future internet

MDPI

Article

Comparing Blockchain Standards and Recommendations

Lukas König *, Yuliia Korobeinikova, Simon Tjoa and Peter Kieseberg

Josef Ressel Centre for Blockchains and Security Management, St. Pölten University of Applied Sciences, 3100 St. Pölten, Austria; yuliia.korobeinikova@fhstp.ac.at (Y.K.); simon.tjoa@fhstp.ac.at (S.T.); peter.kieseberg@fhstp.ac.at (P.K.)

* Correspondence: is191836@fhstp.ac.at; Tel.: +43-680-2382-190

Received: 12 November 2020 ; Accepted: 4 December 2020; Published: 7 December 2020

Abstract: Since the introduction of Bitcoin, the term "blockchain" has attracted many start-ups and companies over the years, especially in the financial sector. However, technology is evolving faster than standardization frameworks. This left the industry in the position of having to use this emerging technology, without being backed by any international standards organization regarding for neither the technology itself, nor for a blockchain specific information security framework. In times of the General Data Protection Regulation and growing international trade conflicts, protecting information is more relevant than ever. Standardization of blockchains is an appeal to raise the development of information technologies to the next level. Therefore, this paper shall provide an overview of standardization organization's publications about blockchains/distributed ledger technologies, a set of comparison criteria for future work and a comparison of the existing standards work itself. With that information, aligning to existing standardization efforts becomes easier, and might even present the possibility to create frameworks where there are none at the moment.

Keywords: blockchain; standardization; distributed Ledger; GDPR; standardisation life cycle; information security management; smart contracts

1. Introduction

Distributed ledger technology (DLT) has many use cases throughout various economic sectors and even for individual beings, as shown by the plethora of use cases in [1]. Nevertheless, despite the global possibilities, blockchains are not yet widely used in our everyday lives. One of the reasons for this is the lack of standardization [2–4]. There are still no standards catering to the mass implementation of blockchain and the situation must change to ensure a sustained survival of the DLT ecosystem as a major part of modern technology. In this regard, several industry alliances and standardization authorities are now working together to create global DLT and blockchain standards. Rating agency Moody's [5] experts believe that standardization will accelerate the process of technology implementation, reduce transaction costs, level out regulatory risks, improve the interoperability of systems, and improve the quality of interaction between market participants, as well as it will increase the attractiveness of securing assets on a blockchain.

According to a forecast by researchers at MarketsandMarkets, the market of blockchain IoT will reach up to USD 113.1 million with an average annual growth rate of 92.92% over a period of 5 years by 2024 [6]. While these numbers are focused on just one single field of application, the Internet of Things, there are various additional sectors where blockchains and the distributed ledger technology can be utilized, suggesting a number that is higher by a multifold for the entirety of the technology. The impact of blockchains on the generation of value in different industries is outlined in [7].

Standardization of blockchain technology is an important step towards a common concept, interoperability, scaling, auditing and possible further regulation of the technology. The overall lack of standardization and clarity is considered as an obstacle to the adoption of the technology [3]. Besides the sometimes negatively afflicted image of blockchains stemming from cyber crime, its compatibility to existing laws and regulations, as well as internal policies is hard to assess without internationally and universally valid standardization which can be used for orientation.

The main contributions of this work can be summarized as follows:

- We give an overview on existing (final) standardization efforts concerning blockchain and digital ledger techniques.
- Furthermore, we provide a set of criteria for comparing these standards and recommendations aimed at blockchains and related technologies that can be used in future work.
- Existing standards and publications of major standardisation organisations are compared using these criteria in order to provide a comprehensive, yet fast to read, overview on standardisation activities in this field.
- We discuss dependencies of the selected publications to other standardization work. These interconnections can reveal valuable information about the content.

This paper is organized in the following way:

- Section 2 explains related concepts and the importance of standardization in IT.
- Section 3 lists the criteria we used to compare the source material and our selection process.
- Section 4 provides an overview of the selected source material.
- Section 5 compares the standards according to our criteria and highlights interconnections to other standards.
- Section 6 is used to explain our results and contains concluding thoughts.
- Section 7 is a discussion on further points of relevancy.

We are convinced that such a comparison is of great value for the blockchain community, as it provides an overview of a topic that is usually not the center of attention. As mentioned in Section 2.1, there was only limited research on the topic in the past and since then many new developments emerged, which are still unaccounted for. Additionally, to our knowledge we provide the first comparison that goes beyond enumerating bodies of standardization and their working groups on blockchain. With our set of criteria and reasoning we generate new insights.

2. Background & Related Work

2.1. Related Concepts

During our research, we found a couple examples of work focusing on standardization of distributed ledgers. Starting with the first one, *Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies* [8], a group report from ETSI. It is part of an Industry Specification Group working on distributed ledgers which is not limited to standardization activities and therefore includes research activities and initiatives concerning blockchain and the distributed ledger as well. The document states that distributed ledger technology could have great potential, underlined with a selection of possible fields of usage in various domains. Its core, however, is the discussion of current standardization and research activities. Since we focus on standardization activities in this paper, the first part is of special interest to us. Standardization activities are relatively underrepresented compared to the other content, which suggests that at the time there was only a limited amount of efforts on blockchain and DLT standardization. Furthermore, the presented information consists of a list of organizations and a description of the general working direction and does not include an analysis of the published work itself. The document also mentions regulatory aspects and difficulties that

could arise for distributed ledger technologies. Additionally, it includes a short list of different data structures for ledgers and a substantial overview of research and innovation projects on the matter.

The second related work is the *Distributed ledger technology standardization landscape* [9] technical report by ITU-T Focus Group on Application of Distributed Ledger Technologies (FG DLT). This document focuses on the standardization landscape, not including research or industrial initiatives. The core part of this report mainly consists of an in-depth overview of the cumulative activities of study groups at ITU-T, including not only the FG DLT, but also focus groups with similar research directions but differentiating main topics. These include for example focus groups on the internet of things and smart cities, and digital financial services. The overview of other bodies of standardization is more detailed than in [8]. Nonetheless, the work done by ITU-T in this report is still in the form of an enumeration of standardization activities, without evaluating the content of the mentioned documents.

In [10], the authors point out the importance of blockchain standardization to overcome a number of problems. Furthermore, they provide an overview of standardization efforts of international organizations from early 2016 which includes ISO, IEEE, ITU and W3C. At the time of publication of this source, none of these organisations have produced publications and are merely at an early formation stage of several working groups. In the article it becomes apparent however, that standardization of blockchain technologies is of national interest for China.

Our own research differs from these related work examples in multiple ways. For one, the number of included standardization activities is more thorough than those of the previous examples. Not only concerning the state of published work, which could be easily explained by acknowledging the point in time of the research, but also because we include several organizations that had been left unmentioned previously because they are more relevant for the field of information security instead of distributed ledger technology. Second, the core of this paper is not to simply provide a list of existing documents, but rather to look at their contents. As already mentioned in the introduction 1, we focus on providing a thorough catalogue of criteria to compare and analyze the presented standardization efforts.

2.2. Standardization in Traditional IT

Standardization in the world of IT is nothing new. Without standardized procedures and processes, worldwide communication would not be possible. Especially organizations like *IEEE* are well known for providing technical standardization [11]. Information stored on IT systems becomes more and more sensitive which in turn raises the need for appropriate protection. Organizations providing internationally accepted frameworks for information security can thus help in increasing the overall level of security of information systems. A prime example is *ISO* with their standards series 27k. These are incredibly important for both, organizations and governments eager to improve in the field of information security. Nowadays, managerial tools like an information security management system are well known constructs and their importance for company success is undoubted as it leverages the overall security and possibility of universally understandably auditing and measuring of information security [12–14]. Standardization is an important aspect of technology development. Information technologies are facilitating process standardization and process control and creating business value. A standardized framework will allow objective information security auditing of blockchain systems on a larger scale. [15–17].

3. Materials and Methods

The research methodology was composed of comparative, analytical methods and system approach. A tailored review of the existing standards was conducted.

3.1. Standard Selection

For this research we solely selected published work from organizations that focus on standardization, such as ISO, and do not discuss drafts of any stage as the content of these can

be the subject of change before a final release version is available. Similarly, we do not consider company specific protocols or processes which are sometimes falsely called "standard" that are solely used in i.e., Ethereum in the form of specific Tokens, as such implementations are only relevant for individual solutions and not globally applicable standardization that is independent from the chosen blockchain platform. Such elements are not relevant for this research. The selection of standardization efforts presented in this paper is based on two approaches. At first, we started researching for publications and activities of well known standardization organizations and organizations which work more specifically towards information security. For the second approach, we expanded our research and standardization coverage by including additional information which we were able to gather through related work references, stated in Section 2. Information presented in these serves as a complement for our own research.

3.2. Comparison Criteria

Since the selection of standards and recommendations that will be discussed and compared within this work is very broad, with a wide variety of targets of the documents in question, the comparison criteria also need to reflect this diversity. Furthermore, the level of details these standards provide is very different, especially concerning special topics like GDPR compliance and the integration of legal issues. Still, even from a technical and managerial viewpoint, the different focus points of the standards make comparison difficult and not doable using a single metric. In addition it must be noted that not all documents mentioned in this section actually focus on blockchain or digital ledger technologies, for some this is only a side issue that is taken into account, but not the main topic. Still, such documents can be very valuable, especially when they are focusing on best practices inside a specific application domain, thus being of significance for the field in questions.

The selected standards and best practices were structured along the following criteria, which were grouped into four sets: (i) Criteria reflecting on the document, its applicability, meta information and domain itself (*document criteria*), and (ii) criteria reflecting the actual content of the documents (*content criteria*). It must be mentioned again that we only considered standards that are already published in their final form, no drafts or intermediate discussion results were included, as these (a) are often not widely available and (b) might be subject to considerable changes before final release. Furthermore, none of these documents comprises a normative document, all of these documents are of informative nature only.

3.2.1. Document Criteria

These criteria deal more with the document and its nature itself than with content details, still, they are important for comparing the documents at hand:

- Type: Several standardization institutions provide different types of publications. Thus, in order to provide comparability, we generalized these to the following types: "best practice", "report", "recommendation" and "standard".
- Technical Specification: Defines, whether the document constitutes normative or informative information. All of the documents analyzed in this work are of informative nature, i.e., they are not legally binding or can be used for certification per se.
- Document Objective: This criterion provides a rough categorization on the objective of each document, i.e., whether it lies in defining terminology ("definitions"), give an overview on the field or a sub field ("topic overview"), provides support when deciding whether to blockchain technology or what type of digital ledger ("decision support"), provide recommendations on design and implementation ("recommendations"), provides use cases ("use case collection") or best practices examples ("best practices"). Furthermore, some documents provide details on how to do standardization on blockchain topics in the respective organisation in the future

("standardization metainfomation") or details open questions for research and standardization ("research directions").
- Type of Issuing Organisation: Discerns between national and international/multinational standardization organisations.
- Certifiable/Auditable: Provides information, whether an organisation or a person/system can be audited against or certified for this document/standard.
- Latest Revision: Date of the latest revision. This can give an indication, how modern and up to date the standard is. Still, the value of this criterion differs a lot between high level standards and those providing a lot of technical details.
- Accessibility: This criterion describes, whether the standard is accessible by the general public for free or if it needs to be purchased.
- Price: Price of the document.
- Pages: Number of pages of the document. The value of this criterion is questionable in many aspects, still it can serve as an indicator for the level of detail.

3.2.2. Content Criteria

These criteria deal with the actual content of the document, covering depth of details, as well as the range of the topics covered:

- Domain: Gives a short description of the target domain of the document, e.g., a document targeting general blockchain systems, or rather special use cases for blockchains in a specific field or industry.
- Grand Focus of the Document: What is the actual focus of the document, is it focused towards blockchains, or is blockchains just a (small) part, e.g., in of forensics standard.
- Level of Abstraction: How abstract is the standard with respect to concrete implementations and techniques (High (organizational), Medium (operational), Low (technical)).
- Security Management Considerations: Is Security Management part of the document, or at least mentioned?
- Technical Security Considerations: Is this document recommending technical details for securing IT systems?
- Privacy Considerations: Is privacy, especially the GDPR in the European context, considered in this document?
- Legal Considerations: Does this document include legal aspects of blockchains or (distributed) IT systems in general.
- Provides Blockchain Definition/Terminology: This criterion indicates, whether the document provides a definition for blockchains and/or digital ledger systems, or just refers to them either harkening back at an external definition, or used them without any clear definition at all.
- Blockchain Type: Defines the types and sub types of blockchain based systems and digital ledgers, the document is focusing on, e.g., permissioned blockchains or blockchain generations.
- Focus Regarding Integration: Indicates, whether the document focuses on pure blockchain based systems (e.g. crypto currencies), or on the integration into traditional IT systems (or both).
- Document/Standard Life Cycle: States, whether the document in itself provides a method for updating information and a document life cycle?

In the end, the interconnection and dependencies between standards is of great importance in order to get an overview on the standardization landscape in this field. Thus, in Section 5 we give an overview on this issue. This overview can then again be used for further conclusions on which direction an organization could or should take, in order to get the most out of the introduction of blockchains/distributed ledger technologies and take respective standardization efforts into considerations, depending on the field of operations.

4. Selected Standards

In this section we will provide an overview of the selected publications and their contents that form the foundation of our research.

4.1. National Institute of Standards and Technology (NIST)

In 2018, NIST published the document *NISTIR 8202 - Blockchain Technology Overview* [18]. As the title suggests, it presents a collection of information about blockchain technology to its readers. Fundamental functionalities and components of a blockchain system are discussed. What starts out as a high-level technology overview continues to address and include common misconceptions and technological limitations, as well as concerns about cybersecurity and the general applicability of blockchains for organizations. This document serves as an entry point to blockchains and the distributed ledger technology, as it explains the structure and models, consensus mechanisms and well known examples of it, as well as a number of blockchain specific problems and considerations. Additionally, the appended glossary provides a concise overview of the blockchain terminology, ideal for novices. However, specific use-cases are not included within this document.

Pros: This document is great for providing a substantial overview of both what "Blockchains" are as well as a number of technical guidelines.

Cons: The lack of use-cases and evolution of the field as a whole locks it in place as just a primer.

4.2. ANSI Accredited Standards Committee X9

ASC X9 released the final version of the *Distributed Ledger and Blockchain Technology Study Group Report* [19] in 2018. In their study they worked together with experts of various fields and assessed what types of standardization effort would be both needed and beneficial especially for the financial sector but also other industries, as well as to increase the adoption of DLT. However, the study only focuses on permissioned blockchains, as it is deemed necessary for compliance with existing regulations for the market. Throughout their report, each section is marked with either *high*, *medium* or *low*. The authors use this indicator to express the urgency on how much standard is needed for each specific part, each supplemented with a recommendation on how to proceed. The majority of the document focuses on and explains security needs and issues of blockchains, especially for finance. Their overall recommendations are for developers to be cautious and for the industry to take a three staged approach consisting of assessing whether there are existing non-blockchain standards that cover the same topic, using incremental improvements for blockchain specific implementations and as a third, stirring discussion in areas where there is immediate need for standardization. To provide better understanding of the key components of blockchain systems, there is a high-level reference architecture included in the appendix which is used to generally explain how a DLT system works.

Pros: ANSI provides a substantial overview of possible and needed standardization directions that can be of immense value for bodies of standardization and companies trying to fill the gap.

Cons: As this report is technically just a list of suggestions for possible standardization, there is limited value for regular end users and organizations which are looking for guidance.

4.3. International Organization for Standardization (ISO)

While the overall work of the ISO TC 307 comprises of eleven work items at the moment of research [20], only one of them reached a maturity level required to be released so far. It is the *ISO/TR 23455:2019 Blockchain and distributed ledger technologies—Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems* [21]. This report provides a detailed overview and lengthy discussion of smart contracts within a blockchain/distributed ledger system and their operation. This is supported by a number of graphs to visually represent the processes. Important parts are amongst others the platform specific deployment, life cycles and security of smart contracts. Additionally, the report explores the possibility of legally binding smart contracts,

as well as using them for sidechains or cross-chaining. The Annex focuses heavily on existing smart contract implementations, as well as a comprehensive overview of possible applications and use cases. Overall, the document provides substantial guidance for a proper and secure operation of smart contracts and could be useful for a general increase in quality of smart contracts across the board.

Pros: ISO/TR 23455:2019 is incredibly substantial when it comes to smart contracts, not only including the technical functionality but also a generous amount of use cases.

Cons: Outside of the field of smart contracts this standard is of limited use.

4.4. German Institute for Standardization (DIN)

At the time of this research, the German Institute for Standardisation has published a number of specifications relating to blockchain technology and distributed ledgers.

- DIN SPEC 16597 [22]: DIN provides a *terminology for blockchains* with this specification. It aims at being relevant for a broader audience and not bound to a single usage area or industrial sector. It covers terminology from traditional IT and cryptography before delving into blockchain specifics. This terminology is referenced in the other specifications mentioned here and part of a larger industry cooperation project

  Pros: The provided terminology is good to get into blockchains and understand the individual components.

  Cons: It is used as a preliminary for the other documents and therefore missing out on "out of scope" elements.
- DIN SPEC 3103 [23]: The specification *Blockchain and Distributed Ledger Technologies in Application Scenarios for Industry 4.0* presents application scenarios for the technology in the field of modern industry. The presented information should provide decision makers with enough information to evaluate a possible benefit of introducing distributed ledger technology. The document presents a number of use cases and describes respective problems that can occur. These problems then get addressed by introducing a solution by using blockchains/distributed ledger technology, including user stories and sequence diagrams to reinforce the understanding. Reoccurring elements of these scenarios are then formed to be building blocks, which get expounded accordingly so it can be used for other use cases as well.

  Pros: This document provides a proper outlook and guideline for industry 4.0

  Cons: Outside of that its use can be rather limited.
- DIN SPEC 3104 [24]: In their specification about *blockchain-based validation of data*, they heavily focus on data correctness of blockchains. To achieve what they call *Proof of Correctness*, they propose a technical framework and process descriptions for a blockchain validation software and the verification of this validation. Their technical framework comes in the form of a step by step overview where each block or process is explained and what its requirements are.

  Pros: They provide a guiding framework for "blockchain-based validation of data"

  Cons: It is not particularly useful for a more generalised approach on the technology.
- DIN SPEC 4996 [25]: SPEC 4996, *blockchain-based approach to the transfer of software licenses*, focuses on providing for the establishment of a standardized procedure for digital trade, transfer and management of software licenses using distributed ledger technology by determining a set of requirements. Additionally, they define required information elements to conduct software and licensing operations. The specification informs the reader on how the transparency and tamper-proof attributes of a blockchain can be used to prevent loss or multiple usage of one license. An overview of various roles involved in licensing operations is explained, as well as a design overview of how a proposed system could look like.

Pros: They provide a guiding framework for a "blockchain-based transfer of licenses"

Cons: It is not particularly useful for a more generalised approach on the technology.

- DIN SPEC 4997 [26]: The specification *Privacy by Blockchain Design: A standardized model for processing personal data using blockchain* concerns itself with the EU General Data Protection Regulation (GDPR), especially *art. 25, Privacy by design*. The aim of this specification is to support data protection and privacy compliance in blockchain/distributed ledger technology systems. It is explained what personal data means and how such information can be identified. This is reinforced by stating a number of possibilities where personal data can be found and where it is processed. The specification lists concerns of combining blockchains with the GDPR and which legal issues it might bring like ownership and data erasure. A substantial overview of risks of and mitigations for data protection principles are outlined with a clear focus on privacy by design, as well as a blueprint for a *privacy by design blockchain architecture blueprint*. Additionally, the specification includes an annex to stir up awareness of the GDPR and the data subject rights.

  Pros: This document provides an approach on how to combine the restrictions of the GDPR with blockchain technology.

  Cons: It is more just a theoretical approach and no definitive framework.

4.5. The European Union Agency for Cybersecurity (ENISA)

In their Publication *Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector* [27], ENISA states their opinion on what they think are the benefits of adopting DLT for financial institutions, additionally, they break down DLT into its components and explain the individual parts, their different forms and what their function within a blockchain is. These components include e.g., the consensus protocols, sidechains, smart contracts and cryptography. One section of the report focuses on cybersecurity challenges, both traditional and technology specific. For further guidance, essential *Good Practices* are mapped to specific challenges to provide a quick overview and to help organizations to implement blockchains/distributed ledger systems in a secure way, which can be seen as the most important part of the report. These good practices can be used to bridge the time until there is a standardized framework, even for non-financial applications, as the stated challenges are mostly generic and thus applicable for more than just the financial sector. ENISA concludes their report by summarizing the challenges and issues that are still unanswered. In the annex, ENISA provides Blockchain Use Cases, a short study on the famous Etherum DAO hack, as well as an overview of several distributed ledgers.

Pros: They include a number of best practice implementation guidelines.

Cons: Their work is heavily focused on the financial sector with according complementary compliance requirements from there.

4.6. German Federal Office for Information Security (BSI)

The German Federal Office for Information Security published the document *Towards Secure Blockchains* [28] in 2019. This document is sectioned into four different parts and provides substantial overview on blockchains and according considerations. Part one focuses on the fundamental principles of blockchain technology, listing definitions and explaining blockchain specific matters like trust, consensus and smart contracts. The second and longest part highlights security features and properties of blockchains including possible attacks and long-term solutions. Third is an overview of legal aspects with a strong focus on privacy and data protection. The last part portrays the current use and situation of blockchains and a future trend analysis.

Pros: This substantial document provides a great overview of blockchain and DLT with respective comparisons to regular forms of storing data, including a building block model and considerations about information security as well as legal compliance.

Cons: Newer forms of blockchains and DLT are not included.

Additionally, the BSI published the second edition of the *Franco-German IT-Security Situation Overview* in cooperation with the French agency ANSSI. A major section of it is, as in their previous report, dedicated to cryptocurrency crime. In the report they give an overview of some of the most prominent attack types and surfaces with a strong focus on cryptocurrencies [29]. However, this obviously tends more to law enforcement than standardization efforts. It can be used as informative input to find ways for a standardized preventative method for the mentioned threats nonetheless.

Pros: It shows the increasing prevalence of cryptocrime.

Cons: It does not show anything beyond that.

4.7. International Telecommunication Union (ITU)

The *ITU-T Focus Group on Application of Distributed Ledger Technology*, founded in May 2017, has published a number of technical specifications and reports concerning the terminology, architecture and perspectives of blockchains and distributed ledger technology, as well as a proposed framework.

- FG DLT D1.1 [30]: Their first publication is a technical specification about terminology and definitions for distributed ledger technology. This document includes example figures to underline some definitions. It is appended by a short overview of the functionality of the distributed ledger technology.

  Pros: The provided terminology is a good starting point to understand the elements and components of a blockchain.

  Cons: It's preliminary use is to serve as a guiding reference for the other documents of the working group.
- FG DLT D1.2 [31]: This document is titled *Distributed ledger overview, concepts, ecosystem* and it does exactly that, providing an overview of the technology and its components. The main focus of this document is centered around discussing the distributed ledger ecosystem and its aspects. It can be useful to get more familiar with the overall topic.

  Pros: New readers will get a broad overview of distributed ledger systems.

  Cons: It is not particularly suitable for experienced readers.
- FG DLT D2.1 [1]: In their technical report about distributed ledger technology use cases ITU starts with a discussion about possible benefits and competitive advantages for the industry, achieved through the adoption of the distributed ledger technology. This point is then elaborated on by presenting domain slices, both vertically and horizontally, where the authors describe potential room for adoption of distributed ledger technologies in various sectors and fields of application. Additionally, ITU states their concerns and considerations on adoption barriers. The core of this report lies in its comprehensive collection of use cases for the previously mentioned domains.

  Pros: They offer a substantial list of sector specific use cases for distributed ledger systems.

  Cons: It is simply an overview and offers no guidance.
- FG DLT D3.1 [32]: This technical specification contains a full *reference architecture for distributed ledger systems*, which serves as a guiding tool for both, new users and service providers of distributed ledger technology alike. Each element or component is described in according depth and detail, including a generalized overview of architectural information.

  Pros: The provided reference architecture offers a substantial outlook on how a DLT-system can be implemented.

  Cons: Legal and other compliance requirements are not considered in this document.

- FG DLT D3.3 [33]: In D3.3, *Assessment criteria for distributed ledger platforms*, ITU presents a catalogue of criteria, by which a distributed ledger system can be assessed. The technical specification includes a description on how to use the defined criteria and should serve as a guiding document for distributed ledger technology platform assessment.

  Pros: They present a number of assessment criteria which can be useful when deciding on a potential use of the technology.

  Cons: Assessing different platforms themselves is only of use for limited purposes.
- FG DLT D4.1 [34]: ITU outlines existing regulatory issues that can slow down the adoption rate of distributed ledger technologies in their *Distributed ledger technology regulatory framework*. A selection of specific DLT attributes is analyzed and coupled with according challenges. Additionally, they provide possible mitigations on how to overcome these regulatory issues.

  Pros: It is one of the very rare frameworks that actually focuses on regulatory issues.

  Cons: Information security standards and compliance (i.e. ISO 27k series) is still lacking.
- FG DLT D5.1 [35]: This report is the final document of the work of the ITU-T Focus Group on Application of Distributed Ledger Technology. It provides an overview of future predictions for DLT on the subjects *governance and legal regulation, computation networks, identity and privacy, security and resilience*, and *risk and audit*. These subjects are each split into a number of subsections which discuss their current situation, their outlook and a standardization roadmap. The comprehensive information presented in this report provides good insight on the evolution and development of distributed ledger systems and definitely useful for the further development of the technology.

  Pros: This document tries to make substantial predictions for the development of the distributed ledger technology field. Such predictions could be useful to stir up research and innovation towards certain areas.

  Cons: As the content is about predicting the future, these predictions can very well become untrue.

4.8. European Committee for Electrotechnical Standardization (CENELEC)

In their report *Recommendations for Successful Adoption in Europe for Emerging Technical Standards on Distributed Ledger/Blockchain Technologies* [36], they set out to identify specific European needs in the field of distributed ledger technology and blockchain standardization. A set of important domains of DLT that might still be uncertain (e.g. digital identity and signature management) are well explained and concluded with a set of recommendation each. These presented recommendations towards bodies of standardization aim to support their efforts in creating a standard fit for the European Union. Furthermore, a comprehensive overview of well described use cases of different domains is provided as part of its annex.

Pros: The document could prove as a useful guiding direction for bodies of standardization.

Cons: The document is heavily EURO-centred and could therefore be of lesser relevance for other parts of the world.

5. Comparison and Interdependencies

This section compares the standards according to our criteria and highlights interconnections to other, pre-existing standards.

5.1. Comparison of Document Criteria

Table 1 provides an overview of the selected standards according to their document criteria. As mentioned in Section 3.2, these contain mostly meta information about the reviewed publications. As clearly visible, all of the work done so far is merely informative and we have yet to wait for

normative standardization. For this reason we did not include the criteria "Technical Specification" in the table, as all of the documents can be categorized as informative. Additionally, we merged the criteria for accessibility and price into one column in the table. The majority of the documents are technical reports, many of them providing comprehensive information about blockchains and the distributed ledger technology itself, before going on with their actual topic. This reinforces that blockchain/DLT still is mostly uncharted territory. While the technology itself is well studied from a technical perspective, organizational observations are still lacking behind. Only one document provides a substantial catalogue for best practice implementation of the technology, but these practices are tailored towards the financial sector. As shown in the many documents which list possible use cases and fields of applications for blockchains, the stark contrast between possibilities and actual normative standardization work is astonishing. Nonetheless, many of the standardization organizations provide their recommendations on how to implement blockchains/distributed ledger systems. Especially looking at the DIN specifications, which are usually a precursor for upcoming normative standards.

Table 1. Comparison of Document Criteria of Standards.

Standard	Type	Document Objective	Issuing Organization	Certifiable	Latest Revision	Accessibility	Pages
NISTIR 8202	Report	Topic overview	National	No	October 2018	Free	68
ASC X9 [19]	Report	Research Directions	National	No	April 2018	Free	39
ISO/TR 23455:2019	Recommendation	Topic Overview	International	No	September 2019	CHF 158,-	42
DIN SPEC 16597	Recommendation	Definitions	National	No	February 2018	Free	15
DIN SPEC 3103	Recommendation	Decision Support	National	No	June 2019	Free	26
DIN SPEC 3104	Recommendation	Recommendations	National	No	April 2018	Free	14
DIN SPEC 4996	Recommendation	Recommendations	National	No	April 2020	Free	26
DIN SPEC 4997	Recommendation	Recommendations	National	No	April 2020	Free	58
ENISA [27]	Best Practices	Decision Support	International	No	January 2018	Free	36
BSI [28]	Report	Recommendations	National	No	May 2019	Free	92
BSI/ANSSI [29]	Report	Topic Overview	National	No	May 2019	Free	17
ITU DLT 1.1	Report	Definitions	International	No	August 2019	Free	18
ITU DLT 1.2	Report	Topic Overview	International	No	August 2019	Free	13
ITU DLT 2.1	Report	Use Cases	International	No	August 2019	Free	112
ITU DLT 3.1	Report	Best Practices	International	No	August 2019	Free	42
ITU DLT 3.3	Report	Best Practices	International	No	August 2019	Free	22
ITU DLT 4.1	Report	Recommendations	International	No	August 2019	Free	43
ITU DLT 5.1	Report	Research Directions	International	No	August 2019	Free	60
CENELEC [36]	Report	Recommendations	International	No	September 2018	Free	87

5.2. Comparison of Content Criteria

While the document criteria from Section 5.1 can provide a general overview of the direction of a document, the content criteria are equally as important. Table 2 shows the standards in relation to selected topics. What becomes clearly visible is that the financial sector seems to be one of the most interested in this technology. Besides the general domain of Blockchain/DLT, finance and cryptocurrency, especially with regards to often stated legal requirements (i.e. AML/KYC), is often a driving force behind publications. Security Management is of special interest for us. While some of the standards mention certain elements of security management, it is far from being substantial enough for proper guidance. As for technical security, there are many references to traditional IT security practices and guidelines. Nonetheless, privacy remains a major concern when dealing with blockchains and distributed ledgers. Especially where there are many legal and moral obligations about personal data, a normative reference could be highly beneficial. Another insight is that the majority of the published standards cover Blockchains/DLT in general without being too specific about their implementation or direction. Specialized work regarding the many varying forms of Blockchain, possibly according to the plethora of presented use cases and fields of applications could help in catering to sectors other than finance that might not be fully aware of the capabilities of this technology.

Table 2. Comparison of Content Criteria of Standards.

Standard	Domain	Grand Focus	Abstraction	Security Management	Technical Security	Privacy	Legal Considerations	Terminology	Type	Integration	Life Cycle
NISTIR 8202	Blockchain /DLT	Blockchain	High	Yes	Yes	Yes	No	Yes	Multiple	Standalone	No LC
ASC X9 [19]	Finance	Blockchain	High	Yes	Yes	No	Yes	Yes	Multiple	Standalone	No LC
ISO/TR 23455:2019	Blockchain /DLT	Blockchain	Medium	Yes	Yes	No	Yes	Yes	Smart Contracts	Standalone	Yes
DIN SPEC 16597	Blockchain /DLT	Blockchain	High	No	No	No	No	Yes	Multiple	Standalone	Yes
DIN SPEC 3103	Industry 4.0	Other	High	Yes	Yes	No	No	Yes	Multiple	Integration with IT	Yes
DIN SPEC 3104	Blockchain /DLT	Blockchain	Medium	No	Yes	No	No	Yes	Multiple	Standalone	Yes
DIN SPEC 4996	License Management	Other	Medium	No	No	No	Yes	Yes	Multiple	Standalone	Yes
DIN SPEC 4997	Blockchain /DLT	Blockchain	High	Yes	Yes	Yes	Yes	Yes	Multiple	Multiple	Yes
ENISA [27]	Finance	Blockchain	High	No	Yes	Yes	No	Yes	Multiple	Multiple	Yes
BSI [28]	Blockchain /DLT	Blockchain	High	Yes	Yes	Yes	No	Yes	Multiple	Standalone	No LC
BSI/ANSSI [29]	Finance	Blockchain	High	No	Yes	No	Yes	No	Crypto Currency	Standalone	No LC
ITU DLT 1.1	Blockchain /DLT	Blockchain	High	No	No	No	No	Yes	Multiple	Standalone	No LC
ITU DLT 1.2	Blockchain /DLT	Blockchain	Medium	No	No	No	No	Ref.	Multiple	Standalone	No LC
ITU DLT 2.1	Blockchain /DLT	Blockchain	Medium	Yes	Yes	Yes	Yes	Yes	Multiple	Multiple	No LC
ITU DLT 3.1	Blockchain /DLT	Blockchain	Medium	Yes	No	Yes	No	Ref.	Multiple	Multiple	No LC
ITU DLT 3.3	Blockchain /DLT	Blockchain	High	Yes	Yes	Yes	Yes	No	Multiple	Multiple	No LC
ITU DLT 4.1	Blockchain /DLT	Blockchain	Low	Yes	No	Yes	Yes	Ref.	Multiple	Multiple	No LC
ITU DLT 5.1	Blockchain /DLT	Blockchain	Medium	Yes	No	Yes	Yes	Ref.	Multiple	Multiple	No LC
CENELEC [36]	Blockchain /DLT	Blockchain	High	Yes	Yes	Yes	Yes	Yes	Multiple	Integration with IT	No LC

5.3. Interconnection between Documents

In this section we discuss, how the selected documents are related to each other, as well as additional standards and legal frameworks. This is especially interesting, as changes in selected documents might introduce changes in dependent standards transitively. Notably in the area of blockchain technologies, where definitions in research work are often used differently, even small changes can have great impact in other documents. Table 3 gives an overview on these interdependencies, i.e., for each document discussed, we provide a list of standards, recommendations and laws this document relies on or uses to define parts of its content. While there are more references per document overall, the references included in this table are focused on publications of standardization authorities and for legal aspects, the laws of the European Union. The most common legal reference throughout the documents we included in this work here is the General Data Protection Regulation. The positive factor of this is that at least some of the documents acknowledge the need for proper data protection and the vulnerability of personally identifiable information. Other than that, it becomes quite obvious that some of the organizations are relying heavily on their own work with proportionally high self references, as can be seen with the work of ITU. Another factor that becomes apparent is that there is a substantial variety in references for terminologies. This suggests that there is still no definitive or clear line to define the components of a distributed ledger system.

Table 3. References/Dependencies to other Standards and Laws.

Standard	Terminology Ref.	Technical Ref.	Legal Ref.	Standard Ref.
NISTIR 8202	---	NIST FIPS 180-4, 186-4, 202	---	NIST Cybersecurity Framework
ASC X9 [19]	---	ISO 13491; NIST SP 800-57; NIST FIPS 140, 180, 186, 198	---	ISO 20022; NIST SP 800-162; ANSI/INCITS 359
ISO/TR 23455:2019	ISO/DIS 22739; ISO/TS 19299; ISO/IEC 14776, 13888; ISO/TR 26122	---	---	ISO 639, 3166, 4127, 8601
DIN SPEC 16597	ISO 2789; ISO/IEC 20002, 9798, 8211, 2382; IEC/TR 62541, 62210	---	---	---
DIN SPEC 3103	DIN SPEC 16597	---	---	DIN SPEC 91345; ISO 14440; ISO/TC 307
DIN SPEC 3104	DIN SPEC 16597; ISO/IEC 2382; ETSI EN 319 132-1; ETSI TS 119 142-3; IEC 61499-1	ISO/IEC 9796, 10118, 14888; ETSI EN 319 132-1; BSI TR-03111; NIST FIPS 180-4, 186-4; RFC 3447; PKCS; SOG-IS [37]	---	ISO/IEC 27000, 27001, 27002, 27003, 27004, 27005
DIN SPEC 4996	DIN SPEC 16597; ISO/DIS 22739; ISO/IEC 19770	---	Directive 91/250/EEC	ISO/IEC 19770; NISTIR 8202
DIN SPEC 4997	DIN SPEC 16897; ISO/IEC 19790, 14662; ITU FG DLT D1.1; ISO/DIS 22739	DIN SPEC 3104; NISTIR 8105	Regulation (EU) 2016/679 (GDPR); Art. 29 WP 242, 243, 248, 251; Handbook [38]; EuGH — Rs. C-101/01	BSI SDM [39]; NIST SP 800-63B; ISO/IEC 27018
ENISA [27]	---	---	Regulation (EU) 2016/679 (GDPR)	---
BSI [28]	BSI-IT baseline security; ETSI ISG PDL ToR	ETSI TS 119 312; BSI AIS 20, 31, 46; BSI TR-03147	Regulation (EU) 910/2014, Regulation (EU) 2016/679 (GDPR)	BSI-IT baseline security; ISO/TC 307
BSI/ANSSI [29]	---	---	---	---
ITU DLT 1.1	ITU-T Y.2091; ISO/TC 307; ISO 2382, 7498; IEC 38500; NISTIR 8202	---	---	ITU-T FG DLT D2.1
ITU DLT 1.2	ITU-T FG DLT D1.1	---	---	NISTIR 8202
ITU DLT 2.1	ITU-T FG DLT D1.1	---	ITU-T FG DLT D4.1	ITU-T FG DLT D3.1 D3.3
ITU DLT 3.1	ITU-T FG DLT D1.1	ISO/IEC 10118-3	---	---
ITU DLT 3.3	ITU-T FG DLT D1.1	---	---	ITU-T FG DLT D3.1
ITU DLT 4.1	ITU-T FG DLT D1.1; ISO/IEC 17788	ISO/IEC 20008, 11770; ZKP Standardization	Art. 29 WP 216; Directive 95/46/EC; Regulation (EC) No 45/2001; Judgement (ECJ) C-101/01	ISO 16759; ISO/IEC 30141; ITU-T X.509, X.1255
ITU DLT 5.1	ITU-T FG DLT D1.1	---	Art. 29 WP 216	ITU-T FG DLT D1.3, D2.1, D3.3, D4.1
CENELEC [36]	---	---	Regulation (EU) 2016/679 (GDPR)	ISO/TC 307; ISO/JTC 1/SC27; ITU-T FG DLT, DFC; ISO 17442

6. Results

While we were able to find a large number of publications on blockchains and the distributed ledger done by standardization authorities already, all of them are merely informative. Of course, this provides a good overview and starting point for implementing this technology, but the severe lack of normative reference material could hinder the adoption of Blockchains/DLT as organizations could decide to wait for standards to cling to. That said, especially the works of the German Institute for Standardization provided more than just a report on the technology or its aspects. Namely, clear outlines and implementation guidelines for specific use cases of blockchain applications. For actors in the financial or banking sector, the document by ENISA will prove itself useful, as the provided best practices are tailored to overcome existing cybersecurity and legal problems of that sector.

While it can be observed that there is a progress in the quality and substantiality of blockchain standards development over the years, we have yet to see an actual normative standard that can be used for a compliant implementation of blockchains and auditing thereof, similar to the ISO 27,001 for information security. Most of the standardization efforts so far are focused on the technology itself. For future developments, specialized standardization for the various economic sectors and industries can be beneficial since compliance requirements differ from one industry to another.

Additionally, both [7,40] state the importance of demystifying blockchains and distributed ledgers and that there are still many misunderstandings and misconceptions about the technology. They are often seen as a synonym for cryptocurrency or Bitcoin. Decoupling this line of thought and having

clear a clear definition and understanding of what the technology actually is and what it can do serves as a basis for further standardization efforts. Therefore, the pace of distributed ledger standardization is directly linked to the understanding of the actual abilities and possibilities of the technology. As long as the majority just see Blockchains as a toy for generating digital wealth, the success of the technology is vastly limited in scale and functionality.

One important factor, especially in the field of information security management is that there is a severe lack of legal references and references to certain standards of the ISO 27k series. Without a clear path on how compliance and especially integration of blockchains into existing information security management systems can be done, it could result in negligence of the technology due to potentially high risks.

7. Discussion

Privacy is still very much a concern when it comes to the use of blockchains. Most of the publications focus on the functionality and usage of the technology, while offering little to no guidance for compliance. Cross-country data flow entails various legal issues that could easily become reality for a distributed system. A proper set of normative guidelines and frameworks of standardized procedures for the implementation and operation of Blockchains will bolster its overall success as a technology. In the X9 Report [19], there is a mention of a possible risk that comes with standardization of the technology. Namely, the stagnation of innovation of technological developments of young technologies. They specifically point out that certain economic sectors are still missing out on more secure cryptographic implementations because they were not included in standards and are therefore not seen as a needed upgrade to be compliant. Countering such problems is fairly easy. First and foremost, Blockchain technology is not particularly new anymore as it has been around for more than a decade by now. However, innovation should be encouraged nonetheless. Combined with standards an obvious choice is demanding the state-of-the-art of specific technological implementations and appropriate measures as a requirement. By doing so, innovation can go any direction and the standard still accounts for new developments as it is not fixated on one, possibly out-dated, form of implementation but rather aligned with the flow of progress.

Since the introduction rate of normative standards is quite low, it is advisable to find stability in currently available frameworks and laws concerning technology, security and privacy which are already referenced in the available informative standardization work (as shown in Table 3), as it is likely that final works will use a similar basis for their assessments instead of creating an entirely new environment. Further Guidance could also be found by incorporating standards that focus on distributed systems in general. Even though these would lack the focus on blockchains, they could very well serve as reference points for distributed ledger technologies.

Additionally, while some of the documents focus on specific sectors or problems, the majority is just a generic overview of Blockchains/DLT. This is important for getting familiar with the topic, but separate industrial and economic sectors would profit from specialised standardization work, catering to them and incorporating the according domain knowledge and legal requirements.

As outlined in [7], the introduction and effective use of blockchains across the industries has varying results and impacts. One of the industries with relatively high impact levels and a feasibility of introducing standards and regulations, it would be a prime candidate to advance with new standardization approaches. Using blockchains for the agriculture sector and its supply chains can not only transparently proof i.e., sustainable use of resources, but bring the concept of blockchains closer to the consumers of these agricultural products to spread awareness for a use of blockchains and distributed ledger technology other than cryptocurrency to the masses.

Author Contributions: Conceptualization, L.K. and P.K.; methodology, L.K., Y.K., P.K. and S.T.; resources, L.K. and Y.K.; writing—original draft preparation, L.K. and Y.K.; writing—review and editing, L.K., Y.K., S.T. and P.K.; supervision, S.T. and P.K.; project administration, P.K.; funding acquisition, P.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Josef Ressel Center for Blockchain Technologies & Security Management (BLOCKCHAINS). The financial support by the Austrian Research Promotion Agency, the Federal Ministry for Digital and Economic Affairs and the Christian Doppler Research Association is gratefully acknowledged.

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

References

1. ITU. *Focus Group on Application on Distributed Ledger-D2.1, Distributed Ledger Technology Use Cases*; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2019.
2. Institute, E.P.R. *Program on Technology Innovation: Blockchain—U.S. and European Utility Insights Market Intelligence Briefing Report*; Technical Report; Electric Power Research Institute: Palo Alto, CA, USA, 2019.
3. Deshpande, A.; Stewart, K.; Lepetit, L.; Gunashekar, S. *Understanding the landscape of Distributed Ledger Technologies/Blockchain: Challenges, Opportunities, and the Prospects for Standards*; Technical Report; British Standards Institution: London, UK, 2017.
4. Deshpande, A.; Stewart, K.; Lepetit, L.; Gunashekar, S. Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards; Overview report; The British Standards Institution (BSI): London, UK, 2017.
5. Frank Cerveny, T.K. Research Announcement: Moody's-Blockchain Standardisation will Amplify Benefits for Securitisations. 2019. Available online: https://www.moodys.com/research/Moodys-Blockchain-standardisation-will-amplify-benefits-for-securitisations--PBS_1193318?stop_mobi=yes&showPdf=true (accessed on 19 April 2020).
6. MarketsandMarkets. *Blockchain IoT Market by Offering (Hardware, Software, and Infrastructure Provider), Application (Smart Contract, Data Security, Data Sharing/Communication, and Asset Tracking & Management), End User, and Geography-Global Forecast to 2024*. 2019. Available online: https://www.marketsandmarkets.com/Market-Reports/blockchain-iot-market-168941858.html (accessed on 19 April 2020).
7. Carson, B.; Romanelli, G.; Walsh, P.; Zhumaev, A. *Blockchain Beyond the Hype: What Is the Strategic Business Value*; McKinsey & Company: Sydney, Australia, 2018; pp. 1–13.
8. ETSI. *001—Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies*; Technical Report; European Telecommunications Standards Institute: Sophia Antipolis, France, 2020.
9. ITU. *Focus Group on Application on Distributed Ledger—D1.3, Distributed Ledger Technology Standardization Landscape*; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2019.
10. Li, M.; Yang, J.; Ding, X. Overview and Thoughts on Standardization of China's Blockchain Technology. In Proceedings of the CCF China Blockchain Conference, Chengdu, China, 11–13 October 2019; pp. 220–230.
11. Hurd, J.; Isaak, J. It standardization: The billion dollar strategy. In *Standardization Research in Information Technology: New Perspectives*; IGI Global, Aachen University: Aachen, Germany, 2008; pp. 20–26.
12. Meyers, M.; Rogers, M. Computer forensics: The need for standardization and certification. *Int. J. Digit. Evid.* **2004**, *3*, 1–11.
13. Disterer, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *J. Inform. Secur* **2013**, *4*, 92–100. [CrossRef]
14. Boehmer, W. Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In Proceedings of the 2008 Second International Conference on Emerging Security Information, Systems and Technologies, Darmstadt, Germany, 20 April 2009; pp. 224–231.
15. Beimborn, D.; Gleisner, F.; Joachim, N.; Hackethal, A. The role of process standardization in achieving IT business value. In Proceedings of the 2009 42nd Hawaii International Conference on System Sciences, Big Island, HI, USA, 5–8 January 2009; pp. 1–10.
16. Vrancken, J.L. Layered models in IT standardization. In Proceedings of the 2006 IEEE International Conference on Systems, Man and Cybernetics, Taipei, Taiwan, 8–11 October 2006; Volume 5, pp. 3862–3865.
17. van Wessel, R. *Toward Corporate IT Standardization Management: Frameworks and Solutions: Frameworks and Solutions*; IGI Global, Tilburg University: Tilburg, The Netherlands, 2010.
18. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. *NISTIR 8202 Blockchain Technology Overview*; Internal Report 8202; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.

19. Accredited Standards Committee X9 Study Group Report by the Distributed Ledger and Blockchain Technology Study Group. 2018. Available online: https://x9.org/wp-content/uploads/2018/04/Distributed-Ledger-and-Blockchain-Technology-Study-Group-Report-FINAL.pdf (accessed on 4 December 2019).
20. ISO/TC307. Standards by ISO/TC 307—Blockchain and Distributed Ledger Technologies. 2020. Available online: https://www.iso.org/committee/6266604/x/catalogue/ (accessed on 20 April 2020).
21. ISO/TC307. *23455:2019 Blockchain and Distributed Ledger Technologies-Overview of and Interactions between Smart Contracts in Blockchain and Distributed Ledger Technology Systems*. 2019. Available online: https://www.iso.org/standard/75624.html (accessed on 20 April 2019).
22. DIN. *16597:2018-02 Terminology for Blockchains*. 2018. Available online: https://www.beuth.de/de/technische-regel/din-spec-16597/281677808 (accessed on 20 April 2020).
23. DIN. *3103:2019-06 Blockchain und Distributed Ledger Technologien in Anwendungsszenarien für Industrie 4.0*. 2019. Available online: https://www.beuth.de/de/technische-regel/din-spec-3103/306199037 (accessed on 20 April 2020).
24. DIN. *3104:2019-04 Blockchain-Based Validation of Data*. 2019. Available online: https://www.beuth.de/de/technische-regel/din-spec-3104/301837615 (accessed on 20 April 2020).
25. DIN. *4996:2020-04 Blockchain-Based Approach to the Transfer of Software Licenses*. 2020. Available online: https://www.beuth.de/de/technische-regel/din-spec-4996/321277534 (accessed on 20 April 2020).
26. DIN. *4997:2020-04 Privacy by Blockchain Design: A Standardised Model for Processing Data Using Blockchain Technology*; 2020. Available online: https://www.beuth.de/de/technische-regel/din-spec-4997/321277504 (accessed on 20 April 2020).
27. Network, E.U.A.F.; Security, I. *Distributed Ledger Technology & Cybersecurity—Improving Information Security in the Financial Sector*. 2017. Available online: https://www.enisa.europa.eu/publications/blockchain-security (accessed on 20 April 2020).
28. BSI. *Towards Secure Blockchains*; Technical Report; German Federal Office for Information Security: Bonn, Germany, 2019.
29. BSI.; ANSSI. *Second Franco-German IT-Security Situation Overview*; Technical Report; German Federal Office for Information Security, Agence Nationale de la Sécurité des Systèmes d'Information: Bonn, Germany, 2019.
30. ITU. *Focus Group on Application on Distributed Ledger—D1.1, Distributed Ledger Technology Terms and Definitions*; Technical Report; International Telecommunication Union: Geneva, Switzerland,2019.
31. ITU. *Focus Group on Application on Distributed Ledger—D1.2, Distributed Ledger Technology Overview, Concepts, Ecosystem*; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2019.
32. ITU. *Focus Group on Application on Distributed Ledger—D3.1, Distributed Ledger Technology Reference Architecture*; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2019.
33. ITU. *Focus Group on Application on Distributed Ledger—D3.3, Assessment Criteria for Distributed Ledger Platforms*; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2019.
34. ITU. *Focus Group on Application on Distributed Ledger—D4.1, Distributed ledger technology regulatory framework*; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2019.
35. ITU. *Focus Group on Application on Distributed Ledger—D5.1, Outlook on Distributed Ledger Technologies*; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2019.
36. CEN-CENELEC. *Focus Group on Blockchain and Distributed Ledger Technologies, Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies*; Technical Report; European Committee for Electrotechnical Standardization: Bruxelles, Belgium, 2018.
37. SOG-IS. *Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*. 2018. Available online: https://www.sogis.eu/documents/cc/crypto/obsolete/SOGIS-Agreed-Cryptographic-Mechanisms-1.0.pdf (accessed on 20 April 2020).
38. Kotschy, W. *Handbook on European Data Protection Law*; Ludwig Boltzmann Institute for Human Rights: Vienna, Austria, 2018.
39. Unabhängiges Landeszentrum für Datenschutz. *The Standard Data Protection Model-A method for Data Protection Advising and Controlling on the Basis of Uniform Protection Goals*; Unabhängiges Landeszentrum für Datenschutz: Kiel, Germany, 2019.

40. Lima, C. Developing Open and Interoperable DLT/Blockchain Standards. *Computer* **2018**, *51*, 106–111. [CrossRef]