H. Roßnagel, C. H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 49

Criteria for trustworthy digital transactions – Blockchain/ DLT between eIDAS, GDPR, Data and Evidence Preservation

Tomasz Kusber[1], Steffen Schwalm[2], Kalinda Shamburger[3] and Ulrike Korte[4]

Abstract: With the help of eIDAS [Re14], legislators have created a resilient framework in EU and EFTA to place trustworthy digital transactions more and more in the centre of business relationships. The regulated use of the trust services (e.g. qualified electronic signature or seal etc.) as well as that of the secure electronic identities provides a solid foundation for the advancement of digitization. The adequate evidence of electronic records as long as they are needed is a critical success-factor for trustworthy digital transactions. The trustworthiness of the transactions must be based on compliance with the basic values of authenticity, integrity, reliability, availability, confidentiality and transferability. After a first hype there are increasingly more considerations also in regulated industries to use DLT for digital processes which have to be accountable. In order to make them evident and to fulfil documentation requirements it is necessary that DLT fulfils the legal framework and prior art based on defined criteria for trustworthy digital transactions. This paper focuses on the challenges and requirements for utilisation of DLT for trustworthy digital processes including long-term preservation.

Keywords: DLT, Blockchain, eIDAS, Trust Service, evidence preservation, trustworthiness

1 Introduction

Since some years, Blockchain and Distributed ledger technology (DLT) generate a real hype in particular with the most famous use case Bitcoin [OE17]. A great potential is seen for the technology e.g. in finance industry, utilities, logistics or public sector. [We17]. Distributed ledger technology (DLT) is basically a peer-to-peer network of nodes sharing decentralized, distributed, digital data. It allows the transfer of data or value from one party to another without having intermediates involved. Each node has a copy of the ledger, to which all network transactions are written and which is only updated throughout all nodes after consensus between the nodes has been reached [IS20b]. Once written to the ledger the transactions are immutable. Any transaction can reliably be tracked on the chain. The well-known Blockchain is a special category of DLT, which organizes data/transactions in blocks that are sequentially linked to each other by incorporating a hash of the previous block [IS20b]. The hash protection also exists in DLT while the transactions are not organized in blocks. DLT does not necessarily require the elimination of an operator/consortium providing the peer-to-peer

[1] Fraunhofer Institute for Open Communication Systems, Kaiserin-Augusta-Allee 31, 10789 Berlin, Germany
[2] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany
[3] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany
[4] Federal Office for Information Security. Heinemannstr. 11,-13, 53175 Bonn, Germany

network, this depends on the type of DLT. In terms of access and participation DLT can be public, making it possible for anyone to participate, or private, granting access only to specific parties. There is a differentiation regarding permissions as well. DLT that offer full transparency and allow every party to take part in issuance and validation of transactions are called permissionless (unpermissioned). Whereas permissioned platforms do not allow their participants to be freely engaged in the platform, restricting reading access, transaction validation and issuance. Because of that, this later type of DLT is widely used in regulated environments such as aerospace, healthcare, life sciences and pharma, logistics or public sector. Some main platforms are e.g. Hyperledger Fabric and Corda in comparison to the much more famous Ethereum [Fe19], [OE17], [UK16], [Ya18].

2 Fundamental requirements on trustworthy digital transactions

2.1 Trustworthiness of digital transactions and records

Trustworthiness of digital transactions and records means that the process and the records are really what they seem to be and that this is provable by independent 3rd parties. Trustworthy digital transactions ensure the unique and lossless evidence of authenticity, integrity, reliability of the electronic records which are created, received, stored and managed during the life-cycle of transaction against independent 3rd parties as long as they are needed. This means typically until the end of the defined retention periods based on and compliant to existing laws (between 2 & 110 years or permanent). Some main pre-condition are their availability as well as the protection of the confidentiality of records worthy of protection. The records contain content, metadata and transaction (process) data. The basic preconditions for this is the transferability [UN17] of the records. The evidence will be proven based on the records themselves so the named requirements and in consequence the evidence value of a record are significant properties of the electronic record itself ([WE18], [KHS14], [Ro07]). The utilization of cryptographic measures, e.g. qualified e-signatures, seals and time stamps acc. to eIDAS [Re14], enables users to preserve the evidence of their electronic records without losing the transferability of the records. The evidence value of a qualified electronic signature (e-signature) is the same as a handwritten signature, the seal makes the authenticity and integrity of the sealed record evident. These cryptographic measures are inherent and significant properties of the records. They require measures concerning long-term preservation focusing on the record itself not the storage, the software environment etc. to keep the trustworthiness of the records in the sense of preservation of the information of the data record and its evidence ([Sc17] [Fi06] [KHS14], [ET19b], [ET20]). Main precondition is the establishment of a valid records management according to [IS16]. This includes established policies, roles & responsibilities, processes as well as appropriate functionalities in business-IT to managing records properly during their whole life-cycle from the creation or receiving over utilisation and storage until archiving and disposition ([We18], [IS16]).
These basic burdens of proofs and requirements on trustworthy digital records and transactions are independent from used IT-system, organization or process. Currently there is no regulation defining technology or institution as trustworthy by themselves.

Trustworthiness always requires the evidence of the significant properties based on the records themselves as long as they are needed and without any losses. This requires especially the transferability of the records and so the utilisation of (qualified) electronic signatures, seals and timestamp acc. to eIDAS [Re14], [KHS14]. An evidence value of a record is an inherent property of the record itself. That is why records should only be archived in self-contained AIP which contain any necessary information (metadata, content, evidence relevant and technical evidence data) in a standardized container acc. to [IS12a]. The proof is typically done by trustworthy 3rd parties such as courts, regulative authorities, auditors etc. depending on the legal requirements [We18]. This means trustworthiness can be achieved only by proof not by self-declaration. Essentially it is necessary to make compliance to legal requirements and prior art – so technical standards given and audited by trustworthy 3rd parties – evident [KKS18], [We18], [He18].

2.2 Legal and organizational requirements

Since September 2014, the eIDAS regulation was defined, which came fully into force in July 2016 as a European wide mandatory legal framework for trustworthy digital transactions between citizens, business and government. The eIDAS-regulation contains two parts which both affect trustworthy digital transactions in any business IT-systems: secure digital identities (identification systems) and trust services, in the context of this paper especially, of creation and validation of (qualified) electronic signatures, seals and timestamps as well as preservation services. Any notified electronic identification scheme has to be recognized and accepted by any public administration. Any minimum advanced electronic signature, seal or timestamp from any qualified trust service provider has to be accepted and validated by any public administration. Regarding retention periods between 2 and 110 years or more the long-term preservation of electronic signatures, seals, timestamps and the corresponding data is a mandatory need to ensure the traceability of digital transactions by their records as long as they are needed ([Sc15], [We18]). This was recognized by legislators, e.g. in Europe by the Articles 34 and 40 in eIDAS [Re14] and in Germany with the obligation for long-term evidence preservation (§ 15 VDG [Ve17]). In combination of secure digital identification and trust services the eIDAS [Re14] enables public administration and private companies to establish trustworthy digital transactions and to make them evident against regulative authorities, auditors, courts etc. as well as to preserve the evidence value as long as necessary. eIDAS [Re14] is technically underpinned by corresponding European Standards of ETSI and CEN with Mandate 460. The standards are tied to special state-of-the-art-technologies, which achieve the technical and security requirements.

Furthermore the General Data Protection Regulation GDPR [Re16] has to be recognized to ensure the confidentiality of personal data in digital transactions. The technical and organizational measures to ensure confidentiality of personal data acc. to GDPR [Re16] can also be used to keep trade and business secrets to achieve a holistic management of protective records. In Art. 6 GDPR [Re16]), the obligation for information (Art. 13+14 GDPR [Re16]) as well as the rights of the affected person are in focus so right of access, right of rectification, right to erasure and right of data portability. These obligations and

rights require not only organizational and technical measures included in a well-defined data protection management system but also the technical ability of the applied IT-system to change, export or delete personal data as well as a defined access management or functionalities to decrease amount of the processing of personal data. Taking into account retention periods for decades as well as existing documentation obligations and burden of proof the GDPR [Re16] reflects the ensuring, preservation and evidence of the significant properties of electronic records: authenticity, integrity and reliability (e.g. evidence for consent, obligation of information, access, data portability), availability (e.g. rectification, erasure, portability). This means if DLT is used in processes where personal data are collected, managed and stored, the requirements of GDPR [Re16] have to be fulfilled [We18].

The eIDAS [Re14] and the GDPR [Re16] are underpinned by sector specific regulations concerning the documentation and traceability of digital transactions and records e.g. EASA [EA20], FDA [CF19], EGovG [EG13].

2.3 Relevant Standards

The picture below shows the main organizational and technical standards for the traceability and long-term preservation of digital transactions as preservation objects or preservation object containers based on [IS16] and [Fe18]. One main basis is a valid records management according to [IS16]. The preservation of information requires a trustworthy digital archive compliant to [IS12a], [IS12b] with well-defined processes and information packages to achieve independence from a special soft- or hardware environment. Measures and protocols concerning long-term data preservation are specified in [Fe18] and [ET20], especially on basis of the preservation evidence formats Evidence Records according to RFC4998 [GBP07], RFC 6382 [JSG11] and {C/X/P}AdES Archive Timestamps.

3 DLT in trustworthy digital transactions

3.1 Assessment of DLT against requirements on trustworthy digital transactions

If DLT should be used for trustworthy digital transactions, it is mandatory to long-term preserve their data and evidences, also against 3rd parties, until the end of the retention periods in force and to keep them provable – as it is required for any business IT-system. This means a valid records management incl. evidence preservation is mandatory. The table below shows an overview how DLT achieves or does not achieve the named requirements currently without additional measures [FE19], [KKS18], [Ko18], [Ko19], [DI20A], [Le16], [We18].

Property	Degree of fulfilment	Justification
Authenticity	Very Limited	Commonly, there are no standardized measures for unique linking of transactions or records on DLT to

Property	Degree of fulfilment	Justification
		corresponding legal or natural entities (persons). Further investigation of currently existing mechanisms, e.g. e-signature or -seals acc. to eIDAS [Re14] in order to be used in pair with DLT is necessary. Standardization of such approaches should be aimed for in parallel. At the present, only private, permissioned DLT instances could fulfil this requirement, especially while implementing a proprietary solution.
Integrity	Limited	Immutability is built on the hash protection of blocks/transactions but no resilient[5] Proof of Existence (PoE)[6]. Furthermore, no rehashing & resigning measures acc. to prior art exist. Especially the use of hash algorithms, which became weak, leads to loss of the integrity (c.f. Fig. 1).
Confidentiality	Limited	Only private, permissioned DLT seems to fulfil this requirement. Fulfilment of GDPR [Re16] is only possible with off-chain storage of affected data. (Keeping crucial data on-chain prevents the fulfilment of deletion of those data without having the chain integrity unaffected. Anonymization and pseudonymization can become critical concerning transparency of transactions also in private, permissioned DLT.
Transferability	Very Limited	No standardized migration or ex-/import measures exist. At this stage, there is no common standard or mechanism, which could be used in order to retrieve the data (transaction or a set of them) from one DLT-based application and put it on the other one. This includes also the use case of providing the evidence data based on DLT to the authorities (e.g. to fulfil legal requirements).

Tab. 1: Assessment of DLT against core requirements of records management

In the conclusion of the DLT assessment against significant requirements on records management to achieve trustworthiness it can be ascertained that DLT needs further, additional measures to be enabled for the execution of trustworthy digital transactions. Furthermore it can be determined that only permissioned DLT with limited reading and writing rights for the participants (e.g. consortium or private DLT) and an off-chain storage of the records are currently recommended. Only data about the transaction, not the content itself should be stored on-chain [Ko18], [DI20a], [Le16], [Fe19]. This need is recognized by national and international standardization to define a valid

[5] There used to be applied a system time stamp, but not a trustworthy timestamp issued by corresponding authority, e.g. a qualified trust service provider for qualified time stamp acc. to [eIDAS].
[6] Evidence that proves that an object existed at a specific date/time (c.f. [ETSI119102-1])

organizational and technical framework for trustworthy utilization of DLT.

3.2 Relevant Standardization of DLT and interim conclusion

Currently the standardization in subject of this paper focuses on complementing DLT with the needed tools for long-term traceability and preservation of its transactions and their records, e.g. using secure digital identities and trust services regarding eIDAS [Re14]. So especially the [DI20a] defines determined and provable criteria to use DLT for trustworthy digital transactions by fulfilling records management and long-term data preservation with focus on eIDAS [Re14] and GDPR [Re16].The DIN-specification normatively references corresponding national and international standards regarding DLT e.g. [DI20b] concerning privacy or [W320] for self-sovereign-identity as well as [IS16] regarding records and [ET19b], [ET20], [Fe18] reg. long-term data and evidence preservation. [DI20a] is a main input for [IS20a] which will act as the worldwide pendant.

4 Criteria for trustworthy digital transactions with DLT

The criteria in [DI20a] for trustworthy digital transactions with DLT are discussed under two headings – functional and technical criteria. While the functional criteria describe mainly measures especially regarding general issues, governance, privacy or digital identities that shall be considered, the technical criteria describe in detail, how DLT needs to be set up in order to be used for trustworthy digital transactions.

4.1 Functional criteria

First of all it is necessary to meet requirements described in chap. 3.1 and 3.2 by integrating DLT in a valid records management. This requires the compliance with regulatory requirements is achieved as well as the definition and implementation of well-described roles, responsibilities and policies for records management integrating DLT with the corresponding business-IT. It also requires the records themselves to be stored off-chain for the whole life-cycle of records and their transaction/process information on-chain.

Secure digital Identities & Trust Services

In order to utilize DLT for records management and trustworthy digital transactions, the identities of the participants have to be known unambiguously. This is necessary to make transactions and their records evident against 3rd parties, to fulfil burden of proof and documentation needs compliant to prior art for records management and trustworthy digital transactions [We18], [BB15]. To attain this, DLT inherent functions have to be enhanced with addition of eIDAS [Re14] compliant identification in appropriate level of assurance. This can be achieved with self-sovereign-identity acc. to [W320]. In this case only the anonymized or pseudonymized data are stored on-chain. The identity data itself is stored off-chain in order to ensure compliance to GDPR [Re16]. Decentralized identifiers (DIDs based on W3C standard [W320]) are suitable to be integrated for this

purpose and maintain compliance to privacy regulations as no identifying data is stored on chain. In fact the holder of the DID has complete control over the DID and there is no central authority needed to implement it. The inclusion of identities provides the basis for assignment of permissions to these identities further improving security of the system. It should be carefully considered which participant should be allowed to execute what type of actions within the system. A trusted authority in role of gatekeeper assigns permissions to nodes operated by trusted identities thus defining the actions these are allowed to execute. This approach is currently executed e.g. by ESSIF [ES20] and EBSI [EB20] in EU but also several other initiatives around Europe.

Furthermore DLT inherent functions have to be enhanced with addition of eIDAS [Re14] compliant identification in appropriate level of assurance and by trust services. Especially the trust services for creation of qualified electronic signatures, seals (X.509 based or token based using content of X.509 envelope) and timestamps are needed to provide genuine verifiability of digital processes using DLT authenticity, reliability and integrity of transactional data by keeping provability by independent 3rd parties. This means in fact that a trusted "gatekeeper" could enable the DLT with secure digital identities and trust services acc. to eIDAS [Re14] to be used for trustworthy digital transactions.

Privacy

Setting up and running a system for records management and preservation of evidences should always be done with consideration of data protection regulations. If personal data is involved the system needs to be GDPR [Re16] compliant. This requires that affected data are strictly stored off-chain and can be deleted on demand. There are some solutions in the field of applied research for GDPR [Re16] compliance of DLT, e.g. [Bu18], but currently neither standardized nor matured. Any access to data on-chain needs valid access rights management. DLT have to be integrated in data protection management including appropriate technical and organizational measures [Ko18], [Zi17], [Fe19].

4.2 Technical criteria

One main challenge concerning the long-term stability of DLT is the possibility to migrate data stored on-chain. Currently only migration between different DLT-platforms is possible via a bridge but standardized migration from DLT to another business – necessary e.g. to fulfil the right of data portability GDPR [Re16] – is still in research stage. That is why personal data should be stored off-chain only.

Information Security

Although DLT contains properties to ensure integrity of the transactions there are also different security vulnerabilities against possible attacks. Before DLT is used, a security concept is necessary which covers a well-grounded risk management and detailed security measures including further information concerning consensus mechanism and its fault tolerance [Fe19]. The cryptographic mechanisms shall be based on state-of-the-art algorithms as recommended e.g. in [SO16] or [ET19a].

Long-Term Preservation and Proof of Existence

A main vulnerability concerning long-term burden of proof of digital transactions in DLT is the lack of standardized rehashing and resigning measures as well as Proof of Existence. In DLT the blocks or ledger are hashed in the father-son-principle but without a standardized procedure for the rehashing of the whole chain in case that the cryptographic algorithms or their parameters lose their suitability as security measures over the course of time. This lack can lead to recalculation of old hash algorithms and manipulation of the chain by an attacker without notice

The reason for this is that with obsolete hash-algorithms the secured data can be changed by recalculation and afterwards replacement of the hash protection**,** which still seem to protect the original data but were manipulated.[FE19] [SM17] [DI20a]. This vulnerability is well-known since hash and also signature integrity protection is used and not exclusive to DLT. Furthermore, there is also no Proof of Existence acc. [ET18] and [ET19b] with a trustworthy time for transactions in DLT. Existing time-stamps in DLT only make evident a period of time, but not a point of time where a transaction was executed or transaction/data were still unaltered from a trustworthy source e.g. (qualified) trust service provider acc. to Art. 41 eIDAS [Re14].

The hash-based integrity protection in DLT uses Merkle-Trees [Me80]. This makes it possible to use well-established measures e.g. acc. to TR-03125 [Fe18] and RFC4998 [GBP07], also included in the standards for (qualified) preservation services eIDAS [Re14] and [ET19b], [ET20] to solve the rehashing and Proof of Existence challenge in DLT. In this case the system for long-term preservation regarding the [Fe18] in connection with a (qualified) preservation service on basis of [ET19b], [ET20] is connected and complements it with the missing functionalities. The picture below illustrates a possible solution [Ko18], [SM17].

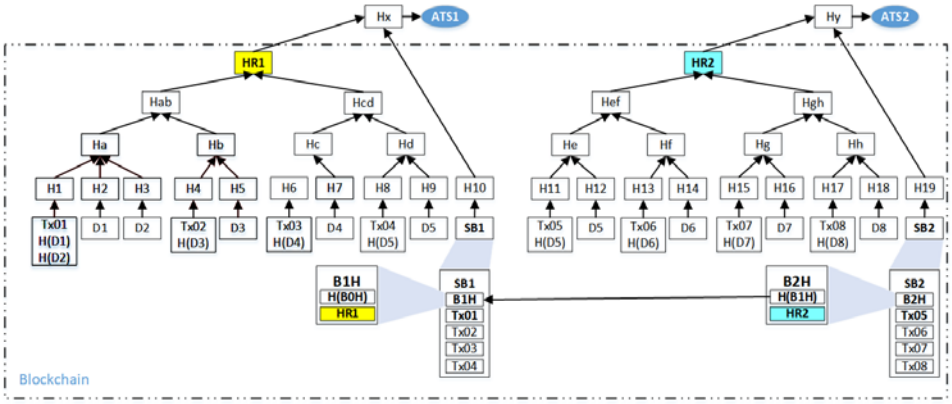

Fig. 1: Evidence Preservation in DLT

The transactions form a data object group acc. to [GBP07] together with the referenced records (content) e.g. Tx01 with D1 and D2 or Tx04 with D5. A Merkle- Hashtree [Me80] is created over all transactions and the referenced records which will be closed with the root-hash-value e.g. HR1. The calculated root-hash-value will be stored in the belonging blockheader e.g. B1H inside the block-description, e.g. SB1, and protected with the same hash-tree. As a result the hash-tree of the block gets a new root-element,

e.g. Hx, which will input for hash-tree acc. [GBP07] e.g. in a [Fe18] compliant system for evidence preservation or preservation service acc. to eIDAS [Re14] and [ET20] and closed by a qualified archive timestamp [Ad01] e.g. ATS1. Some procedure can be done with the next block (B2) so that the needed concatenation of the blocks will be achieved. The same system or preservation service can be used for the off-chain stored records too. In the result the evidence preservation as well as rehashing and Proof of Existence of on-chain transaction information and the referenced records can be done in this way.

5 Perspective and Need for further Standardization

In summary it can be determined that a valid records management together with appropriate security measures, evidence preservation as well as the identification systems and trust services acc. to eIDAS [Re14] enable DLT to be used for trustworthy digital transactions. Secure digital identities and trust services can be easily added to DLT networks to achieve non-repudiation and thus long-term preservation of evidences on authenticity and integrity of on-chain stored transaction data. Although further standardization is ongoing in CEN concerning interoperability of digital identities, especially self-sovereign-identity in DLT according to ESSIF-initiative as well as to identify and realize further development of eIDAS [Re14] and corresponding European standards for user-friendly and compliant utilisation of digital identities in DLT.

The well-described connection between DLT and corresponding business-IT, where the records and especially personal data are stored off-chain, achieves compliance to GDPR [Re16]. The combination makes it possible to use the advantages of both worlds DLT and eIDAS [Re14], GDPR [Re16] and establishes the basis for innovative network based business models G2B2C in trustworthy digital ecosystem. In order to make the business models easier as well as to ensure long-term stability, further standardization concerning GDPR [Re16] but also migration facilities of DLT is recommended. Another subject for further standardization is appropriate security measures, especially the long-term stability of hash algorithms and Proof of Existence in DLT as well as their preservation of evidence to fulfil legally binding burden of proof or documentation needs.

Bibliography

[Ad01] Adams, C. et al.: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). IETF RFC 3161. 2001.

[BB15] Buchmann, N.; Baier, H.: Elektronische Identifizierung und vertrauenswürdige Dienste. In D-A-CH Security 2015. Bestandsaufnahme - Konzepte - Anwendungen - Perspektiven. 08. - 09. September 2015, St. Augustin, 2015.

[Bu18] Bundesdruckerei GmbH: From the Almighty Administrator to the Self-determined User. An Innovative Approach from Bundesdruckerei's Research Lab: Identity and Rights Management with FIDES, 2018.

[CF19] CFR: Title 21 - Part 11 Electronic Records; Electronic Signatures. 21CFR11. 2019

[DI20a] DIN SPEC 31648: Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain. 2020.

[DI20b] DIN SPEC 4997: Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology. 2020.

[EA20] EASA: Part 21 - Airworthiness and Environmental Certification. https://www.easa.europa.eu/acceptable-means-compliance-and-guidance-material-group/part-21-airworthiness-and-environmental, accessed: 30/03/2020.

[EB20] EBSI, European Blockchain Services Infrastructure, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI, accessed: 30/03/2020.

[EG13] E-Government Act. EgovG. 2013.

[ES20] ESSIF, European Self-Sovereign Identity Framework, https://www.eesc.europa.eu/en/news-media/presentations/european-self-sovereign-identity-framework, accessed: 30/03/2020.

[ET18] ETSI: TS 119102-1 – V1.2.1 - Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, 2018.

[ET19a] ETSI: TS 119 312 - V1.3.1 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. 2019.

[ET19b] ETSI: TS 119 511 - V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques. 2019.

[ET20] ETSI: TS 119 512 - V1.1.1 - Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services. 2020.

[Fe18] Federal Office for Information Security (BSI): BSI Technical Guideline 03125, TR-ESOR – Preservation of Evidence of Cryptographically Signed Documents.v.1.2.2, https://www.bsi.bund.de/EN/tr-esor, 2018

[Fe19] Federal Office for Information Security (BSI): Towards Secure Blockchains. Concepts, Requirements, Assessments. 2019.

[Fi06] Fischer-Dieskau, S.: Das elektronisch signierte Dokument als Mittel zur

Beweissicherung. Anforderungen an seine langfristige Aufbewahrung. Kassel, 2006.

[GBP07] Gondrom, T.; Brandner, R.; Pordesch, U.: Evidence Record Syntax (ERS), IETF RFC 4998. 2007

[He18] Henne, T.: Juristische Anforderungen an die Beweiswerterhaltung bei digitaler Archivierung. Marburg, 2018.

[IE17] IEEE: ICCCN 2017. 26th International Conference on Computer Communications and Networks (ICCCN) July 31-August 3, 2017, Vancouver, Canada. IEEE, Piscataway, NJ, 2017.

[IS12a] ISO 14721:2012 Space data and information transfer systems - Open archival information system (OAIS) - Reference model, 2012.

[IS12b] ISO 16363:2012 Space data and information transfer systems - Audit and certification of trustworthy digital repositories, 2012.

[IS16] ISO 15489-1:2016 Information and documentation - Records management - Part 1: Concepts and principles, 2016.

[IS20a] ISO/AWI TR 24332 Information and documentation - Blockchain and DLT and records management: Issues and considerations, 2020.

[IS20b] ISO/DIS 22739: Blockchain and distributed ledger technologies - Terminology, 2020.

[JSG11] Jerman, A.; Saljic, S.; Gondrom, T.: Extensible Markup Language Evidence Record Syntax (XMLERS). IETF RFC 6283. 2011.

[KHS14] Korte, U.; Hühnlein, D.; Schwalm, S.: Standards for the preservation of evidence and trust. Proceedings Archiving 2014, Springfield 2014, S. 9-14.

[KKS18] Korte, U.; Kusber, T.; Schwalm, S.: Vertrauenswürdiges E-Government - Anforderungen und Lösungen zur beweiswerterhaltenden Langzeitspeicherung, 2018.

[Ko18] Korte, U. et al.: Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain, DACH-Security 2018. S. 177-191 Frechen 2018.

[Ko19] Korte, U. et al.: Vertrauenswürdige digitale Transaktionen - Records Management und Beweiswerterhaltung mit Blockchain, 2019.

[Le16] Lemieux, V. L.: Trusting records: is Blockchain technology the answer? In Records Management Journal, 2016, 26; S. 110–139.

[Me80] Merkle, R. C.: Protocols for Public Key Cryptosystems. In: 1980 IEEE Symposium on Security and Privacy. IEEE, Oakland, CA, 1980. S. 122-134.

[OE17] OECD: OECD Digital Economy Outlook 2017. Organisation for Economic Co-operation and Development OECD, Paris, 2017.

[Re14] Regulation (EU) No 910/2014 of the European Parliament and of the Council - of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. eIDAS, 2014.

[Re16] Regulation (EU) 2016/ 679 of the European Parliament and of the Council - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation). GDPR, 2016.

[Ro07] Roßnagel, A. et al.: Langfristige Aufbewahrung elektronischer Dokumente. Anforderungen und Trends. Baden-Baden, 2007.

[Sc15] Schwalm, S. et al.: Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden - Neue Chancen und Herausforderungen für vertrauenswürdige elektronische Geschäftsprozesse in Europa. Berlin, 2015.

[Sc17] Schwalm, S.: A service for the preservation of evidence and data – a key for a trustworthy & sustainable electronic business. Open Identity Summit 2017. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2017 S. 131-144

[Sc18] Schwalm, S. et al.: Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain, 2018.

[SM17] Sato, M.; Matsuo, S.'i.: Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography. In ICCCN: 26th International Conference on Computer Communications and Networks (ICCCN) July 31-August 3, 2017, Vancouver, Canada. IEEE, Piscataway, NJ; 2017, S. 1–8.

[SO16] SOG-IS Crypto-Evaluation Scheme - Agreed Cryptographic Mechanisms-1.0. 2016.

[UK16] UK Government Chief Scientific Adviser: Distributed Ledger Technology: beyond block chain, 2016.

[UN17] UN United Nations Commission on International Trade: UNCITRAL model law on electronic transferable records. United Nations, New York, 2017.

[Ve17] Vertrauensdienstegesetz. VDG, 2017.

[W320] W3C: Decentralized Identifiers (DIDs) v1.0. 2020.

[We17] Welzel, C. et al.: Mythos Blockchain: Herausforderung für den öffentlichen Sektor. Kompetenzzentrum Öffentliche IT, Berlin, 2017.

[We18] Weber, M. et al.: Records Management nach ISO 15489. Einführung und Anleitung. Beuth Verlag, Berlin, 2018.

[Ya18] Yaga, D. et al.: Blockchain technology overview. National Institute of Standards and Technology, Gaithersburg, MD, 2018.

[Zi17] Zimprich, S.: Blockchain. Der Hype und das Recht, Hamburg, 2017.