A State-of-the-Art Blockchain Approach to the ETSI Implementation for Long-Term Preservation Solutions

Sorin Țeican[1(✉)] and Andreea-Elena Drăgnoiu[2(✉)]

[1] certSIGN SA, Bucharest, Romania
sorin.teican@certsign.ro
[2] Department of Computer Science, University of Bucharest, Bucharest, Romania
andreea-elena.panait@drd.unibuc.ro

Abstract. Lately, blockchain technology has been used in various use case scenarios. Our research focuses on whether long-term preservation of digital signatures/seals (for which we introduce the abbreviation LTP-DS) solutions could benefit from using this technology. In this paper, we give an outline on the stateof-the-art blockchain-based LTP-DS-related solutions, while considering the ETSI standards for LTP-DS, and offer directions on how such systems could be implemented.

Keywords: Long-term preservation · Blockchain · Notarization

1 Introduction

The European Commission plans to define a pan-European regulatory sandbox for use cases such as data portability, B2B data spaces, smart contracts, and digital identity (Self-Sovereign Identity), we address what parts of the PKI ecosystem implemented by qualified LTP-DS (long-term preservation of digital signatures) systems can be replaced by blockchain mechanisms. Most Qualified Trusted Service Providers have conventional PKIs with digital certificates issued by certification authorities. A blockchain component has to offer clear advantages, both technical and from the business point of view, to replace or to be added in a qualified setup. An LTP-DS would have to inherit suitability with blockchain mechanisms due to the operations involved essentially providing digital transactions recording and easily (publicly) accessible proof of preservation over time to clients.

The remainder of our paper is structured as follows: Sect. 2 defines the background and related academic work, Sect. 3 describes the ETSI standard for an LTP-DS system, Sect. 4 defines blockchain basic knowledge and blockchain notarization, Sect. 5 gives an overview of the state-of-the-art blockchain LTP-DS-related solutions, Sect. 6 presents characteristics of how LTP-DS blockchain systems should be implemented, propose an SSI implementation, and finally, we conclude.

S. Paiva et al. (Eds.): SmartCity360° 2021, LNICST 442, pp. 550–562, 2022.
https://doi.org/10.1007/978-3-031-06371-8_35

2 Background and Related Work

To our knowledge, most of the blockchain research done in the field of long-term preservation omits the qualified digital signatures/seals which require the availability of information needed to check the validation status of the digital signature/seal that would not be publicly available until the end of the preservation period.

Otto et al. provides an overview of the corresponding standards for long-term preservation of qualified electronic signatures, which are currently developed within ETSI Technical Committee (TC) Electronic Signatures and Infrastructures (ESI), and outline the design of a corresponding reference implementation [1].

Bralić et al. investigate the challenges of the expiration of digital signatures in the context of digital archiving by identifying requirements for the long-term preservation of digitally signed records and comparing them with the existing approaches. The TrustChain 2.0 model is based on previous research conducted as part of the InterPARES Trust project. It builds on TrustChain 1.0 by including digital signature certificate chain validity information in a blockchain thus avoiding the issues concerning records confidentiality and privacy information disclosure [2].

Hyla and Pejaś propose a scheme that would allow maintaining signature validity without the necessity to use timestamps from trusted third parties is proposed. The Round-based Blockchain Time-stamping Scheme is proposed to be scalable, i.e., it requires embedding a constant number of bytes into a blockchain independent from several input documents. The scheme allows proving that a document existed not only before a certain date but after a certain date as well. Moreover, the purpose of the scheme is to meet non-repudiation requirements for digitally signed documents. The scheme allows verifying signature validity using a chain model and a modified shell model [3].

Thompson explores whether blockchain technology is a suitable platform for the preservation of digital signatures and public/private key pairs. This paper suggests that the blockchain's hash functions offer a better strategy for signature preservation than digital certificates [4].

3 Standards for Long-Term Preservation of Digital Signatures

3.1 ETSI

ETSI technical specifications [5, 6] define long-term preservation for qualified electronic signatures as the extension of the validity status of a digital signature over long periods and/or of provision of proofs of the existence of data over time, despite 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. [5] identifies three main security risks involved with preserving qualified cryptographic material for long periods:

Risks Based on Collision Attacks of One-Way Hash Functions used within a Digital Signature. In case the preservation service has access to the signed data it can compute

a new digital signature or time assertion based on a new hash value of the signed data, calculated with a suitable hash algorithm and suitable parameters, to guarantee the integrity and proof of the existence of the signed data before the original hash algorithm becomes weak. In case the preservation submitter only submitted the hash of the digitally signed data to the preservation service, e.g., because it is very large or due to privacy reasons, the preservation service cannot recompute on its own a new hash of the signed data. The client may submit two hash values computed by two different hash algorithms, based on different mathematical principles, to reduce the risk of possible collision attacks. In any case, the preservation service cannot know if the hash value(s) corresponds to the signed data, and can treat them only as arbitrary data related to the signature.

Risks Based on the Digital Signature Algorithm and Key Length. It might be possible that at some moment in time it cannot be guaranteed anymore that the private key by which a specific signature was created, is still private and secret. This problem can be avoided if the digital signature including the certificate is covered by a time assertion that proves that it already existed before a specific time from which such an attack became possible. However, some time assertions rely upon mechanisms that will be subject to the same problems. To counter this problem, time assertions are protected by obtaining a new time-stamp that covers the original data, its time-stamps, and the corresponding validation data before the compromise of mechanisms used to generate the time assertions;

Risks Based on the Revocation of a Signing Key. To be able to trust that a digital signature was created by the signer, the certificate needs to be checked that it was not revoked at the signing moment or before. This can be done by using revocation information, like certificate revocation lists (CRLs) or online certificate status protocol (OCSP) responses of the certificate. The preservation service captures and protects revocation information in the preservation evidence, using proof of existence over it, to avoid problems because revocation information is not available anymore.

There are three main variants for a preservation service whether it uses long-term storage, temporary storage, or no storage. When it uses storage, the preservation service may use internal or external storage under its control for preservation. A preservation service can pursue different preservation goals, which influences the supported operational tasks. [6] specifies the following three goals which may be used separately or in combination: *preservation of general data* provides proof of existence over long periods of the submission data object submitted to the preservation service, *preservation of digital signatures* extends over time the ability to validate a digital signature, to maintain its validity status and to get a proof of the existence of the associated signed data, and *augmentation* which indicates that the preservation service supports the augmentation of submitted preservation evidence.

According to [6], a preservation service may support different preservation schemes. A preservation scheme supports at least one preservation goal and is operating in exactly one storage model. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider. The preservation service shall preserve all information needed to check the qualification status of the electronic signature or seal that would not be publicly available until the end of the preservation

period. Time-stamps used within the preservation evidence should be provided by a qualified TSA (Time Stamping Authority).

As stated in the EIDAS Trusted Service Provider (TSP)-Map [7], 15 countries across the European Union have implemented qualified LTP-DS systems, with the most notable countries by the number of implementations being Hungary, Spain, and Slovakia each with 3 qualified LTP-DS systems.

3.2 ISO

ISO 14641. Describes a reference framework for digital archiving of digital documents (also ones originating from physical) in a manner that covers aspects such as long-term preservation, integrity, ease of access, and use. Storage options considered being physical/logical WORM (write once read many) and rewritable. In the case of digital documents kept on rewritable storage the specification details integrity maintenance procedures such as encryption-like techniques, in particular with checksum calculation or hash function, date and time stamp, or digital signatures [8].

ISO 14721 OAIS. Open Archival Information Systems defines the OAIS model for preserving archival information on a channel accessible to the public. In the OAIS model, there are four types of Preservation Description information: prove-nance, context, reference, and fixity [9, 10]. The OAIS reference model describes concepts, responsibilities, detailed models, preservation perspectives, and archive interoperability. OAIS It takes into account the impacts of changing technologies, including support for new media and data formats, or with a changing user community, stating that the long-term may extend indefinitely. Standards developers are expected to use this model as a basis for further standardization.

ISO 16363. Provides an overview of audit and certification criteria for organizational infrastructure, digital object management, and infrastructure and security risks [11]. [12] provides general requirements for storage with preservation of evidence including legal framework conditions, a middle-ware architecture composed of the following components: ArchiSafe, ArchiSig, Upload & Download module, and a cryptographic module. To validate the implementation conformity and interoperability tests are specified for the architecture.

4 Blockchain and LTP-DS-Related Systems

4.1 Key Blockchain Concepts

A blockchain peer-to-peer network (formed of a "chain of blocks") allows creating a decentralized and distributed environment, where transaction data is cryptographically validated and recorded on a publicly accessible ledger, with no third party in control of the network.

Blockchain blocks are interconnected using hash functions and those generated hash values will be preserved on the blockchain as long as the network continues to operate.

In the blockchain environment, hash values are used to authenticate block data as well as transaction data, and can be stored separately from the application that generated the hash values [13]. Hash values can be grouped to form a single hash, called a root hash, and the structure is called a Merkel tree.

A blockchain network is formed of nodes and recording new information on the blockchain implies that the nodes reach a consensus. The consensus mechanism is based on cryptogr validation methods and ensures the right sequence of blockchain transactions. There are various consensus algorithms among them we mention Proof of Work, Proof of Stake, Proof of Authority, etc. Blockchains make use of signature schemes to sign (authenticate) the transactions and the most common ones are the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Schnorr signatures. Another key concept is that the blocks are timestamped before being recorded in the ledger and do not require intermediaries such as Time Stamping Authoritaphicies (TSA).

4.2 Blockchain Technology and Notarization Standards

Blockchain can be used for document management processes: for version tracking of documents, tracing, change verification, document content, and structure. Each time a new document is created, it can be registered on the blockchain, together with a block timestamp to date the document in time. In this way, the initial document version becomes clear, as well as future document versions, which can be traced back and verified accordingly, if desired. Moreover, document registration on the blockchain represents proof that it was not tampered with, useful when sending document evidence to other parties. The hash values, which are independent of the file format and are used in the blockchain technology allows this technology to be compliant with the preservation standard ISO 18492:2005 (a guide on long-term preservation of electronic document-based information).

The ISO 14721 OAIS can be applied to the blockchain technology. Any document change results in a new document hash value, with a corresponding identifier, so that the digital transitions maintain the history of the document provenance. Blockchain technology is not interested in the context of document creation. The hash value identifies (references) the document version at a certain time, whereas the fixity information for blockchain concerns its immutability property.

For the management and control of records and the associated metadata, the set of rules is defined by ISO 15489-1:2016 standard. The fact that the document is separated from the metadata (usually the document remains on the archive's database, whereas its metadata is recorded on the blockchain platform) enables the blockchain technology to easily comply with this standard, by using metadata formats that are not conditioned by a document type.

Other standards, such as RFC 3161 and ANSI X9.95, describe how digital notaries and trusted third parties (known as TTP) should govern timestamps. While RFC 3161 describes the timestamp request and response format [14], the ANSI X9.95 standard is more focused on the security of financial transactions [15]. The timestamping service, defined in RFC 3161 as a proof mechanism for demonstrating the existence of data at a particular time, can be mapped with the blockchain technology.

5 Comparison Between LTP-DS Blockchain-Relat Solutions

In this section, we introduce several solutions that use blockchain technology in imimplementingedTP-DS related systems. We distinguish between qualified and non-qualified LTP-DS-related solutions. We consider a qualified solution one that makes use of a certified authority (an entity that issues digital certificates) in its implementation. We note that none of them comply with the ETSI standard for LTP-DS systems and that they are mainly notarization solutions. To the best of our knowledge, at the moment, we are not aware of ETSI compliant LTP-DS qualified blockchain solutions. For our research, we considered all the blockchain solutions that were available or mentioned in the literature, at the moment of writing. For this paper, we were only interested in presenting the qualified solutions in more detail. In Table 1, we summarize the gathered information for the qualified solutions into the following properties: the used blockchain platform, timestamp type, type of solution (private or public subscriptions), type of service offered (web or mobile applications), usage of certified authority, and available documentation.

The qualified blockchain LTP-DS-related solutions we found use either their blockchain solution (Guardtime KSI solution [16]), the Bitcoin platform (Enigio [17] solution), or multiple blockchain platforms (Proofstack [18] and Bernstein [19] solutions). All qualified solutions offer private subscription plans, as well as publicly available solution demos, and all of them are accessible via web applications. We remark that the Proofstack solution seems to offer more features than the rest of the solutions from Table 1.

Guardtime KSI [16] uses Keyless Signature Infrastructure (KSI) that allows the verification to be based only on the security of the used hash functions and the public ledger. This permissioned blockchain solution is a "mirror" system, i.e., a solution where the blockchain is used as a repository for digital fingerprints, which are the hash values used, whereas the original records could be in a digital or paper form. It can be considered that Guardtime differs from other blockchain providers by the industrial capacity of their solution. Moreover, Guardtime benefits from the NIST Crypto Algorithm Validation Program, Common Criteria, and NIAP Accreditation, as well as participation in cybersecurity programs.

The Enigio [17] solution, called Enigio time:stamp, uses a timestamp part and a blockchain one. The solution is compliant with the ISO/IEC 18014-3 principles, which are augmented with the company's patents. The company created their blockchain where they aggregate references to other blockchains, such as Bitcoin, and use their time: beat patent, for introducing real references into their blockchain. By using a blockchain aggregator as a service, the solution allows access to an easy-to-use API, which abstracts the processes. Among advantages, Enigio claims that their solution enables easy access and a lower cost, strong traceability, continuous monitoring, speed, and better model performance (compared to proof of work or mining-based models).

Proofstack [18], which was formally known as Copyrobo, claims to be the world's online notary and is the first blockchain startup that uses both qualified authorities and blockchain protocols in a single platform, to create legal global and local proofs via multiple platforms. Their website provides the user with the necessary steps to verify proof, which is called Proof.Link. The Proof.Link unique identifier allows securing, organizing, and distribution of proofs. The company offers different timestamping methods and file

options: proof options (blockchain, qualified authority), integration and device options (computer, mobile, Google Drive), backup (email, Google Drive, FTP), and maximum file size.

Bernstein [19] offers a web application in which users can create a digital track of their processes, by using the Bitcoin platform, as well as timestamping national authorities. For using the solution, the user should only upload the chosen document in the application and Bernstein will create a blockchain transaction that contains the cryptographic fingerprint of the documents that were uploaded based on IP, together with the document proof. The digital assets can be secured both with Bitcoin certificates, as well as digital timestamps from trusted timestamping authorities from the EU and China. The registration protocol is completely blockchain agnostic and aalthoughthe solution is implemented on the Bitcoin platform, it can be ported on any type of private or public blockchain.

Table 1. LLTP-DS-relatedblockchain solutions.

Name	Blockchain platform	Timestamp type	Type of solution	Type of service offered	Usage of certified authority	Resources
Guardtime KSI [16]	KSI Blockchain	Qualified Timestamp, eIDAS compliant	Private plan Public demo solution	KSI command-line tool Web app	Yes	GitHub and website
Enigio [17]	Bitcoin	eIDAS compliant	Private plan Public demo solution	Web app	Yes	Website
Proofstack [18]	Bitcoin, Ethereum, Litecoin, EOS, NEO, Stellar	Qualified Timestamp	Free trial Enterprise version	Web app Android iOS	Yes, multiple	Website
Bernstein [19]	Bitcoin, Agnostic Blockchain protocol	Qualified Timestamp	Free plan Subscriptions Payment on using	Web app	Yes, qualified national authority	Website

Similarly, in our research, we have also analyzed the non-qualified solutions. The majority of the solutions use the Bitcoin blockchain for timestamping (OriginStamp [20], NotBot [21], Blocksign [22], Bitcoin.com Notary [23], The Stampd [24], Stampery.com [25], Proof of Existence [26], ProveBit [27], Bitnotar [28]). Only Acronis Notary [29] and CTIE Solution – NotarChain [30] use the Ethereum blockchain. The solutions are either open-source (NotarChain, Proof of Existence, ProveBit, Bitnotar), or available online for usage (NotBot, Bitcoin.com Notary, The Stampd). For the solutions which are

not open-source, there are different subscription plans from which the user can choose. The documentation for the solutions is either on Github (Proof of Existence, ProveBit, Bitnotar) or the company website (The Stampd, Stampery.com, Bitcoin.com Notary, OriginStamp, Acronis Notary). The solutions provided are mainly web applications, but some are only Github resources (Proof of Existence, ProveBit, Bitnotar).

As a general remark, we note that there are more non-qualified than qualified LTP-DS-related blockchain solutions available and that the qualified ones seem to be more mature and used in practice by users. There are other systems for the long-term preservation of digitally signed documents that use blockchain technology, such as the ones that are proposed in [1, 31].

6 Discussion

Digital archives can store data either centralized or in a distributed manner. For centralized data storage, data recovery can be difficult at times, but if there are disturbances, there are chances of solving them. On the other hand, in a distributed system, the archive is spread among different geographical locations, and any disturbance in one location, will not affect the other locations.

6.1 LTP-DS Properties that Apply in Blockchain Technology

According to [32], to be able to deliver trustworthy records, blockchain-based systems aiming at long-term preservation should satisfy some properties: the records should be accurate, reliable, and authentic. Accuracy concerns the truth-value of the record's content. To be able to achieve reliability, records should have three characteristics: completeness at the point of creation, consistency with formal rules of creation, and impartiality [32]. Last, but not least, a record is considered authentic, if its origin is genuine if it is authorized, or entitled to acceptance. The digital signatures could serve as a test for authenticity because it does not only identify the creator but also provides a connection between the record and the creator. Moreover, to establish the authenticity of the record, the record should satisfy the identity and integrity properties.

Concerning the accuracy and reliability properties, it is possible that unauthorized, erroneous, or faulty information that has entered into the transactional operational system, to be recorded on the blockchain. For information that is recorded automatically using smart contract code, reliability relies on the developed code of the smart contract creators. Due to interoperability uncertainty between various components of a decentralized system, there is a higher possibility that the above-mentioned properties would be rather negatively influenced, than positively [32]. Accuracy in block-chain can also be affected by the inconsistencies between nodes, or from the different components of the decentralized system. Moreover, network timestamp is important to be accurate, and possible network time attacks should be mitigated. Another inconsistency in the transactional record flow could result from deficient communication among the various system components. Once inaccuracies are introduced in the blockchain system, there should be means of alleviating them. For authenticity purposes, mechanisms to connect the blockchain hashed records with their context should be implemented with care (e.g.,

link records with unique IDs, use a meta-document with multiple document hashes, use of transaction metadata, use ontologies, etc.).

Thus, when adopting blockchain technology for long-term preservation (and in our case, for notarization), one should be aware of the possible problems that could arise from the previously mentioned properties, i.e., accuracy, reliability, authenticity, integrity Furthermore, it is important to state other notarization problems to be considered, namely persistence, uniqueness, undemocratic operation, anonymity, use of resources, and legal certainty [33].

When using blockchain technology for the long-term preservation of digital signatures/seals, one should carefully balance the pros and cons of using such technology. On one hand, some consider that blockchain technology should not be considered as a panacea for all records management problems [33]. On the other, there are advantages of using blockchain timestamping over TSA timestamping [34]: long-term preservation could be achieved without the costs of maintaining TSA-issued certificates and signature verification of the document signature and the public key is more convenient because the digital signature is not guarded on a central server.

6.2 Designing a Blockchain-Based LTP-DS System

Regulated implementations assure users that their data is acted upon and secured according to strict procedures validated by entities that conform to open and legally defined specifications. Such specifications and procedures currently apply only to PKI implementations of an LTP-DS system. Qualified LTP-DS (QLTP-DS) systems require that components such as signing services, signature validation services, and timestamping services should also be qualified. One place where these services can be integrated into a blockchain implementation is the consensus algorithm. Mining nodes can interface with qualified services for constructing preservation data, such as signing the preservation data object that contains validity reports of user signatures and timestamps attesting that the data existed at a certain point in time.

Irrespective of the nature of the LTP-DS system in question, whether qualified or not, blockchain technology must demonstrate irrefutable advantages over the actual PKI implementation. A key aspect such as the identity of the signatory, which must be vouched for by an entity trusted by the clients that consume preservation evidence seems to take away from the decentralized characteristic of blockchain.

Consensus algorithms can be classified based on the reward mechanism that participating nodes receive, resulting in two classes of consensus, incentivized and non-incentivized. Incentivized consensus algorithms are exclusively used in public blockchain systems to motivate participating nodes to behave accordingly. In the absence of a reward mechanism, the nodes participating in a non-incentivized consensus algorithm are considered trusted and only authorized nodes can help in the block creation process. In [35], the authors define four major groups of properties for consensus algorithms: structural, block & reward, security, and performance. Based on these classifications, properties, and the architecture required to implement an LTP-DS system, non-incentivized consensus algorithms seem to be the most appropriate to be used in LTP-DS systems.

Given the architecture components required by an LTP-DS system (Signing Application, Signature Validation Application, and Time-Stamping Authorities), we consider

analyzing the possibility of using the YAC consensus algorithm which is provided by the Hyperledger IROHA [36] open-source blockchain framework because of the mapping of the aforementioned components to the authorized nodes (client, ordering service, peer). An important part that must be considered if the chosen block-chain implementation must store the preservation evidence records inside the block structure, is that said framework must allow custom block structure.

Given that an LTP-DS system should mitigate cryptographic obsolescence, we note that the hash algorithms used for linking blocks that constitute the blockchain should be updated during the preservation duration. If hash values for obsolete algorithms can be reproduced from any input, it remains an open question whether linking the newest block to the chain that used such algorithms with a secure one can maintain the immutability of the previous records.

Maintaining validity status by storing data preservation objects which contain PKI validation responses implies additional storage logic to be implemented by the QLTP-DS system, or the client in case the QLTP-DS system does not support storage. This aspect can be mitigated by implementing the LTP-DS procedure using Self-Sovereign Identity (SSI) if the LTP-DS system can be registered as a service provider using an SSI ecosystem. This is because an SSI architecture can remove the need for storing validation material due to the way user identity claims are stored on a blockchain. If the claims become cryptographically compromised, they will be updated by the SSI provider. The storage transaction containing the data to be preserved can be append-ed on the SSI blockchain, effectively linking the data to the user identity (Fig. 1).

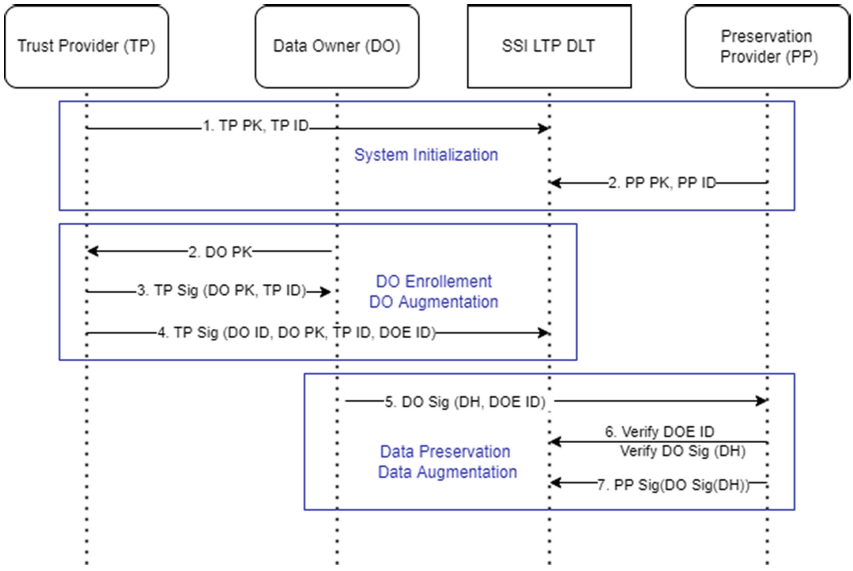

Fig. 1. SSI LTP DLT.

In the context of the proposed permissioned blockchain SSI scheme for long-term preservation which removes the need for augmentation data of the X.509 certificate

that contains the public key linked to the key that was used to compute the digital signature, the entity that requires evidence of data ownership may obtain and validate it by querying the distributed ledger for preservation transactions that are executed by long-term preservation service providers that implement cryptographic augmentation logic and requests the owner pprovidea hash of data computed using algorithms accepted as secure.

To obtain verifiable credentials that prove his identity stored on a personal digital wallet, the data owner must first register with an SSI trust provider. After registration, the trusted provider logs the generated SSI credential on the permissioned blockchain using an identifier, the verifiable credential is then sent to the user which stores it in his digital wallet. The process of enrolment between the SSI trusted provider and the user may require the user to generate an RSA, or elliptic curve key pair protected by his digital wallet, sharing the public key through authenticated and secure channels, allowing the trust provider to link it to his identity.

Another aspect of the blockchain SSI implementation requires the trust and service providers to register the cryptographic material (RSA public key, or elliptic curve public key) proving their identity in the genesis blocks. If the cryptographic material becomes obsolete due to new computation techniques or attack vectors, they can update their identities with the SSI blockchain consortium administrators.

Revocation information is one of the most important augmentation data that the qualified preservation implementation used to prove link-ability between cryptographic material and user identity, the new SSI blockchain implementation will allow the trust and preservation providers to invalidate verifiable credentials that prove identity and data ownership in the augmentation process by appending revocation transactions to the SSI blockchain. The data ownership augmentation process requires the preservation provider to notify the user in case of cryptographic material obsolescence, or periodic update of cryptographic algorithms used to compute data hash. In case of augmenting identity cryptographic material, the trust providers can periodically, or in case of urgency (attack vectors, or computational advances) append revocation transactions on the SSI blockchain.

7 Conclusion

In conclusion, this paper aims at presenting state-of-the-art LTP-DS-related blockchain solutions, focusing on the qualified ones. We give directions on how LTP-DS (qualified) blockchain solutions could be implemented, like integration of qualified services into the blockchain consensus algorithm, possibility of using a self-sovereign identity ecosystem. As future work, we plan to continue this research and build such an architecture.

Acknowledgments. This research was financed by European Regional Development Fund, Competitiveness Operational Program 2014–2020 under the project LTPS (code SMIS 2014+: 123423).

References

1. Otto, F., Wich, T., Hühnlein, T., Prechtl, M., Hühnlein, D.: Towards a standardised preservation service for qualified electronic signatures and qualified electronic seals, Open Identity Summit 2019 (2019)
2. Bralić, V., Stančić, H., Stengård, M.: A blockchain approach to digital archiving: digital signature certification chain preservation, Records Management Journal (2020)
3. Hyla, T., Pejaś, J.: Long-term verification of signatures based on a blockchain. Comput. Electr. Eng. **81**, 106523 (2020)
4. Thompson, S.: The preservation of digital signatures on the blockchain, the University of British Columbia iSchool Student J. **3** (2017)
5. ETSI TS 119 511: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques (2018)
6. ETSI TS 119 512: Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services (2018)
7. eIDAS TSP map, Accessed 3 June 2021
8. ISO 14641: Electronic document management - Design and operation of an information system for the preservation of electronic documents – Specifications (2018)
9. ISO 14721: Space data and information transfer systems - Open archival information system (OAIS) - Reference model (2012)
10. OCLC/RLG Working Group: Preservation metadata and the OAIS Information Model: A metadata framework to support the preservation of digital objects, http://www.oclc.org/content/dam/research/activities/pmwg/pm_framework.pdf Accessed 3 June 2021
11. ISO 16363: Space data and information transfer systems - Audit and certification of trustworthy digital repositories (2012)
12. BSI TR-ESOR-03125: Preservation of Evidence of Cryptographically Signed Documents (2019)
13. Pedro, F.: Understanding Bitcoin: Cryptography, Engineering and ECOnomics. John Wiley & Sons Ltd, Chichester (2015)
14. RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). https://doi.org/10.17487/RFC3161. Accessed 3 June 2021
15. ANSI X9.95-2012: Trusted Time Stamp Management and Security, https://www.sec.gov/rules/proposed/s72703/iac120105.pdf Accessed 3 June 2021
16. Guardtime: KSI Blockchain Timestamping, https://guardtime.com/timestamping Accessed 3 June 2021
17. Enigio, time:beat Proving Data Integrity, https://www.enigio.com/timebeat Accessed 3 June 2021
18. Proofstack, Legal Proof, https://proofstack.io Accessed 3 June 2021
19. Bernstein Technologies GmbH: Own what you make, https://www.bernstein.io Accessed 3 June 2021
20. OriginStamp AG: https://originstamp.com Accessed 3 June 2021
21. e-Genèse France, NotBot, https://notbot.me Accessed 3 June 2021
22. Blocksign, https://blocksign.com Accessed 3 June 2021
23. Saint Bitts LLC Bitcoin.com, https://notary.bitcoin.com Accessed 3 June 2021
24. Stampd, https://stampd.io Accessed 3 June 2021
25. Stampery, https://stampery.com Accessed 3 June 2021
26. Proof of Existence, https://proofofexistence.com Accessed 3 June 2021
27. ProveBit Github Contributors, ProveBit, https://github.com/thereal1024/ProveBit Accessed 3 June 2021

28. Bitnotar, https://github.com/bitcoinaustria/bitnotar Accessed 3 June 2021
29. Acronis International GmbH, Acronis Technology Notary, https://www.acronis.com/en-us/technology/blockchain-notary Accessed 3 June 2021
30. Pinto, A., Silva, J.: Revisiting Blockhain use in notary services: an european perspective. In: Prieto, J., Pinto, A., Das, A.K., Ferretti, S. (eds.) BLOCKCHAIN 2020. AISC, vol. 1238, pp. 101–110. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-52535-4_11
31. Collomosse, J., et al.: Archangel: trusted archives of digital public documents. arXiv preprint arXiv:1804.08342 (2018)
32. Lemieux, V.L.: Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems An Archival Theoretic Evaluation Framework (2018)
33. Van Garderen, P.: Decentralized Autonomous Collections, Medium On Archivy, https://medium.com/on-archivy/decentralized-autonomous-collections-ff256267cbd6 Accessed 26 Apr 2021
34. Amati, F.: Using the blockchain as a digital signature scheme, Medium Signatura, https://blog.signatura.co/using-the-blockchain-as-a-digital-signature-scheme-f584278ae826 Accessed 26 Apr 2021
35. Sadek V., Mohammad J.M.C., Mohammed A.H., Alan W.C.: Blockchain Consensus Algorithms: A Survey, ResearchGate (2020)
36. The Linux Foundation: Hyperledger IROHA, https://www.hyperledger.org/use/iroha, Accessed 3 June 2021