis can be summarized as follows.

- The blockchain technology enables payments and several other financial tools in a decentralized way, which may be very relevant for IoT ecosystems. We listed a number of IoT projects and functioning ecosystems that are based on blockchain technologies to support payments and other economic aspects (like tuning a service price to compensate for exchange rate fluctuations).
- A wide range of IoT applications require the blockchain to support a high transaction throughput, which usually depends on the amount of smart devices deployed. On the contrary, in current blockchain technology, the maximum transaction throughput does not increase when new nodes are added. This require a careful planning, and/or design, to avoid the risk of the blockchain being a choke point in the development of an IoT network. However, approaches such as sidechains, payment channels, or dedicated blockchains may mitigate this problem.
- The landscape of the projects that exploit blockchain capabilities to support the IoT-based economy has currently only a few highlights. In our opinion, currently, the most interesting projects are Helium [66] and Power Ledger [77] for their integrated approach, their ambitious goals, and the degree of development. We found promising projects that are, however, currently only starting; some adopt a simple and old approach, and others are run by a single company with a centralized approach.

The analysis carried out in this paper led us to recognize the following problems that are relevant and, in our opinion, if successfully addressed, can ease the adoption of blockchain in an IoT ecosystem as payment enabler.

- The IoT–blockchain integration has many problems and many opportunities. From the projects we analyzed, we understand that, currently, a regular blockchain is very often adopted, overlooking problems (mostly those that are scalability-related) and not exploiting opportunities (especially those related to new economic/financial tools enabled by the blockchain). We think there are two reasons for this: (1) lack of comprehensive information on the topic and (2) difficulty in realizing the needed solutions from current available technology elements.
- Regular blockchains are quite general but may not be very well suited for IoT integration. In particular, the main concerns are scalability, transaction cost, possibly

unneeded functionalities (such as smart contracts), and the general requirements of quite powerful hardware to run a regular node. On the other hand, we understand that a project may not have resources and/or expertise to develop an ad hoc blockchain for its own ecosystem from scratch.

With respect to the second item, it is interesting to note that most of the listed concerns are likely to be of interest to most IoT projects that aim to scale to a large number of devices and transactions.

From the above considerations, there are some research directions that can be suggested. The following are those that we think may be more valuable to pursue to ease adoption of blockchain as an IoT economy enabler.

- Devise a methodology to guide IoT ecosystem designers to exploit the blockchain-based financial tools and the available blockchain architecture alternatives.
- Develop an open-software low-footprint easily customizable blockchain to be used as unpermissioned ad hoc blockchain in an IoT ecosystem. This would ease the blockchain adoption in new IoT ecosystems at low cost without introducing a dependency on any general-purpose blockchain.
- Evolve the blockchain state of the art toward scalable models that can be adopted in IoT ecosystems.

Author Contributions: All authors contributed equally to the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by Sapienza Ateneo Research grant "La disintermediazione della Pubblica Amministrazione: il ruolo della tecnologia blockchain e le sue implicazioni nei processi e nei ruoli della PA"This research was partially funded by POR FESR LAZIO 2014–2020, call for "Gruppi di ricerca 2020". Det. n. G04052 of 4 April 2019, under the "LazioChain" project, CUP F85F21001550009 - POR project code A0375E0116.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Rathore, M.M.; Paul, A.; Hong, W.H.; Seo, H.; Awan, I.; Saeed, S. Exploiting IoT and big data analytics: Defining Smart Digital City using real-time urban data. *Sustain. Cities Soc.* **2018**, *40*, 600–610. [CrossRef]
2. Compare, M.; Baraldi, P.; Zio, E. Challenges to IoT-Enabled Predictive Maintenance for Industry 4.0. *IEEE Internet Things J.* **2020**, *7*, 4585–4597. [CrossRef]
3. Borelli, E.; Paolini, G.; Antoniazzi, F.; Barbiroli, M.; Benassi, F.; Chesani, F.; Chiari, L.; Fantini, M.; Fuschini, F.; Galassi, A.; et al. HABITAT: An IoT Solution for Independent Elderly. *Sensors* **2019**, *19*, 1258. [CrossRef] [PubMed]
4. Gupta, D.; Bhatt, S.; Gupta, M.; Tosun, A.S. Future Smart Connected Communities to Fight COVID-19 Outbreak. *Internet Things* **2021**, *13*, 100342. [CrossRef]
5. Huckle, S.; Bhattacharya, R.; White, M.; Beloff, N. Internet of Things, Blockchain and Shared Economy Applications. *Procedia Comput. Sci.* **2016**, *98*, 461–466. [CrossRef]
6. Tan, L. *Token Economics Framework*; SSRN Scholarly Paper ID 3381452; Social Science Research Network: Rochester, NY, USA, 2019. [CrossRef]
7. Ishmaev, G. The Ethical Limits of Blockchain-Enabled Markets for Private IoT Data. *Philos. Technol.* **2020**, *33*, 411–432. [CrossRef]
8. Mercan, S.; Kurt, A.; Erdin, E.; Akkaya, K. Cryptocurrency Solutions to Enable Micro-payments in Consumer IoT. *IEEE Consum. Electron. Mag.* **2021**, 97–103. [CrossRef]
9. Robert, J.; Kubler, S.; Ghatpande, S. Enhanced Lightning Network (off-chain)-based micropayment in IoT ecosystems. *Future Gener. Comput. Syst.* **2020**, *112*, 283–296. [CrossRef]
10. Ensor, A.; Schefer-Wenzl, S.; Miladinovic, I. Blockchains for IoT payments: A survey. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6. [CrossRef]
11. Strugar, D.; Hussain, R.; Mazzara, M.; Rivera, V.; Young Lee, J.; Mustafin, R. On M2M micropayments: A case study of electric autonomous vehicles. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green

Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1697–1700. [CrossRef]
12. Lundqvist, T.; de Blanche, A.; Andersson, H.R.H. Thing-to-thing electricity micro payments using blockchain technology. In Proceedings of the 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6. [CrossRef]
13. Burchert, C.; Decker, C.; Wattenhofer, R. Scalable funding of Bitcoin micropayment channel networks. *R. Soc. Open Sci.* **2018**, *5*, 180089–180089. [CrossRef]
14. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors* **2018**, *18*, 2575. [CrossRef]
15. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
16. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
17. Salman, O.; Elhajj, I.; Chehab, A.; Kayssi, A. IoT survey: An SDN and fog computing perspective. *Comput. Netw.* **2018**, *143*, 221–246. [CrossRef]
18. LoRa Alliance®. LoRaWAN for Developers. 2021. Available online: https://lora-alliance.org/lorawan-for-developers (accessed on 29 November 2021).
19. SIGFOX.COM. 2022. Available online: https://www.sigfox.com/en/what-sigfox/technology (accessed on 11 March 2022).
20. Beniwal, G.; Singhrova, A. A systematic literature review on IoT gateways. *J. King Saud Univ. Comput. Inf. Sci.* **2021**, *in press*. [CrossRef]
21. Bormann, C.; Ersue, M.; Keränen, A. *Terminology for Constrained-Node Networks*; RFC 7228; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2014. [CrossRef]
22. Prince, B.; Prince, D. Embedded Flash and EEPROM for Smart IoT. In *Memories for the Intelligent Internet of Things*; John Wiley & Sons, Ltd.: Chichester, UK, 2018; pp. 89–168. [CrossRef]
23. Tosi, J.; Taffoni, F.; Santacatterina, M.; Sannino, R.; Formica, D. Performance Evaluation of Bluetooth Low Energy: A Systematic Review. *Sensors* **2017**, *17*, 2898. [CrossRef] [PubMed]
24. Farahani, S. Chapter 2—ZigBee/IEEE 802.15.4 networking examples. In *ZigBee Wireless Networks and Transceivers*; Elsevier: Amsterdam, The Netherlands, 2008; pp. 25–32. [CrossRef]
25. Adelantado, F.; Vilajosana, X.; Tuset-Peiro, P.; Martinez, B.; Melia-Segui, J.; Watteyne, T. Understanding the Limits of LoRaWAN. *IEEE Commun. Mag.* **2017**, *55*, 34–40. [CrossRef]
26. Yousefpour, A.; Fung, C.; Nguyen, T.; Kadiyala, K.; Jalali, F.; Niakanlahiji, A.; Kong, J.; Jue, J.P. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *J. Syst. Archit.* **2019**, *98*, 289–330. [CrossRef]
27. Antal, C.; Cioara, T.; Anghel, I.; Antal, M.; Salomie, I. Distributed ledger technology review and decentralized applications development guidelines. *Future Internet* **2021**, *13*, 62. [CrossRef]
28. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
29. Xiong, H.; Chen, M.; Wu, C.; Zhao, Y.; Yi, W. Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms. *Future Inter.* **2022**, *14*, 47. [CrossRef]
30. Ferdous, M.S.; Chowdhury, M.J.M.; Hoque, M.A. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *J. Netw. Comput. Appl.* **2021**, *182*, 103035. [CrossRef]
31. Tamassia, R. Authenticated data structures. In *Algorithms—ESA 2003*; Springer: Berlin/Heidelberg, Germnay, 2003; Volume 2832, pp. 2–5.
32. Pennino, D.; Pizzonia, M.; Papi, A. Overlay indexes: Efficiently supporting aggregate range queries and authenticated data structures in off-the-shelf databases. *IEEE Access* **2019**, *7*, 175642–175670. [CrossRef]
33. Pennino, D.; Pizzonia, M.; Griscioli, F. Pipeline-integrity: Scaling the use of authenticated data structures up to the cloud. *Future Gener. Comput. Syst.* **2019**, *100*, 618–647. [CrossRef]
34. Bernardini, M.; Pennino, D.; Pizzonia, M. Blockchains meet distributed hash tables: Decoupling validation from state storage. In Proceedings of the Second Distributed Ledger Technology Workshop, DLT@ITASEC 2019, Pisa, Italy, 12 February 2019; Volume 2334, pp. 43–55.
35. Leung, D.; Suhl, A.; Gilad, Y.; Zeldovich, N. Vault: Fast bootstrapping for the Algorand Cryptocurrency. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA, 24–27 February 2019.
36. Ethereum Nodes and Clients. Available online: https://ethereum.org/en/developers/docs/nodes-and-clients/ (accessed on 17 January 2022).
37. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
38. Eosio Documentation. 2021. Available online: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md (accessed 20 December 2021).
39. Al-Breiki, H.; Rehman, M.H.U.; Salah, K.; Svetinovic, D. Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE Access* **2020**, *8*, 85675–85685. [CrossRef]
40. Ethash. Available online: https://eth.wiki/en/concepts/ethash/ethash (accessed on 28 March 2022).
41. Popov, S. The Tangle White Paper. 2018. Available online: http://www.descryptions.com/Iota.pdf (accessed on 28 March 2022).
42. Churyumov, A. Byteball: A decentralized system for storage and transfer of value. Available online: https://byteball.org/Byteball.pdf (accessed on 28 March 2022).

43. Nano. Eco-Friendly and Feeless Digital Currency. Available online: https://nano.org/ (accessed on 17 January 2022).
44. The Ethereum Community. ERC-20 Token Standard. Available online: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/ (accessed on 18 January 2022).
45. Zhang, E. NEP-17 Token Standard. Available online: https://github.com/neo-project/proposals/blob/master/nep-17.mediawiki (accessed on 18 January 2022).
46. Algorand. Algorand Standard Assets (ASAs). Available online: https://developer.algorand.org/docs/get-details/asa/ (accessed on 18 January 2022).
47. Dotan, M.; Pignolet, Y.A.; Schmid, S.; Tochner, S.; Zohar, A. Survey on blockchain networking: Context, state-of-the-art, challenges. *ACM Comput. Surv.* **2021**, *54*, 1–34. [CrossRef]
48. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy Challenges. *Internet Things* **2019**, *8*, 100107. [CrossRef]
49. Ethereum Wiki Project. Scalability Trilemma. Available online: https://eth.wiki/en/sharding/Sharding-FAQs#this-sounds-like-theres-some-kind-of-scalability-trilemma-at-play-what-is-this-trilemma-and-can-we-break-through-it (accessed on 26 January 2022).
50. Cirillo, A.; Dalena, V.; Mauro, A.; Mogavero, F.; Pennino, D.; Pizzonia, M.; Vitaletti, A.; Zecchini, M. Empowering citizens by a blockchain-Based Robinson list. *Int. J. Comput. Appl.* 2021, *to appear*.
51. Monte, G.D.; Pennino, D.; Pizzonia, M. Scaling blockchains without giving up decentralization and security: a solution to the blockchain scalability trilemma. In Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems, London, UK, 25 September 2020; pp. 71–76.
52. Yu, G.; Wang, X.; Yu, K.; Ni, W.; Zhang, J.A.; Liu, R.P. Survey: Sharding in blockchains. *IEEE Access* **2020**, *8*, 14155–14181. [CrossRef]
53. Chen, J.; Micali, S. Algorand: A secure and efficient distributed ledger. *Theor. Comput. Sci.* **2019**, *777*, 155–183. [CrossRef]
54. How Algorand Is Building a Scalable Blockchain Ecosystem. Available online: https://www.algorand.com/resources/blog/algorand-building-scalable-sustainable-blockchain-ecosystem (accessed on 9 March 2022).
55. Sguanci, C.; Spatafora, R.; Vergani, A.M. Layer 2 blockchain scaling: A survey. *arXiv* **2021**, arXiv:2107.10881.
56. Poon, J.; Dryja, T. The Bitcoin Lightning Network: Scalable off-Chain Instant Payments. 2016. Available online: https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf (accessed on 28 March 2022).
57. Raiden Network. 2021. Available online: https://raiden.network (accessed on 26 January 2022).
58. Polygon Technology. 2021. Available online: https://polygon.technology/lightpaper-polygon.pdf (accessed on 20 December 2021).
59. Buterin, V. Zk-SNARKs: Under the Hood—Vitalik Buterin—Medium. 2018. Available online: https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6 (accessed on 26 January 2022).
60. Hermez. 2022. Available online: https://hermez.io (accessed on 26 January 2022).
61. Optimism. 2022. Available online: https://www.optimism.io (accessed on 26 January 2022).
62. Offchain Labs—Building Arbitrum for Secure Ethereum Dapps. 2022. Available online: https://offchainlabs.com/#tech (accessed on 26 January 2022).
63. Blockchainsllc. In3. 2021. Available online: https://github.com/blockchainsllc/in3 (accessed on 12 December 2021).
64. Mina Protocol Overview. 2021. Available online: https://docs.minaprotocol.com/en (accessed on 9 November 2021).
65. Page, M.J.; Moher, D.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. *BMJ* **2021**, *372*, n160. [CrossRef]
66. Helium, People-Powered Networks. 2021. Available online: https://www.helium.com/ (accessed on 30 November 2021).
67. Haleem, A.; Allen, A.; Thompson, A.; Nijdam, M.; Garg, R. Helium Whitepaper: A Decentralized Wireless Network. 2021. Available online: http://whitepaper.helium.com/ (accessed on 30 November 2021).
68. Planetwatch|Air Quality Affects Your Health. Look After the Air You Breath. Available online: https://www.planetwatch.io (accessed on 29 October 2021).
69. Planetwatch|Whitepaper. Available online: https://www.planetwatch.io/white-paper/pdf/white-paper.pdf (accessed on 29 October 2021).
70. Trace Protocol—Fishcoin Project. Available online: https://fishcoin.co/fishcoin-protocol (accessed on 29 October 2021).
71. Single.Earth. Make a Positive Climate Impact NATURE-BACKED FINANCE. Available online: https://www.single.earth/ (accessed on 29 October 2021).
72. SavePlanetEarth (SPE). Whitepaper: A Carbon Sequestration Crypto Project. Available online: https://saveplanetearth.io/SPE_WhitePaper.pdf (accessed on 30 November 2021).
73. Medicalchain. Whitepaper: Own Your Health. Available online: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf (accessed on 30 November 2021).
74. Solarcoin. Whitepaper. Available online: https://www.allcryptowhitepapers.com/solarcoin-whitepaper/ (accessed on 29 October 2021).
75. On the Money: Earn as You Drive with Jaguar Land Rover. 2019. Available online: https://www.jaguarlandrover.com/news/2019/04/money-earn-you-drive-jaguar-land-rover (accessed on 16 November 2021).

76. ElaadNL Develops Autonomous Self-Balancing Power Grid Using IOTA. 2019. Available online: https://blog.iota.org/elaadnl-develops-autonomous-self-balancing-power-grid-using-iota-de52e9638548/ (accessed on 16 November 2021).
77. Power Ledger Whitepaper. Available online: https://www.powerledger.io/company/power-ledger-whitepaper (accessed on 29 October 2021).
78. IoTA Marketplace. Available online: https://data.iota.org/#/ (accessed on 29 October 2021).
79. Valaštín, V.; Košt'ál, K.; Bencel, R.; Kotuliak, I. Blockchain based car-sharing platform. In Proceedings of the 2019 International Symposium ELMAR, Zadar, Croatia, 23–25 September 2019; pp. 5–8. [CrossRef]
80. Zhou, Q.; Yang, Z.; Zhang, K.; Zheng, K.; Liu, J. A decentralized car-sharing control scheme based on smart contract in internet-of-vehicles. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5. [CrossRef]
81. Elsevier. About Scopus—Abstract and Citation Database|Elsevier. 2022. Available online: https://www.elsevier.com/solutions/scopus (accessed on 11 Marh 2022).
82. Rahman, M.; Rashid, M.; Shamim Hossain, M.; Hassanain, E.; Alhamid, M.; Guizani, M. Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City. *IEEE Access* **2019**, *7*, 18611–18621. ACCESS.2019.2896065. [CrossRef]
83. Fraga-Lamas, P.; Fernández-Caramés, T. A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access* **2019**, *7*, 17578–17598. [CrossRef]
84. Esmaeilian, B.; Sarkis, J.; Lewis, K.; Behdad, S. Blockchain for the future of sustainable supply chain management in Industry 4.0. *Resour. Conserv. Recycl.* **2020**, *163*, 105064. [CrossRef]
85. Ramachandran, G.; Radhakrishnan, R.; Krishnamachari, B. Towards a decentralized data marketplace for smart cities. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), Kansas, MO, USA, 16–19 September 2018. [CrossRef]
86. Wu, Y.; Dai, H.N.; Wang, H. Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0. *IEEE Internet Things J.* **2021**, *8*, 2300–2317. [CrossRef]
87. Lin, W.; Huang, X.; Fang, H.; Wang, V.; Hua, Y.; Wang, J.; Yin, H.; Yi, D.; Yau, L. Blockchain Technology in Current Agricultural Systems: From Techniques to Applications. *IEEE Access* **2020**, *8*, 143920–143937. [CrossRef]
88. Perboli, G.; Manfredi, A.; Musso, S.; Rosano, M. A decentralized marketplace for M2M economy for smart cities. In Proceedings of the 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 12–14 June 2019; pp. 27–30. [CrossRef]
89. Magrini, C.; Nicolas, J.; Berg, H.; Bellini, A.; Paolini, E.; Vincenti, N.; Campadello, L.; Bonoli, A. Using internet of things and distributed ledger technology for digital circular economy enablement: The case of electronic equipment. *Sustainability* **2021**, *13*, 4982. [CrossRef]
90. Rahman, M.; Loukas, G.; Abdullah, S.; Abdu, A.; Rahman, S.; Hassanain, E.; Arafa, Y. Blockchain and IoT-based secure multimedia retrieval system for a massive crowd: Sharing economy perspective. In Proceedings of the 2019 on International Conference on Multimedia Retrieval, Ottawa, ON, Canada, 10–13 June 2019; pp. 404–407. [CrossRef]
91. Themistocleous, M.; Stefanou, K.; Iosif, E. Blockchain in solar energy. *Cyprus Rev.* **2018**, *30*, 203–212.
92. Henesey, L.; Lizneva, Y.; Philipp, R.; Meyer, C.; Gerlitz, L. Improved load planning of RoRo vessels by adopting blockchain and internet-of-things. In Proceedings of the 22nd International Conference on Harbor, Maritime & Multimodal Logistics Modelling and Simulation, Athens, Greece, 15 May–15 June 2020; 58–65. [CrossRef]
93. Chuang, I.H.; Huang, S.H.; Chao, W.C.; Tsai, J.S.; Kuo, Y.H. TIDES: A Trust-Aware IoT Data Economic System with Blockchain-Enabled Multi-Access Edge Computing. *IEEE Access* **2020**, *8*, 85839–85855. [CrossRef]
94. Lamtzidis, O.; Gialelis, J. An IOTA Based Distributed Sensor Node System. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018. [CrossRef]
95. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access* **2018**, *6*, 32700–32726. [CrossRef]
96. Hasan, H.; AlHadhrami, E.; AlDhaheri, A.; Salah, K.; Jayaraman, R. Smart contract-based approach for efficient shipment management. *Comput. Ind. Eng.* **2019**, *136*, 149–159. [CrossRef]
97. 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; pp. 339–346. [CrossRef]
98. Leiba, O.; Yitzchak, Y.; Bitton, R.; Nadler, A.; Shabtai, A. Incentivized delivery network of iot software updates based on trustless proof-of-distribution. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), London, UK, 23–27 April 2018; pp. 29–39. [CrossRef]
99. Suchaad, S.A.; Mashiko, K.; Ismail, N.B.; Abidin, M.H.Z. Blockchain use in home automation for children incentives in parental control. In Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence, Hanoi, Vietnam, 28–30 September 2018; pp. 50–53. [CrossRef]
100. Mahmoud, O.; Kopp, H.; Abdelhamid, A.T.; Kargl, F. Applications of smart-contracts: anonymous decentralized insurances with IoT sensors. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1507–1512. [CrossRef]

101. Youssef, S.B.H.; Rekhis, S.; Boudriga, N. A blockchain based secure IoT solution for the dam surveillance. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6.
102. Oktian, Y.E.; Lee, S.G.; Lee, H.J. Hierarchical multi-blockchain architecture for scalable internet of things environment. *Electronics* **2020**, *9*, 1050. [CrossRef]
103. Umamaheswari, S.; Sreeram, S.; Kritika, N.; Prasanth, D.J. Biot: Blockchain based IoT for agriculture. In Proceedings of the 2019 11th International Conference on Advanced Computing (ICoAC), Chennai, India, 18–20 December 2019; pp. 324–327.
104. Fotiou, N.; Siris, V.A.; Polyzos, G.C. Interacting with the Internet of Things using smart contracts and blockchain technologies. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Melbourne, NSW, Australia, 14–17 July 2018; pp. 443–452.
105. Gong, X.; Liu, E.; Wang, R. Blockchain-based IoT application using smart contracts: Case study of M2M autonomous trading. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15–18 May 2020; pp. 781–785.
106. Jabbar, R.; Fetais, N.; Kharbeche, M.; Krichen, M.; Barkaoui, K.; Shinoy, M. Blockchain for the Internet of vehicles: How to use blockchain to secure vehicle-to-everything (V2X) communication and payment? *IEEE Sens. J.* **2021**, *21*, 15807–15823. [CrossRef]
107. Leiba, O.; Bitton, R.; Yitzchak, Y.; Nadler, A.; Kashi, D.; Shabtai, A. IoTPatchPool: Incentivized delivery network of IoT software updates based on proofs-of-distribution. *Pervasive Mob. Comput.* **2019**, *58*, 101019. [CrossRef]
108. Weerasinghe, N.; Hewa, T.; Liyanage, M.; Kanhere, S.S.; Ylianttila, M. A novel blockchain-as-a-service (BaaS) platform for local 5G operators. *IEEE Open J. Commun. Soc.* **2021**, *2*, 575–601. [CrossRef]
109. 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; pp. 312–320.
110. Javaid, A.; Zahid, M.; Ali, I.; Khan, R.J.U.H.; Noshad, Z.; Javaid, N. Reputation system for IoT data monetization using blockchain. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Antwerp, Belgium, 7–9 November 2019; pp. 173–184.
111. Hamdaoui, B.; Alkalbani, M.; Rayes, A.; Zorba, N. IoTShare: A blockchain-enabled IoT resource sharing on-demand protocol for smart city situation-awareness applications. *IEEE Internet Things J.* **2020**, *7*, 10548–10561. [CrossRef]
112. Fan, C.; Ghaemi, S.; Khazaei, H.; Musilek, P. Performance Evaluation of Blockchain Systems: A Systematic Survey. *IEEE Access* **2020**, *8*, 126927–126950. [CrossRef]
113. Smetanin, S.; Ometov, A.; Komarov, M.; Masek, P.; Koucheryavy, Y. Blockchain Evaluation Approaches: State-of-the-Art and Future Perspective. *Sensors* **2020**, *20*, 3358. [CrossRef]
114. More on Distributed Ledger Technologies|JRC Smart Electricity Systems and Interoperability. Available online: https://ses.jrc.ec.europa.eu/node/31975 (accessed on 9 March 2022).
115. de Camargo Silva, L.; Samaniego, M.; Deters, R. IoT and blockchain for smart locks. In Proceedings of the 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 17–19 October 2019; pp. 262–269.
116. Han, D.; Kim, H.; Jang, J. Blockchain based smart door lock system. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 18–20 October 2017; pp. 1165–1167.
117. Au, S.; Power, T. *Tokenomics: The Crypto Shift of Blockchains, ICOs, and Tokens*; Packt Publishing Ltd.: Birmingham, UK, 2018.
118. Lamberty, R.; de Waard, D.; Poddey, A. Leading Digital Socio-Economy to Efficiency: A Primer on Tokenomics. *arXiv* **2020**, arXiv:2008.02538.
119. Liu, Z.; Luong, N.C.; Wang, W.; Niyato, D.; Wang, P.; Liang, Y.C.; Kim, D.I. A Survey on Applications of Game Theory in Blockchain. *arXiv* **2019**, arXiv:1902.10865.
120. Kim, H.M.; Laskowski, M.; Zargham, M.; Turesson, H.; Barlin, M.; Kabanov, D. Token Economics in Real Life: Cryptocurrency and Incentives Design for Insolar's Blockchain Network. *Computer* **2021**, *54*, 70–80. [CrossRef]
121. Oliveira, L.; Zavolokina, L.; Bauer, I.; Schwabe, G. To token or not to token: Tools for understanding blockchain tokens. In Proceedings of the International Conference of Information Systems (ICIS 2018), San Francisco, CA, USA, 12–16 December 2018.
122. Florie Mazzorana-Kremer. Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs). 2018. Available online: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en (accessed on 28 March 2022) .
123. Home | Uniswap Protocol. Available online: https://uniswap.org/ (accessed on 18 January 2022).
124. Warren, W.; Bandeali, A. 0x: An Open Protocol for Decentralized Exchange on the Ethereum Blockchain. 2017. Available online: https://github.com/0xProject/whitepaper (accessed on 18 January 2022).
125. 0x: Powering the Decentralized Exchange of Tokens on Ethereum. Available online: https://0x.org/ (accessed on 18 January 2022).
126. Urdaneta, G.; Pierre, G.; Steen, M.V. A Survey of DHT Security Techniques. *ACM Comput. Surv.* **2011**, *43*, 1–49. [CrossRef]
127. Pennino, D.; Pizzonia, M.; Vitaletti, A.; Zecchini, M. Efficient Certification of Endpoint Control on Blockchain. *IEEE Access* **2021**, *9*, 133309–133334. [CrossRef]
128. Coutinho, K.; Clark, P.; Azis, F.; Lip, N.; Hunt, J. Enabling Blockchain Scalability and Interoperability with Mobile Computing through LayerOne. X. *arXiv* **2021**, arXiv:2110.01398.
129. Keep–Keep Network. Available online: https://keep.network/ (accessed on 18 January 2022).

130. Livepeer—Tokenholders. Available online: https://livepeer.org/tokenholders (accessed on 18 January 2022).
131. Factom | Blockchain Data Integrity. Available online: https://www.factomprotocol.org/ (accessed on 18 January 2022).
132. Samani, K. New Models for Utility Tokens—Multicoin Capital. 2018. Available online: https://multicoin.capital/2018/02/13/new-models-utility-tokens/ (accessed on 18 January 2022).
133. Khamisa, A. Token economies. In *The Emerald Handbook of Blockchain for Business*; Emerald Publishing Limited: Bradford, UK, 2021.
134. Häfner, S. *Utility Token Design*; Available at SSRN 3954773; Research at W3F Fundation: Zug, Switzerland, 2021.
135. Huberman, G.; Leshno, J.D.; Moallemi, C. Monopoly without a monopolist: An economic analysis of the bitcoin payment system. *Rev. Econ. Stud.* **2021**, *88*, 3011–3040. [CrossRef]
136. Wilson, K.B.; Karg, A.; Ghaderi, H. Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. *Bus. Horizons* 2021, *in press*.
137. Ray, P.P.; Kumar, N.; Dash, D. BLWN: Blockchain-Based Lightweight Simplified Payment Verification in IoT-Assisted e-Healthcare. *IEEE Syst. J.* **2021**, *15*, 134–145. [CrossRef]
138. Käbisch, T. *Verification of Bitcoin in the Incubed Protocol*; Hochschule Mittweida: Mittweida, Germany, 2020.
139. Danzi, P.; Kalør, A.E.; Stefanović, Č.; Popovski, P. Delay and Communication Tradeoffs for Blockchain Systems With Lightweight IoT Clients. *IEEE Internet Things J.* **2019**, *6*, 2354–2365. [CrossRef]
140. Le, T.; Mutka, M.W. A lightweight block validation method for resource-constrained iot devices in blockchain-based applications. In Proceedings of the 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Washington, DC, USA, 10–12 June 2019; pp. 1–9. [CrossRef]
141. Why Can't Contracts Make API Calls? Available online: https://ethereum.stackexchange.com/questions/301/why-cant-contracts-make-api-calls/334#334 (accessed on 9 March 2022).
142. Blockchain Oracles for Hybrid Smart Contracts | Chainlink. Available online: https://chain.link/ (accessed on 18 January 2022).
143. Provable–Blockchain Oracle Service, Enabling Data-Rich Smart Contracts. 2019. Available online: https://provable.xyz (accessed on 26 January 2022).
144. Band Protocol—Cross-Chain Data Oracle. 2022. Available online: https://bandprotocol.com/bandchain (accessed 26 January 2022).
145. Tellor. Available online: https://tellor.io/ (accessed on 18 January 2022).
146. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J. Solutions to Scalability of Blockchain: A Survey. *IEEE Access* **2020**, *8*, 16440–16455. [CrossRef]
147. Swan, M. Blockchain economic networks: Economic network theory—Systemic risk and blockchain technology. In *Business Transformation through Blockchain*; Springer: Cham, Switzerlabd, 2019; pp. 3–45. [CrossRef]
148. Neo. Whitepaper. Available online: https://docs.neo.org/v2/docs/en-us/basic/whitepaper.html (accessed on 17 January 2022).
149. Singh, A.; Click, K.; Parizi, R.M.; Zhang, Q.; Dehghantanha, A.; Choo, K.K.R. Sidechain Technologies in Blockchain Networks: An Examination and State-of-the-Art Review. *J. Netw. Comput. Appl.* **2020**, *149*, 102471. [CrossRef]
150. Inter-Blockchain Communication. Available online: https://ibcprotocol.org/ (accessed on 17 January 2022).
151. Zhao, D. Cross-blockchain transactions. In Proceedings of the Conference on Innovative Data Systems Research (CIDR), Amsterdam, The Netherlands, 12–15 January 2020.
152. Qasse, I.A.; Abu Talib, M.; Nasir, Q. Inter blockchain communication: A survey. In Proceedings of the ArabWIC 6th Annual International Conference Research Track, Rabat, Morocco, 7–9 March 2019; pp. 1–6.
153. Kwon, J.; Buchman, E. Cosmos Whitepaper. Available online: https://cosmos.network/resources/whitepaper (accessed on 17 January 2022).
154. Schulte, S.; Sigwart, M.; Frauenthaler, P.; Borkowski, M. Towards blockchain interoperability. In Proceedings of the International Conference on Business Process Management, Vienna, Austria, 1–6 September 2019; pp. 3–10.
155. Sagirlar, G.; Carminati, B.; Ferrari, E.; Sheehan, J.D.; Ragnoli, E. Hybrid-Iot: Hybrid blockchain architecture for Internet of Things-Pow Sub-Blockchains. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1007–1016.
156. Jiang, Y.; Wang, C.; Wang, Y.; Gao, L. A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management. *Sensors* **2019**, *19*, 2042. [CrossRef]
157. Li, M.; Tang, H.; Hussein, A.R.; Wang, X. A Sidechain-Based Decentralized Authentication Scheme via Optimized Two-Way Peg Protocol for Smart Community. *IEEE Open J. Commun. Soc.* **2020**, *1*, 282–292. [CrossRef]
158. Ngubo, C.E.; McBurney, P.J.; Dohler, M. Blockchain, IoT and sidechains. In Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, China,14–16 March 2019.
159. Antonopoulos, A.M. *Mastering Bitcoin: Programming the Open Blockchain*; O'Reilly Media, Inc.: Newton, MA, USA, 2017.
160. Dannen, C. *Introducing Ethereum and Solidity*; Springer: Cham, Switzerland, 2017; Volume 318.
161. Ethereum Virtual Machine (EVM). Available online: https://ethdocs.org/en/latest/introduction/what-is-ethereum.html#ethereum-virtual-machine (accessed on 17 January 2022).
162. Atzei, N.; Bartoletti, M.; Cimoli, T. A survey of attacks on Ethereum smart contracts (Sok). In Proceedings of the International Conference on Principles of Security and Trust, Uppsala, Sweden, 22–29 April 2017; pp. 164–186.

163. Helium Explorer. Available online: https://explorer.helium.com/ (accessed on 18 January 2022).
164. Amoretti, M.; Brambilla, G.; Medioli, F.; Zanichelli, F. Blockchain-based proof of location. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 146–153.
165. Boeira, F.; Asplund, M.; Barcellos, M.P. Vouch: A secure proof-of-location scheme for Vanets. In Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Montreal, QC, Canada, 28 October–2 November 2018; pp. 241–248.
166. Bodkhe, U.; Mehta, D.; Tanwar, S.; Bhattacharya, P.; Singh, P.K.; Hong, W.C. A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems. *IEEE Access* **2020**, *8*, 54371–54401. [CrossRef]
167. Oyinloye, D.P.; Teh, J.S.; Jamil, N.; Alawida, M. Blockchain Consensus: An Overview of Alternative Protocols. *Symmetry* **2021**, *13*, 1363. [CrossRef]