Insight and Background of a Blockchain-based IoT economy

Subjects: Others

Contributor: Marco Zecchini, Diego Pennino, Maurizio Pizzonia, Andrea Vitaletti

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.

Keywords: Internet of Things (IoT) ; blockchain ; economy

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 people 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. It can be expected 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, the integration of IoT with that kind of blockchain gets the spotlight, 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, here 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. 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.

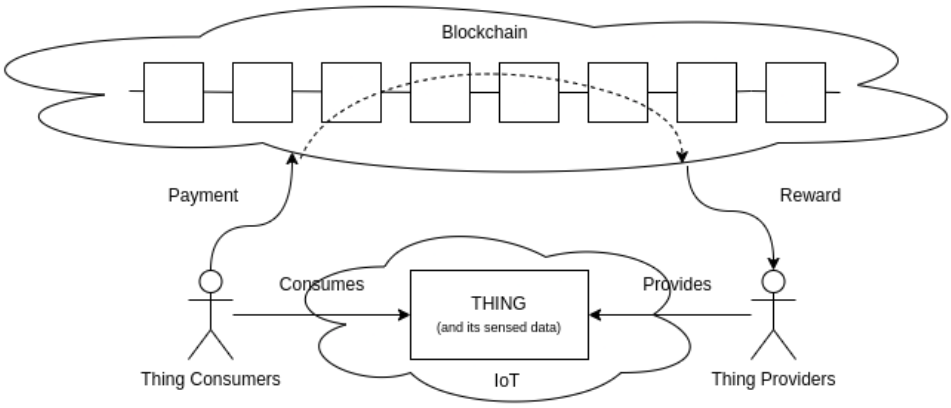

Figure 1. A schematic representation of the reference scenario. Thing consumers pay on a blockchain to use things or the data they gather.

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, here 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 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 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.

2. 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 [6].

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 [6].

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**) [7]. Usually, things support power-efficient wireless technologies (e.g., LoRaWAN [8], Sigfox [9]) 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 [10]. The trade-off between energy consumption, expected network lifetime, and connection quality (in terms of bandwidth, latency, and coverage) are application-specific.

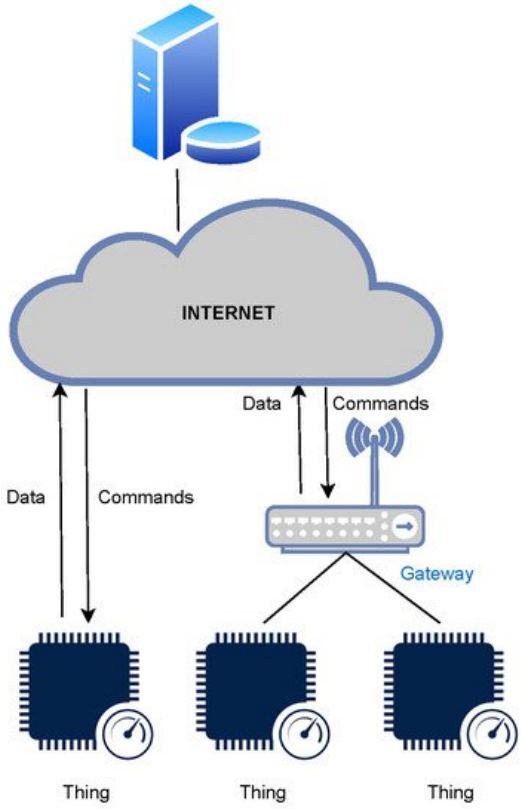

Figure 2. A schematic representation of a typical IoT architecture.

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 [7]. However, when compared even to low-end notebooks, they are usually devices with very limited resources. This is extremely important, since most current blockchain technologies have requirements that cannot be easily satisfied even by low-end notebooks.

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 [11]. 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 [7].

3. 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 [12]). 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 portion here 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. Here 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 [13][14][15]) is the decentralized process by which a block is finally stored in the ledger.

For the sake of simplicity, in the blockchain, it can be assumed 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) [16][17][18], which efficiently links their content with a cryptographic hash r_{body}. For the sake of simplicity, the header can be summarized as a tuple $\langle r_p, r_{body}, sec \rangle$, 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 ≈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 it also consider the limitations of the IoT devices. To mitigate this problem, some solutions (such as [19][20][21]) 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 here it also use the term *unpermissioned*), 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 [22], EOS [23]) 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 was considered in here, there is a need to access off-chain data. This is addressed by an architectural solution that is called *oracle* (for more details, see [24]).

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 [25]), IOTA [26], Obyte [27], and Nano [28].

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., [29][30]). Alternatively, some technologies have specific support for the streamlined creation of new tokens, such as, for example, Algorand [31]. 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, here suggest [32][33].

4. Decentralization and Scalability: The Blockchain Scalability Trilemma

As here stated in previous, 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 [34], 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. Here will 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 [35], 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 [36][37].

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.

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 [26] 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 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.

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.

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.
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.
4. Gupta, D.; Bhatt, S.; Gupta, M.; Tosun, A.S. Future Smart Connected Communities to Fight COVID-19 Outbreak. Internet Things 2021, 13, 100342.
5. Huckle, S.; Bhattacharya, R.; White, M.; Beloff, N. Internet of Things, Blockchain and Shared Economy Applications. Procedia Comput. Sci. 2016, 98, 461–466.
6. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. Comput. Netw. 2010, 54, 2787–2805.
7. Salman, O.; Elhajj, I.; Chehab, A.; Kayssi, A. IoT survey: An SDN and fog computing perspective. Comput. Netw. 2018, 143, 221–246.
8. LoRa Alliance®. LoRaWAN for Developers. 2021. Available online: https://lora-alliance.org/lorawan-for-developers (accessed on 29 November 2021).
9. SIGFOX.COM. 2022. Available online: https://www.sigfox.com/en/what-sigfox/technology (accessed on 11 March 2022).
10. Beniwal, G.; Singhrova, A. A systematic literature review on IoT gateways. J. King Saud Univ. Comput. Inf. Sci. 2021, in press.
11. 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.
12. Antal, C.; Cioara, T.; Anghel, I.; Antal, M.; Salomie, I. Distributed ledger technology review and decentralized applications development guidelines. Future Internet 2021, 13, 62.
13. 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.
14. 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 Internet 2022, 14, 47.
15. 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.
16. Tamassia, R. Authenticated data structures. In Algorithms—ESA 2003; Springer: Berlin/Heidelberg, Germnay, 2003; Volume 2832, pp. 2–5.
17. 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.
18. 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.
19. 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, 2019, Pisa, Italy, 12 February 2019; Volume 2334, pp. 43–55.
20. 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.
21. Ethereum Nodes and Clients. Available online: https://ethereum.org/en/developers/docs/nodes-and-clients/ (accessed on 17 January 2022).
22. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. 2014, 151, 1–32.
23. Eosio Documentation. 2021. Available online: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md (accessed on 20 December 2021).
24. 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.
25. Ethash. Available online: https://eth.wiki/en/concepts/ethash/ethash (accessed on 28 March 2022).
26. Popov, S. The Tangle White Paper. 2018. Available online: http://www.descryptions.com/Iota.pdf (accessed on 28 March 2022).

27. Churyumov, A. Byteball: A Decentralized System for Storage and Transfer of Value. Available online: https://byteball.org/Byteball.pdf (accessed on 28 March 2022).
28. Nano. Eco-Friendly and Feeless Digital Currency. Available online: https://nano.org/ (accessed on 17 January 2022).
29. The Ethereum Community. ERC-20 Token Standard. Available online: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/ (accessed on 18 January 2022).
30. Zhang, E. NEP-17 Token Standard. Available online: https://github.com/neo-project/proposals/blob/master/nep-17.mediawiki (accessed on 18 January 2022).
31. Algorand. Algorand Standard Assets (ASAs). Available online: https://developer.algorand.org/docs/get-details/asa/ (accessed on 18 January 2022).
32. 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.
33. 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.
34. 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).
35. 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.
36. 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.
37. Yu, G.; Wang, X.; Yu, K.; Ni, W.; Zhang, J.A.; Liu, R.P. Survey: Sharding in blockchains. IEEE Access 2020, 8, 14155–14181.