Tracking (Autonomous) Provenance and Lifecycle Events (TAPLE)

Antonio Estévez García[1*], Yeray Rodríguez Rodríguez[1†] and Juan Luis Gozalo Fernández[1†]

[1*]Research and Development, Open Canarias, Elías Ramos González, 4, ofc. 304, Santa Cruz de Tenerife, 38001, Santa Cruz de Tenerife, Spain.

*Corresponding author(s). E-mail(s): aestevez@opencanarias.es;
Contributing authors: yrodriguez@opencanarias.es;
jgozalo@opencanarias.es;
†These authors contributed equally to this work.

Abstract

With the advances of recent years in Distributed Ledger Technologies (DLT) in general, and especially the impact that blockchain technology has had, we find ourselves in a scenario of potential applications that can change the rules of operation of the Internet itself, promoting concepts such as Web 3.0. This article describes the Open Canarias DLT proposal to achieve reliable traceability of the life cycle of entities and processes, with unprecedented scalability characteristics, reducing implementation costs and achieving maximum energy efficiency.

Keywords: DLT, blockchain, p2p, cryptography

1 Introduction

Since the beginning of the bitcoin cryptocurrency in late 2008 [26], the blockchain technology embedded in it has emerged as a disruptive innovation in information technology. Beyond the initial goal of a digital currency and its ability to represent and transfer value over the Internet (avoiding the problem of double spending [8]), its evolution and the potential of its features have had

a multiplier effect on the number of applications. These use cases have served as feedback for new technological approaches to the problems blockchain is intended to solve. All these different approaches can be included in Distributed Ledger Technology or DLT.

This UK government report [34] describes the concept of DLT: "A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network."

With DLT, we have the capability of a shared, distributed, immutable ledger that, when properly implemented, is resistant to tampering. Also, if we add the capabilities of so-called "smart contracts" [37], we add additional logic computation to the ledger record. From these foundations, many possibilities open up, ranging from the simple decentralization of digital interactions between companies, governments, and citizens, through creating new digital business models to a paradigm shift in the digitization strategy itself.

On the other hand, the increased bandwidth available on the Internet and the enormous computing capacity of current devices offer an additional paradigm shift perspective. Furthermore, the number of Internet of Things (IoT) devices worldwide is forecast to triple from 9.7 billion in 2020 to more than 29 billion IoT devices in 2030 [30]. In short, we have billions of devices with computing capacity and bandwidth availability, which represents a challenge to extract the full potential of data from the digital interactions of these devices.

Another aspect to consider in this type of DLT network is energy consumption. We must consider the paradigmatic example of bitcoin [6], which consumes more energy per year than countries like Switzerland or Chile. From the perspective of sustainability and compliance with the 2030 objectives [35], we must consider that the DLT value proposition must also address energy efficiency, even more so in use cases such as the circular economy and agri-food traceability.

These challenges have been the primary motivation for developing the "Tracking (Autonomous) Provenance and Lifecycle Events" (TAPLE) project. With the technology resulting from this project, we offer a DLT solution to traceability of the life cycle for billions of entities and processes, maintaining decentralization, security, and privacy, with the immense additional value of the environmental sustainability of the technology as a support for compliance with the SDGs 2030 [35].

2 Background

As a company specializing in applying Software Engineering to solve complex problems, we identified enormous potential in the DLT for specific scenarios that we were facing. Initially, we focused on using this technology for the reliable traceability of assets and processes. Almost all the applications we have developed with DLTs in the last five years are of this type (water cycle, energy production, mobility, construction, and public tenders). In all cases, we have had to approach hybrid architectures to combine the capabilities of different DLTs in solutions that, while maintaining the features of a distributed, shared, and immutable registry, could allow scenarios of thousands of transactions per second (TPS). While these projects are considered success stories, we knew we were near the limits of available technology, so we decided to consider a new strategy.

First of all, in 2019, we tackled a basic research project to establish state of the art and the basis of a reference architecture for the challenges we had set for a traceability-oriented DLT: (a) scalable to billions of nodes and hundreds of billions of transactions; (b) ability to run nodes on devices with limited resources; (c) flexible and adaptable cryptographic schemes, and with capacity for post-quantum cryptography (PQC) [5]; and (d) be much more efficient from the energy viewpoint compared to other DLTs, providing sufficient evidence. The results of this preliminary research are described below to establish the background of this technology.

For this research, we conducted a systematic review of the literature. The objective of any systematic review is to synthesize the available literature in an organized, transparent, and reproducible way, which, combined with previous experiences in developing this type of solution, would provide us with the starting point for industrial research. In addition, in 2019, we already had a reference architecture for DLT within the standards of the International Telecommunication Union (ITU) [19], which served us for the individualized analysis of the building blocks of DLT (Figure 1).

2.1 Increase scalability

In our experience with implemented use cases, the primary goal with DLT was to achieve tamper-proof event logging. Starting from this premise, one of the illustrative examples of the problem can be found in the work of Belchior et al. [4], oriented to the use of blockchain technology as an enhancer of secure, distributed, and more automated audits. The proposed solution is based on a blockchain infrastructure with private permissions built on Hyperledger Fabric, like the proposed solutions in our projects. Other proposals have adopted the immutability characteristics of public blockchains to protect logs and personal data [9][31][41], but the cost associated with transaction fees represents a barrier to adoption. The study of these works helped us corroborate one of the findings we have extracted from our experience: the source of truth is unilateral in traceability.

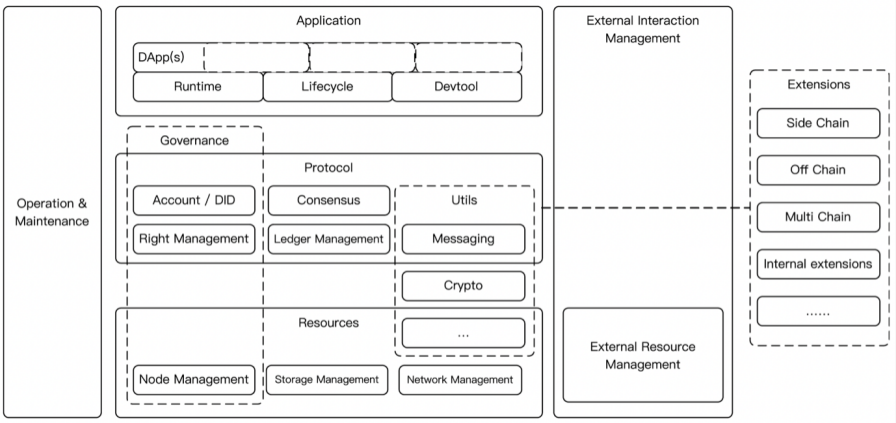

Fig. 1 High-level conceptual architecture of DLT

Let's explain this idea better. The fundamental problem to be solved with blockchain technology was the possibility of double spending [8] on digital currencies. The critical component of the architecture to solve this problem is Consensus, whose function is to order the transactions through a decentralized time stamp. All consensus mechanisms, from the Proof of Work [20] used by Bitcoin [26], and Ethereum [39] to more lightweight solutions like Practical Byzantine Fault Tolerance [7], are based on ensuring that the order of transactions is the same for all nodes. But can there be a disagreement in traceability events? It is at this point that we define the concept of traceability subject. A traceability subject can be an entity (physical or logical) or a process that emits events throughout its life cycle, with an order of emission determined by the subject itself. In short, in a traceability-oriented DLT, the subject is a unilateral source of truth; therefore, the consensus was the first component to improve and simplify.

The next point we faced was the management of the ledger itself, focused on the two aspects that we consider fundamental: the treatment of transaction blocks (Layer1) and the propagation of data between all the nodes of the DLT (Layer0). It is important to emphasize that from the first moment, we ruled out off-chain solutions (Layer2) that did not impact other objectives, such as execution on devices with limited resources and energy efficiency. In this line, the survey of Zhou et al. [40] was essential for synthesizing the different approaches to existing scalability (Table 1).

We first identified that block size and generation interval impacted throughput and latency. Increasing the blocks' size allows for more transactions, but it affects the generation interval and the propagation capacity (which we will see later). Another alternative is reducing transaction data, including compaction and compression methods. And it is at this point where the concept of the one-sided source of truth on the subject of traceability also acquires relevance. Why not have a ledger per subject? This is where we incorporate the Microledger concept.

Table 1 Category of solutions per layer

Layer	Solution Category
Layer 0	Data propagation
Layer 1	Block data Consensus Sharding DAG
Layer 2	Payment channel Side chain Cross chain Off-chain computation

Source: Solutions to Scalability of Blockchain: A Survey.[40]

We found the idea of the Microledger in an inspiring talk by Daniel Hardman of Evernym at the Hyperledger Global Forum 2018 [18]. In his dissertation, he defines his trajectory with blockchain technology, from an initial stage of great expectations, through the different problems detected in its application until he and his colleagues began to outline the concepts that led to Microledgers and Edgechains. This evolution, which many of us have followed, leads us to apply equivalent solutions since we started talking about subchains or sidechains until only using the blockchain as an evidence anchor and finally staying on edge, the Edgechain protocol. In his dissertation, to define an Edgechain protocol, the following questions must be answered: (i) what are the roles in my protocol? (ii) what types of messages do we exchange? (iii) what stage or sequencing rules apply? and (iv) how is our trust and incentives managed?

Other approaches similar to the Microledger idea can be found in the Key Event Receipt Infrastructure (KERI) [29] proposal, in which the ledger collects a chain of events linked by their hashes. We must acknowledge a strong inspiration in his proposal, so much so that the initial code base for the TAPLE technology came from a preliminary implementation of KERI. Concepts such as the roles of the controller, validator, and witness, the way of chaining events in the leger, and the treatment of cryptographic material (which we will see later) are proof of this.

In summary, we arrive at a solution in which we propose a ledger per traceability subject, in which the owner of said subject acts as controller of its life cycle. The replica of the ledger would be limited to the validators and witnesses, the former overseeing, validating, and attesting to the chain of events and the latter simply holding a replica of the ledger for the value that the information provides them. With this partitioning in Microledgers, we can achieve the scalability established in our objectives.

2.2 Devices with limited resources

Taking the size of the ledger of the most popular blockchains, we have a size close to 500 GB for Bitcoin and practically double that for Ethereum (1 TB). It is inconceivable that specific devices (such as smartphones) become nodes of this type of blockchain, even with approaches to reduce their size [10]. For this reason, the partitioning that we adopt with the idea of a Microledger per traceability subject and the limitation in need for replication by limiting the number of nodes involved to validators and witnesses is a starting point for a solution to this type of device.

The Internet of Things (IoT) is different. We can find significant limitations in memory capacity, processing power, consumption, networks, and data transfer capabilities compared to nodes with more resources. Many, such as PLCs and microcontrollers, only allow minimal single-threaded code execution with little memory capacity [2]. Due to these limitations, we evaluate a potential design based on "fog computing" [3] (Figure 2). "Fog computing" provides processing and storage of IoT data locally in intermediate IoT devices that act as a gateway to the local IoT network instead of sending it to the cloud. Unlike the cloud, fog provides faster response and higher quality services. We envision partitioning the TAPLE node, leaving the IoT with few resources for basic cryptographic operations and limited communications. At the same time, the Fog gateway would assume complete management of the ledger and communications to the cloud.

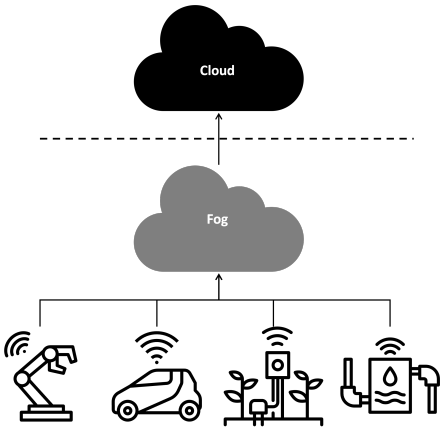

Fig. 2 Fog computing schema

2.3 Flexible and adaptable cryptography

Cryptography is a fundamental aspect of any DLT solution, offering veracity about the registered information and guaranteeing its immutability to make it immune to manipulation. Almost all existing solutions, including the different

technologies based on blockchain, use a single public key scheme, from the pioneers such as bitcoin and Ethereum, which use the Koblitz elliptic curve [23], to proposals such as Cardano and Solana, based on EdDSA [22]. By simplifying the architecture, we can consider a single cryptographic scheme adequate. Still, in our proposal, this simplification presents more problems than benefits: (i) the ability to coexist with different cryptographic schemes facilitates the possibility of incorporating advances such as post-quantum cryptography; and (ii) it allows devices to be incorporated as DLT nodes with limitations derived from their cryptographic capabilities.

In this case, the design decisions are also heavily inspired by KERI [29]. It is about exploiting the characteristics of public key cryptography [36] to extract what is defined in KERI as a self-certified identifier [16], representing a way to create secure identifiers based on decentralized control. In addition, this concept strongly connects with our traceability-oriented ledger approach, in which the devices themselves become subjects of traceability, which, according to the Trusted Computing Group [32], facilitates the idea of "implicit identity" and "embedded certificate authority" to describe the process in which the corresponding device automatically generates identifiers. This binding between the public key and an identifier also applies to hashes and signatures.

Another decision, and one that also emanates from KERI[29], is the support for multiple cryptographic schemes. We start with the fact that many devices have cryptographic capabilities, which may differ from each other. Therefore, a requirement that we initially set out was that the public cryptographic material allowed us to derive not only the type of identifier (public key, hash, or signature) but also the cryptographic scheme that applied to it to enable the nodes to use the corresponding operations. This infrastructure design opens the door, for example, to incorporating post-quantum [5] public key schemes.

2.4 Low energy consumption

The last aspect to address in this preliminary investigation is linked to energy efficiency in DLTs. It is fair to acknowledge that one of the most justified criticisms of blockchain technology is the impact on energy consumption [17][33][14], and with good reason. The study of the effect on the energy consumption of the blockchains is made up of two components: the consensus mechanism and the redundant execution of certain operations, such as the verification of signatures and the adjustment of "account balances" in the database of local data of each node ("state transitions")[28].

Since our approach is based on the Microledger concept, we start from a single and autonomous source of truth. The consensus and the management of "state transitions" are the first elements to be optimized, and said optimization is also implicit in the solution design to improve scalability. Also, the approaches to get our DLT nodes to run on devices with limited resources represent an immediate improvement in energy consumption. Finally, signatures and verification cryptographic operations are crucial for drastically reducing

consumption. Still, ultimately, they are also an essential part of scalability and execution with few resources.

In summary, we hypothesized that energy consumption would benefit from all the optimizations studied in the previous points. In this aspect, we only address the design of the experiment to offer evidence on said consumption. This experiment establishes a comparative study of the same use case with other DLTs (at least two), using joules per transaction as a consumption indicator.

3 Technology fundamentals

In this section, we will present the concepts that support the development of TAPLE technology and that, in its composition, allow us to achieve the objective of offering traceability and transparency in the life cycle of entities and processes, being tamper-proof.

3.1 Key concepts

3.1.1 Subject

Based on the background exposed above, the first fundamental concept of our solution is the "subject" of traceability, given that a large part of the design decisions we have adopted revolve around it. The definition would be the following:

Subject: *An entity (physical or logical) or a process that generates events throughout its life cycle, with an order of emission determined by the subject itself.*

Starting from this concept we can better understand the principle of "onesidennes" that we apply to our ledger design. If we add to this principle the other principle that we have established for subjects, that of "single ownership", we derive a tuple $\langle S, O \rangle$, where S is the subject and O is the owner (a concept that we develop in section 3.2.1).These principles allow us to simplify the consensus on the order in which the insertions are produced in the ledger since that order is set by this tuple, and we do not face the problem of double spending [8].

To understand the real impact, it is worth remembering the concept of consensus in the blockchain. In blockchain networks, tens, hundreds, or thousands of nodes are connected, and they all must share and agree on the same information. When a set of nodes do not agree, a bifurcation or branching of the network occurs, basically a split in which the global state differs from that of the original chain. This is a situation that blockchains are trying to avoid since it would violate the single truth principle and give rise to uncertain scenarios. A blockchain network that is prone to these situations and cannot recover (reorganizations) loses its usefulness. This need is known as consensus, and there are various techniques, called consensus mechanisms, to implement it, and they intervene mainly when new content needs to be added to the chain.

In TAPLE, the above problems do not arise because no consensus mechanism is required, and the tuple (subject and the owner) determines the ledger's order. This means it is possible to modify a subject from any other node in the network, thus avoiding inconsistency in the chains and the need to reach that consensus. However, there is a problem with the principles we have established, and that is that they are not sufficient in scenarios where an owner acts maliciously. This has nothing to do with the validity of the data being recorded since such a situation cannot be verified at the time of insertion but rather because it tries to share different information with different nodes on the network. The solution to this problem is described in the protocol in section 3.2.

3.1.2 Microledger

The next aspect to consider is the microledger [18] concept, which is critical in the design of our solution. Each "subject" contains internally a ledger in which the events that affect only that subject are recorded, the microledger. This microledger is a set of events chained together using cryptographic mechanisms. It is similar to a blockchain in that the different elements of the chain are related by including the cryptographic fingerprint of the immediately preceding element, but, unlike blockchains in which each block can include a set of transactions, possibly from different accounts, in the microledger each element represents a single event of the subject itself.

TODO.

3.1.3 Events

The following fundamental element of our solution is the event since it is the unit of information related to the life cycle of the subject. From this perspective, it is natural to use an approach based on an Event Sourcing design[15], in which the facts and states that affect an object are collected in a sequence of events [24]. Writing an event to the log is a single operation, therefore atomic, so if we consider the idea of one-sidedness discussed above, the log becomes a reliable source of truth.

Our solution can be framed within the Event Sourcing System (ESS) design [25]. This design revolves around the concept of the event, which we can formally define as follows:

Event: *An event is a discrete data object specified in domain terms that represent a state change in an ESS.*

In our provenance and life cycle traceability domain, we establish five types of events (Table 2). It is convenient to specify at this point that the only type of event that modifies the state from the ESS perspective is the *State* event. The *Fact* event is the result of the function or environment of the subject, such as the measurement of a sensor, the kilometers traveled by a connected vehicle, or its transport in a supply chain. They do not modify the subject's properties, but they provide an essential context for the traceability of its life

cycle. The *Start*, *Transfer*, or *EOL* events also do not modify the properties of the subject but are an essential part of its life cycle.

Table 2 Event types

Event	Description
Start	Initializes the event log for a subject, establishing the participants and governance of the ledger.
State	Records change the subject's properties, so its state is modified.
Fact	Facts related to the function or environment of the subject but that does not modify its properties.
Transfer	Transfer the property of the subject to a new owner. A key rotation occurs to prevent tamper with previous events by the new owner.
EOL	End of Life event that ends the event log, preventing new additions.

Regarding the structure and contents of the events, we have based ourselves on design solutions recognized by the industry [13]. The usual approach is to structure the event in a header, with a common structure for all events, including their metadata, and a payload with specific information for each event.

3.1.4 Identifiers

Another concept to highlight is the "identifier" for the elements involved in the network protocol. Given the strong influence of KERI[29] in our project, the reflection on the reference model to establish the identifiers in our protocol starts from the Zooko' triangle[38]. It is a trilemma that defines three desirable properties in the identifiers of a network protocol, of which only two can be present simultaneously. These properties are:

- *Human-meaningful*: Meaningful and memorable (low-entropy) names are provided to the users.
- *Secure*: The amount of damage a malicious entity can inflict on the system should be as low as possible.
- *Decentralized*: Names correctly resolve to their respective entities without using a central authority or service.

Although several solutions to the trilemma have already been proposed, we have prioritized decentralization and security to apply a design equivalent to the Ethereum Name Service[12] shortly. Specifically, in our approach, we have considered three types of identifiers, which in turn represent three types of cryptographic material: (i) public key, (ii) message digest, and (iii) cryptographic signature. The public key is the identifier of the participating roles in the network, the message digest is the identifier of the content of the messages

resulting from applying a hash function to this content, and the cryptographic signature identifies the signatures made by the roles on the messages, which serves as verifiable proof.

Fig. 3 Derivation Scheme for Identifiers

This cryptographic material is large binary numbers, representing a challenge when used as identifiers. The best way to handle identifiers is through a character string, and for the conversion, we have adopted Base64 encoding[21], which encodes every 3 bytes of a binary number into 4 ASCII characters. As the cryptographic material being managed is not a multiple of 3 (32 bytes and 64 bytes), it is padded with one additional character (32 bytes) or two (64 bytes). As in KERI[29], we have taken advantage of these additional characters to establish a derivation code to determine the type of material, placing the derivation character(s) at the beginning. Figure 3 shows this solution.

The following table details the derivation codes of the identifiers of the first version of the TAPLE technology:

Table 3 Derivation codes for identifiers

Code	Identifier type
E	Ed25519 Public Key
S	Secp2556k1 Public Key
J	Blake3 Digest (256 bits)
OJ	Blake3 Digest (512 bits)
L	SHA2 Digest (256 bits)
OL	SHA2 Digest (512 bits)
M	SHA3 Digest (256 bits)
OM	SHA3 Digest (512 bits)
SE	Ed25519Sha512 Signature
SS	ECDSAsecp256k1 Signature

New types of cryptographic material are already incorporated in the roadmap, thinking of devices limited to operations with RSA[27] or P256[1], and post-quantum cryptography, such as Crystal-Dilithium[11]. In the case of RSA or Crystal-Dilithium, we are dealing with a binary size of the cryptographic material that is too large to be represented as identifiers, so we will need to incorporate a different derivation mechanism for these scenarios.

3.2 The protocol

3.2.1 Participating roles

TODO.

3.2.2 Messages structure

TODO.

3.2.3 Rules for event log

TODO.

3.2.4 Incentives for participation

TODO.

3.3 Governance

TODO.

4 Architecture Description

TODO.

5 Conclusion

TODO.

Acknowledgments. APLET Project File (TAPLE): 2021/C005/00141250, financed by the EU through the European Regional Development Fund. A way of making Europe.

Appendix A Use cases

References

[1] Mehmet Adalier and Antara Teknik (2015) "Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P-256.". NIST. http://csrc.nist.gov/groups/ST/ecc-workshop-2015/papers/session6-adalier-mehmet.pdf

[2] Aristidis G. Anagnostakis, Nikolaos Giannakeas, Markos G. Tsipouras, Euripidis Glavas, and Alexandros T. Tzallas (2021) "IoT Micro-Blockchain Fundamentals." Sensors 21, no. 8: 2784.

[3] Hany F. Atlam, Robert J. Walters, and Gary B. Wills (2018) "Fog Computing and the Internet of Things: A Review." Big Data Cogn. Comput. 2018, 2, 10. https://doi.org/10.3390/bdcc2020010.

[4] Rafael Belchior, Miguel Correia, and André Vasconcelos (2020) "Towards Secure, Decentralized, and Automatic Audits With Blockchain." In Proceedings of the 28th European Conference on Information Systems (ECIS), An Online AIS Conference, June 15-17, 2020. https://aisel.aisnet.org/ecis2020_rp/68.

[5] Daniel J. Bernstein and Tanja Lange (2017) "Post-quantum cryptography." Nature 549, 188–194. https://doi.org/10.1038/nature23461.

[6] University of Cambridge (2022) "Cambridge Bitcoin Electricity Consumption Index." https://ccaf.io/cbeci/index. (Accessed on 11 October 2022).

[7] Miguel Castro and Barbara Liskov (1999) "Practical byzantine fault tolerance." In OsDI (Vol. 99, No. 1999, pp. 173-186).

[8] Usman W. Chohan (2021) "The Double Spending Problem and Cryptocurrencies." Available at SSRN: https://ssrn.com/abstract=3090174 or http://dx.doi.org/10.2139/ssrn.3090174.

[9] Jordi Cucurull and Jordi Puiggali (2016) "Distributed Immutabilization of Secure Logs." In Barthe, G., Markatos, E., and Samarati, P., editors, Security and Trust Management, pages 122–137, Cham. Springer International Publishing.

[10] Xiaohai Dai, Jiang Xiao, Wenhui Yang, Chaofan Wang and Hai Jin (2019) "Jidar: A jigsaw-like data reduction approach without trust assumptions for bitcoin system." In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE, pp. 1317–1326.

[11] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé (2021) "CRYSTALS-Dilithium – Algorithm Specifications and Supporting Documentation (Version 3.1)." Specification document (update from February 2021).

[12] ENS (2022) "Ethereum Name Service." https://ens.domains/. (Accessed on 11 October 2022).

[13] Opher Etzion, Peter Niblett (2010) "Event Processing in Action." Manning Publications Co.3 Lewis Street Greenwich, United States. ISBN:978-1-935182-21-4

[14] Yudi Fernando and Rubakanthan Saravannan (2021) "Blockchain Technology: Energy Efficiency and Ethical Compliance." Journal of Governance and Integrity, 4(2), 88–95. https://doi.org/10.15282/jgi.4.2.2021.5872.

[15] Martin Fowler (2005) "Event Sourcing.". Blog entry. https://martinfowler.com/eaaDev/EventSourcing.html

[16] Marc Girault (1991) "Self-certified public keys." In: Davies, D.W. (eds) Advances in Cryptology — EUROCRYPT '91. EUROCRYPT 1991. Lecture Notes in Computer Science, vol 547. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-46416-6_42.

[17] Julija Golosova and Andrejs Romanovs (2018) "The Advantages and Disadvantages of the Blockchain Technology," IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018, pp. 1-6, DOI: 10.1109/AIEEE.2018.8592253.

[18] Daniel Hardman (2018) "Microledgers and Edge-Chains: A Primer." Hyperledger Global Forum 2018. https://www.youtube.com/watch?v=iK5vd7-b1zA. (Accessed on 11 October 2022).

[19] ITU (2019) "Technical Specification FG DLT D3.1 Distributed ledger technology reference architecture". International Telecommunication Union: Geneva, Switzerland.

[20] Markus Jakobsson and Ari Juels (1999) "Proofs of Work and Bread Pudding Protocols (Extended Abstract)." In: Preneel, B. (eds) Secure Information Networks. IFIP - The International Federation for Information Processing, vol 23. Springer, Boston, MA.

[21] S. Josefsson (2006) "The Base16, Base32, and Base64 Data Encodings." RFC4648. Network Working Group. https://www.rfc-editor.org/rfc/rfc4648.

[22] S. Josefsson and I. Liusvaara (2017) "Edwards-Curve Digital Signature Algorithm (EdDSA)." IRTF. doi:10.17487/RFC8032. ISSN 2070-1721. RFC 8032. https://www.rfc-editor.org/rfc/rfc8032. (Accessed on 11 October 2022).

[23] Neal Koblitz (1993). "Introduction to Elliptic Curves and Modular Forms." Graduate Texts in Mathematics. Springer New York, NY. ISBN 978-0-387-97966-3.

[24] Stanley Lima, Jaime Correia, Filipe Araujo and Jorge Cardoso (2021) "Improving observability in Event Sourcing systems." Journal of Systems and Software. 181. 111015. 10.1016/j.jss.2021.111015.

[25] Michiel Overeem, Marten Spoor, Slinger Jansen, Sjaak Brinkkemper (2021) "An empirical characterization of event sourced systems and their schema evolution — Lessons from industry." Journal of Systems and Software. Volume 178. 110970. ISSN 0164-1212. https://doi.org/10.1016/j.jss.

2021.110970.

[26] Satoshi Nakamoto (2009) "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf. (Accessed on 3 October 2022).

[27] Ron Rivest, Adi Shamir and Leonard Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the ACM. 21 (2): 120–126. CiteSeerX 10.1.1.607.2677. doi:10.1145/359340.359342. S2CID 2873616.

[28] Johannes Sedlmei, Hans Ulrich Buhl, Gilbert Fridgen and Robert Keller (2021) "Recent Developments in Blockchain Technology and their Impact on Energy Consumption." Cryptography and Security (cs.CR). arXiv:2102.07886 [cs.CR]. https://doi.org/10.48550/arXiv.2102.07886.

[29] Samuel L. Smith. 2021. "Key Event Receipt Infrastructure (KERI)." V2.58 2021/01/11, original 2019/07/03. https://github.com/decentralized-identity/keri/blob/master/kids/KERI_WP.pdf. (Accessed on 2 October 2022).

[30] Lionel Sujay Vailshery (2022) "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030". Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. (Accessed on 2 October 2022).

[31] Andrew Sutton and Reza Samavi (2017) "Blockchain Enabled Privacy Audit Logs." In: et al. The Semantic Web – ISWC 2017. ISWC 2017. Lecture Notes in Computer Science(), vol 10587. Springer, Cham. https://doi.org/10.1007/978-3-319-68288-4-38

[32] TCG (2018) "Implicit Identity Based Device Attestation. " https://trustedcomputinggroup.org/wp-content/uploads/TCG-DICE-Arch-Implicit-Identity-Based-Device-Attestation-v1-rev93.pdf. (Accessed on 2 October 2022).

[33] Jon Truby (2018) "Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies." Energy Research and Social Science, volume 44, 2018, pages 399-410, ISSN 2214-6296. https://doi.org/10.1016/j.erss.2018.06.009.

[34] UK Government Chief Scientific Adviser (2016) "Distributed Ledger Technology: beyond blockchain." (PDF) (Report). Government Office for Science (UK). January 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. (Accessed on 6 October 2022).

[35] United Nations (2015) "Sustainable Development Goals." https://sdgs.un.org/goals. (Accessed on 3 October 2022).

[36] Wikipedia (2022) "Public-key cryptography." https://en.wikipedia.org/wiki/Public-key_cryptography. (Accessed on 11 October 2022).

[37] Wikipedia (2022) "Smart Contract." https://en.wikipedia.org/wiki/Smart_contract. (Accessed on 6 October 2022).

[38] Wikipedia (2022) "Zooko's triangle." https://en.wikipedia.org/wiki/Zooko%27s_triangle. (Accessed on 11 October 2022).

[39] Gavin Wood (2014) "Ethereum: A secure decentralized generalized transaction ledger." Ethereum project yellow paper, vol. 151, pp. 1–32.

[40] Qiheng Zhou, Huawei Huang, Zibin Zheng and Jing Bian (2020) "Solutions to Scalability of Blockchain: A Survey." In IEEE Access, vol. 8, pp. 16440-16455, DOI: 10.1109/ACCESS.2020.2967218.

[41] Guy Zyskind, Oz Nathan and Alex 'Sandy' Pentland (2015) "Decentralizing Privacy: Using Blockchain to Protect Personal Data." In 2015 IEEE Security and Privacy Workshops pages 180–184.