Qualified Ledgers – Breakthrough for proven security and legal trust in DLT through eIDAS2 Regulation?

Ignacio Alamillo [1], Steffen Schwalm[2] , Carsten Stoecker[3] , Ricky Thiermann[4]

Abstract: eIDAS 2.0 as a legal and technical framework for trustworthy, decentralized identities in conjunction with the EU digital wallet and various trust services could lead to a rise in distributed ledger technologies (DLT) and European Blockchain Services and Infrastructure (EBSI). A variety of possible uses of distributed ledger technologies in conjunction with the EU digital wallet under the regulatory requirements of eIDAS 2.0 are conceivable and could also lead to broader use of EBSI with the qualified trust service for electronic ledgers.

Keywords: eIDAS2, EU Digital Wallet, Architecture Reference Framework, DLT, EBSI, Electronic Ledger

1 Introduction and status of DLT in Europe

Until 2019 the Distributed-Ledger-Technology (DLT) and its most famous representative blockchain generated a real hype particularly the well-known use case Bitcoin [Ko21]. After the bitcoin crash and especially the security concerns of German National Cybersecurity Authority [TO19] as well as the issues around the German ID Wallet [ID21] first doubts about the real capacity, security and trust 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] [AS22]. Within framework of the European Blockchain Partnership (EBP), the European Commission established a European DLT-infrastructure provided by the Member States [EBSI]. This means that the DLT nodes are under the responsibility of the Member States and so ensure a government trust anchor. Since [EBSI] contains its own governance and technical specifications together with conformance tests for wallets it could solve the trustworthiness issues in DLT but, as it lacks security standards and independent audit processes, the growth of [EBSI] was limited. Beside [EBSI] also other national or private DLT networks have appeared e.g. [Alastria] in Spain, [ID Union] in Germany, [Findynet] in Finland or [Comercio] in Italy. In most cases DLT was used as a form of decentralized PKI for the execution of the new SSI paradigm [AS22] based in wallets as well as in the issuance and verification of verifiable credentials, such as digital

[1] Universidad de Murcia. Facultad de Derecho, Campus La Merced. 30001 Murcia.
[2] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany
[3] Spherity GmbH, Emil-Figge-Straße 80, 44227 Dortmund, Germany
[4] Spherity GmbH, Emil-Figge-Straße 80, 44227 Dortmund, Germany

doi:10.18420/OID2024_19

diploma, mobile driver license or power of attorney. Other use cases such as cryptocurrencies, supply chain or notarization can be mentioned.
To use DLT for trustworthy digital transactions, it is necessary to make transactions and their records evident against third parties, to fulfil burden of proof and documentation needs [AS22] [Ko20]. Due to the lack of appropriate measures to fulfil such requirements of state-of-the-art record management it was not possible to use DLT for trustworthy digital transactions in general and decentralized identities in particular as needed in regulated environments [Ko20], [AS22]. Those shortages and the lack of proven security of DLT networks and their providers lead to the de facto ban of DLT for regulated industries in some EU member states like e.g. Germany [AC24], [TO19], [EC21].

The [eIDAS2] establishes, as an amendment of [eIDAS1], a legal and technical framework for trustworthy decentralized identities with the EU Digital Wallet (EUDIW) and related (qualified) trust services, using or not DLTs, on one hand but with a new dedicated QTSP for Electronic Ledger on the other hand. Although the term Electronic Ledger in [eIDAS2] does not necessarily mean only DLT – even less, blockchain – this regulation seems like a step forward to close the gaps and to enable DLT to be used in regulated environments with typically comprehensive requirements on proven security and legal trust [AS22], [Ko20]. But what's the role of DLT within [eIDAS2]? How to differentiate the different possibilities in using DLT for EUDIW and QTSP but especially the new QTSP for Electronic Ledger? As [EBSI] already exists the question on its integration in [eIDAS2] occurs too.

The paper describes based on introduction on electronic ledger in general and DLT in particular (Section 2), the main changes of [eIDAS2] and the role of DLT in the new ecosystem, especially the new QTSP for Ledger. This description will lead to the role of [EBSI] as a European DLT network within the [eIDAS2] and its transformation according to the trust model of the regulation (Section 3). The paper closes (Section 4) with considerations on the future of DLT in high-regulated industries based on [eIDAS2], including possible use cases and an outlook on necessary standardization and research in the development of the [eIDAS2] ecosystem.

2 Distributed Ledger Technology

Basically, DLT is a decentralized distributed peer-to-peer network of technical nodes for data exchange and transaction execution. According to [IS20] a distributed ledger is in this case shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism, which ensures that all transactions are valid and unaltered. Once written to the ledger the transactions are immutable, mainly based on hash protection of data stored on the chain. Any transaction can reliably be tracked on the chain. In case the DLT is organized in blocks it's called blockchain, so basically a blockchain is a special kind of DLT [AS22], [Ko21]. Blockchain is not a simple

algorithm, but a technological construct and enabling protocol that facilitates the decentralized intermediation of data between participants [HKH20]. 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.

If DLT is to be used for trustworthy digital transactions, it is mandatory to fulfil requirements on records management including long-term preservation of the evidence of authoritative records 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 ensuring integrity, authenticity, reliability, confidentiality, and transferability of so authoritative records by trusted 3rd parties incl. evidence preservation for the whole retention period. Additionally proven security of a DLT network done by independent 3rd party based on international standards is an additional core requirement to use DLT in regulated environments with the need to fulfil burden of proof. Without additional measures like given in [DI21] DLT is currently not able to fulfil those as comprehensively described in [Ko20], [Ko21], [AS22] [IS23].

3 A QTSP for Electronic Ledger. The EBSI portfolio challenge

Section 11 [eIDAS2] introduces (qualified) trust services for Electronic Ledger (Art. 45k and following). [eIDAS2] mandates that qualified ledger "are created and managed by one or more qualified trust service provider or providers, establish the origin of data records in the ledger, ensure the unique sequential chronological ordering of data records in the ledger and record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time". Although [eIDAS2] is technology neutral the description in Art. 45l is in line with the definition of DLT in international standards [IS20] and contains core properties of DLT. As [eIDAS2] contains the requirement of mandatory implementing acts referring to European standards it ensures coherent technical framework for DLT. Since the requirements on QTSP also apply for QTSP for Ledger these standards will also be the basement for certification by independent conformity assessment body and so ensure proven security and trust in DLT. It must be stated that Section 11 focus on all use cases not covered by the European digital identity wallet (EUDIW) nor any other (qualified) trust services so e.g. (qualified) signatures, seals, timestamps, attestations electronic delivery etc. This means that DLT can be used as infrastructure for any EUDIW as well as any other QTSP too, as the security will be proven within the conformity assessment of the CAB, but there's no need to use QTSP for Ledger as precondition to provide another (qualified) trust service nor an EUDIW [Sc24] [eIDAS2]. This differentiation is important as it leads to the core use cases for QTSP for Electronic Ledger as e.g. tokenization or digital assets, cryptocurrencies or traceability in supply chains and digital product pass. [Al24] shows the possible use case scenarios for electronic ledger (DLT) within [eIDAS2]

ecosystem.

There's no trust by default in the European Union. Trust only occurs based on European law, supervised by European and national supervisory bodies, accreditation of conformity assessment bodies under European standards, certification of trust services by CAB under supervision of national supervisory bodies and verifiable via European wide trusted lists [AS22], [Sc23]. As DLT can be used as infrastructure for all QTSP but also EUDIW and especially the new QTSP for Electronic Ledger the role of [EBSI] as European Blockchain Service Infrastructure needs to be analysed further.

The European Blockchain Services and Infrastructure ([EBSI]) is a project initiated by the European Commission and a group of 29 European countries. The project, which was set up in 2018, aims to lay the foundation for future EU public services. The [EBSI] project is currently run by nodes operated by member states. Each country is expected to operate at least one node of [EBSI] at full scale. This approach aligns with the decentralized nature of blockchain technology and is suitable for multi-party cooperation. [EBSI] on one and it ensures a governmental trust anchor and so clear responsibility on the other hand this approach leads to the question on how such a network might be provided (QTSP for Electronic Ledger) or use (by EUDI Wallet Issuer or QTSP using DLT) by a certain provider. With the introduction of [eIDAS2] and the concept of qualified electronic ledgers, the [EBSI] could potentially not only evolve from an 'electronic ledger' into a 'qualified electronic ledger' enhancing security and reliability of the network, and providing legal certainty for use cases that build on the EDIC's electronic ledger. [EBSI] could also act as decentralized, pan-European Infrastructure for other (qualified) trust services such as issuance of (qualified) certificates, eDelivery (as e.g. planned in [TRACE4EU] project) or Archiving as well as the EUDI Wallets but also for infrastructure components like a trust issuer registry as possibly more scalable replacement of the trust list [ET21].

Much more complex in case of DLT is the portfolio of a QTSP for Electronic Ledger. This applies especially on [EBSI] where the main nodes remain in responsibility of member states and so the possible QTSP must deal with already existing authorities taking one main task in the DLT network – running the main nodes – per default. As it's currently not planned to change this governmental trust anchor in the EDIC it limits the portfolio of the future QTSP for Electronic Ledger in case of [EBSI]. One possibility could be that the QTSP provides only the validating nodes and so controls the execution of transactions in the network, similar approach would be the provision of the consensus mechanism and/or the responsibility for the whole security and trust in the network. As [EBSI] is designed as pan-European network it's also thinkable that 1-n QTSP may provide certain parts like validating nodes or sub-nodes or e.g. the implementation and operation of special applications like smart contracts.

4 Considerations for the future of DLT in eIDAS ecosystem

[eIDAS2] defines the legal and through mandatory implementing acts for de facto all components also the technical framework for trustworthy decentralized ecosystem in Europe. As the regulation is technology neutral it also allows the utilization of DLT for each component from EUDI Wallet and all QTSP. With the QTSP for Electronic Ledger [eIDAS2] establishes a dedicated (qualified) trust service for DLT. Due to the integration of DLT in the eIDAS trust framework all requirements on EUDI Wallet and QTSP like liability (EUDIW = member state), conformity assessment by independent CAB apply which ensures the proven security, legal trust and so solves the main gaps mentioned in Section 1 which limited a broad utilization of DLT in Europe. QTSP for ledger can be a game-changer for Industry 4.0, particularly in sectors such as energy, supply chain, and manufacturing. For instance, qualified DLT can be used for secure authentication, authorisation, service discovery, and data sharing in the energy system. It can support use cases such as flexibility aggregation, load shifting, EV charging forecasting and settlement, Guarantee of Origin, smart dispatch, smart city, and customer switching processes. In the manufacturing sector, qualified DLT can also play a significant role. Industrial use cases such as Third-Party Risk Management, smart manufacturing, digital product passports (DPPs), and supply chain optimisation can benefit from a qualified DLT infrastructure. In the industry section qualified electronic ledgers may enable execution of European Supply Chain Regulation for proof of origin of products but also product-/data and document traceability. Trusted Digital Product Passports can be enabled using qualified ledger. Document traceability might be also exciting for public sector and e-commerce for audit trails on any online service - a combination with eDelivery could also ensure evident confirmation of receipt in decentralized ecosystems. Public sector applications will benefit as well from the QTSP for Ledger service [SA21] [RCG19].

In summary [eIDAS2] creates the basement for possible breakthrough of DLT to be used in high-regulated industries while ensuring burden of proof and documentation requirements as the main requirements must be fulfilled by QTSP for Ledger or Providers of EUDIW resp. QTSP using Ledger. [EBSI] can act as common European infrastructure as its governmental trust anchor ensures an additional advantage in comparison to complete private networks. As regarding regulation, the implementing acts have to be published not later than May 20th, 2025, the research shall focus on definition of concrete security and technical requirements for certification of EUDIW/QTSP using DLT as well as QTSP for Ledger. Especially the portfolio definition of QTSP for Ledger and in this context the adjustment of [EBSI] regarding [eIDAS2] seem to be most important issues to be solved.

Bibliography

[AS22] Alamillo, Dr. I., Schwalm, S.: Self-Sovereign-Identity & eIDAS: a Contradiction?

Challenges and Chances of [eIDAS2]. European Review of Digital Administration & Law - Erdal2021, Volume 2, Issue 2, pp. 89-108

[Al24] Alamillo, Dr. I., Schwalm S., Stoecker, C., Thiermann, R.: Qualified Ledgers: Bridging the Gap between Blockchain Technology and Legal Compliance. 2024.

[AC24] eIDAS 2.0 Architecture Concept – Public, https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept-v1, accessed: 30/01/2024

[To19] Federal Office for Information Security (BSI): Towards Secure Blockchains. Concepts, Requirements, Assessments. 2019

[Ec21] Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT). Bundesamt für Sicherheit in der Informationstechnik. Bonn 2021

[DI21] DIN TS 31648:2021. Criteria for trusted transaction. Records Management and Evidence Preservation in Distributed Ledger Technologies and Blockchain.

[ET21] ETSI TS 119 612 Electronic Signatures and Infrastructures (ESI); Trusted Lists.

[HKH20] Hellwig, D., Karlic, G., & Huchzermeier, A. Build Your Own Blockchain. Springer International Publishing. 2020

[ID24] ID Wallet des Bundeskanzleramts, ein Projekt der Bundesregierung: Datenschutzrechtliche Aspekte, https://fragdenstaat.de/anfrage/id-wallet-des-bundeskanzleramts-ein-projekt-der-bundesregierung-datenschutzrechtliche-aspekte/#nachricht-643462, accessed: 30/01/2024

[IS20] ISO 22739:2020: Blockchain and distributed ledger technologies - Terminology, 2020

[IS23] ISO DTR 24332. Information and documentation — Blockchain and DLT in relation to authoritative records, records systems, and records management

[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

[Ko21] Korte, U. et. Al.: Records Management and Long-Term Preservation of Evidence in DLT. In: Roßnagel, H., Schunck, C. H. & Mödersheim, S. (Hrsg.), Open Identity Summit 2021. Bonn: Gesellschaft für Informatik e.V.. (131-142)

[RCG19] Reddick, C. G., Cid, G. P., & Ganapati, S. Determinants of blockchain adoption in the public sector: An empirical examination. Information Polity, 24(4), 379–396.

[Sc23] Schwalm S.: Trusted transaction in Electronic Ledger?. Overview on international standardization in DLT. Seeblock Webinar DLT Standardization. 10.11.2023.

[SA21] Sobolewski, M., & Allessie, D. Blockchain Applications in the Public Sector: Investigating Seven Real-Life Blockchain Deployments and Their Benefits. In M. P. and S. H. J. Reddick Christopher G. and Rodríguez-Bolívar (Ed.), Blockchain and the Public Sector: Theories, Reforms, and Case Studies (pp. 97–126). Springer International Publishing.