H. Roßnagel, C. H. Schunck, S. Mödersheim (Hrsg.): Open Identity Summit 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 131

Records Management and Long-Term Preservation of Evidence in DLT

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

Abstract: DLT improves decentralized business models and transactions from supply chain or cryptocurrencies to shared mobility, electronic registries or proof of origin. The planned enhancement of European Blockchain Service Infrastructure approximately 2021-2022 is expected to accelerate these developments based on a scalable, standardized framework. Like any infrastructure or IT-system used for business relevant transactions also in DLT is has to be possible to make decisions and processes evident against 3rd parties such as courts, auditors or regulative authorities. This leads to the challenge to fulfil requirements on a valid records management acc. to current standards [IS20b] [IS16] as well as to preserve the evidences of electronic records as long as they are needed according to current regulations and standards [eIDAS] [ETS19b] [VDG]. Based on international standardization the authors are taking part in, this paper focuses on the challenges and requirements for records management and preservation of evidence in DLT as well as possible solutions and needs for further standardization.

Keywords: DLT, blockchain, eIDAS, long-term preservation, digital evidence, blockchain security, records management

1 Introduction

In the last years Distributed-Ledger-Technology (DLT) and its most famous representative blockchain generated a real hype in particular the well-known use case Bitcoin. After the bitcoin crash in 2019 first doubts about the real capacity of DLT occurred. In this context standardization on DLT increased and industry as well as public sector used the chance to enable the technology for high-regulated industries with corresponding requirements on records management and trust [Le17]. Basically, DLT is a decentralized distributed peer-to-peer network of technical nodes for data exchange and transaction execution. According to [IS20a] a distributed ledger is in this case shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism. The consensus mechanism ensures that all transactions are valid and unaltered. Its manner depends on the type of DLT so that the well-known prejudice that DLT implies unacceptable high energy need is only valid for some consensus mechanisms e.g. Proof of Work, other ones are much more efficient especially those ones in DLT with restricted access rights e.g. BFT, Proof of Authority, Proof of Stake etc. [IS20b]. DLT networks allow the transfer of data or value from one party to another without having intermediates involved. Once written to the ledger the transactions are immutable, mainly based on hash protection of data

[1] Fraunhofer Institute for Open Communication Systems, Kaiserin-Augusta-Allee 31, 10789 Berlin, Germany
[2] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany; Convenor ISO Tc 46 Sc 11 JWG 1
[3] Federal Office for Information Security. Heinemannstr. 11,-13, 53175 Bonn, Germany
[4] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany

stored on the chain. Any transaction can reliably be tracked on the chain [Ko20], [IS21]. If the factual distributed data set or transactions are bundled in sequential linked blocks it is called a blockchain – a special kind of DLT. The blocks can also include the hash of the previous block and so build the mentioned hash-protection [IS20b] and a so called "timestamp". This DLT-"timestamp" has to be differentiated from timestamps acc. to [RFC3161], defined in [eIDAS] and related standards [EN319421] due to its lack of a trustworthy source of time, missing creation and validation of digital signatures by trust service provider and missing Proof of Existence created by 3rd party instead of the system, here DLT, itself. The hash-based integrity protection of each block is based on Merkle-trees [Ko20] [Xu19]. In comparison to the original ideas of blockchain, DLT does not mandatorily require the elimination of an operator or consortium providing the distributed network, this depends on the kind of DLT which can be distinguished regarding the access rights and transparency of the transactions. In public DLT everybody can view all transactions and data so there is full transparency, in private DLT only authorized users are allowed, similar conditions apply concerning execution of transactions. In permissionless DLT every user is allowed to validate and persist transactions, in permissioned DLT it depends on the access rights who has the authorization to do so. Furthermore, DLT is differentiated concerning data storage, on chain if data are stored on the ledger or off-chain if data are only represented by hash in DLT. At minimum the transaction documented by ledger records or referred records acc. to [IS20b] are stored on chain together with hash values of the related off-chain records. Due to performance limitations and privacy reasons e.g. [GDPR] off-chain storage is currently widely used [Ko18], [An18]. In summary, DLT can be characterized as distributed system which derives its trust from the immutability due to cryptographic protection and integrity, as well as the consistency (not completeness) check by the consensus mechanism so that any unauthorized alteration will be transparent and, at best, no central authority or intermediary is needed. This also means that DLT is typically only useful in distributed ecosystems with more than 2 parties involved where distribution is reasonable and the parties typically do not trust each other, so that trust in the technology seems to be necessary [An18], [Wer18].

Currently the European Union is improving the European Blockchain Service Infrastructure as a pan-European DLT-network with a focus on use cases like e.g.:

- Notarization or data validation
- Self-sovereign identity
- Digital proofs or evidences
- Electronic registries and tokenization
- Cross-industry trade platforms or data exchange platforms

In most cases the DLT acts as a transaction layer or in case of SSI also as an anchoring layer where the records will mostly be stored off-chain, only anonymized or pseudonymized equivalents e.g. DIDs in SSI are on-chain. Together with scalability also trustworthiness and security shall be improved within [EBSI] until 2022.
Regardless of these properties and goals there are some challenges to use DLT in regulated industries with typically extensive documentation requirements and a burden of proof associated with retention periods between 5 and 100 years, some only starting after decades depending on a future event. This leads to the question how DLT could fulfill the

requirements for a valid records management, which ensures the authoritativeness of records to achieve compliance with burden of proof and documentation requirements. Associated with this is the preservation of evidence to make transactions and records evident against 3rd parties such as courts, regulative authorities etc. for as long as the records are needed [Ko18], [Di21], [We18]. Against this background the paper shows the main areas of action focused on records management, evidence preservation and related questions.

After the introduction in the first chapter, the second chapter of this document summarizes the legal and technical requirements of evidence of electronic records and long-term preservation. The third chapter explains unsolved, open challenges in DLT in connection with records management and preservation of evidence under the perspectives of privacy [GDPR], and the missing crypto stability [ET19a] in connection with long-term preservation of evidence in DLT. Chapter 4 provides a feasible solution to preserve the authenticity and integrity of on-chain and off-chain records in connection with their evidence by combining DLT with a Preservation Service pursuant to [eIDAS] and [TR-ESOR] in order to archive long-term crypto stability and preservation of evidence in DLT.

2 Fundamental Requirements for Evidence of Electronic Records and Long-Term Preservation

2.1 Legal Requirements

The [eIDAS]-regulation which came fully into force in July 2016 provides a Europe-wide mandatory legal framework for digital identities and trust services. It enables trustworthy digital transactions between public administrations, companies and citizens with or without DLT. [eIDAS] contains two main parts: digital identities and trust services. Concerning identities [eIDAS] currently only defines requirements on identity of natural and legal entities. The levels of assurance from high to low according to Art. 8 [eIDAS] and [2015/1502] define graded security requirements on identity-verification-procedures (LoA). Any notified eID has to be accepted by any public administration. Along with digital identities [eIDAS] also defines trust services. In the context of records management especially creation, validation and preservation of electronic signatures, seals, timestamps have to be recognized. Cryptographic electronic signatures or seals make the authenticity and integrity of electronic records evident against 3rd parties, a (qualified) timestamp gives a valid Proof of Existence (PoE) and evidence for the time of transactions. In all cases a successful validation and preservation is necessary. Any at least advanced signature, seal or timestamp from each qualified trust service provider has to be accepted and validated by any public administration. Based on a valid as well as technology neutral standardization framework [eIDAS] also ensures acceptance and interoperability of trust services [eIDAS]. Currently [eIDAS] is under revision so that new trust services e.g. regarding SSI or DLT might arise. Furthermore, different industry-specific requirements have to be mentioned in context of records management such as [EASA] Part 21 in aerospace, [FDA] or [GxP] in pharma and chemicals or anti-money laundering laws in banking or in the public sector. All of them require the proof of authenticity, integrity and

traceability of electronic records against 3rd parties for as long as those records are needed. Considering these decade-long retention periods, the legislators defined obligations for long-term evidence preservation and qualified preservation services in Art. 34 and 40 [eIDAS] as well as § 15 [VDG] in Germany. The [GDPR] defines requirements on the confidentiality of personal data in electronic records and digital transactions [GDPR]. Apart from appropriate technical and organisational measures to protect the confidentiality of personal data especially the evidence for consent of the affected person, the obligation to inform (Art. 13+14) as well as the rights of the affected person have to be taken into account [We18].

2.2 Documentation and Technical Requirements

Records Management

In accordance with applicable law and international standardization e.g. [IS16], [IS20b] a valid records management with or without DLT provides the necessary processes, roles and responsibilities, governance and technical solutions for the management of electronic records which provide the evidence for business transactions. Essential characteristics are the authenticity, integrity and traceability of electronic records as well as their availability and transferability. These inherent properties have to be ensured and preserved as long as the records are needed. This requires the availability and transferability of the records – so their evidence based on the records themselves and their useability acc. to retention requirements e.g. readability, analysability etc. Records fulfillling these requirements are called authoritative records and their authoritativeness, so their authenticity, integrity and traceability, has to be preserved until the end of the retention period. A system creating, capturing, storing records until disposition, is called record system [We18] [IS16] [IS20]. So, if DLT is used in high-regulated industries where typically a valid records management is necessary, it acts as a record system and so has to fulfil the requirements on record systems and records management [IS16], [IS21a]. In DLT with on-chain and off-chain storage the evidence for a transaction needs the transactions records which are stored on-chain and the corresponding off-chain records for a valid records management [VL17], [IS21a].

Long-Term Preservation

Cryptographical measures such as (qualified) electronic signatures and seals from qualified trust service providers [eIDAS] enable the non-repudiation and thus unique evidence of the authenticity of records as well as their integrity by trusted 3rd party. There is no trust by self-confirmation as done by DLT, only by proof and therefore by trust services [NIST], [Ko20]. Together with a qualified timestamp they also allow a valid PoE at the given time. DLT inherent cryptographical protocols do currently not fulfil the requirements on (qualified) signatures, seals or timestamps [eIDAS] and have to be enhanced with addition of eIDAS-compliant trust services needed to provide genuine verifiability of digital transactions as well as a PoE in DLT and the legal effects (equivalent to handwritten signature) of (qualified) e-signatures pursuant to [eIDAS]. This effectively requires the combination of DLT with trust service providers acting like a “trusted gatekeeper” to enable DLT for trustworthy digital transactions as it is currently also

required by first standards [Ko20], [DI21]. Cryptographical signature techniques (e.g. seals, signatures, timestamps, and evidence records) also enable the preservation of evidence of the records without losing the negotiability of the records [UN17]. That requires that measures regarding long-term preservation must focus on the record itself and not on the system or infrastructure in which they are stored [Sc17], [IS12], [KSH14]. Preservation of evidence over decade-long retention periods is currently executed by preservation mechanisms based on cryptographic measures by re-signing and rehashing of (qualified) signatures/seals in combination with a qualified electronic timestamp or evidence records pursuant to RFC4998 [GBP07] "in spite of obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or of the loss of the ability to check the validity status of public key certificates" [ET19b]. Utilization of Merkle Hash trees acc. to RFC4998 ensures an efficient approach as illustrated below.

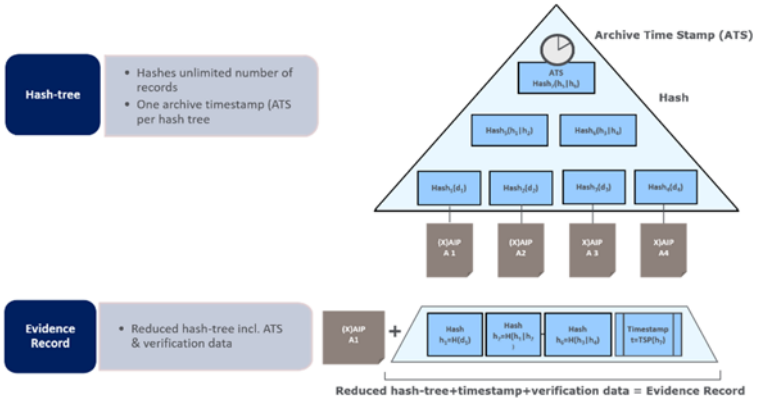

Figure 1: Hash-Tree and Evidence Record acc. to RFC 4998/6283

This procedure was adopted for (qualified) preservation services acc. to Art. 34 and 40 [eIDAS] by standards like [ET19b] [ET20a] for the service provider and in Germany [TR-ESOR] for the used preservation product. Since version 1.2.1 the [TR-ESOR] whose main content was adopted in [ET19b] and [ET20a] for European preservation services, is fully compliant to [eIDAS] and since version v1.2.2 it provides full interoperability to European ETSI standards. The [TR-ESOR] defines a reference architecture for evidence preservation service as well as container formats of self-contained archival information packages which contain all necessary information (metadata, content, credentials) to preserve evidence of electronic records and the records themselves. In addtition to preservation of evidence also the traceability and availability of electronic records as well as the reliability of the transaction in which it was created have to be preserved, also in case of DLT. A comprehensible approach ensures both – the preservation of evidence and information of electronic records using well-defined processes and self-contained information packages in a trustworthy digital archive based on established international standards [IS12], [Sc17], [KoSH14].

3 Challenges in Records Management and Preservation of Evidence in DLT

Since currently there are no standardized measures in DLT to fulfil privacy requirements according to the [GDPR], it is recommended to store electronic records off-chain, if possible. In this case, only the transaction records remain on the chain. This leads to a complexity in the operation of DLT because the link between on-chain and off-chain records has to be preserved for as long as the records are needed. Another challenge stems from the fact that there are no standardized measures to preserve the information itself, i.e. its availability or technical interpretability over a retention period of 10, 20 or more years. To make the authenticity and integrity of on-chain records (e.g. transactions) evident towards 3rd parties, it is necessary to ensure crypto agility and the preservation of the evidence of records, and to renew the underlying hash protection in the light of technical improvements in cryptoanalysis, and to couple it with a valid proof of existence including utilisation of state of the art hash-algorithms [ET19a] [SOGIS], [DI21], [Ko20], [Ya18]. A typical DLT application implies the storage of the relevant data (at minimum transaction records) in a dedicated transaction object (e.g. Tx01 on Figure 2) directly on the chain, possibly linked to off-chain records. The transaction records are protected by a Merkle-tree (by using the hash algorithm H), which's root (e.g. HR_1) is placed in the block header (e.g. B_1H) and together with the tree constitutes a single block (e.g. B_1) on the chain [NA08]. On the other hand, the block header together with the tree constitutes a single block (e.g. B_1) on the chain [NA08].

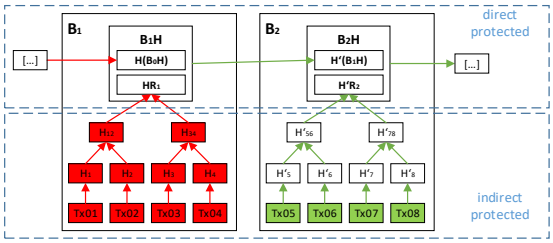

Figure 2: A sample of a blockchain with on-chain and off-chain storage – rehashing issue.

In case the used hash algorithm H (see block B_1) is about to become weak, a hash algorithm change has taken place and the new block B_2 is using the new stronger hash algorithm H', which means sufficient protection (because directly hashed with H') for B_2 and the header of B_1 (pointed at with green arrows), but not for the Merkle-tree of B_1 (because only indirectly hashed with H' – actually only root of the tree) and all blocks before B_1 (red marked parts). It means, it is not definitely excluded, that possible manipulation of those transaction data remains undetected, which means, that the integrity protection and further the evidence preservation of those data is irrevocable lost. This also means that there is no long-term crypto stability in DLT currently as well as no PoE acc. to state-of-the-art technology as needed for burden of proof [We18], [eIDAS]. In order to preserve the evidence of the "red marked data" a suitable mechanism has to be applied to refresh the hash values of the all relevant data stored on and perhaps referenced from the chain as well as to provide a valid proof of existence. So, measures for crypto-stability and

preservation of evidence in DLT have to focus their actions on DLT.

4 Possible Solution

As mentioned above the hash protection in DLT is using Merkle-trees similar to preservation of evidence acc. to current standards in [ET19b], [ET20a] and [TR-ESOR]. This is the key for possible solutions. As mentioned in chap. 1 transaction records are always stored on-chain but any other records e.g. content etc. may also be stored off-chain and only referenced. As a direct implication of such an approach, an additional level of indirection is created, "double indirect protection" (see Figure 3). It means, the issues discussed in section 3 apply a fortiori.

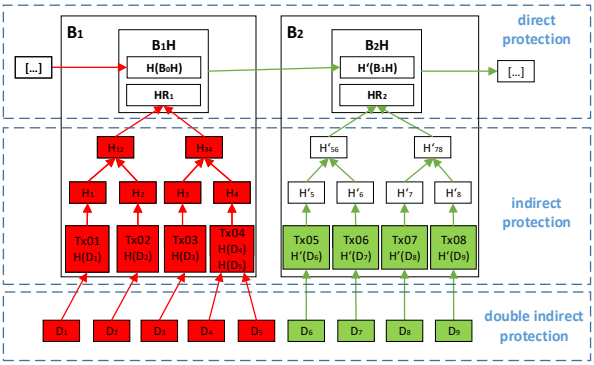

Figure 3: Blockchain example with off-chain transaction data and rehashing issue.

Due to the weakness of the hash algorithm H, which has been used in the block B_1 and before the next block, B_2 is using a stronger hash algorithm H'(typical blockchain rehashing approach). In such a case all the information hashed directly with H' is still sufficiently protected (marked green), but the parts of the chain, which have not been directly hashed with H', became weak (marked red) – the evidence would be lost [eIDAS], [VDG]. In order to keep the evidence on the whole chain, the approach of a "logical blockchain", which based on the evidence record method described in RFC4998 [GBP07], has been developed. The RFC4998-method of the evidence preservation is purely based on the Merkle-trees and does in particular support the rehashing mechanisms. By using this approach, the whole blockchain data will be protected by a dedicated RFC4998-enabled tree. Following Figure 4 depicts the approach of "logical blockchain" by using the example of the blockchain illustrated in Figure 3.

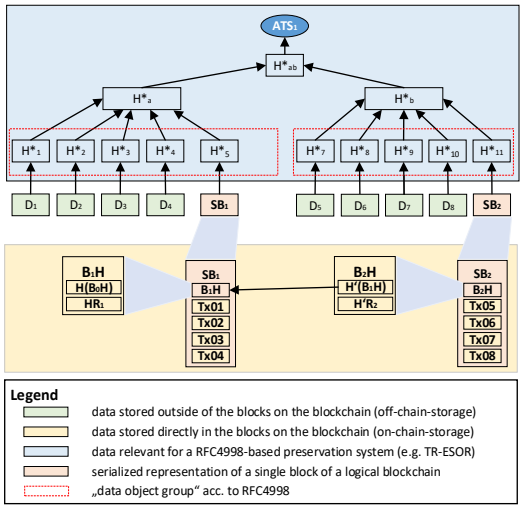

Figure 4: "Logical" blockchain

Every single block from the chain (here B_1 and B_2) has to be slightly prepared in advance and suitably submitted to the RFC4998-based system. The following steps have to be performed:

1. A serialized replication of a block on the chain (serialized block, e.g. SB_1 on Figure 4) has to be created by the DLT for every single block to be protected on the RFC4998-based system. The serialized block does contain the data of the single block (especially the transaction data with the hash references on the external documents, but also the header and the hash tree) stored in a well-defined manner. The hash from the referenced off-chain records are renewed in this step.
2. For every block the serialized block (e.g. SB_1) and (optional) a collection of the referenced documents (e.g. D_1, D_2, D_3, D_4 and D_5) build so called data object groups acc. to RFC4998.
3. Depending on the implemented approach by the preservation service to be used, it is possible either to submit the whole data object group built in step 2, or only the suitable hash value list, containing a hash of every single object in the group to the preservation service [TR-ESOR], [ET20a].
4. The preservation service internally builds the Merkle-tree and seals it with an archive-timestamp (e.g. ATS_1).
5. The preservation service provides a unique id (AOID[5]) for every submitted data object group, which has to be stored for further purposes.
6. By using the received AOID it is possible to obtain the corresponding evidence record for the protected block incl. referenced off-chain records (e.g. $ER_1^*=\{<[\{(H^*_1, H^*_2, H^*_3, H^*_4, H^*_5, H^*_6),(H^*_b)\}, ATS_1]>\}$[6]).

[5] AOID – Archive Object ID

[6] An evidence record with one archive timestamp chain, reduced hash tree for data object group of SB_1 and a corresponding archive time stamp ATS_1.

In case the hash algorithm of the preservation service (here H^*) is about to lose its security suitability, the rehashing operation acc. to RFC4998 (see [GBP07], chapter 5.2) shall be applied in advance (by using a new hash algorithm e.g. H^{**}) including the replicated block and sends notification to the DLT to rehash the off-chain-records referenced from the transaction records. This means it is an interaction of preservation service, DLT and off-chain storage. The resulted rehashed hash tree will preserve the evidence of the whole block data (on- and off-chain records). In order to perform the rehashing operation, the preservation service has to have access either to every corresponding data or its new hash value (see step 3 above). The renewed (rehashed) evidence record for a particular block, can be obtained by providing the corresponding AOID (see step 5 above) directly from the preservation service (e.g. $ER_1^{**}=\{<[\{(H^*_1, H^*_2, H^*_3, H^*_4, H^*_5, H^*_6),(H^*_b)\}, ATS_1]>, <[\{(H^{**}_1, H^{**}_2, H^{**}_3, H^{**}_4, H^{**}_5, H^{**}_6),(H^{**}_b)\}, ATS_2]>\}$[7]). Even if the data of B_1 is protected by a weak algorithm H, the possible manipulation of it could be easily detected by verifying the corresponding evidence record, respectively ER_1^* or ER_1^{**}. The provided solution makes use of 3 components, the preservation service, the DLT and the data storage with the off-chain records. The preservation service ensures the preservation of evidence acc. to [ET20a], [ET19b], [TR-ESOR] and the crypto-stability of the DLT as transaction- and or anchoring layer itself. The DLT represents the distributed application and contains the transaction records, the storage contains the off-chain records. To make a transaction evident the authenticity and integrity of on-chain transaction records as well as the linked off-chain records are needed [Ve16], [Ve17], [IS20], [IS21]. Picture below shows the interaction.

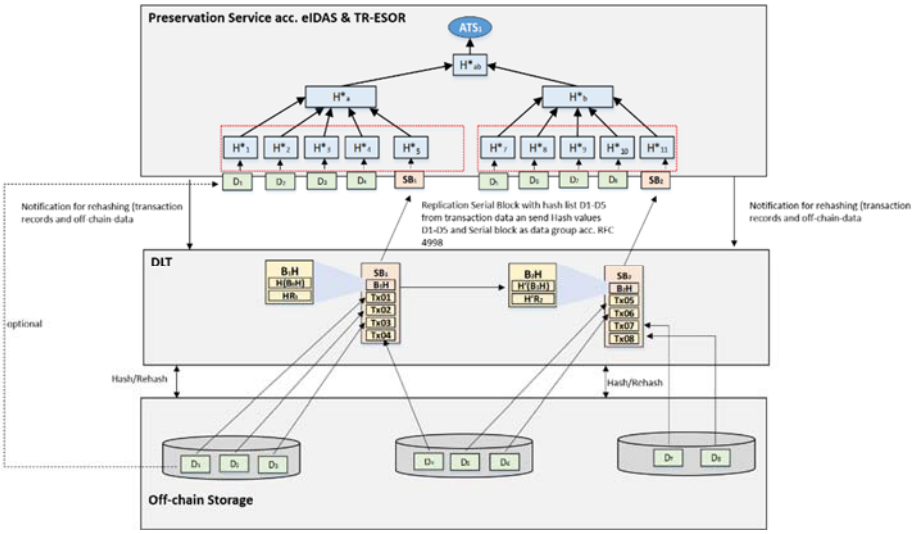

Figure 5: Solution example

[7] An evidence record with two archive timestamp chains, corresponding two reduced hashed trees of SB_1, one with H^* and another one with H^{**} and two corresponding archive time stamps for every chain, ATS_1 respectively ATS_2.

5 Conclusion and Needs for further Research

The utilisation of DLT increases also in regulated industries. This leads to the need for fulfilling burden of proof and documentation requirements so to achieve requirements on a valid records management as well as evidence against 3rd parties. Currently there are some challenges in DLT to reach legal verification needs as they are common in regulated environments such as deletion, portability or change of records but also evidence for authenticity, integrity and reliability of on-chain and off-chain records. With supplement of trust services acc. to [eIDAS] some challenges may be solved. But concerning decade-long retention periods the crypto stability, preservation of evidence and preservation of especially on-chain records themselves seem to be some of the main critical challenges for a wider DLT-utilisation. The approach mentioned in chap. 4 provides a feasible solution to preserve the authenticity and integrity of on-chain and off-chain records and so their evidence and to achieve crypto stability in DLT. De facto it probably must be done for each node.

This requires further technical standardization on DLT. Main requirements are the ability to create the serial block with all transactions from the block it contains including new hashes of the referenced off-chain records, the replication of the serial block to the preservation service including hash list of related off-chain records, receive and send notifications from and to the preservation service in case of rehashing to ensure the rehashing of off-chain records linked to the transactions in the serial block. A valid standardization should develop a generic solution which can be assessed and adopted for at minimum the leading DLT protocols e.g. Ethereum, Hyperledger Fabric, Hyperledger Indy (used for SSI) and Corda. The example described in the paper will be input for international standardization efforts in ISO and CEN, where the authors are taking part in.

6 Bibliography

[An18] Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2017

[BSI19] Federal Office for Information Security (BSI): Towards Secure Blockchains. Concepts, Requirements, Assessments. 2019.

[DI21] DIN TS 31648: Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain. 2021.

[DN21] UNE 71307-1 "Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. N72 CEN/CENELEC JTC19, Brussels 2021

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

[eIDAS] 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.

[ESSIF] European Self-Sovereign-Identity Framework https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505734

[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.

[ET20a] ETSI: TS 119 512 - V1.1.2 - Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services. 2020.

[ET20b] ETSI Group Report 003. Permissioned Distributed Ledger (PDL). Application Scenarios

[ET21] ETSI Group Report 004. Permissioned Distributed Ledgers (PDL) Smart Contracts. System Architecture and Functional Specification. 2021

[EU18] Blockchain and the GDPR. EU Blockchain Observatory and Forum. Version 1.0. Brussels 2018

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

[GDPR] 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.

[IS12] ISO 14721:2012 Space data and information transfer systems - Open archival information system (OAIS) - Reference model, 2012.

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

[IS20a] ISO 22739:2020: Blockchain and distributed ledger technologies - Terminology, 2020.

[IS20b] ISO 30300:2020 Information and documentation — Records management. Core concepts and vocabulary

[IS21a] ISO/WD TR 24332 Information and documentation - Blockchain and DLT and records management: Issues and considerations, 2021.

[IS21b] ISO/DIS 23257 Blockchain and distributed ledger technologies — Reference architecture. 2021.

[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.

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

[Ko20] Korte, U. et. al.: Criteria for trustworthy digital transactions – Blockchain/ DLT between eIDAS, GDPR, Data and Evidence Preservation. OpenIdentity Summit 2020. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2020 S. 49-60

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

[Le17] Lemieux, V.: A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. 2017 IEEE International Conference on Big Data (Big Data). DOI: 10.1109/BigData.2017.8258180

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

[NIST] NIST Special Publication 800-207. Zero Trust Architecture. 2020

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

[RFC3161] Adams, C. et al.: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). IETF RFC 3161. 2001.

[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

[Schu19] Schütz, A. et al.: Blockchain für Entwickler. Das Handbuch für Software Engineers. Grundlagen, Programmierung, Anwendung. Bonn 2019

[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.

[TR-ESOR] 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, 2019

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

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

[VDG] Vertrauensdienstegesetz. VDG, 2017.

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

[Wer18] Werbach, K.: The Blockchain and the New architecture of Trust. Massachusetts Institute of Technology. 2018

[Xu19] Xu, X. et. al.: Architecture for Blockchain Applications. Cham 2019

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

[Yak18] Yakubov et.al.: A Blockchain based PKI Management Framework. NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium. April 2018 DOI: 10.1109/NOMS.2018.8406325

[Zi18] Zile, Kaspar et. Al.: Blockchain Use Cases and Their Feasibility. Applied Computer Systems May 2018, vol. 23, no. 1, pp. 12–20. doi: 10.2478/acss-2018-0002