People-Centered Distributed Ledger Technology-IoT Architectures: A Systematic Literature Review

ABSTRACT

To understand how distributed ledger technology (DLT) enables people-centered IoT solutions we conducted a systematic literature review of tested implementations since 2017. We created a people-centered classification to analyze 39 implementations. We found that people-centered DLT-IoT architectures are in their infancy and detected no evidence of emerging patterns. We observed that Ethereum is the most used DLT. Fit-for-purpose technologies like IOTA and concepts like Self-Sovereign Identity (SSI) were underrepresented. We noted an increased interest in privacy-preserving and edge-computing mechanisms, and identified three areas for future research. We hope this survey will assist others learning more about people-centered IoT solutions.

Keywords: Internet of Things (IoT); Distributed Ledger Technology (DLT); People-centered; Data economy

1 INTRODUCTION

The continuous advancements and miniaturization of chip design along with ubiquitous connectivity has made it attractive for original equipment manufacturers (OEMs) to embed processors, sensors, and actuators into consumer products. This trend is expected to accelerate with 5G network expansion (*Fortune Bus. Insights*, 2020), OEM's embrace of digital twins (Tao et al., 2019) and as people seek more convenience in their lives ("SmartCities World," 2017). Digital twins are smart-service enablers that offer OEMs a path towards Service Dominant (S-D) logic (Vargo and Lusch, 2008) and the *servitization* of their products (Meierhofer et al., 2020). While digital twins can improve OEM competitiveness (Tao and Zhang, 2017), people's quality of life and human sustainability (Nižetić et al., 2020), they also introduce privacy, security and ethical issues. They pierce people's private sphere by capturing large amounts of fine-granularity and high-frequency data. They sense, watch, listen, communicate, and learn in what Jens-Erik Mai coined as the datafication of personal information (Mai, 2016) from which not even the technically savvy (Allana and Chawla, 2021) nor the children are immune (Allana and Chawla, 2021). These activities are supported by OEM-controlled cloud-based data silos. Besides being single points of failure and cybercriminal honeypots (Tobin and Reed, 2017), these data silos offer end-users no mechanisms to control who, when and how the data about them is used. As sole controllers of IoT data OEMs seize to themselves all IoT-enabled productivity gains and data monetization rewards. This organization-centric approach to data led to the concept of surveillance capitalism (Zuboff, 2015). This situation has driven digital data-activists, researchers, and legislators to organize to counter it. For instance, the MyData Global[1] initiative (Langford et al., 2020) advocates "the human-centric control of personal data" through the definition of principles that guide the operation of personal data operators and personal data stores (PDS). They seek to turn individuals who currently trade their privacy for IoT solutions' benefits, from digital life management *passive* targets to *active* actors. This people-centered approach has been elusive up until the emergence of distributed ledger technology. DLT's strong cryptographic foundation, immutable and tamper-proof nature, and smart contract support, provides individuals with the missing mechanism for IoT data control (Tom Lyons, 2020). By controlling the data generated by the IoT devices they own, individuals can aspire to a more ethical distribution of the IoT rewards. This is of particular importance as IoT-based smart-contracts are expected to generate considerable savings by bringing entire ecosystems together with business-processes orders of magnitude more efficient than the ones used today (Christidis and Devetsikiotis, 2016).

To assess the state-of-the-art of people-centered DLT-IoT architectures, we conduct a systematic literature review. The objective was to identify and document different approaches, patterns and architectures and assess solutions that offer individuals control of the IoT data about them. While there are several surveys focusing on the state-of-the-art of the integration of DLT and IoT (Zhu et al., 2019), our work is unique because it focused on the use of DLT to give individuals control and agency of IoT data about them. To improve the quality of our

[1] https://mydata.org

results, we focused our efforts on papers that test their proposed solutions. We aim to answer the following research questions (RQs):

- **RQ1**: How does DLT enable a people-centered approach in IoT?
- **RQ2**: What are the people-centered IoT solutions' publication trends?

We identified over five hundred articles from four central online publication databases (IEEE Xplore, SCOPUS, Web of Science, ACM Digital Library) which we systematically filtered down to thirty-nine (39) papers. We analyzed the latter in detail with the objective of answering our RQs and identifying research gaps. Results show that there is a rise in the number of people-centered DLT-IoT architectures since 2019. However, we identified gaps that if addressed will improve future solutions' people centeredness.

The remainder of the paper is organized as follows. In Section 2 we introduce the people-centered approach, distributed ledger technology, and IoT. Section 3 introduces the methodology used for paper selection and data collection processes. Section 4 presents the DLT-IoT people-centered taxonomy. In Section 5 we present our results and in Section 6 we discuss our findings and propose topics of future research. Section 7 presents our conclusions.

2 BACKGOUND

2.1 People-Centered Approach

The people-centered concept is an evolving concept with roots in the psychotherapy work of Carl Ransom Rogers who coined the "person-centered" term in 1978. The term has since then been expanded to "people-centered" and it is now an emerging paradigm. In the context of data economy ecosystems it is an approach that "adopts individuals' and communities' perspectives as equal participants in, and beneficiaries of, trusted data economy ecosystems" and it is based on the principle that people "have the education and support they need to make decisions" (Koskinen et al., 2019, p. 332). Unfortunately, individuals are not equals in todays' digital world. Far from it. The reason why can be traced back to a technical solution devised back in the 60s to identify the users on the first multi-user operations system Figure 1. Of the many solutions that could have been devised the user-password was the one chosen (McMillan, 2012). In the 90s, in the absence of an identity layer, the Internet adopted again the user-password identity management strategy. What could have been just another innocuous technical decision led to today's situation in which digital identity is based on a "patchwork of identity one-offs" (Cameron et al., 2005) where contracts of adhesion manage the feudal-like relationship between people and their service providers (Searls, 2012). These one-side contracts force people to provide all types of personal identifying information to access services which can be interrupted at any time if the provider so pleases.

By 2005 people started to organize to fight this *status quo*. The Internet Identity Workshop[2] (IIW) biannual events started and the Laws of Identity (Cameron et al., 2005) were published. Both sought to put people in control of their identities and private information. At around the same time, businesses like Google, Amazon, Facebook, Apple (in the west) Baidu, Alibaba, and Tencent (in the east) were mastering the data-economy by monetizing everyday social acts captured by their service platforms (Couldry and Mejias, 2019). In 2008 the concept of blockchain emerged through Bitcoin (Nakamoto, 2008) and soon after it entered the identity realm with decentralized identifiers (i.e. name-value pairs). NameCoin[3] in 2010 started to offer a decentralized DNS service, and Blockstack[4] a decentralized public key (DPKI) in 2013. In 2014 Cambridge Analytica started using information from 50M Facebook users to influence elections through micro-targeting (Berghel, 2018). In 2016 the European Union (EU) published the General Data Protection Regulation (GDPR)[5] and the Self-Sovereign Identity (SSI) concept emerges (Kim et al., 2018). With SSI people have the possibility of controlling their personal data and share it or even sell it if they so choose (Lyons et al., 2019a). In 2018 the MyData Global

[2] https://internetidentityworkshop.com/
[3] https://www.namecoin.org
[4] https://www.blockstack.org
[5] https://eur-lex.europa.eu/eli/reg/2016/679/oj

was created with the objective of empowering individuals by "improving their right to self-determination regarding their personal data" and California released the California Consumer Privacy Act (CCPA) (Baik, 2020).

The efforts to develop a more humane data-economy though legislation and technology are beginning to challenge the data-economy *status quo*. Together they are converging towards people-centered data economy ecosystems (Koskinen et al., 2019). People-centered concepts are emerging at a critical juncture in which developments in artificial intelligence (AI), 5G (Mir et al., 2020) and the growth of IoT-enabled devices are expected intensify pressure on privacy. The International Data Corporation (IDC) projects the latter devices to reach 41.6 billion generating 79.4 zettabytes of data by 2025 ("IDC," 2019). This sequence of events is portrayed in Figure 1.

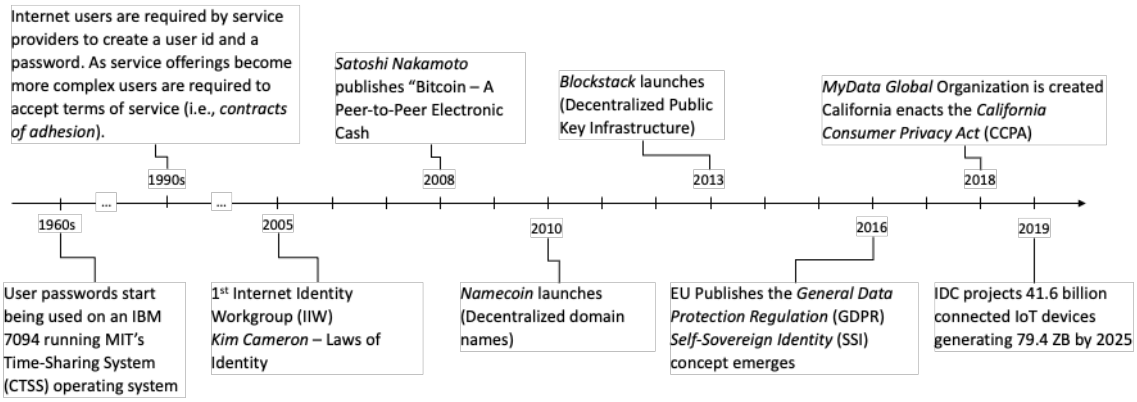

Figure 1: People-centered data control milestones.

2.2 Distributed Ledger Technology (DLT)

Distributed ledger technology enables a non-fully trusted network of peers to self-organize around a consensual version of a truth stored in a distributed, shared, immutable, and cryptographically[6] secure way. The mechanism was first articulated by Satoshi Nakamoto to enable digital currency payments absent of a trusted third-party (Nakamoto, 2008) and implemented in 2009 when Bitcoin became operational (web.archive.org, 2010). The technology builds upon forty years of research in cryptography by thousands of researchers, and on twenty years of research into digital cash. Until blockchain, digital cash was infinitely copyable and there was no way to eliminate double spending without a central intermediary (Swan, 2015).

Since blockchain nodes do not fully trust each other, a combination of computing concepts and cryptography is used to enable trust in the network. Blockchain technology is based on an append-only, distributed ledger of cryptographically linked blocks[7] containing digitally signed transactions shared among participating nodes architecture. Adopting an append-only strategy ensures that blocks are not overridden, enabling full transactional history. Embracing a distributed architecture increases blockchain resiliency to attacks by bad actors, making it tamper resistant. Using cryptographically backed-linked hash pointers (i.e., keyless cryptography) makes blockchain tamper evident. Requiring nodes[8] to sign each transaction using asymmetric cryptography makes blockchain secure and attestable. Finally, sharing information among participants makes blockchain transparent and auditable (Yaga et al., 2018).

Three different phases have been identified since blockchain emerged: currency, contracts, and applications beyond finance like government, health, media, the arts, and justice (Swan, 2015). Whereas initially permissionless blockchains were prevalent, permissioned blockchains that limit the participation to specific

[6] "Cryptography is a branch of mathematics that is based on the transformation of data and can be used to provide several security services: confidentiality, identity authentication, data integrity authentication, source authentication, and support for non-repudiation"(Barker, 2016)

[7] Except for the first block (i.e., the genesis block)

[8] Blockchain nodes can be person or non-person entities (e.g. organization, system) (Heather Vescent, 2018).

people or organizations and allow finer-grained controls gained traction specially among industry or sector consortia. The interoperability between these private and public blockchains as well as the integration with the off-chain world creates the *blockchain multiverse* (Lyons et al., 2019b) and enables the Internet of Value (Skinner, 2016).

Blockchain can anchor any form of asset registry, inventory, and exchange, including every area of finance, economics, and money; physical assets; and intangible assets like votes, ideas, reputation, intention, health data, and information (Swan, 2015). Coined (digital) tokens, they represent a quantity of something that is in control of an entity which can reassign it to another entity (Lewis., 2015). They are value containers that enable the transmission of value over the internet (Pilkington, 2016). Given their divisibility and tradability tokens have grown in numbers and complexity driving the need to understand and classify them with formal taxonomies (Oliveira et al., 2018).

Normal economy activity often requires more than just a protocol to exchange value (e.g., using cryptocurrency to pay for service) (Nick Szabo, 1997). First conceptualized by Nick Sbazo in 1994 as "a computerized transaction protocol that executes the terms of a contract such as payment terms, liens, confidentiality, and even enforcement" with the intent of minimizing "exceptions both malicious and accidental, and the need for trusted intermediaries" (Szabo, 1994), smart contracts utilize protocols and user interfaces to facilitate all steps of the contracting process introducing a way to formalize and secure digital relationships (Szabo, 1997). Even though Nakamoto envisioned the notion of programmable money and a full feature set to enable (Swan, 2015), it was Vitalik Buterin who in 2013 conceptualized ("Ethereum.org," 2013) and launched Ethereum in 2015 ("Ethereum Foundation," 2015).

Smart contracts enable the development of decentralized applications (Dapps). Multiple smart contracts can be bundled to define how an organization should operate. These decentralized (autonomous) organizations can be considered open-sourced as their operations (and thus trust) relies on the security and auditability of its underlying smart-contract code, whose operations can be scrutinized by millions of eyes (Wright and De Filippi, 2015).

Tokens and smart contracts pave the path towards a decentralized economy. The latter is not defined by a geographic location, political structure, and legal system. It does not rely on trusted third parties nor in the existence of social capital for economic development. The economic agents can be human, autonomous organizations, or contracts, and transact goods and services priced in a crypto-currency, recording all transactions to blockchain (Babbitt and Dietz, 2014). Cryptoeconomics is a science that characterizes and designs protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy (Pilkington, 2016).

2.3 IoT/Digital Twins/Service Dominant Logic

The term Internet of Things (IoT) was coined by Kevin Ashton in 1999 (Ashton, 2009). Along with cloud computing and AI, IoT is at the core of Digital Twins. Digital Twins leverage IoT to collect information about the state and usage of physical devices with the intent of updating a software counterpart (i.e., the twin) that exists on the cloud, where AI is used to respond to everyday events (Batty, 2018). The concept of Digital Twin originated at NASA and was introduced in 2003 by Michael Grieves in his Product Lifecycle Management (PLM) executive course (Grieves, 2014). The concept of PLM had been introduced in 1985 by François Castaing to manage production from conceptualizing the product (ideation), definition (spec definition), realization (manufacturing), use by the end-user, and disposal (Stark, 2018). By the 2010s the aforementioned technologies lead to the emergence of several smart manufacturing strategies such as Germany's "Industrie 4.0", the US's "Industrial Internet" and the Chinese's "Made in China 2025" (Tao and Zhang, 2017). Whereas the German initiative places more focus on the use of IoT-enabled devices in the manufacturing process, the US initiative led by Industrial Internet Consortium (IIC) does so on IoT applications (Sendler, 2018). Besides enabling smart production and precision management (Qi and Tao, 2018), Digital Twins also enable the servitization of manufacturing. The servitization concept is generally recognized as the process of creating value by adding services like customization, monitoring, predictive maintenance, performance optimization, or

consulting services to products (Meierhofer et al., 2020). Servitization is driven by OEM's need to differentiate products and people's shift towards business models that offer them access to a process or to an outcome instead of traditional product access models (Paiola and Gebauer, 2020). This increasing focus on services led Steven Vargo and Robert Lush to explore value creation in an era of increasing tokenization (liquification) and specialization (unbundling) of economic relations. Their research gave birth to Service Dominant (S-D) logic (Vargo and Lusch, 2008).

It is in this rapidly evolving context, in which OEMs are creating a business-centric, cloud-based, and proprietary *product-servitization* layer that DLT-based concepts like SSI are promoting an owner-centric, decentralized, standards-based approach to IoT data management (Fedrecheski et al., 2020).

3 METHOD

This section describes the research method used namely the eligibility criteria, information sources and search, study selection and data collection.

3.1 Research Questions

Our study was based on two RQs. Each of the RQs was further extended with three sub-questions.

- **RQ1**: How does DLT enable people-centered approach in IoT?
  - **RQ 1.1.** – *Are there* DLT-IoT *people-centered emerging patterns?* Answering this question allows us to understand whether researchers are starting to converge towards a type of architecture and/or implementation pattern. That could include a specific distributed ledger (e.g., IOTA), or towards a deployment strategy (e.g., permissioned/consortium) and whether the concepts of SSI or PDS are being used by researchers.
  - **RQ 1.2** – *Are people-centered DLT-IoT implementations domain-specific?* Addressing this question could enables us to understand whether different IoT domains (e.g., Smart-Transportation) influence implementations or whether they pose specific challenges that lead to implementation differences (e.g., edge computing, privacy preserving).
  - **RQ 1.3** – *Are there gaps in the solutions analyzed?* The answer to this question could indicate technical implementations' unexplored research directions, and/or implementation domains' specific unaddressed challenges.
- **RQ2**: What are the people-centered DTL-IoT strategies publishing trends?
  - **RQ 2.1** – *In which years were the papers published?* Answering this question provides clues to assess at what time the topic started to get attention as well as how recent the research on this topic is.
  - **RQ 2.2** – *What are the knowledge domains (e.g., IoT, Networking, Cloud, and Software Engineering) and publication type (i.e., Journal, Conference)?* Answering this question could allow us to understand better the interdisciplinarity of the topic as data privacy, security and ethics crosses several related research areas. Additionally, understanding the papers' venue enables us to assess the papers' maturity as journal tend to publish more mature studies than conferences.
  - **R 2.3** – *What is researchers' country of affiliation?* Answering this question allows us to understand whether legislation (e.g., GDPR, CCPA) or manufacturing strategies (e.g., China 2025 - China, Industrie 4.0 – Germany, Industrial Internet Consortium (IIC) - US) have an impact on the published papers.

3.2 Search and Selection

The following automated search engines were used.

- IEEE Xplore;
- ACM Digital Library (ACMDL);
- Scopus;

- Web of Science (WOS).

The first two engines are hosted by the two arguably most renowned scientific technological associations, the IEEE and the ACM, while the last two are the most reputable and worldwide adopted generic scientific databases. To improve search criteria readability, we divided it into three groups of terms:

- Distributed ledger.
- IoT.
- People-centered.

To eliminate researcher bias and ensure we identified all relevant papers, we started by running preliminary search queries to study "word associations" within the three groups. Instead of "smart-contract", "internet of medical things" or "privacy preserving", we searched by "contract", "internet" and "privacy" as depicted in Table 1.

Table 1- Word Association Preliminary Search Criteria

Topic	Contains Any of These
Distributed ledger	blockchain OR ledger OR dlt OR contract OR tangle
IoT	iot OR internet OR things OR edge OR smart
People-centered	privacy OR security OR trust OR data OR gdpr OR sovereign

Based on a manual analysis of the papers' abstract and keywords, we were able to find unfamiliar terms and new word associations that were unknown to us. Examples include: "smart speaker", "smart toilet", "patient-centric" and "usage consent". This extra step allowed us to define a more deterministic list of terms for our study (Table 2). Additionally, allowed us to assess that prior to 2017 people centered papers were mostly theoretical.

Table 2 - Search Criteria

Topic	Contains Any of These
DLT	blockchain OR "distributed ledger" OR DLT OR "smart contract" OR tangle OR BIoT OR BoT
IoT	IoT OR "Internet of Thing" OR "Internet of Medical Thing" OR "Internet of Vehicle" OR IoV OR edge OR "digital twin" OR cps OR "cyber-physical system" OR "industry 4.0" OR "industrie 4.0" OR IIoT OR "smart device" OR "smart object" OR "smart mobility" OR "smart car" OR "smart vehicle" OR "smart city" OR "smart cities" OR "smart health" OR "smart e-health" OR "smart grid" OR "smart meter" OR "smart home" OR "smart building" OR "smart insurance" OR "smartwatch" OR "smart toilet" OR "smart speaker" OR "smart living"
People-centered	sovereign OR "data market" OR "data economy" OR "data ownership" OR "personal data" OR "data trust" OR "data rights" OR gdpr OR "data protection" OR ccpa OR "usage consent" OR "user centric" OR "patient-centric"
Filters	Publish date >=2017

The paper selection followed the inclusion criteria from Table 3.

Table 3 - Inclusion Criteria

No	Criteria	Justification
1	The solution must use distributed ledger and IoT centric.	The solution makes use of blockchain and not just as one of many other solutions.
2	The solution must address security, privacy, and the fair use of IoT data.	The solution must improve individual protection and control of the data.
3	The study's solution must be evaluated.	The paper must show more than just a theoretical solution.

The papers were assessed in accordance with Figure 2.

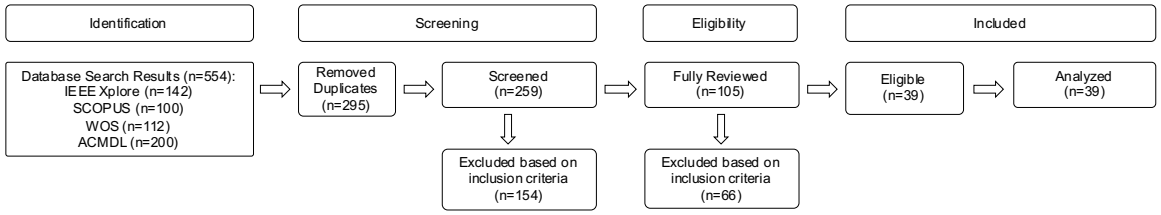

Figure 2 – Study process workflow diagram

4 CLASSIFICATION

We define a people-centered IoT Ecosystem as a network of entities such as OEMs, service providers, regulators, law enforcement, and individuals that exchange data in an *IoT domain* by leveraging a system that supports a set of *capabilities* that offer the individual level of privacy and security as well as some level of control over how data is exchanged. We leverage this definition to create a DLT-focused people-centered IoT ecosystem classification as defined in Figure 3.

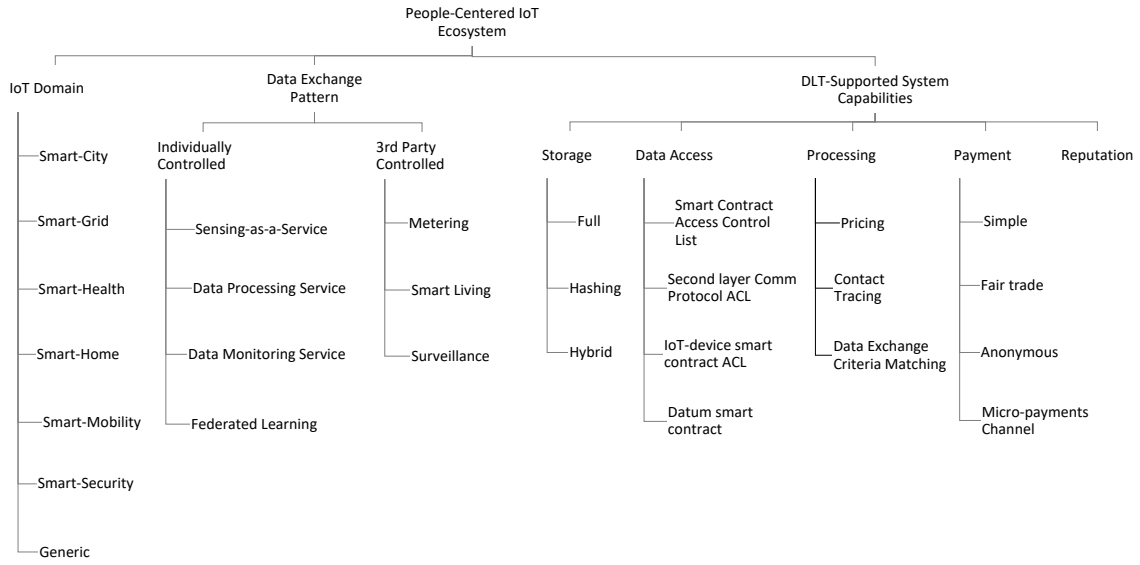

Figure 3 – DLT-focused people-centered IoT ecosystem classification

The *IoT domain* represents the sector of the ecosystem: Smart-City, Smart-Grid, Smart-Health, Smart-Home, Smart-Mobility, Smart-Security, and Generic (i.e., not defined). The *data-exchange pattern* represents how the data is exchanged:

- **Individual Controlled** – the individual controls the IoT device and data storage and voluntarily exchanges data. Within this pattern we identified the following *sub-data exchange patterns*:
  - **Sensing-as-a-Service** – the individual submits data with the purpose of receiving a reward. This is usually associated with the concept of sensing-as-a-service (Zichichi et al., 2020) or crowdsensing (Liu et al., 2019).
  - **Data Processing Service** – the individual shares data with a service provider that uses an algorithm to process the individual's information and returns a response. The response may be a rate for auto insurance based on previous driving data (Dib et al., 2020), or even a way to get the best route from the current location to the destination (Zhang and Fan, 2020).
  - **Data Monitoring Service** – the individual shares the data with a service provider with the objective of monitoring a continuous data stream for anomalies which can involve monitoring biometrics for cardiovascular dangerous situations, or to analyze the

individual's location to assess whether the latter came in contact with an infected individual (Lv et al., 2020).

- **(Voluntarily) Ecosystem Data Sharing** – the individual shares information within the ecosystem with the objective of assessing whether the individual can join a clinical trial (Angeletti et al., 2017), increasing transparency about the asset and the individual's skills and knowledge about using the said asset (Saldamli et al., 2020), or to give access to an insurance company to assess responsibility on an accident (Md Abdur Rahman et al., 2020), or to receive tasks based on the individual's location (i.e., crowdsourcing) (Zhang et al., 2021), or to share transit and location-based services (Pu et al., 2020). To encourage participants to exchange trustworthy information, incentive-punishment mechanisms may exist (Pu et al., 2020) (Makhdoom et al., 2020).
- **Federated Learning** – the individual shares the machine learning coefficients executed with the individual's data (Mohamed Abdur Rahman et al., 2020).

- **3rd Party Controlled** – the service provider controls the IoT device and storage. The individuals may or not engage in the data exchange voluntarily but at a minimum the individual is aware that data exchange can occur.
  - **Metering** – measures utilities consumption (Dimitriou and Mohammed, 2020; Gur et al., 2019; Wang et al., 2019).
  - **Smart living** – an entity monitors environmental, user-proximity and wearable sensor-devices within a given space with the intent of optimizing living conditions, optimize resources and ensure the safety and well-being of those within the space (Barati et al., 2020).
  - **Surveillance** – authorities-lead surveillance (e.g., license plate recognition (Ochoa et al., 2019)).

To better understand the role of DLT on people-centered ecosystems we focused on the following capabilities:

- **Storage** – three patterns were identified:
  - **Full** – IoT data is stored on a distributed ledger to share data among multiple parties. It is used to eliminate single-points of failure and single-points of trust (Wang et al., 2019), or to broadcast data among a set of nodes (Zichichi et al., 2020).
  - **Hashing** – IoT full-data is stored outside the ledger and solely the hash is stored on the ledger as a mechanism to ensure non-repudiation and trustworthiness, i.e., data provenance (e.g., (Dib et al., 2020; Kim and Lampkins, 2019)).
  - **Hybrid** – the full-data is stored in different locations including local, cloud and on-ledger based on an algorithm (Uddin et al., 2018).
- **Data Access control**: the four following patterns were identified:
  - **Ecosystem Smart Contract Access Control List (ACL)** – the ecosystem has a smart contract that defines the access control list of nodes with access to specific data. The exchange of data is enabled for as long as the data access is not revoked. The data exchange can use multiple mechanisms like API-call and OAuth 2.0 (Makhdoom et al., 2020),
  - **Second layer Comm Protocol ACL** – the ledger offers a way for a node to create an encrypted channel that other nodes can subscribe to (Lucking et al., 2020).
  - **IoT-device smart contract ACL** – each IoT device has its own smart contract. The requester requires access and if approved is added to the device's smart contract ACL (Fan et al., 2020).
  - **Datum smart contract** – each datum available for trading has its own smart contract. The requester requires access and if all conditions are met the requester is added to the

streaming channel (Chuang et al., 2020), or the requester sends the data encryption key (Chuang et al., 2018).

- **Data Processing** – in this context, any implementation that uses smart contracts is technically using DLT for some type of data processing. We tried to identify implementations that use smart contracts beyond data processing transparency like token management or access-control lists. Three patterns were identified:
    - **Pricing** – the data-marketplace uses smart contracts to assess the data value (Liu et al., 2019)
    - **Contact-tracing** – smart-contracts are used to assess contamination events, i.e. whether an infected individual came in contact with a non-contaminated individual (Lv et al., 2020).
    - **Data Exchange Criteria Matching** – smart contracts are used to match the data provider and requester privacy policy requirements (Dib et al., 2020; Lopez and Farooq, 2019; Loukil et al., 2018; Nawaz et al., 2020; Rantos et al., 2019).
- **Payment** – the ecosystem allows data trading via crypto or micro payments. Within payment scenarios we identified the following patterns:
    - **Simple** – represents a payment with a traditional crypto currency.
    - **Fair trade** – smart contracts enforce the fairness of the trade by ensuring the data provider is paid and the data requester obtains the data without the need for a trusted third party (Li et al., 2021).
    - **Anonymous** – the payment does not reveal any information about the payer or the amount of the transaction (Ou et al., 2019).
    - **Micro-payments Channel** – a side chain is created to support micro-payments between the data provider and the data requester. This system is put in place to resolve the performance problems usually associated with public ledgers like Bitcoin (Robert et al., 2020) or Ethereum (Radhakrishnan et al., 2019). These types of solutions support a continuous exchange of data which occurs via a channel. One of those solutions is the Open Messaging Interface (O-MI) from The Open Group Standard for the Internet of Things (IoT) (Robert et al., 2020).
- **Reputation** – the ledger keeps track of the reputation of the nodes which may reflect the node's ability to provide accurate information to the ecosystem (Pu et al., 2020). Even though certain implementations do not make direct references to the concept of "reputation" they do process data in a way that amounts to node reputation (Saldamli et al., 2020).

5 RESULTS AND FINDINGS

This section presents the results and discusses the main findings by answering the raised RQs.

Our research started by analyzing the types of distributed ledgers used in the studied implementations and how they were being deployed.

Some of implementations used publicly available distributed ledgers while others are custom ledgers. As shown in Figure 4, by far the most used is Ethereum, followed by Hyperledger Fabric. Almost a quarter of the implementations used a custom ledger. We also identified different ledger deployment types as depicted on Figure 5. While 87% of the implementations used a single ledger, 13% use a multiple ledger approach. Of those two used a *Hierarchical* deployment in which more than one blockchain of the same type is used to distribute transaction load across its nodes. For instance, the metering implementation in (Wang et al., 2019) uses regional and wide area blockchains. This strategy is both a scalability mechanism and an additional privacy layer as the subledger gateways only transmit aggregated information to the root blockchain. The Automated Data Trading in (Chuang et al., 2020) uses sub-blockchains at the edge to improve request response time. Two implementations used a *Hybrid* deployment in which the implementation uses more than one ledger type each executing a different role. The data marketplace in (Lopez and Farooq, 2019) uses Hyperledger Iroha and Hyperledger Indy. The prior ledger is used to enable transaction control, while the latter is used for identity and

data exchange protocol. The decentralized Digital Rights Management scheme in (Zhaofeng et al., 2020) uses Hyperledger Fabric and Ethereum. The prior acts as a storage mechanism and data exchange control that prevents public access to the data being protected, while the latter supports token economics and usage control mechanism. The intelligent traffic system in (Zichichi et al., 2020) uses IOTA and Ethereum. The prior acts as a low cost and scalable storage mechanism and the latter provides data access control smart contract support. Finally, one used a *Side-chained* in which the implementation uses a sub-blockchain to handle transactions quickly and then write the results to the main chain. In (Robert et al., 2020) the implementation sidechains Bitcoin to enable micropayments.

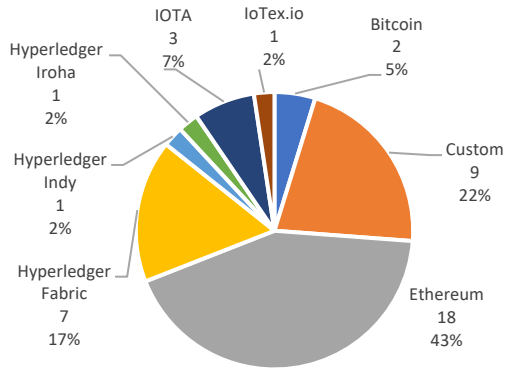

Figure 4 – Implementations' distributed ledgers.

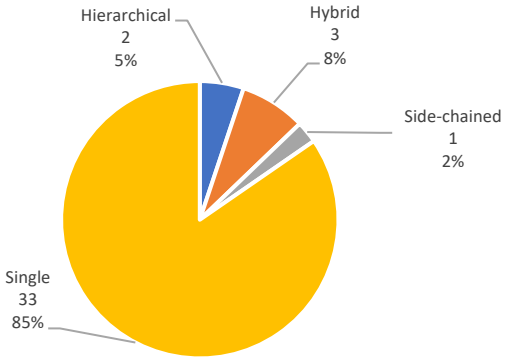

Figure 5 – Implementations' distributed ledgers deployment types.

RQ1: *How does DLT enables the people-centered approach in IoT?*

Our review of the selected papers in accordance with the *people-centered DLT roles classification* is shown on Table 4. The results we observed align with our expectations. Storage is used by 19 studies (34%) making it the most used DLT capability. As mentioned in Section 2.2 anchoring data to the ledger protects it from tampering and promotes accountability. Also as discussed in Section 2.2, the use of digital payments (22%) is completely justifiable since that was the reason for the invention of Bitcoin, the first DLT. Smart-contracts are a known mechanism to implement access-control (Cruz et al., 2018), and are used by 11 implementations (22%). Finally, performance, scalability, and cost (in the case of public ledgers) can explain the low percentage of studies that used smart contracts for data processing (13%) or reputation management (7%).

Table 4 – DLT uses in people-centered IoT ecosystems

Capability	Pattern	Papers
IoT Storage	Full	(Dimitriou and Mohammed, 2020; Gur et al., 2019; Lv et al., 2020; Ochoa et al., 2019; Pu et al., 2020; Wang et al., 2019; Zhang et al., 2021; Zhou et al., 2018)
	Hashing	(Angeletti et al., 2017; Dib et al., 2020; Kim and Lampkins, 2019; Makhdoom et al., 2020; Ou et al., 2019; Md Abdur Rahman et al., 2020; Mohamed Abdur Rahman et al., 2020; Rifi et al., 2018; Zhaofeng et al., 2020)
	Hybrid	(Uddin et al., 2018; Zichichi et al., 2020)
Data Access Control	Ecosystem Smart Contract	(Barati et al., 2020; Ding and Sato, 2020; Gur et al., 2019; Makhdoom et al., 2020; Sultana et al., 2020; Zichichi et al., 2020)
	IoT-device Smart Contract	(Fan et al., 2020; Md Abdur Rahman et al., 2020; Rifi et al., 2018)
	Second layer Channel ACL	(Lucking et al., 2020)
	Datum Smart Contract	(Chuang et al., 2020, 2018)
Data Processing	Pricing	(Liu et al., 2019)
	Contact Tracing	(Lv et al., 2020)

Capability	Pattern	Papers
	Data Exchange Criteria Matching	(Dib et al., 2020; Lopez and Farooq, 2019; Loukil et al., 2018; Nawaz et al., 2020; Rantos et al., 2019)
Digital Payment	Traditional	(Chuang et al., 2020, 2018; Dimitriou and Mohammed, 2020; Fan et al., 2020; Nawaz et al., 2020; Zhaofeng et al., 2020; Zichichi et al., 2020)
	Anonymous	(Ou et al., 2019)
	Fairtrade	(Li et al., 2021; Zhao et al., 2019)
	Micro-payments	(Radhakrishnan et al., 2019; Robert et al., 2020)
Reputation	-	(Chuang et al., 2020, 2018; Pu et al., 2020; Mohamed Abdur Rahman et al., 2020; Saldamli et al., 2020)

As shown on Figure 6, 19 implementations (49%) use ledger technology as a storing mechanism. Of those, 8 store the full data set, 9 store the hash of the data set, and 2 use a policy to store the complete data set on or off-ledger. We researched what ledgers were being used for full set data storage on Figure 7. Of those implementations that store the full data set, the ones that use Ethereum store small data sets. One stores worker location and task policy information in a crowdsourcing platform (Zhang et al., 2021), and the other stores license plate scanning owner's privacy preferences (Ochoa et al., 2019). The implementation that uses IOTA leverages the Masked Authenticated Messaging (MAM) (Shafeeq et al., 2019) feature and is used as distributed storage of the patient data (Lucking et al., 2020).

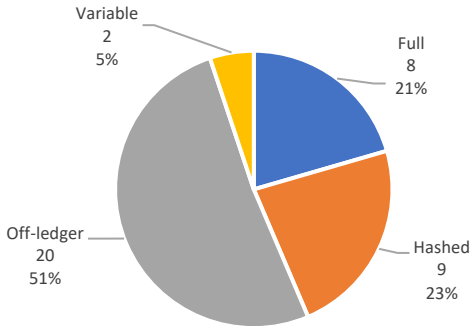

Figure 6 – Implementation's storage mechanism.

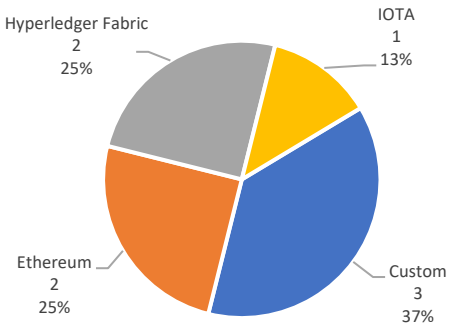

Figure 7 – On-ledger full data storage implementations' distributed ledgers.

We identified 14 sensing-as-a-service implementations (i.e., rewarded data sharing). Of those 12 used a ledger with crypto payment support. In the case of (Lopez and Farooq, 2019) it is stated that the reward layer can "be added in future with minimum effort". In the case of (Liu et al., 2019) it was not clear how the permissioned blockchain custom implementation enabled payments. As shown in Figure 8 most of those payments followed a simple crypto exchange, while five used specific strategies to improve payment performance, protected against malicious behavior from either the data provider or the data requester, and ensured no data about the payer, including the amount, could be inferred. In Figure 9 we show the ledgers used by these implementations.

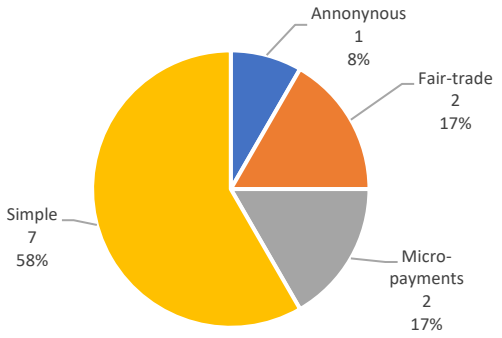

Figure 8 – Implementation's crypto payment types.

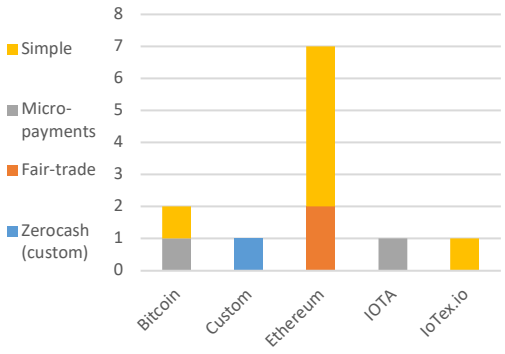

Figure 9 – Crypto-payment supported implementations' distributed ledgers.

As illustrated on Figure 10, most of the implementations that use smart contracts to define access control lists (ACL) use a single ecosystem smart contract. The Hyperledger framework (i.e., Fabric and Iroha) account for 4 of those implementations while Ethereum accounts for 2. Ethereum is used across all the different patterns apart from the second layer channel ACL (Figure 11).

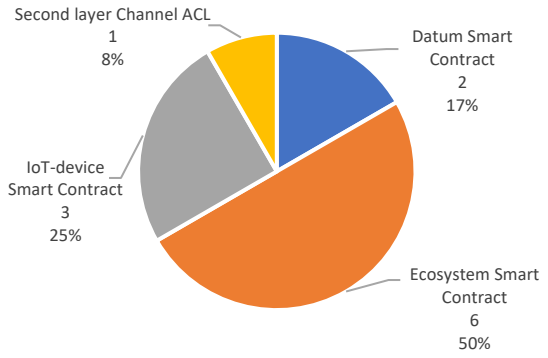

Figure 10 – Implementations' ledger-based ACL types.

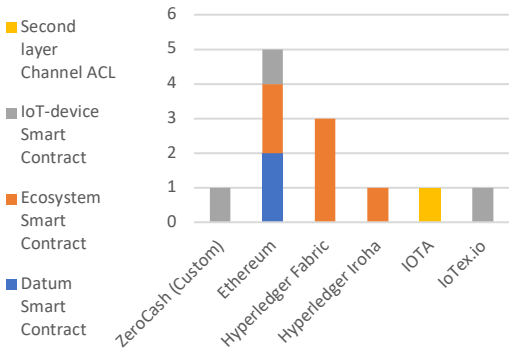

Figure 11 – Ledger-based ACL implementations' distributed ledgers.

RQ 1.1. – *Are there DLT-IoT people-centered emerging patterns?*

We found a wide diversity of DLT-based architectures used to implement people-centered IoT solutions. We found no evidence of emerging patterns. However, we were able to observe that:

- Ethereum is the dominant ledger with 44% of the implementations, while Hyperledger the distance second only has 20% (Figure 4).
- IOTA, a fit-for-purpose IoT distributed ledger, was only used in three implementations, one of which also utilized Ethereum.
- Self-Sovereign Identity (SSI), an approach that offers individuals agency of the data about them, was only used by two implementations. Both implementations were data-marketplaces. One used Hyperledger Indy (Lopez and Farooq, 2019) while the other used IoTex.io (Fan et al., 2020). SSI is an emerging concept that uses DLT to create decentralized identifiers (DIDs) which are under the sole control of consumers and offer strong support for consumer-controlled data management (Ferdous et al., 2019). Each DID has an associated set of cryptographic metadata which allows to establish an end-to-end secure channel using a transport-agnostic protocol called DIDComm ("DIDComm Messaging," 2020). In the context of IoT ecosystems the SSI concept facilitates device ownership, enhances privacy, and enables the exchange of data without the dependency on third parties. While it could be argued that the low number of SSI-based implementations is due to its

novelty or even to the difficulty of running SSI implementations like Hyperledger Indy/Aries over computing and bandwidth-constrained networks we were still surprised that more implementations did not consider using the identity and communication mechanisms provided by SSI implementations.

- Edge computing was only used in eleven implementations (28%) (Figure 12) however, its use grew significantly since 2019 (Figure 13). This increase is explained by the need to improve system performance and network resource utilization by off-load blockchain and/or ecosystem management functions from IoT nodes (Chuang et al., 2018).
- The term *data owner* is dominant to describe the individual who controls the IoT device. It is used in fifteen implementations (Figure 14), while the term *data consumer* and *data buyer* are dominant describing the entities who seek access to the IoT device data (Figure 15). While we could observe a tendency towards the use of "data owner" designation, we did not observe the same level of convergence towards the designation of entities seeking IoT data. We think that the standardization of IoT ecosystem vocabulary will eventually happen driven by IoT consortia. However, we also think that the "data owner" concept may end up not being used because there are voices cautioning and opposing data propertization (Ishmaev, 2020)
- Privacy preserving schemes adoption has been steadily growing since 2018 and in 2020 almost 40% of the implementations used it and in 2020 four of the implementations offered multiple preserving schemes (Figure 16) (Li et al., 2021; Lv et al., 2020; Pu et al., 2020; Mohamed Abdur Rahman et al., 2020; Zhang et al., 2021). As shown in Figure 17 the most common strategies are zero knowledge and homomorphic encryption. While privacy preserving schemes increase system complexity and require additional resources, it seems that there is a clear tendency towards its utilization. This observation seems to be further confirmed by a tendency in 2020 to use multi-level schemes towards protecting the confidentiality of not only the data being sharing but also the requests for data.

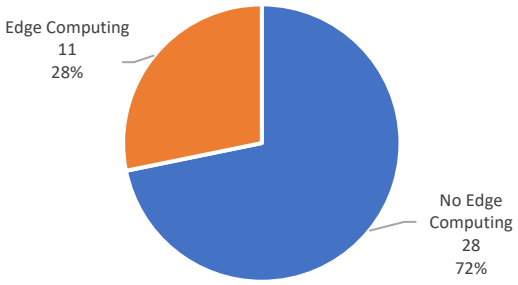

Figure 12 – Implementations' overall edge computing support.

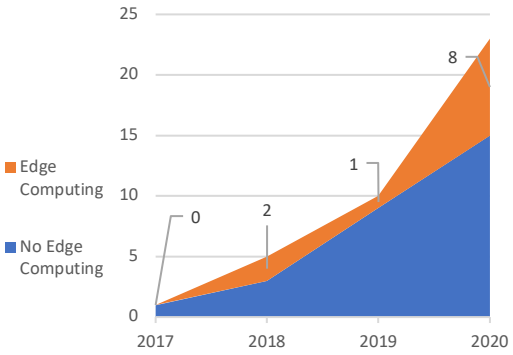

Figure 13 – Implementations' edge computing support growth over time.

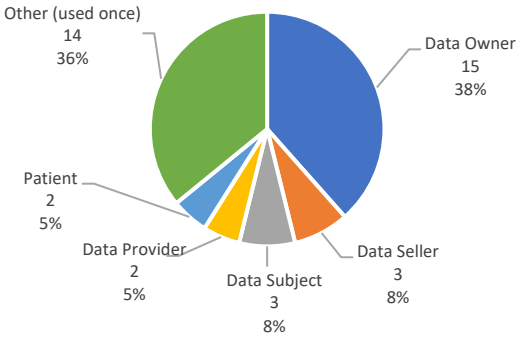

Figure 14 – Implementations' terms to refer to the indiviual who controls the IoT device.

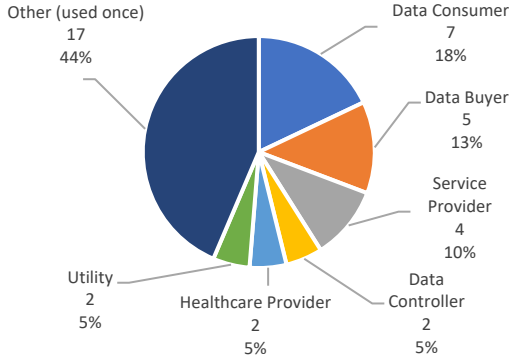

Figure 15 – Implementations' terms to refer to entity that seeks access to the IoT device's data.

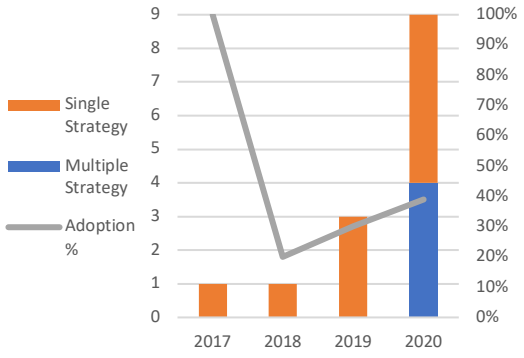

Figure 16 – Implementations' privacy-preserving growth over time (left axis) and single versus multiple privacy preserving support (right axis), over imposed with the privacy preserving schemes growth trend (in gray).

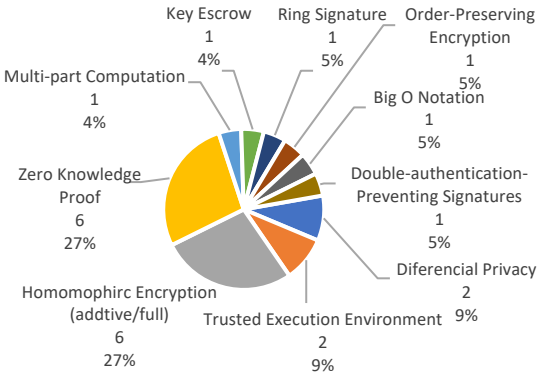

Figure 17 – Implementations' privacy preserving schemes.

RQ 1.2 – *Is there a correlation between a DLT-IoT implementation and an IoT application domain?*

We reviewed the studies in accordance with the *IoT application domain classification* defined in section 4 as shown on Table 6.

Table 5 – IoT Application Domain

Sub Exchanged Pattern	Papers
Generic	(Chuang et al., 2020; Fan et al., 2020; Kim and Lampkins, 2019; Li et al., 2021; Liu et al., 2019; Loukil et al., 2018; Nawaz et al., 2020; Radhakrishnan et al., 2019; Rantos et al., 2019; Robert et al., 2020; Sultana et al., 2020; Zhang and Fan, 2020; Zhao et al., 2019; Zhaofeng et al., 2020; Zhou et al., 2018)
Smart-City	(Makhdoom et al., 2020)
Smart-Grid	(Dimitriou and Mohammed, 2020; Gur et al., 2019; Wang et al., 2019)
Smart-Health	(Angeletti et al., 2017; Ding and Sato, 2020; Kumar et al., 2020; Lucking et al., 2020; Lv et al., 2020; Mohamed Abdur Rahman et al., 2020; Rifi et al., 2018; Uddin et al., 2018)
Smart-Home	(Barati et al., 2020, 2019)
Smart-Mobility	(Chuang et al., 2018; Dib et al., 2020; Lopez and Farooq, 2019; Ou et al., 2019; Pu et al., 2020; Md Abdur

Sub Exchanged Pattern	Papers
	Rahman et al., 2020; Saldamli et al., 2020; Zhang et al., 2021; Zichichi et al., 2020)
Smart-Security	(Ochoa et al., 2019)

To assess a potential relationship between DLT type and the *IoT application domain* we created the bubble chart (Figure 18).

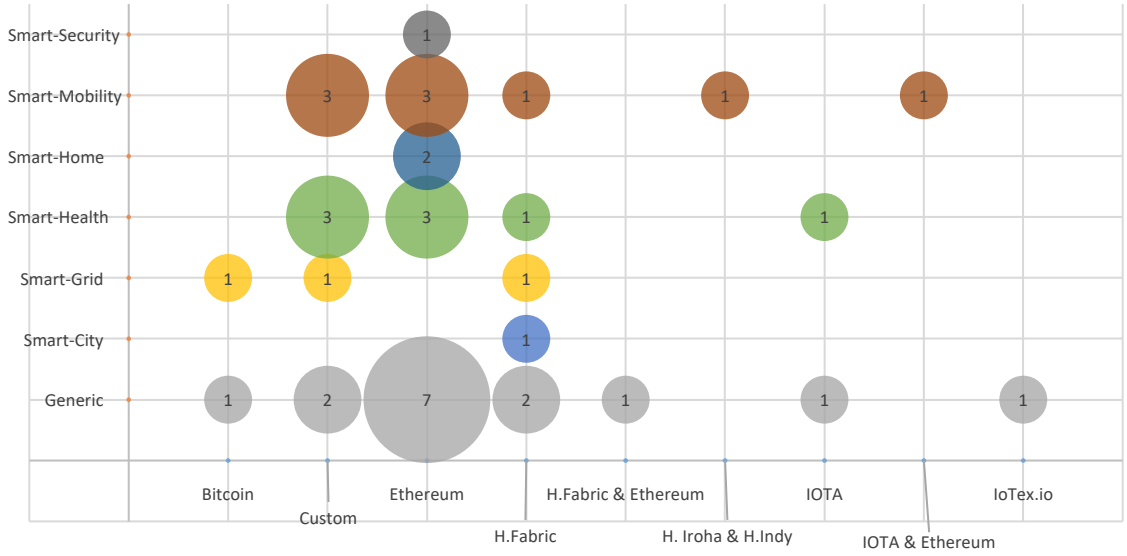

Figure 18 – Implementations' distributed ledger versus IoT application domain.

The "generic" IoT application domain is implemented by all types of DLT types which indicates that there is no correlation among them. As such, we decided to research whether there is a relationship between *data exchange* and the DLT type. We applied the *data exchange* classification to the papers as shown on Table 6.

Table 6 – IoT Data Exchange Patterns

Exchanged Pattern	Sub Exchanged Pattern	Papers
Individual Controlled	Sensing-as-a-Service	(Chuang et al., 2020; Dimitriou and Mohammed, 2020; Fan et al., 2020; Liu et al., 2019; Lopez and Farooq, 2019; Nawaz et al., 2020; Ou et al., 2019; Radhakrishnan et al., 2019; Robert et al., 2020; Zhao et al., 2019; Zhaofeng et al., 2020; Zichichi et al., 2020)
	Data Processing	(Dib et al., 2020; Lv et al., 2020; Zhang and Fan, 2020)
	Monitoring	(Ding and Sato, 2020; Lucking et al., 2020; Uddin et al., 2018)
	Voluntary Ecosystem Sharing	(Angeletti et al., 2017; Kim and Lampkins, 2019; Kumar et al., 2020; Loukil et al., 2018; Makhdoom et al., 2020; Md Abdur Rahman et al., 2020; Rantos et al., 2019; Rifi et al., 2018; Saldamli et al., 2020; Sultana et al., 2020; Zhang et al., 2021; Zhou et al., 2018; Zichichi et al., 2020)
	Federated Learning	(Mohamed Abdur Rahman et al., 2020)

Exchanged Pattern	Sub Exchanged Pattern	Papers
Service Provider Controlled	Metering	(Gur et al., 2019; Wang et al., 2019)
	Smart living	(Barati et al., 2020, 2019)
	Surveillance	(Ochoa et al., 2019)

As depicted in Figure 19, 90% of the papers we analyzed reflected an individual-controlled scenario. Of those 79% were Sensing-as-a-Service and voluntary ecosystem sharing scenarios (Figure 20).

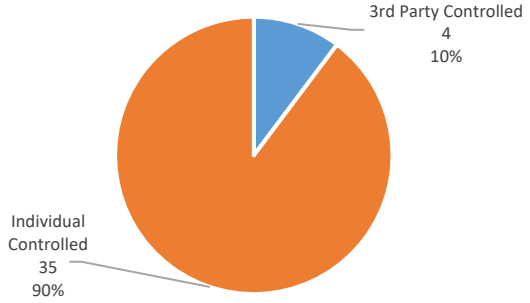

Figure 19 – Implementations' individual-controlled versus third party-controlled data exchange patterns.

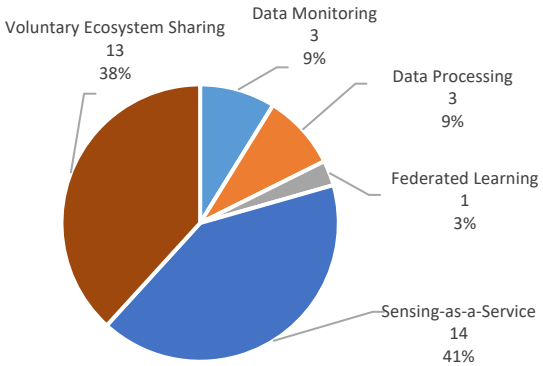

Figure 20 – Implementations' individual-controlled data sub-exchange patterns.

As we had concluded from Figure 18 that there was no correlation between DLT type and *IoT application domain*, we also found no correlation between DLT type and *sub-data exchange pattern* (Figure 21).

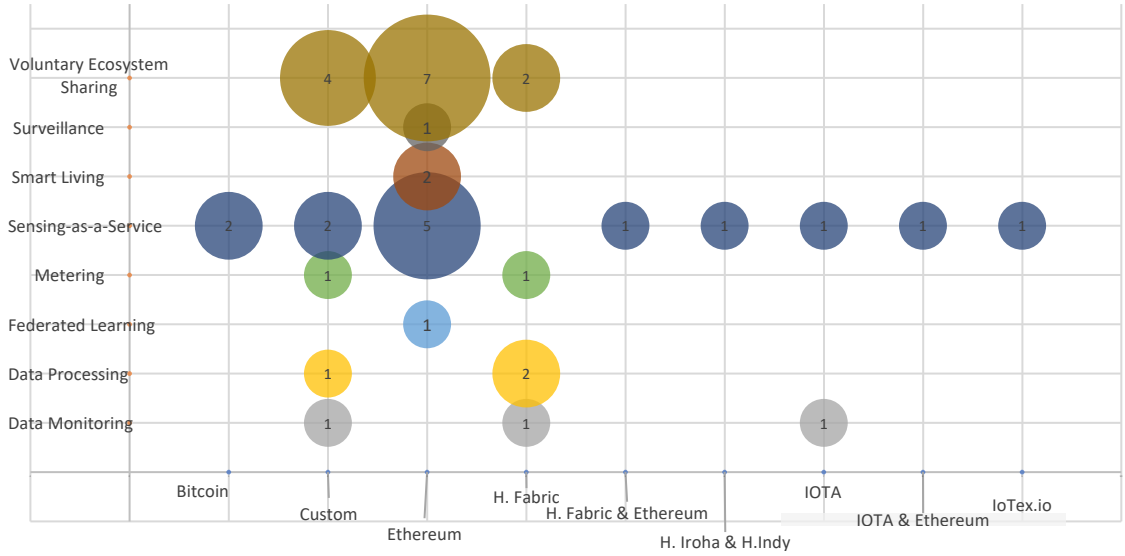

Figure 21 – Implementations distributed ledger versus IoT sub-data-exchange pattern.

RQ 1.3 – Are there gaps in the solutions analyzed?

The following gaps were identified:

- No implementation addresses the issues pertaining to the user experience.
- Except for implementations (Dib et al., 2020; Lopez and Farooq, 2019; Loukil et al., 2018; Nawaz et al., 2020; Rantos et al., 2019) that have smart contracts that pair data providers with data

requesters the aspects pertaining the discovery of data or services that need data is not appropriately discussed.

- Except for (Zhaofeng et al., 2020) no other paper talks about digital management rights. Once the data providers exchange or sell data they have little or no insight to what data requesters do with the data. In other words, the implementations have sophisticated data exchange capabilities but offer no functionality to manage any data economy events associated with the exchange.

RQ 2 –*What are the people-centered DTL-IoT strategies publishing trends?*

RQ 2.1 – *In which years were the papers published?*

As shown on Figure 22, the year 2020 represents a transition year during which the number of papers published on journals clearly outnumbers those published in conferences for the first time. From an *IoT application domain* point of view *smart mobility* and *smart health* gained momentum (Figure 23). In Figure 24, it can be observed that *voluntary sharing* and *sensing-as-a-service* are the two dominant sub-data exchange patterns over time. Except for *metering* and *surveillance*, that were only found in 2019, and *smart living* that has kept constant, all other exchange patterns are growing.

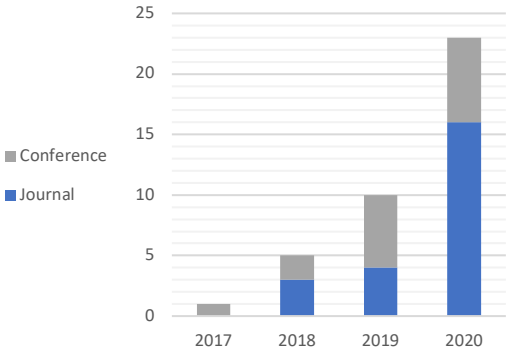

Figure 22 – Publications' type over time.

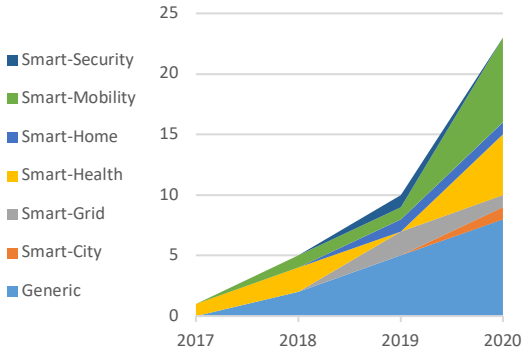

Figure 23 – Publications' IoT application domain over time.

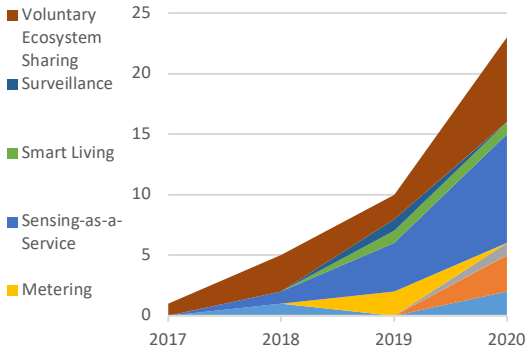

Figure 24 – Publications' data sub-exchange pattern over time.

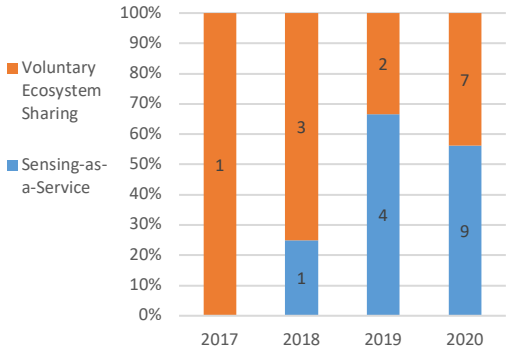

Figure 25 – Publications' rewarded versus unrewarded sub-data exchange patterns over time.

Finally, while we cannot infer a future pattern in terms of whether "rewarded data exchange" is gaining an edge over "voluntary sharing", it is still possible to observe that "sensing-as-a-service" solutions are a topic of interest among the research community (Figure 25).

RQ 2.2 – *What are the knowledge domains (e.g., IoT, Networking, Cloud, and Software Engineering) and publication type (i.e., Journal, Conference)?*

Except for the MDPI Sensors[9], IEEE Internet of Things Journal[10], IEEE Access each with three papers and the IEEE Network with two papers, no other journal or conference has more than one paper. This confirms the cross-disciplinarian nature of people-centered IoT solutions. In terms of the knowledge domain most papers are published in "networks" followed by "IoT" and "computer science" as can be seen in Figure 26.

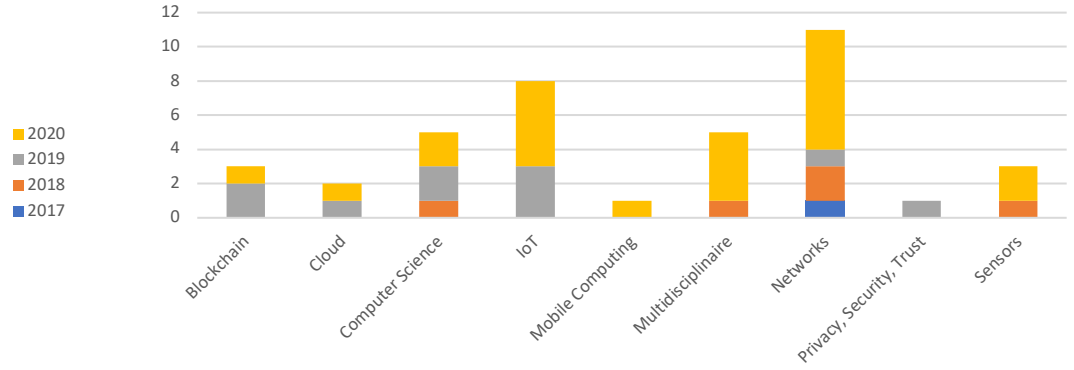

Figure 26 – Publications' knowledge domain over time.

R 2.3 – *What is researchers' country of affiliation?*

After analyzing the researchers' affiliation country, we observed that Chinese researchers have produced more than twice the number of papers than the next country which is the US. However, when we aggregate the European Countries (EC), we observed that European affiliated researchers lead over Chinese researchers (Figure 27).

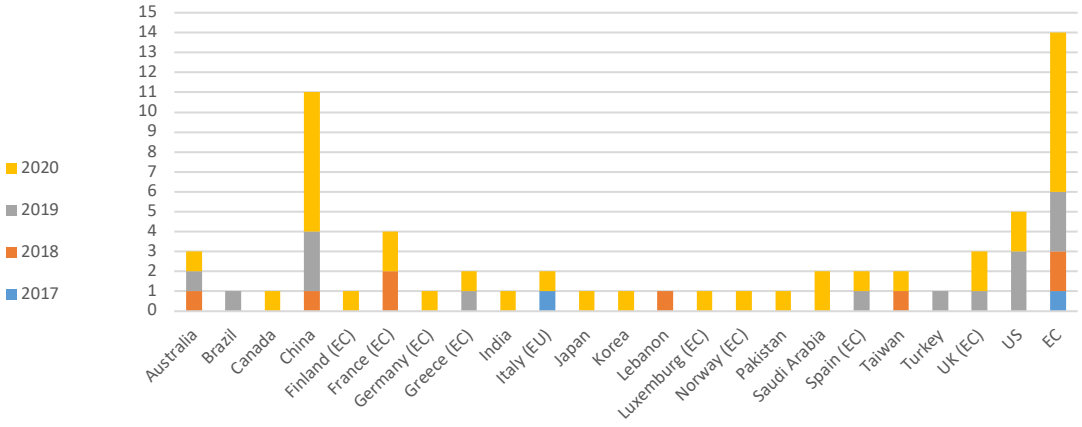

Figure 27 – Publications' author's affiliation country over time with EC grouped on the last bar.

While we did not observe any references to manufacturing national strategies (e.g., China 2025 - China, Industrie 4.0 – Germany, Industrial Internet Consortium (IIC) - US), we did find abundant references to GDPR (Barati et al., 2020, 2019; Dib et al., 2020; Gur et al., 2019; Kumar et al., 2020; Lopez and Farooq, 2019; Loukil et al., 2018; Lucking et al., 2020; Lv et al., 2020; Makhdoom et al., 2020; Ochoa et al., 2019; Rantos et al., 2019; Zichichi et al., 2020). While the prior observation could be indicative of a lack of coordination between OEMs' IoT standards and the research community, the latter observation is an indication that GDPR is influencing researchers. However, that impact is mostly observed among European affiliated researchers (Figure 28). It is important to note that no references were registered for the California Consumer Privacy Act

[9] https://www.mdpi.com/journal/sensors
[10] https://ieee-iotj.org/

(CCPA). Lastly, we observed that Chinese researchers have an edge on privacy preserving strategies (Figure 29) as they used it more frequently including multiple strategies combined.

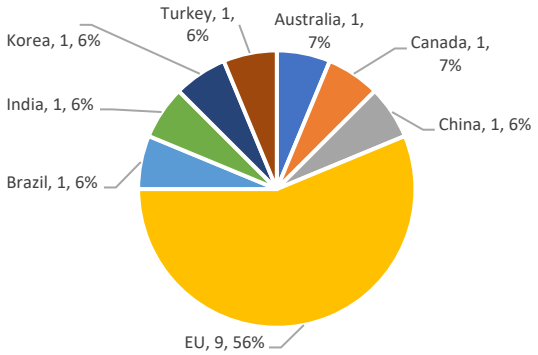

Figure 28 – Publications' GDPR mentions per authors' affiliation country.

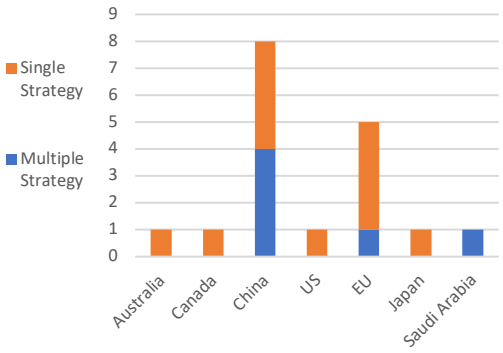

Figure 29 – Publications' privacy-preserving strategies versus authors' affiliation country.

6 DISCUSSION AND FUTURE RESEARCH DIRECTIONS

Despite very encouraging signs on the potential of people-centered DLT-IoT solutions, success depends on the future research of several important topics.

While we observed that Ethereum seems to be the dominant ledger among people-centered DLT-IoT architectures, each one of the implementations used its unique architecture. This situation leads to the impossibility of comparing solutions side-by-side. Research is necessary to define a minimum set of capabilities of a people-centered IoT solution. Even though we did not observe a consistent set of capabilities, we measured an increased interest over "edge computing" and "privacy preservation" (Figure 13, Figure 16). *Governments* (e.g., NIST), *business consortia* (e.g., Industrial Internet Consortium (IIC)[11], Digital Twin Consortium[12]), *professional associations* (e.g., IEEE[13]) and *non-profits* (e.g. Sovrin Foundation[14]) should work together to help define and standardize those capabilities (Bello and Zeadally, 2019). A wider consensus platform will balance individuals' interests better and those of market players that invest in product development thereby contributing to innovation. Per our research, this cooperation has yet to start as none of the studies made a single reference to the concept of digital twin, a term of great interest to OEMs.

Even though we identified implementations seeking to improve profit and/or fairness of individuals in sensing-as-a-service scenarios, they were limited in scope. Except for (Zhaofeng et al., 2020) no other studies offered individuals control of how data could be used (i.e., usage control). To improve data-economy fairness, individuals must be able to understand why data is collected and how it is used so they can make informed decisions about the use of their private data (Koskinen et al., 2019). To enable it, further research is needed to increase *data economy's value chains' transparency*. Along with personal data stores it will make individuals active stakeholders in data value creation (Lehtiniemi, 2017) granting them "*data outcome-control*". However, making individuals active participants in data value-chains will have to be further understood as *data propertization* can lead to counter intuitive results (Ishmaev, 2020).

Finally, while data value-chain transparency is key for individual data control it requires the existence of personal data stores. While 90% (Figure 19) of the implementations we studied assumed the individual had control over IoT data storage, most of today's IoT-enable devices do not allow it. Further research is necessary in the articulation of SSI and PDS in DLT-IoT implementations. While we observed little interest by the research

[11] https://www.iiconsortium.org/
[12] www.digitaltwinconsortium.org
[13] P2418.1 - Standard for the Framework of Blockchain Use in Internet of Things (IoT)
[14] https://sovrin.org/library-iot/

community in SSI, we think it will gain a lot more attention in the future given its foundational nature in allowing individuals to have control over the data about them.

7 CONCLUSIONS

The need to improve the privacy, security, ethics, and fairness of IoT data exchange has led to a growing interest in distributed ledger technology. DLT-IoT enables a people-centered approach to data exchange. It offers individuals a more active role in the exchange, allowing them to participate in the outcomes of the data economy.

This review examined the state-of-the-art of people-centered DLT-IoT architectures. The aim of this work was to assess whether there are architecture patterns emerging, and what the DLT-IoT's publication trends are. We surveyed solely papers that tested the proposed implementations. We manually reviewed over five hundred papers of which we selected thirty-nine (39).

We observed that DLT is used in different IoT solutions for different purposes and that there is no relation between the IoT application domain (i.e., smart-health) or data exchange pattern (e.g., sensing-as-a-service). While we found no evidence of emerging patterns, we noted a growing interest in privacy-preserving and edge computing mechanism.

We also observed that European affiliated countries researchers have a slight edge in terms of volume over Chinese researchers. However, the latter are using more sophisticated privacy-preserving schemes.

Based on our observations we proposed three vectors for future research: definition of the minimum capability-set of a people-centered DLT-IoT solution, definition of "data outcome-control" concept, SSI and PDS integration.

We conclude that DLT-IoT architectures and the protection of individuals' interests in the data economy is in an embryonic state. While there is a need for additional technological research advances to mature DLT-IoT architectures, continuous privacy leaks, IoT's continued explosive growth, and the interest in global passports triggered by COVID pandemic, may lead to increased collaboration between organizations and governments. This will accelerate the emergence of accessible, scalable, and reliable people-centered IoT solutions based on DLT.

ACKNOWLEDGMENTS

Funding acknowledgement statement: This work was supported by the Fundação para a Ciência e Tecnologia (FCT) within the following Projects: UIDB/04466/2020 and UIDP/04466/2020.

REFERENCES

Allana, S., Chawla, S., 2021. ChildShield: A rating system for assessing privacy and security of internet of toys. Telemat. Informatics 56, 101477. https://doi.org/10.1016/j.tele.2020.101477

Angeletti, F., Chatzigiannakis, I., Vitaletti, A., 2017. The role of blockchain and IoT in recruiting participants for digital clinical trials. 2017 25th Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2017. https://doi.org/10.23919/SOFTCOM.2017.8115590

Ashton, K., 2009. That 'Internet of Things' Thing | RFID JOURNAL [WWW Document]. URL https://www.rfidjournal.com/that-internet-of-things-thing (accessed 6.28.20).

Babbitt, D., Dietz, J., 2014. Crypto-economic Design: A Proposed Agent-Based Modelling Effort. Swarm Fest 2014 18th Annu. Meet. Agent-Based Model. Simul. 2–3.

Baik, J. (Sophia), 2020. Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). Telemat. Informatics 52, 101431. https://doi.org/10.1016/j.tele.2020.101431

Barati, M., Petri, I., Rana, O.F., 2019. Developing GDPR Compliant User Data Policies for Internet of Things, in: Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing, UCC'19. ACM, New York, NY, USA, pp. 133–141. https://doi.org/10.1145/3344341.3368812

Barati, M., Rana, O., Petri, I., Theodorakopoulos, G., 2020. GDPR Compliance Verification in Internet of Things. IEEE Access 8, 119697–119709. https://doi.org/10.1109/ACCESS.2020.3005509

Barker, E.B., 2016. Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, NIST Special

Publication. Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-175B

Batty, M., 2018. Digital twins. Environ. Plan. B Urban Anal. City Sci. 45, 817–820. https://doi.org/10.1177/2399808318796416

Bello, O., Zeadally, S., 2019. Toward efficient smartification of the Internet of Things (IoT) services. Futur. Gener. Comput. Syst. 92, 663–673. https://doi.org/10.1016/j.future.2017.09.083

Berghel, H., 2018. Malice Domestic: The Cambridge Analytica Dystopia. Computer (Long. Beach. Calif). 51, 84–89. https://doi.org/10.1109/MC.2018.2381135

Cameron, K., Nanda, A., Durand, A., Barnes, B., Ellison, C., Bowden, C., Burton, C., Kearns, D., Winer, D., Hardt, D., Searls, D., Reed, D., Mcdermott, E., Norlin, E., Dyson, E., Labalme, F., Kaliya, I.W., Cannon, J.C., Kobielus, J., Governor, J., Lewis, J., Shewchuk, J., Razzell, L., Canter, M., Wahl, M., Jones, M., Becker, P., Janocek, R., Pandya, R., Scoble, R., Lem-, S.C., Davies, S., Brands, S., Kwan, S., Heath, W., 2005. The Laws of Identity, Microsoft.

Christidis, K., Devetsikiotis, M., 2016. Blockchains and Smart Contracts for the Internet of Things. IEEE Access 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Chuang, I.-H., Huang, S.-H., Chao, W.-C., Tsai, J.-S., Kuo, Y.-H., 2020. TIDES: A Trust-Aware IoT Data Economic System With Blockchain-Enabled Multi-Access Edge Computing. IEEE Access 8, 85839–85855. https://doi.org/10.1109/ACCESS.2020.2991267

Chuang, I.-H., Weng, T.-C., Tsai, J.-S., Horng, M.-F., Kuo, Y.-H., 2018. A Reliable IoT Data Economic System Based on Edge Computing, in: 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, pp. 1–5. https://doi.org/10.1109/PIMRC.2018.8580742

Couldry, N., Mejias, U.A., 2019. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. Telev. New Media 20, 336–349. https://doi.org/10.1177/1527476418796632

Cruz, J.P., Kaji, Y., Yanai, N., 2018. RBAC-SC: Role-Based Access Control Using Smart Contract. IEEE Access 6, 12240–12251. https://doi.org/10.1109/ACCESS.2018.2812844

Dib, O., Huyart, C., Toumi, K., 2020. A novel data exploitation framework based on blockchain. Pervasive Mob. Comput. 61, 101104. https://doi.org/10.1016/j.pmcj.2019.101104

DIDComm Messaging [WWW Document], 2020. . DIF. URL https://identity.foundation/didcomm-messaging/spec/ (accessed 11.6.21).

Dimitriou, T., Mohammed, A., 2020. Fair and Privacy-Respecting Bitcoin Payments for Smart Grid Data. IEEE Internet Things J. 7, 10401–10417. https://doi.org/10.1109/JIOT.2020.2990666

Ding, Y., Sato, H., 2020. Derepo: A Distributed Privacy-Preserving Data Repository with Decentralized Access Control for Smart Health, in: 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). IEEE, pp. 29–35. https://doi.org/10.1109/CSCloud-EdgeCom49738.2020.00015

Ethereum.org [WWW Document], 2013. URL https://ethereum.org/en/whitepaper/ (accessed 7.3.20).

Ethereum Foundation [WWW Document], 2015. URL https://blog.ethereum.org/2015/07/30/ethereum-launches/ (accessed 7.3.20).

Fan, X., Chai, Q., Xu, L., Guo, D., 2020. DIAM-IoT: A decentralized identity and access management framework for internet of things. BSCI 2020 - Proc. 2nd ACM Int. Symp. Blockchain Secur. Crit. Infrastructure, Co-located with AsiaCCS 2020 186–191. https://doi.org/10.1145/3384943.3409436

Fedrecheski, G., Rabaey, J.M., Costa, L.C.P., Calcina Ccori, P.C., Pereira, W.T., Zuffo, M.K., 2020. Self-Sovereign Identity for IoT environments: A Perspective, in: 2020 Global Internet of Things Summit (GIoTS). IEEE, pp. 1–6. https://doi.org/10.1109/GIOTS49054.2020.9119664

Ferdous, M.S., Chowdhury, F., Alassafi, M.O., 2019. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access 7, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173

Grieves, M., 2014. Digital Twin : Manufacturing Excellence through Virtual Factory Replication. White Pap.

Gur, A.O., Oksuzer, S., Karaarslan, E., 2019. Blockchain Based Metering and Billing System Proposal with Privacy Protection for the Electric Network, in: 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG). IEEE, pp. 204–208. https://doi.org/10.1109/SGCF.2019.8782375

Heather Vescent, K.Y.& J.C., 2018. Entities, identities, registries. Exploring the Gaps in Corporate & IoT Identity.

IDC [WWW Document], 2019. . IDC. URL https://www.idc.com/getdoc.jsp?containerId=prUS45213219 (accessed 10.1.21).

Ishmaev, G., 2020. The Ethical Limits of Blockchain-Enabled Markets for Private IoT Data. Philos. Technol. 33, 411–432. https://doi.org/10.1007/s13347-019-00361-y

Kim, T.H.-J., Lampkins, J., 2019. SSP: Self-Sovereign Privacy for Internet of Things Using Blockchain and MPC, in: 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, pp. 411–418. https://doi.org/10.1109/Blockchain.2019.00063

Kim, W., Duffy, H., Sabadello, M., Zagidulin, D., Caballero, J., Vescent, H., Young, K., Kim, W., Duffy, H., Sabadello, M., Zagidulin, D., Caballero, J., 2018. A Comprehensive Guide To Self Sovereign Identity. The Purple Tornado, Inc.

Koskinen, J., Knaapi-Junnila, S., Rantanen, M.M., 2019. What if we Had Fair, People-Centred Data Economy Ecosystems?, in: 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, pp. 329–334. https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00100

Kumar, A., Sharma, D.K., Nayyar, A., Singh, S., Yoon, B., 2020. Lightweight proof of game (LPoG): A proof of work (PoW)'s extended lightweight consensus algorithm for wearable kidneys. Sensors (Switzerland) 20. https://doi.org/10.3390/s20102868

Langford, J., Poikola, A., Janssen, W., Lähteenoja, V., Rikken, M., 2020. Understanding MyData Operators 40.

Lehtiniemi, T., 2017. Personal Data Spaces: An Intervention in Surveillance Capitalism? Surveill. Soc. 15, 626–639. https://doi.org/10.24908/ss.v15i5.6424

Lewis., A., 2015. A gentle introduction to digital tokens – Bits on Blocks [WWW Document]. URL https://bitsonblocks.net/2015/09/28/gentle-introduction-digital-tokens/ (accessed 7.3.20).

Li, Y., Li, L., Zhao, Y., Guizani, N., Yu, Y., Du, X., 2021. Toward Decentralized Fair Data Trading Based on Blockchain. IEEE Netw. 35, 304–310. https://doi.org/10.1109/MNET.011.2000349

Liu, K., Qiu, X., Chen, W., Chen, X., Zheng, Z., 2019. Optimal Pricing Mechanism for Data Market in Blockchain-Enhanced Internet of Things. IEEE Internet Things J. 6, 9748–9761. https://doi.org/10.1109/JIOT.2019.2931370

Lopez, D., Farooq, B., 2019. A multi-layered blockchain framework for smart mobility data-markets. Transp. Res. Part C Emerg. Technol., UCC'19 111, 588–615. https://doi.org/10.1016/j.trc.2020.01.002

Loukil, F., Ghedira-Guegan, C., Boukadi, K., Benharkat, A.N., 2018. Semantic IoT Gateway: Towards Automated Generation of Privacy-Preserving Smart Contracts in the Internet of Things, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 207–225. https://doi.org/10.1007/978-3-030-02610-3_12

Lucking, M., Manke, R., Schinle, M., Kohout, L., Nickel, S., Stork, W., 2020. Decentralized patient-centric data management for sharing IoT data streams, in: 2020 International Conference on Omni-Layer Intelligent Systems (COINS). IEEE, pp. 1–6. https://doi.org/10.1109/COINS49042.2020.9191653

Lv, W., Wu, S., Jiang, C., Cui, Y., Qiu, X., Zhang, Y., 2020. Towards Large-Scale and Privacy-Preserving Contact Tracing in COVID-19 pandemic: A Blockchain Perspective. IEEE Trans. Netw. Sci. Eng. 1–1. https://doi.org/10.1109/TNSE.2020.3030925

Lyons, T., Courcelas, L., Timsit, K., 2019a. Blockchain and Digital Identity.

Lyons, T., Courcelas, L., Timsit, K., 2019b. Scalability Interoperability And Sustainability Of Blockchains.

Mai, J.-E., 2016. Big data privacy: The datafication of personal information. Inf. Soc. 32, 192–199. https://doi.org/10.1080/01972243.2016.1153010

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., Ni, W., 2020. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Comput. Secur. 88, 101653. https://doi.org/10.1016/j.cose.2019.101653

McMillan, R., 2012. The World's First Computer Password? It Was Useless Too | WIRED [WWW Document]. Wire Mag. URL https://www.wired.com/2012/01/computer-password/ (accessed 5.14.20).

Meierhofer, J., West, S., Rapaccini, M., Barbieri, C., 2020. The Digital Twin as a Service Enabler: From the Service Ecosystem to the Simulation Model, in: Lecture Notes in Business Information Processing. pp. 347–359. https://doi.org/10.1007/978-3-030-38724-2_25

Mir, A., Zuhairi, M.F., Musa, S., Syed, T.A., Alrehaili, A., 2020. POSTER: A Survey of Security Challenges with 5G-IoT, in: 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH). IEEE, pp. 249–250. https://doi.org/10.1109/SMART-TECH49988.2020.00063

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

Nawaz, A., Peña Queralta, J., Guan, J., Awais, M., Gia, T.N., Bashir, A.K., Kan, H., Westerlund, T., 2020. Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain. Sensors 20, 3965. https://doi.org/10.3390/s20143965

Nižetić, S., Šolić, P., López-de-Ipiña González-de-Artaza, D., Patrono, L., 2020. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. J. Clean. Prod. 274, 122877. https://doi.org/10.1016/j.jclepro.2020.122877

Ochoa, I., Calbusch, L., Viecelli, K., de Paz, J., Leithardt, V., Zeferino, C., 2019. Privacy in the Internet of Things: A Study to Protect User's Data in LPR Systems Using Blockchain, in: 2019 17th International Conference on Privacy, Security and Trust (PST). IEEE, pp. 1–5. https://doi.org/10.1109/PST47121.2019.8949076

Oliveira, L., Bauer, I., Zavolokina, L., Schwabe, G., 2018. To token or not to token: Tools for understanding blockchain tokens. Int. Conf. Inf.

Syst. 2018, ICIS 2018. https://doi.org/https://doi.org/10.5167/uzh-157908

Ou, W., Deng, M., Luo, E., 2019. A Decentralized and Anonymous Data Transaction Scheme Based on Blockchain and Zero-Knowledge Proof in Vehicle Networking (Workshop Paper), in: Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. Springer International Publishing, pp. 712–726. https://doi.org/10.1007/978-3-030-30146-0_48

Paiola, M., Gebauer, H., 2020. Internet of things technologies, digital servitization and business model innovation in BtoB manufacturing firms. Ind. Mark. Manag. 89, 245–264. https://doi.org/10.1016/j.indmarman.2020.03.009

Pilkington, M., 2016. Blockchain technology: principles and applications, in: Research Handbook on Digital Transformations. Edward Elgar Publishing, pp. 225–253. https://doi.org/10.4337/9781784717766.00019

Pu, Y., Xiang, T., Hu, C., Alrawais, A., Yan, H., 2020. An efficient blockchain-based privacy preserving scheme for vehicular social networks. Inf. Sci. (Ny). 540, 308–324. https://doi.org/10.1016/j.ins.2020.05.087

Qi, Q., Tao, F., 2018. Digital Twin and Big Data Towards Smart Manufacturing and Industry 4.0: 360 Degree Comparison. IEEE Access 6, 3585–3593. https://doi.org/10.1109/ACCESS.2018.2793265

Radhakrishnan, R., Ramachandran, G.S., Krishnamachari, B., 2019. SDPP: Streaming Data Payment Protocol for Data Economy, in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, pp. 17–18. https://doi.org/10.1109/BLOC.2019.8751291

Rahman, Mohamed Abdur, Hossain, M.S., Islam, M.S., Alrajeh, N.A., Muhammad, G., 2020. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. IEEE Access 8, 205071–205087. https://doi.org/10.1109/ACCESS.2020.3037474

Rahman, Md Abdur, Hossain, M.S., Rashid, M.M., Barnes, S., Hassanain, E., 2020. IoEV-Chain: A 5G-Based Secure Inter-Connected Mobility Framework for the Internet of Electric Vehicles. IEEE Netw. 34, 190–197. https://doi.org/10.1109/MNET.001.1900597

Rantos, K., Drosatos, G., Demertzis, K., Ilioudis, C., Papanikolaou, A., Kritsas, A., 2019. ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT Using Blockchain Technology, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer International Publishing, pp. 300–313. https://doi.org/10.1007/978-3-030-12942-2_23

Rifi, N., Agoulmine, N., Chendeb Taher, N., Rachkidi, E., 2018. Blockchain Technology: Is It a Good Candidate for Securing IoT Sensitive Medical Data? Wirel. Commun. Mob. Comput. 2018. https://doi.org/10.1155/2018/9763937

Robert, J., Kubler, S., Ghatpande, S., 2020. Enhanced Lightning Network (off-chain)-based micropayment in IoT ecosystems. Futur. Gener. Comput. Syst. 112, 283–296. https://doi.org/10.1016/j.future.2020.05.033

Saldamli, G., Karunakaran, K., Vijaykumar, V.K., Pan, W., Puttarevaiah, S., Ertaul, L., 2020. Securing Car Data and Analytics using Blockchain, in: 2020 Seventh International Conference on Software Defined Systems (SDS). IEEE, pp. 153–159. https://doi.org/10.1109/SDS49854.2020.9143914

Searls, D., 2012. The Intention Economy: When Customers Take Charge. Harvard Business Review Press.

Sendler, U., 2018. The Initiative in Germany, in: The Internet of Things. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 49–66. https://doi.org/10.1007/978-3-662-54904-9_4

Shafeeq, S., Alam, M., Khan, A., 2019. Privacy aware decentralized access control system. Futur. Gener. Comput. Syst. 101, 420–433. https://doi.org/10.1016/j.future.2019.06.025

Skinner, C., 2016. ValueWeb: How Fintech Firms are Using Bitcoin Blockchain and Mobile Technologies to Create the Internet of Value.

SmartCities World [WWW Document], 2017. URL https://www.smartcitiesworld.net/news/news/cisco-study-reveals-iot-data-paradox-2392 (accessed 2.16.21).

Stark, J., 2018. Product Lifecycle Management (Volume 3): The Executive Summary, Decision Engineering. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-72236-8

Sultana, T., Ghaffar, A., Azeem, M., Abubaker, Z., Gurmani, M.U., Javaid, N., 2020. Data Sharing System Integrating Access Control Based on Smart Contracts for IoT. pp. 863–874. https://doi.org/10.1007/978-3-030-33509-0_81

Swan, M., 2015. Blockchain Blueprint For a New Economy. O'Reilly.

Szabo, N., 1997. Formalizing and Securing Relationships on Public Networks. First Monday 2. https://doi.org/10.5210/fm.v2i9.548

Szabo, N., 1994. Smart Contracts [WWW Document]. URL https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed 6.30.20).

Tao, F., Zhang, M., 2017. Digital Twin Shop-Floor: A New Shop-Floor Paradigm Towards Smart Manufacturing. IEEE Access 5, 20418–20427. https://doi.org/10.1109/ACCESS.2017.2756069

Tao, F., Zhang, M., Nee, A.Y.C., 2019. Background and Concept of Digital Twin, in: Digital Twin Driven Smart Manufacturing. Elsevier, pp. 3–28. https://doi.org/10.1016/B978-0-12-817630-6.00001-1

Tobin, A., Reed, D., 2017. The Inevitable Rise of Self-Sovereign Identity: A white paper from the Sovrin Foundation [White Paper]. Sovrin.Org 23.

Tom Lyons, L.C., 2020. Convergence of Blockchain, IoT and AI.

Uddin, M.A., Stranieri, A., Gondal, I., Balasubramanian, V., 2018. Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture. IEEE Access 6, 32700–32726. https://doi.org/10.1109/ACCESS.2018.2846779

Vargo, S.L., Lusch, R.F., 2008. Service-dominant logic: continuing the evolution. J. Acad. Mark. Sci. 36, 1–10. https://doi.org/10.1007/s11747-007-0069-6

Wang, Y., Luo, F., Dong, Z., Tong, Z., Qiao, Y., 2019. Distributed meter data aggregation framework based on Blockchain and homomorphic encryption. IET Cyber-Physical Syst. Theory Appl. 4, 30–37. https://doi.org/10.1049/iet-cps.2018.5054

web.archive.org, 2010. Block 0 - Bitcoin Block Explorer [WWW Document]. URL https://web.archive.org/web/20131015154613/http://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f (accessed 6.24.20).

Wright, A., De Filippi, P., 2015. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN Electron. J. https://doi.org/10.2139/ssrn.2580664

Yaga, D., Mell, P., Roby, N., Scarfone, K., 2018. Blockchain technology overview, National Institute of Standards and Technology. Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8202

Zhang, D., Fan, L., 2020. Cerberus: Privacy-preserving computation in edge computing. IEEE INFOCOM 2020 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2020 43–49. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162942

Zhang, J., Yang, F., Ma, Z., Wang, Z., Liu, X., Ma, J., 2021. A Decentralized Location Privacy-Preserving Spatial Crowdsourcing for Internet of Vehicles. IEEE Trans. Intell. Transp. Syst. 22, 2299–2313. https://doi.org/10.1109/TITS.2020.3010288

Zhao, Y., Yu, Y., Li, Y., Han, G., Du, X., 2019. Machine learning based privacy-preserving fair data trading in big data market. Inf. Sci. (Ny). 478, 449–460. https://doi.org/10.1016/j.ins.2018.11.028

Zhaofeng, M., Lingyun, W., Xiaochang, W., Zhen, W., Weizhe, Z., 2020. Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. IEEE Internet Things J. 7, 4000–4015. https://doi.org/10.1109/JIOT.2019.2960526

Zhou, L., Wang, L., Ai, T., Sun, Y., 2018. BeeKeeper 2.0: Confidential Blockchain-Enabled IoT System with Fully Homomorphic Computation. Sensors 18, 3785. https://doi.org/10.3390/s18113785

Zhu, Q., Loke, S.W., Trujillo-Rasua, R., Jiang, F., Xiang, Y., 2019. Applications of Distributed Ledger Technologies to the Internet of Things: A Survey. ACM Comput. Surv. 52. https://doi.org/10.1145/3359982

Zichichi, M., Ferretti, S., D'angelo, G., 2020. A Framework Based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems. IEEE Access 8, 100384–100402. https://doi.org/10.1109/ACCESS.2020.2998012

Zuboff, S., 2015. Big other: Surveillance Capitalism and the Prospects of an Information Civilization. J. Inf. Technol. 30, 75–89. https://doi.org/10.1057/jit.2015.5