MetaverseUA Chair

Academic Chair for the Responsible Development of the Metaverse

Decentralised Digital Identity in the Metaverse under eIDAS 2.0

MetaverseUA Chair Research Paper #4

Steffen Schwalm

André Kudra

catedrametaverso.ua.es

Universitat d'Alacant
Universidad de Alicante

The Chair for the Responsible Development of the Metaverse (MetaverseUA Chair) was created by the University of Alicante (Spain) and financed by Meta Platforms under its XR Program and Research Funds. The Program aims at supporting academic and independent research across Europe into metaverse issues and opportunities. The MetaverseUA Chair is a member of the European Metaverse Research Network. Like all our work, this report has been produced completely independently. The ideas expressed in this paper are the sole responsibility of the author.

How to cite this paper:

Schwalm, S., Kudra, A., 'Decentralised Digital Identity in the Metaverse under eIDAS 2.0', *MetaverseUA Research Paper #4*, https://metaversechair.ua.es/working-papers/

Steffen Schwalm is Senior Manager Digital Identity & Trust at MSG.

Andre Kudra is a strong advocate of Self-Sovereign Identity (SSI) and a Sovrin Board of Trustees member.

Abstract

This article discusses how digital identities and trust services can enable legally compliant transactions within the Metaverse. It focuses on the EU's eIDAS 2.0 regulation, which provides a framework for trustworthy decentralised digital identities. This regulation includes the EU Digital Wallet (EUDIW) and qualified trust service providers (QTSP) for electronic ledgers, which can be based on blockchain technology (DLT). The article argues that eIDAS 2.0, together with the European Blockchain Service Infrastructure (EBSI), can provide the necessary trust anchors for trusted transactions in the Metaverse. It uses a hypothetical example of a "Virtual World Wonderland" to illustrate how eIDAS 2.0 can support Metaverse applications. The article concludes by emphasising the potential of eIDAS 2.0 and EBSI to enable trusted transactions in the Metaverse, but also highlights the need for further standardisation to ensure interoperability and trust.

Keywords: Metaverse, digital identities, trust services, eIDAS 2.0, EU Digital Wallet (EUDIW), European Blockchain Services Infrastructure (EBSI), distributed ledger technology (DLT), tokenization, priva

Table of Contents

1. Introduction

Digital identities are key for trustworthy digital transactions. Only if all actors in a process or ecosystem securely know with whom they act digital trust will be ensured. Unique identification of legal entities or natural persons as well as their objects is the basis for a digital identity that allows the verification of companies (Do they really exist?), of the person acting on behalf of that company (Do they really exist?) and of their authorization (Is Alice authorised to act on behalf of company A?).

This means that digital identities comprise several dimensions including:

- Natural entity: It's me
- Legal entity: It's my company
- Legal roles of a natural entity: It's my power of attorney
- Credentials or attestations of a natural person acting as natural person or on behalf of a legal entity: It's my diploma or my driver licence
- Attestations of a virtual identity related to a natural person or legal entity, or virtual attribute related to natural person or legal entity: It's my virtual me and/or the virtual car of my virtual me
- Attestations allowing a natural entity to access something: It's what I'm allowed to access
- Credentials for signing contracts or sealing documents: It's my signature or the seal of my company

Today, digital identities are typically issued by a centralised authority, at least in the EU. Despite the widely used but privacy exposed social identities, the main electronic identification means of natural entities are government eID issued by member states.

The new eIDAS2 regulation[1] establishes as an amendment of eIDAS 1 a legal and technical framework for trustworthy decentralised identities with the EU Digital Wallet (EUDIW) containing the government eID and related (qualified) trust services for issuance e.g. of digital credentials like diploma etc. (Attestations in terms of eIDAS), using or not using DLT, on one hand but with a new dedicated Qualified Trust Service Provider (QTSP) for Electronic Ledger on the other hand.

This implies the chance to build up a legally compliant decentralised ecosystem using technical approaches known from the new paradigm of Self-Sovereign Identities (SSI). SSI promises identity owners full control over their identity and linked attributes. All identity information is stored decentralised in a *wallet* and only its *holder* can decide to whom he will transmit requested identity information – with the new EUDI Wallet this can be established in a legally compliant way. SSI was adopted and implemented for example within the European Blockchain Service Infrastructure EBSI – an infrastructure provided by Member States which implies self-sovereignty combined with governmental trust anchor. EBSI also emerged decentralised digital ecosystems appearing using DLT in a cross-industry and cross-country fashion. The technology gains its biggest added value in transactions between three or more parties which do not trust each other but trust a distributed network which is immutable by design[2] instead.

With eIDAS 2.0 the SSI paradigm becomes the common logical ground of legally compliant digital identities in Europe – with a compromise between gaining legal trust through EUDI Wallet from Member State and credentials from qualified trust services – so trustworthy 3rd

[1] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework [2024], OJ L, 2024/1183, 30.4.2024.
[2] Ulrike Korte and others, 'Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation' (Open Identity Summit 2020, Lecture Notes in Informatics (LNI), 2020), 49, 60.

parties and full control of user for its data[3].

Beside the developments in digital identities with the *Metaverse* another dimension came up. The commingling of actual and virtual reality leads to combining natural persons and legal entities on one hand but also virtual natural persons (e.g. my avatar) and legal entities (e.g. my company) in virtual reality on the other hand. Combined with real and virtual machines and sensors as well as attestation of attributes for those real and virtual entities, complex new business models can be conceived, from augmented and virtual reality to digital twins or tokenization of real and virtual assets. Technically, in many cases DLT is used as infrastructure for transactions and self-created identities[4]. The integration of legally compliant digital identities, attributes and trust services may enable the Metaverse to be used for legally compliant transactions, too. This could transfer virtual realities, tokenization or digital twins from digital playground or grey zone into regulated and to wider usable ecosystems. Basis are trustworthy digital identities but allow not revealing the actual natural person or legal entity if not needed. This can be achieved by a combination of the possibilities of SSI and an enhancement of the scope of identities (not only identification of persons) and trust services (e.g. for DLT) of eIDAS, for achieving trust in Metaverse transactions.

Considering those developments, the question on how digital identities and trust services may enable the Metaverse for legally compliant transactions by fulfilling relevant requirements arises. Those e.g. are related regulatory requirements on a secure and unique identification of natural persons and legal entities and their natural/virtual attributes or manifestations, the need to fulfil the burden of proof against third parties and balancing privacy requirements in decentralised ecosystems.[5] The potentials of the Metaverse can only be lifted if legally compliant and traceable transactions based on trustworthy digital identities in all their dimensions are possible. This would require the integration of virtual reality of the Metaverse into the legal and technical reality defined by the eIDAS ecosystem in Europe in general. With Tokenization one of the application areas of the Metaverse is already in place and affected by further regulation like MiCAR[6]. In order to show the added value of eIDAS for Metaverse application the tokenization will be used as an example also against the background of existing research projects on the European Blockchain Service Infrastructure focusing on exactly this combination within tokenization.

Against the background of the eIDAS 2.0 proposal which defines e.g. dedicated requirements on an EU Digital Identity Wallet (EUDIW), qualified attestation services as approved issuers for the wallet and so trustworthy third parties or (qualified) trust service providers (abbreviated as TSP or QTSP, respectively) for electronic ledgers a question arises: Can this interaction of real and virtual persons, organisations, objects in actual reality and in the Metaverse be achieved using the tools, roles and responsibilities within the eIDAS ecosystem?

Based on an introduction on the Metaverse and its challenges the paper describes main content of the eIDAS 2.0 followed by an overview about requirements on trustworthy digital transactions with and without DLT. Going further, it shows the main issues and open subjects in using DLT in regulated environments with requirements on burden of proof and possible impact of qualification of ledgers through eIDAS 2.0 in general and EBSI in particular. With this fundament, the paper analyses the resulting consequences on digital identities and qualified electronic ledgers and identifies possible chances for trustworthy transactions in the Metaverse.

---

[3] Ignacio Alamillo and Sebastian Schwalm, 'Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0' (European Review of Digital Administration & Law – Erdal, 2021, Volume 2, Issue 2, pp. 89-100)

[4] Doug Antin, 'The Technology of the Metaverse, It's Not Just VR' (The Startup, 5 May 2020)

[5] Ulrike Korte and others (n 2), 49, 60.

[6] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023], OJ L 150, 9.6.2023, p. 40–205.

The paper concludes with an outlook on needed standardisation and further regulation to reach trustworthiness in Metaverse scenarios, i.e. enable trusted interactions between actual reality and virtual ones using the EBSI as European infrastructure and European Standards as common technical ground.

2. Metaverse

2.1 Fundamentals

The term *Metaverse* is currently in use for a variety of digital contexts and often appears like a mixed bag of futuristic technology approaches and artefacts. Many consider themselves stakeholders, contributors, and beneficiaries in the upcoming Metaversian world, obviously a great lot of those do not understand the term in its entirety or merely have a vague, incomplete, or even wrong understanding of what it is and means. Even though young as a phenomenon, the Metaverse has already taken its place in digital cultures and needs to be interpreted as such, considering all implications on business, legal, and tech.

The following sections add further context and detail by clarifying related, adjacent, overarching, or subsumed terminology and concepts, an understanding which is required to allow a more in-depth discussion of the identity-related aspects.

2.2 Metaverse in a Broader Digital Culture Context

Traditionally, culture takes place in the field of tension between human and society: the concept of culture encompasses value-based ways of expression and behaviour of people, also and especially in social interaction. Culture is variable over time (Zeitgeist) and differs, for example, ethnically, regionally, or according to worldview, so that the plural *culture* is not only permissible but required. An expanded understanding of culture became necessary with human progress; *technology* had to be included in the field of tension. *Digital culture* could only emerge when it manifested itself in the regular reality of life in the elaborately developed form of *computer technology*, i.e. *digital* technology, first for some, then for many, and finally almost ubiquitously. In the course of time, various digital cultures have emerged and established themselves along the technical development since the end of the 20th century. Consequently, an evolutionary differentiation and delimitation of digital cultures is possible. For example, the *internet culture* (or *cyber culture*) could only emerge with increasing technical networking, the internet. It is not identical with the culture of *online gamers*, which does need networking, but for the specific reason of playing computer games together (and flanking communication) over physical distances.

The concrete example of *hackers* makes it clear that terminology is often misunderstood, and digital cultures are inadequately understood. The general image of the hacker could be as follows: “A pale figure wearing a black hoodie, his hood pulled deep into his face, sits in an unlit basement room in front of several screens on which bright lines of code chase across dark backgrounds. How can one who vilely penetrates IT systems of righteous citizens and businesses have a culture?” Such an undifferentiated view and assessment is out of touch with reality and unjustified. In fact, “You're a hacker!” can be a nice compliment. Closer to the original definition and use of the term: a hacker is a person who is exceptionally well versed in a system (or several), who can operate, repair, improve, trick, or exploit it to its limits or even beyond. Who knows that the first hackers were model railway engineers? In fact, the birthplace of hacker culture is the

Tech Model Railroad Club (TMRC) at the Massachusetts Institute of Technology (MIT). A basic understanding of the development of this culture from its origins to its manifestation as *security hackers*, who as *white hats* willingly expose security vulnerabilities and as *black hats* in extreme cases come close to the initial interpretation, makes it possible to better grasp the digital realm overall. Those who want to delve deeper could look at how hackers operate and what cultural practices drive them, for good or ill.

The situation is similar for the other digital cultures. In the absence of this clarity in society at large, a *hyper-connected* world has already emerged that clouds the view of the actual influence of digital technology on people and society. Digital culture is carelessly dismissed as the daily use of technical devices or equated with spending many hours a day in front of screens, small or large. The term *digitisation* is used to explain it, often without any background knowledge or common understanding. The Metaverse further interweaves layers and thus increases the complexity, as the following discussion shows.

2.3 Genesis of the Metaverse

Historically the term *Metaverse* was coined by science fiction author Neal Stephenson in his renowned and awarded novel *Snow Crash*, published in 1992. In his story, the Metaverse resembles a massively multiplayer online game (MMOG) which is populated by both automated agents aka *system daemons* and user-controlled entities called *avatars*. With Snow Crash, Stephenson made avatar the de facto term for a graphical representation of a user or user character online. In his Metaverse, humans interact with each other and software agents via their avatars, in a 3D virtual space, which appears as an urban environment along a single 100-metre-wide road that runs around the entire 65,536 km (2^{16} km) black spherical planet. Virtual real estate can be bought from a property management company and virtual buildings can be put on it. The Metaverse is accessed via terminals – personal goggles with high-quality or public low-quality ones – connected to a global, monopolised telecommunications network which evolved from the phone system. This fiction has fuelled and inspired today's understanding and incarnations of the Metaverse.

Contemporarily, the general idea of the Metaverse is a digital realm in which physical and virtual reality are combined to an extended, more immersive experience in a 3D virtual world, or many of those in a networked, interoperable state. It is perceived as the next evolutionary iteration of the internet, making social and economic connections in the virtual world feel more like physical reality.

2.4 Technology of the Metaverse

Metaverse' technological core is represented by a combination of modern IT concepts, hardware/software products and cryptographic procedures, further outlined in the following:
Virtual reality (VR). The stereotypic notion of VR is a person wearing a helmet-like headset bearing speakers and internal displays in front of the subject's eyes and sensory gloves. This provides an immersive experience for the VR user, who can hear and view as well as interact with the virtual world, a simulated 3D environment with objects and characters/avatars. The term was first used for science fiction in the 1982 novel *The Judas Mandala* by author Damien Broderick and popularised by VR pioneer Jaron Lanier by the end of the same decade. The VR concept has sparked creativity of many authors and movie makers: From headset-less VR fictions like *Tron* (1982, *Tron: Legacy* 2010), *The Thirteenth Floor* (1999) and *The Matrix* (1999 plus later sequels) over

The Lawnmower Man (1992) and *Johnny Mnemonic* (1995) to *Ready Player One* (2018) which became the instant classic and blueprint of what a great VR experience looks like. VR was assumed to make a commercial mainstream breakthrough already in the 1990s, which failed due to required gear being too clunky and expensive while delivering underwhelming experiences. The major technological advancements of the last two decades have changed the picture significantly, now combining affordability and impressive UX. VR now includes the composition of virtual, digital worlds in which digital avatars under control of a real natural person or legal entity, digital objects representing a physical pendant, or complete digital assets exist.

Mixed reality. In mixed reality configurations, the natural perception of a user is blended or mixed with artificial, computer-generated perceivable components. There is a further two-fold differentiation possible in mixed reality. One is *augmented virtuality* as a modification of a VR setup, in which objects or signals from physical reality. Examples are real furniture or walls being visible in the virtual environment or real external sounds being captured and inserted into the virtual audio. More prominent and already much more common is the second variant, *augmented reality* (AR). AR means a user is provided with additional computer-generated information within the real-world environment that enhances his perception of reality. Simple examples are *head-up displays* (HUD) in cars showing vehicle speed and speed limits or smartphones extending a video feed from internal cameras with e.g. names of stars or surrounding mountains. More sophisticated implementations are relatively lightweight eyeglasses which serve as minimally intrusive AR displays.

Digital Twin. Digital twins are on one hand digital representations of physical objects, such as industrial equipment and machinery, vehicles, and buildings. A digital twin is a virtual model designed to accurately reflect a physical object. Hence it is a data set of a real-world object which allows digital representation, modelling, and analyses. Digital twins offer a wide range of possibilities in industrial settings that benefit companies by saving enormous resources. Practical applications are e.g. in supply chain management, prototyping, manufacturing, predictive maintenance, or construction. Building Information Modeling (BIM) is already common practice in the construction industry, digital twins are considered the next evolutionary step there. In virtual reality settings, a digital twin might also contain a digital object representing a natural or legal entity or even a full digital asset, typically manifested as a token.

Digital Asset, Token. In the economic sphere the Metaverse is to some degree intertwined with *Web3*. The latter is a concept of a more decentralised internet in which digital assets can be traded without central intermediaries. This is achieved by cryptographically exchanging *tokens* which either represent the value of such an asset or the asset itself. Digital assets often occur as *Non-Fungible Tokens (NFT)*, which are unique and not divisible, hence can only be transferred as an entire object, as opposed to *cryptocurrencies*, which can be obtained in fractions. NFTs usually represent or point to a digital artefact, like an image. This tokenization is attractive particularly in the Metaverse as virtual goods can be tagged, collected, and traded. Even though NFTs became popular in- and outside the Metaverse, besides a speculative hype they are subject to legal, economic, and ecological criticism. NFTs are mainly anchored in DLTs as decentralised infrastructure. Associated payments are often performed via cryptocurrencies. These require DLTs as transaction store and holder wallets for keeping tokens, executing transactions (i.e. payments) and/or storing identity attestations in form of verifiable credentials (mostly outside of current regulatory frameworks).

Metaverse experience possible today. But the Metaverse is far from being mainstream in 2023. The technological underpinnings have reached a quality level, though, which could invoke a broader interest. Early adopters are often from the gaming scene, as the required equipment is desirable and useful in their core realm as well. Certain VR/AR business applications could drive adoption and generate a pull effect in the personal domain.

2.5 Differentiation of Metaverse and Web3

Besides digital twins which are also used in industry scenarios, the term Metaverse today usually stands for a virtual (or mixed) reality where users interact with each other leveraging digital avatars as their virtual representation as well as digital objects and assets represented as tokens. Web3 on the other hand is used as a term for a completely decentralised internet where no centralised trusted third party or intermediary controls transactions, flow of information or access into the ecosystems. The infrastructure is fully decentralised using DLTs with their inherent properties like immutability and trust on consensus mechanisms as well as decentralised copies of transactions by each node. The absence of any centralised authority de facto lead in its pure – but not necessarily only – form to public permissionless DLT, the original idea of DLT[7]. In regulated environments, applicability of Web3 is limited, as legal trust requires trusted, liable institutions or like in Europe, a trusted third party which is accredited and certified. Web3 comprises the whole space of digital assets manifested in NFTs and payment via cryptocurrencies. Also unregulated decentralised digital identities relying on self-attestation are pertaining to Web3, often leveraging the W3C verifiable credential data model, formats (JSON-LD), and cryptographic signatures (incl. BBS+)[8]. This means Web3 delivers some basic functions and cryptographic procedures which are highly relevant for many Metaverse use cases, but it also goes far beyond the Metaverse scope.

2.6 Interoperability-related technical challenges

The technical challenges of the Metaverse are manifold, at least the domains of 1) humans engaging in a 3D virtual environment and 2) operating and connecting Metaverse platforms need to be differentiated. The prior, i.e. *humans in a virtual world*, occurs to be sorted. A standard track has been established between major industry players with *OpenXR*. It is an open-source, royalty-free standard for access to VR/AR platforms and devices, developed by a working group managed by the Khronos Group consortium.[9] OpenXR defines a standard programming interface which allows developers to build applications that work across a wide variety of devices. It is supported by multiple large-scale vendors and their products, e.g. *HoloLens 2* by Microsoft, *Quest* by Meta, *SteamVR* by Valve. Hence technical interoperability based on common standards for this domain is feasible. Other aspects which might be perceived as current limitations on this layer, like availability of practical use cases (besides gaming), usability, user experience and resource constraints for appropriate hardware as well as their price tags, are assumed to fade soon.

For the latter domain, i.e. *running Metaverse applications and environments* on top of the VR/AR hardware/software layer, the situation differs. Goal is to fulfil promises and implications of the term *Metaverse*, i.e. allowing seamless experiences in connected *Metaverses*. If one has proper AR/VR gear and desires to embark on the Metaverse journey, only proprietary, isolated experiences are possible today. Technical complexity for operating truly interoperable, completely distributed virtual worlds is immense. No common standards ensuring hassle-free cross-platform experiences have emerged today. At least bodies for creating standards have

[7] Bernard Marr, 'The Important Difference Between Web3 and The Metaverse' (Forbes Magazine, 22 February 2022) <https://www.forbes.com/sites/bernardmarr/2022/02/22/the-important-difference-between-web3-and-the-Metaverse/?sh=3d02677e5af3 >

[8] Note that those technologies build the identity framework in EBSI, too. See https://hub.ebsi.eu/vc-framework.

[9] https://www.khronos.org/openxr/

been established, e.g. the *Metaverse Standards Forum* bootstrapped by Khronos, *JTC 1 Standards and Standardization for the Metaverse* by ISO/IEC and IEEE's *Metaverse Standards Committee*. Collaboration and alignment have yet to be proven. Standardisation is not only basic technical interoperability but covers many more relevant domains, e.g., avatars, privacy, geospatial, networking, visual positioning, UX. These and more aspects must be clarified to achieve Metaverse interoperability, in a practical, approachable style with a maximum of user convenience.

eIDAS 2.0 is not able to address most of the diverse technical requirements of Metaverse. But eIDAS 2.0 provides a digital identity framework with a highly reliable technical fundament which can be applied to the Metaverse, and which is easily compatible with it. eIDAS encompasses decentralised architectures, it is meant to facilitate and build trust bridges between ecosystems, physical or digital ones. This will not only be useful in Metaverse scenarios but in many cases mandatory to create trust. eIDAS can provide the necessary trust anchors which reach across Metaverses and back into the real world.

In this context Digital Asset token can be seen as one of the use cases with increasing adoption as affected by current European regulation like MiCAR but also directly intertwined with digital identities for citizens and companies so possible owner of properties represented by a NFT. This relationship to digital identities on one hand and the technical use of DLT for Metaverse Digital Asset Token represent a dedicated use case for the European Blockchain Service Infrastructure EBSI too as it`s piloted within the TRACE4EU project co-funded by European Commission[10]. One idea of TRACE4EU is to implement Digital Asset Token for ownership of intellectual property using e.g. EUDI Wallet for the owner itself and show the ownership via Qualified Attestations of Attributes using EBSI. The property itself is represented by a Non-Fungible Token which contains the DID of the owner so that identity and transaction can be combined on the EBSI.

With the combination of digital identities and Digital Asset Token within the eIDAS Regulation using EUDIW and qualified trust services so attestations of attributes and ledger e.g. EBSI, eIDAS 2.0 can achieve trustworthiness of digital transaction within the Metaverse using NFT.

2.7 Identity-specific trust challenges in the Metaverse

When engaging with the Metaverse, users have a variety of trust challenges to overcome, many of which are related to their relationship with other Metaverse actors, stakeholders, and operators. Critical trust challenges are:

Privacy intrusions. This is a critical area as collecting users' personal information through interactions and possibly biometric data will likely be a standard procedure of platform operators. The amount and depth of data generated in Metaverses will quickly surpass anything possible in online interactions so far. Users will leave a rich data trail which allows behavioural analytics and prediction, potentially turning these deep insights against them. This can easily lead to surveillance capitalism at an intensely heightened level. Targeted advertising to influence purchasing decisions might be one of the lesser concerns. Hence mechanisms for protecting personal privacy and ensuring data sovereignty must be built-in from the start.

Crime. Fraud, theft, and all kinds of harassment and abuse are already significant challenges in online interactions. This is already happening in existing gaming and virtual reality social platforms, and most likely be similar in the Metaverse. Pseudonymity and near anonymity

[10] https://trace4eu.eu/

allow for unpunished misconduct or even criminal action. Attribution is very difficult and accountability hard to enforce. Some online platforms, like the business network *LinkedIn*, are now offering identity verification of account holders to increase trust. This is a model that can and should be applied to the Metaverse as well.

Social exploitation. User addiction and problematic social media use is another concern. The Metaverse could be a more immersive escape from reality than existing internet offerings. In the Metaverse, the negative social impacts of online echo chambers could easily be multiplied, or common social media engagement strategies could be abused to manipulate users with biassed content. Targeted content, stories and narratives presented in the Metaverse are making influence exertion possible for those who control it. So beyond maximised surveillance capitalism, influential misinformation leading to poor decisions for users will be a bigger threat. Ultimately, these possibilities can be turned against personal freedom and democratic structures. Reliable and trustworthy sources of information must be easy to identify in all Metaverse scenarios.

As a future perspective, a digital trust ecosystem as envisioned and regulatorily backed by eIDAS 2.0 can address identity-related aspects of the Metaverse. eIDAS is not limited to digital identity and attributes of natural persons, legal entities and potentially even devices/things are also considered. An abstraction from the physical/"real" world to the Metaverse can be imagined and projected. Associating digital identity and attributes with logical/virtual artefacts like avatars or 2D/3D objects is possible, in fact easier to achieve than a strong binding of a digital identity to a natural person.

2.8 Legal challenges for utilisation in regulated environments

To make interactions in the Metaverse legally binding and not jut an inconsequential game, various challenges need to be solved. Critical legal challenges are:

Intellectual property (IP) rights. The Metaverse often implies de facto or perceived violations of IP rights, which led to calls for new or adjusted regulations to protect users and rights holders. A key demand is that IP laws are extended to both physical and virtual objects and artefacts, ensuring that rights of inventors, designers, trademarks owners, etc. are comprehensively protected, just as they are in the real world.

Relevant jurisdiction. In virtual environments like the Metaverse, it can often be debated which jurisdiction applies. The controversy usually circles around the physical storage and data processing location of the digital avatars, objects, and artefacts vs the nationality, location, or citizenship of the users or legal entities.

Distributed architectures. The Metaverse often employs technologies from Web3 such as DLTs, digital assets, and tokens. Those need to be adopted in a trustworthy manner, i.e. facilitate, and enable a trustworthy Metaverse, and allow use cases comparable to the real world. This means all challenges in the SSI paradigm and DLT application apply on Metaverse applications, too.

Entity identification. The distinct and trustworthy identification of each natural person or legal entity acting within the Metaverse is crucial, be it via digital twin, avatar, or their associated digital artefacts. Currently only proprietary, often self-issued identities are used in Metaverse environments. These identities lack legal trust as involvement of a trusted third party for identity verification or leveraging eID schemes and eID means according to e.g. eIDAS is missing. This identification must comprise the identification of the natural person and legal entity but also include their digital pendants, objects, and assets, i.e. all possible digital identity dimensions defined above.

Regulated trust anchors. Non-repudiation of transactions must be ensured with the utilisation of (qualified) trust services, e.g. these must be also applicable to avatars of natural persons and digital twins of legal entities. Keeping the mandated security measures intact is key, e.g. secure authentication for signature creation according to ETSI EN 319 411[11] for QTSPs. Currently platforms and infrastructures for Metaverse applications are often provided by non-European market-leading providers. This often leads to GDPR issues because of foreseeable data transfer into third countries. Those platforms, tools, and infrastructure often do not fulfil typical measures on privacy protection such as privacy by design or proven security by trusted third parties. However, this is needed to achieve legal trust in the EU, e.g. established with the eIDAS trust framework.

eIDAS might be able to address the identity and trust anchor related challenges. Under the known limitations of eIDAS 1.0, those challenges are not solvable. No digital twin or virtual artefact can be identified legally compliant in this framework, nor can a digital avatar sign a contract on behalf of its owner in the sense of a natural person or legal entity. Even though the requirements on trustworthy digital transactions are clear, their implementation in the Metaverse setting requires a new legal framework. This must recognize developments like decentralisation of infrastructures, identities, and transactions as well as virtualization and augmentation of reality, and a mature understanding of identities in all their dimension, no matter if natural, legal, or virtual[12].

3. Status of DLT in Europe

3.1 Status

Until 2019 the Distributed-Ledger-Technology (DLT) and its most famous representative blockchain generated a real hype in particular the well-known use case Bitcoin[13]. After the bitcoin crash and especially the security concerns of German National Cybersecurity Authority[14] First doubts about the real capacity, security and trust of DLT occurred. In this context standardisation 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[15].

Within the 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 decentralised PKI for the execution of the new SSI paradigm[16] based in wallets as well as in the

[11] ETSI EN 319 411, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General Requirements. Version 1.3.1
[12] See section 1.
[13] Tomasz Kusber and others, 'Records Management and Long-Term Preservation of Evidence in DLT' (Open Identity Summit, 2021), 131.
[14] Federal Office for Information Security (BSI): *Towards Secure Blockchains. Concepts, Requirements, Assessments* (2019).
[15] Alamillo and Schwalm (n 3).
[16] ibid.

issuance and verification of verifiable credentials acc. W3CVCDM[17] such as a digital diploma, mobile driver licence or power of attorney. Other use cases such as cryptocurrencies, supply chain or notarization can be mentioned.

In order 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[18]. 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 decentralised identities in particular as needed in regulated environments. Those shortages and also 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[19].

The eIDAS 2.0 establishes as an amendment of eIDAS 1.0 a legal and technical framework for trustworthy decentralised identities with the EU Digital Wallet (EUDIW) and related (qualified) trust services, using or not DLTs, on one hand but with a new dedicated Qualified Trust Service Provider (QTSP) for Electronic Ledger on the other hand. Although the term Electronic Ledger in eIDAS 2.0 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[20]. But what's the role of DLT within eIDAS 2.0? 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 eIDAS 2.0 and its relationship to the Metaverse occurs too.

3.2 Electronic Ledger and Distributed Ledger Technology

3.2.1 Terminology

The term "Ledger" is defined in ISO 22739:2024[21] which was adopted as CEN EN into European standardisation Framework and is so mandatory in terms of European standardisation:

- Ledger: information store that keeps records of transactions that are intended to be final, definitive and immutable
- Distributed Ledger: ledger that is shared across a set of distributed ledger technology nodes and synchronised between the DLT nodes using a consensus mechanism

This means that DLT is technically only a special kind of ledger and the basic properties like immutability as well as the fact that on ledger records are final per definition are valid for any kind of ledger. The only difference between a ledger and a distributed ledger is the distributed provision. ISO 22739 was adopted into the European Standardization Framework and is mandatory in terms of standardisation (to make evident state of the art technology).

3.2.2 Technical overview

Basically, DLT is a decentralised distributed peer-to-peer network of technical nodes for data

[17] W3C VC Data Model v2.0. 2024
[18] Kusber and others (n 13).
[19] https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept-v
[20] Alamillo and Schwalm (n 3); Korte and others (n 2).
[21] ISO 22739:2024, Blockchain and Distributed Ledger Technologies — Terminology.

exchange and transaction execution. According to ISO 22739 a distributed ledger is in this case shared across a set of DLT nodes and synchronised 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. 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 stored on the chain. Any transaction can reliably be tracked on the chain. In case the DLT is organised in blocks it's called blockchain, so basically a blockchain is a special kind of DLT[22]. Blockchain is not a simple algorithm, but a technological construct and enabling protocol that facilitates the decentralised intermediation of data between participants[23]. The blocks can also include the hash of the previous block and so build the mentioned hash-protection and a so-called "timestamp". This DLT-"timestamp" as well as DLT "signatures" have to be differentiated from timestamps defined in eIDAS and related standards 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 a third party instead of the system, here DLT, itself. The hash-based integrity protection of each block is based on Merkle-trees. This means that if authenticity or Proof of Existence within DLT needed they have to be added from (qualified) trust service providers acc. eIDAS. Similar challenges occur in case the parties participating in a transaction shall be made evident. In this case the DLT has to be combined with external systems to ensure unique and trustworthy identification of legal and/or natural entities[24]. 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 authorised 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[25]. If DLT should 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 ISO TS 23635[26], ISO TS 23353[27] or currently developed in CEN JTC 19 on qualified trust services for electronic ledger DLT is currently not able to fulfil those requirements[28].

[22] Alamillo and Schwalm (n 3); Korte and others (n 2).
[23] Daniel Hellwig and others, *Build Your Own Blockchain* (Springer International Publishing 2020).
[24] Alamillo and Schwalm (n 3); Korte and others (n 2).
[25] Alamillo and Schwalm (n 3); Korte and others (n 2).
[26] ISO/TS 23635:2022, Blockchain and Distributed Ledger Technologies — Governance Guidelines.
[27] ISO WD TS 23353, Blockchain and Distributed Ledger Technologies — Audit Guidelines (2024).
[28] Alamillo and Schwalm (n 3); Korte and others (n 2); International Organization for Standardisation, 'Information and

The following table gives an overview about relevant standardisation regarding Electronic Ledger in general and DLT in particular:

Standardization Organization and status	Relevant standards
ISO Tc 307 published	• ISO 22739 Terminology • ISO TR 22349 Overview of existing DLT systems for identity management • ISO 23257 Reference architecture • ISO TS 23635 Guidelines for governance • ISO TR 23644 Overview of trust anchors for DLT-based identity management
ISO under construction	• ISO DTR 24332 Blockchain and DLT in relation to authoritative records, records systems, and records management • ISO TS 23353 Auditing guidelines • ISO 25126 Information security controls based on ISO/IEC 27002 for distributed ledger services
Europe under construction (CEN JTC 19)	• Policy and security requirements for trust service providers providing electronic ledger services • Functional and interoperability requirements on Decentralised Identifier (DID)

Table 1: Overview on relevant DLT standardisation

4. Regulative Requirements: eIDAS Regulation and technical framework

4.1 Overview

In April 2024 eIDAS 2.0[29] an amendment of eIDAS 1.0 was published.The main goal of the update is not a replacement but further development of eIDAS 1.0 in the context of decentralisation and the upcoming SSI-paradigm but also further development on (qualified) trust service providers (QTSP). The technical framework of eIDAS 2.0 is determined by the Architecture and Reference Framework developed in the eIDAS Toolbox through experts from Member States. As eIDAS 2.0 requires mandatory implementing acts for each component referencing European Standards from ETSI or CEN the regulation also creates a much more coherent technical framework than eIDAS 1.0 where only fewer implementing acts were mandatory[30].

4.2 EUDI Wallets and (qualified) trust services in relationship to DLT

The presumably biggest change in eIDAS 2.0 is the requirement for every Member state to provide an EU-Digital Wallet to its natural entities. The Wallet could be published by member state, under authority of member state or recognized by member state. This also makes private

Documentation — Blockchain and DLT in relation to authoritative records, records systems, and records management', (ISO TR 24332 (DTR)

[29] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework [2024], OJ L, 2024/1183, 30.4.2024.

[30] Alamillo and Schwalm (n 3).

wallets possible under the recognition of a Member State. Any EUDIW will contain a Personal Identification (so called PID for natural or legal entity as wallet holder) based on a notified eID scheme on LoA "high" and has to achieve LoA "high" itself. Directly corresponding with the EU-Digital Wallet the new qualified attestation services acc. Art. 45a-e eIDAS 2.0 has to be taken into account. (Qualified) Attestations (QEAA) are nothing more, nothing less than additional attributes so driver licence, diplomas or vaccine passport of EUDI Wallet holder but with qualified seal from issuing QTSP. This means that EU-Digital Wallet will contain the core identity currently covered by government eID as well as additional attributes. The data to be attested in QEAA will be provided from so-called authentic sources provided by Member States. Recognizing this close relationship between qualified attestation services and the wallet eIDAS 2.0 contains the same requirements for mandatory implementing acts referring to European Standards for both – wallet and (qualified)attestation service. Both will be certified by an independent Conformity Assessment Body which ensures the proven security. In the consequence eIDAS 2.0 crosses digital identity means and (qualified) trust services – they determine each other and for both DLT as infrastructure is possible to use. The core requirements on QTSP like liability, periodical recertification, reporting obligation on security issues etc. remain in eIDAS 2.0. Technically the EUDI Wallet as well as QTSP for QEAA can use DLT as decentralised infrastructure.

The Architecture and Reference Framework[31], the fundamental technical framework for eIDAS 2.0 only defines protocols and formats as well as key management for the Personal Identification (PID) of natural and legal entities but no limitations on the infrastructure. Same applies to current standardisation in this subject in CEN or ETSI. Beside the EUDI Wallet and QEAA the eIDAS 2.0 contains some changes on other (qualified) trust services and introduces new ones like QTSP for Electronic Ledger, (Art. 45h), Management of secure signature creation devices (Art. 29a) or Archiving (Art. 45g). DLT can be used as infrastructure for EUDIW as well as QTSP for QEAA but also any QTSP. Means on the other hand also that the term "Electronic Ledger" not necessarily applies for DLT only. One fundamental change is the binding of QTSP on the NIS2 Directive. In the result any QTSP so also the one on electronic ledger or in context of the paper DLT become part of critical infrastructure and so have to fulfil foreseeable higher security requirements than under eIDAS 1.0 The core requirements on QTSP like liability, periodic recertification, reporting obligation on security issues etc. are applicable for all QTSP in eIDAS 2.0 too. For each (qualified) trust service also mandatory implementing acts are required in eIDAS 2.0 referencing European standards[32].

4.3 Qualified trust service for Ledger

With Section 11 eIDAS 2.0 also introduces (qualified) trust services on Electronic Ledger (Art. 45h following). eIDAS 2.0 defines that qualified ledgers "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 eIDAS 2.0 is technology neutral, the description in Art. 45i is in line with the definition of DLT in international standards like ISO 22739 and contains core properties

[31] The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework. The European Digital Identity Wallet Architecture and Reference Framework. December 2023; <https://github.com/skounis/architecture-and-reference-framework/blob/80d00cf5ad1c3930235e4140b1fc8a975638f787/docs/arf.md >

[32] Ignacio Alamillo and others, 'Qualified Ledgers: Bridging the Gap between Blockchain Technology and Legal Compliance' (2024) *Open Identity Summit 2024*, 10.18420/OID2024_19

of DLT. As eIDAS 2.0 contains the requirement of mandatory implementing acts referring to European standards it ensures a coherent technical framework for DLT. Since the requirements on QTSP also apply to QTSP for Ledger, these standards will also be the basis for certification by an independent conformity assessment body and so ensure proven security and trust in DLT. It has to be stated that Section 11 focuses on all use cases not covered by EUDIW or all other (qualified) trust services 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 – the security will be proven within the conformity assessment of the Conformity Assessment Body (CAB), but there's no need to use QTSP for Ledger as precondition to provide another (qualified) trust service nor an EUDIW. This differentiation is important as it lead to the core use cases for QTSP for Electronic Ledger as e.g. tokenization or digital assets, digital twin or other Metaverse applications. The table below shows the possible use case scenarios for electronic ledger (DLT) within eIDAS 2.0 ecosystem[33]:

#	Use Case Type	Examples Use Cases	Section 11 applicable

1	EUDI Wallet	• Infrastructure for
		  ○ PID
		  ○ (Q)EAA (with QTSP)
		  ○ QES (with QTSP)
		• Trusted Issuer Registries
		• TrustList/Trust Anchors
		• Verifiable Data Registry
			no

2	Other QTSP	• QES • QSeal • QTimestamp • eDelivery and registered mail • Remote signing • Validation • Preservation • Archiving • Trusted Issuer Registries • TrustList/Trust Anchors	no
2	QTSP for Electronic Ledger	• Cryptocurrencies • Supply chain • Data traceability • Product traceability • Document traceability • Web 3	yes
3	Use cases in non-regulated domains	• Dito	yes

Table 2: Applicability Section 11 of eIDAS 2.0

4.4 Trust Model within eIDAS 2.0

[33] Alamillo and others (n 32).

eIDAS 2.0 complements the eIDAS ecosystem (eID or PID in eIDAS2, existing QTSP) with recognition of developments on decentralised identities (EUDIW, QEAA), cybersecurity act[34], as well as (qualified) trust services (e.g. Archiving, Electronic Ledger) and the technology neutrality which allows utilisation of existing technologies like PKI but also DLT for each component. Each element, including decentralised ones like EUDIW or Electronic Ledger/DLT, is directly integrated into the eIDAS trust framework. There's no trust by default in Europe. 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[35].

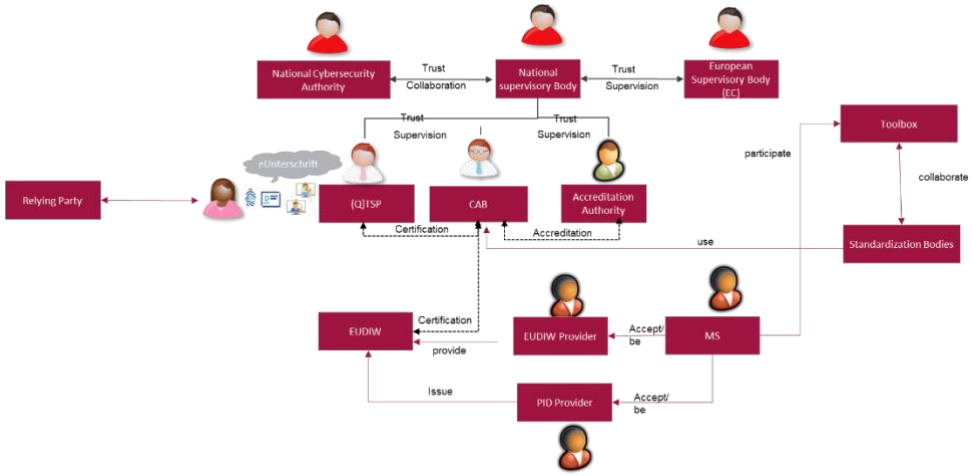

Figure 1: Trust Model in eIDAS 2.0

5. Technical framework of eIDAS 2.0

The Architecture and Reference Framework provided by eIDAS Toolbox Group provides basic technical requirements on EUDIW[36], issuance of the PID so identity of natural or legal entity which may represent a digital twin or owner within the Metaverse and related qualified trust services so especially qualified attestations of attributes – the legal evidence ownership represented by a NFT. It has to be stated that the ARF is a collection of technical standards on formats and protocols but not legally mandatory. The implementing acts required in eIDAS 2.0 will reference the European standards themselves which basically define the formats and protocols to be used by EUDIW and qualified trust services but also requirements for trusted verification of Relying Parties and their access to EUDIW. Those standards are developed in ETSI and CEN[37], mainly:

[34] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019], OJ L 151, 7.6.2019, p. 15–69.

[35] Steffen Schwalm and Ignacio Alamillo, 'Decentralised Digital Identity in the Metaverse under eIDAS 2' (Webinar of Chair for the Responsible Development of the Metaverse, Alicante 2023).

[36] European Digital Identity Architecture and Reference Framework, February 2022. <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/>

[37] Standards from W3C, IETF and OID Foundation will be recognized within the related ETSI/CEN Standards.

Standardization Organization	Topics
ETSI ESI	(Qualified) trust services accept Archiving and Electronic Ledger Interaction EUDI Wallet and (qualified) trust services
CEN Tc 224	Protocols and interfaces of EUDI Wallet Hardware security of EUDI Wallet
CEN JTC 19	Electronic Ledger Technical requirements on decentralised identity management (DID methods)

Table 3: Overview on standardisation Reg. eIDAS 2.0

In parallel, as EBSI introduced a key input for Section 11 in eIDAS 2.0, it is under further development and adjustment to the eIDAS ecosystem. This will provide the basis for the needed proven secure and trustworthy distributed infrastructure for ecosystems like the Metaverse and core input for standardisation in CEN JTC 19. As acc. to Art. 3 of draft implementing act Ares(2024)5786790[38] and Regulation (EU) No 1025/2012[39] standards from ETSI and CEN will be used by Conformity Assessment bodies to certify EUDI Wallet and/or (qualified) trust services in eIDAS 2.0 the incorporation of Electronic Ledger and so DLT in eIDAS is one basis for trustworthy and legally compliant transactions in the Metaverse.

6. Trustworthiness of digital transactions

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 transactions 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[40] 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[41]. The utilisation of cryptographic measures, e.g. qualified e-signatures, seals and time stamps acc. to eIDAS, 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

[38] Ref. Ares (2024) 5786790 - 12 August 2024 Commission Implementing Regulation (EU) .../... laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets.

[39] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC, and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC [2012], OJ L 316, 14.11.2012, p. 12–33.

[40] United Nations Commission on International Trade Law (UNCITRAL), 'Model Law on Electronic Transferable Records' (United Nations, New York 2017).

[41] Matthias Weber and others, 'Records Management acc. ISO 15489: Introduction and Guideline' (Berlin 2018).

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. Main precondition is the establishment of a valid records management accordingly. 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[42]. These basic burdens of proofs and requirements on trustworthy digital records and transactions are independent from used IT-system, organisation 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 Art. 41 and 42 eIDAS. An evidence value of a record is an inherent property of the record itself. The proof is typically done by trustworthy 3rd parties such as courts, regulatory authorities, auditors etc. depending on the legal requirements 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[43].

7. European Blockchain Service infrastructure as public infrastructure for decentralised identities and ecosystems in eIDAS

7.1 Fundamentals

The project, which was set up in 2018, aims to lay the foundation for future ledger based services within the EU and EFTA. The EBSI is currently transitioning into a new organisational entity for the operations of EBSI, the European Digital Infrastructure Consortium (EDIC), which is expected to be fully operational by the end of 2024. It shall be understood that because of GDPR the EBSI design does not intend to anchor any citizen data on immutable electronic ledgers. When it comes to legal entity identity it can be expected that identifiers of and trust registries about legal persons will be anchored on the EDIC ledger. 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 decentralised 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 eIDAS 2.0 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 also providing legal certainty for use cases that build on the EDIC's electronic ledger. EBSI could also act as decentralised, pan-European Infrastructure for other (qualified) trust services such as issuance of (qualified) certificates, or trust issuer registry as possibly more scalable replacement of the trust list and so trustworthy infrastructure for European Metaverse applications[44].

[42] Weber and others (n 41)
[43] Weber and others (n 41)
[44] ETSI TS 119 612, *Electronic Signatures and Infrastructures (ESI); Trusted Lists.*

7.2 EBSI within eIDAS 2.0

Currently the European Union is improving the European Blockchain Service Infrastructure to adjust it according the new eIDAS 2.0 but also to establish cross-border use cases to be adopted and rolled out on a pan-European DLT-network so e.g.:

Project	Subject
Digital Credentials for Europe DC4EU[45]	Large Scale Pilot on EUDIW and related (qualified) trust services Diploma and Social Security
EBSI VECTOR[46]	EBSI Digital Europa programme Project Diploma Social security
TRACE4EU[47]	Product Traceability (e.g. Supply chain and digital product pass) Data and Document Traceability (e.g. digital rights, QEAA, KYC)
EBSI-NE[48]	New EBSI Nodes Standardization on EBSI Adjustment of EBSI Governance

Table 4: Scope of EBSI Projects in context of eIDAS 2.0

The Large Scale Pilot Digital Credentials for Europe (DC4EU) focus on using EBSI as infrastructure for EU Digital Wallet including the technical improvement according to the ARF. The other EBSI Projects funded under Digital Europe Programme support this technical evolution. Regarding the fact that EBSI is widely used across Europe and is a functionable network another task is the contribution to ARF in order to ensure its feasibility within existing infrastructures like EBSI as eIDAS 2.0 in general and the EUDI Wallet or QTSP for QEAA in particular are not built on a green field. The aim is to ensure trustworthy digital transactions within EBSI using secure digital identities in all their dimensions as well as non-repudiable transactions. EBSI-NE ensures the broader development of the EBSI infrastructure and together with VECTOR focus on the qualification of EBSI acc. eIDAS.

8. Towards a trusted Metaverse with eIDAS 2.0 and EBSI

8.1 Trustworthy digital transactions in the Metaverse through eIDAS 2.0

As described in EUDI Wallet will contain the personal identification of its holder as well as related (qualified) attestations of attributes. This means that the relationship between a natural entity and its digital twin so e.g. avatar within the Metaverse can be made evident, same with the digital twin of machines or any other physical object in augmented or virtual reality. Practically the

[45] https://www.dc4eu.eu/
[46] https://www.ebsi-vector.eu/en/
[47] https://trace4eu.eu/
[48] https://www.ebsi-ne.com/

natural entity may identify itself against certain QTSP for QEAA just to get the digital twin e.g. avatar issued into the EUDI Wallet. In case of transactions in a virtual environment e.g. to purchase a virtual asset the EUDI Wallet holder uses its EUDIW to present the QEAA to the certain relying party. The relying party may also be represented by a digital twin referenced to real legal entities (using PID for legal entities+QEAA). The virtual asset can be represented by a Non-Fungible Token which anchored on a Distributed Ledger provided by QTSP for Ledger according Section 11 eIDAS 2.0 and referenced to the EUDI Wallet of holder purchasing e.g. a virtual house or another digital asset in virtual reality. In case of EBSI an infrastructure with governmental trust anchor by default could be used and so additional trust gained. Similar subject possible for any digital twin. A possibly necessary (qualified) signature to sign the purchase contract. In order to ensure the privacy of real legal entities the qualified certificate on which the qualified signature will be based may be issued by QTSP for qualified certificates with a pseudonym – so exactly the name of the digital twin of a related natural entity, or better the QEAA of a certain natural entity. In summary eIDAS 2.0 provides all necessary tools and regulations to establish legal trust in transactions in the augmented and virtual reality or to use digital twins in a legally compliant manner.

The following hypothetical example explains briefly how eIDAS 2.0 may support Metaverse applications.

Virtual World Wonderland

Setup

Entity	Virtual Representation	Roles in Wonderland
Company A	Super Real Estate Ltd	Ownership 5 houses with 1 house located at virtual "Sunset beach"
Mr. Maxman	Manager Smith	Manager at Company A
Mrs. Sanchez	Scientist Muller	none

Table 5: Setup in example Metaverse Application Virtual World Wonderland

Super Real Estate Ltd (alias Company A) represented by Manager Smith (alias Mr. Maxman) sells a house located at virtual "Sunset Beach" to Scientist Muller (alias Mrs. Sanchez). The transaction shall be legally compliant in the virtual and real world.

Implementation with eIDAS 2.0

Task	Relevant measure	Explanation
Identification Company A	EUDI Wallet for legal entities and Personal Identification (PID) for Company A	PID for legal entities identifies certain company unambiguously EUDI Wallet is legally compliant eID mean
Identification Mr. Maxman and Mrs. Sanchez	EUDI Wallet for natural entities and Personal Identification (PID) for Mr. Maxman and Mrs. Sanchez	PID for natural entities identifies certain natural persons EUDI Wallet is legally compliant eID mean
Linking Company A and Mr. Maxman and Mrs. Sanchez to their virtual representation	Qualified Attestation of Attributes issued into their EUDI Wallet	QEAA add identity attributes and evidences like e.g. virtual representations, Power of Attorney etc. to natural/legal entities, typically issued by QTSP in unambiguous manner

Task	Relevant measure	Explanation
Power of Attorney to Manager Smith as virtual representation of Mr. Maxman	Qualified Attestation of Attributes issued into their EUDI Wallet	Dito possibly including binding to QEAA for virtual representation to ensure utilisation in virtual world only if needed
Properties of Super Real Estate Ltd and trade	NFT issued in EUDI Wallet and anchored on qualified ledger, linking to identity via DID of Company A	Qualified ledger from QTSP for Ledger e.g. EBSI ensures trustworthy infrastructure for tokenization EUDI Wallet ensures unique identification of Company A as the real world equivalent of Super Real Estate Ltd. Combination DID and NFT ensures the link between identity and ownership
Transaction	Recorded on ledger so that NFT former related to DID of Company A (Super Real Estate Ltd) now related to DID of Scientist Muller (Mrs. Sanchez) Qualified Signing of transaction with qualified certificates issued to Company A, Mr. Maxman and Mrs. Sanchez with pseudonym in certificate related to the virtual representations	Dito QES ensures replacement of handwritten signature and so trustworthy digital contracts, with pseudonyms the virtual representations could be used
Payment	EUDI Wallet of Scientist Muller used for Payment	EUDI Wallet will contain Strong customer authentication and payment functionalities as banks are obligated for acceptance acc. Art. 5f eIDAS. Identification for KYC done as given in steps before

Table 6: Implementation application example Virtual World Wonderland

8.2 Privacy and Security within Metaverse

As eIDAS 2.0 requires privacy by design the [ARF] defines functionalities like Selective Disclosure or Zero Knowledge Proofs the natural or legal entity holding the EUDIW can decide in its own sovereignty which data they want to provide to the relying party. This data sovereignty is only limited by the documentation requirements of the relying party which may require the provision of personal or other data to be able to use a certain service

The conformity assessment of any EUDIW as well as any QTSP by independent CAB together with the supervision by National Supervisory Bodies and the obligations on liability etc for QTSP and wallet providers ensure proven security and so legal trust in any wallet, personal identification but also QEAA representing digital twins, assets etc. in Metaverse applications.

In the given example *Virtual World Wonderland* the privacy could be ensured with following measures:

Task	Relevant measure	Explanation
Hide real equivalent of Super Real Estate Ltd as well as Manager Smith and Scientist Muller in Identity	QEAA issued for pseudonym (virtual representation) Disclosure for authorised entities only Selective Disclosure Unlinkability	hides real identity for unauthorised people provides real identity authorised parties only provision of necessary data only avoids unauthorised tracing
Hide real equivalent of Super Real Estate Ltd as well as Manager Smith and Scientist Muller in QES	QEAA issued for pseudonym (virtual representation) Disclosure for authorised entities only	hides real identity for unauthorised people provides real identity authorised parties only

Table 7: Provision Privacy with eIDAS 2.0 in Metaverse Application by example

8.3 Trustworthy Tokenization within Metaverse

Non-Fungible Token often used for transactions on digital assets are typically anchored on DLT. With its nodes provided by member states EBSI uses governmental trust anchor. The Digital Europe Programme currently supports dedicated European consortiums in the improvement of EBSI to be used for regulated use cases.

Interesting in context of the Metaverse is especially TRACE4EU as the project pilots exactly the combination of identity and ownership of intellectual and other properties. The ownership is represented by a NFT. The use case can be easily adapted to subjects like e.g. virtual properties in Metaverse represented by a NFT and related to a wallet where a QEAA might be the digital representation of an avatar related to a natural or legal entity holding the wallet and owning the virtual or real property.

In the result a European DLT-infrastructure will be created not only with governmental trust anchor but fully liable QTSP which provides a DLT infrastructure with proven security and trust through the conformity assessment by independent CAB acc. eIDAS 2.0. This means also that Metaverse applications using EBSI or which rely on qualified trust services and/or wallets using EBSI will rely on an additional trust layer as any qualified trust services and/or wallets will be built on top of the fundamental EBSI infrastructure provided by Member States.

Practically the NFT can be issued by a certain relying party for a certain natural or legal entity proven using its EUDIW including the PID or any other wallets in which case a QEAA will be used for identification purposes as it´s explicitly possible within eIDAS. Another QEAA for the digital twin (e.g. avatar in virtual environments) will be the digital representative. The NFT itself will be anchored on a qualified ledger related to certain transactions and matched with EUDIW or another wallet of a certain entity (e.g. via DID).

With this combination of identity and transaction the EBSI allows to build up comprehensive ecosystems within Metaverse with its complexity on:

- Match real citizens and companies with their digital twin.
- Match digital identities of real citizens and companies with their real or virtual properties.
- Ensure transactions between:

- virtual representations of real citizens, companies using real or virtual properties
- manifested / documented within real wallet, identities, attestations and verifiable through signatures and seals.

In the given example *Virtual World Wonderland* the privacy could be ensured as given in Tables 5 and 6 and briefly summarised below:

Task	Relevant measure	Explanation
Match real citizens and companies with their digital twin	QEAA issued into EUDI Wallet of real citizen or company	QEAA add identity attributes and evidences like e.g. virtual representations, Power of Attorney etc. to natural/legal entities, typically issued by QTSP in unambiguous manner
Match digital identities of real citizens and companies with their real or virtual properties	NFT issued in EUDI Wallet and anchored on qualified ledger, linking to identity via DID of Company A	Qualified ledger from QTSP for Ledger e.g. EBSI ensures trustworthy infrastructure for tokenization EUDI Wallet ensures unique identification of Company A as the real world equivalent of Super Real Estate Ltd. Combination DID and NFT ensures the link between identity and ownership
Ensure transactions between - virtual representations of real citizens, companies, issuers and relying parties - real or virtual properties	Recorded on ledger so that NFT former related to DID of Company A (Super Real Estate Ltd) now related to DID of Scientist Muller (Mrs. Sanchez) Qualified Signing of transaction with qualified certificates issued to Company A, Mr. Maxman and Mrs. Sanchez with pseudonym in certificate related to the virtual representations	Dito QES ensures replacement of handwritten signature and so trustworthy digital contracts, with pseudonyms the virtual representations could be used

Table 8: trustworthy tokenization within Metaverse through eIDAS 2.0 by example

8.4 Conclusion and necessary standardisation

eIDAS 2.0 defines the legal and through mandatory implementing acts for de facto all components also the technical framework for trustworthy decentralised ecosystems in Europe. As the regulation is technology neutral it also allows the utilisation of DLT for each component from EUDI Wallet and all QTSP. With the QTSP for Electronic Ledger eIDAS 2.0 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 utilisation of DLT in Europe.

Beside EUDIW and other (qualified) trust services QTSP for ledger can be a game-changer not only in tokenization, product passports and supply chains but also other applications of the Metaverse by matching legal and natural entities with their virtual twins, digital assets in transactions with real or virtual relying parties in real, augmented or virtual realities. eIDAS 2.0 makes it possible to use the identity of natural or legal entities in their complete variety in a legally compliant manner. The regulation together with the de facto mandatory technical framework which applies also for EUDI Wallet and QTSP using ledger but especially the new QTSP for ledger eIDAS 2.0 ensures trustworthy decentralisation of real and virtual ecosystems using digital identities and shown in the picture below:

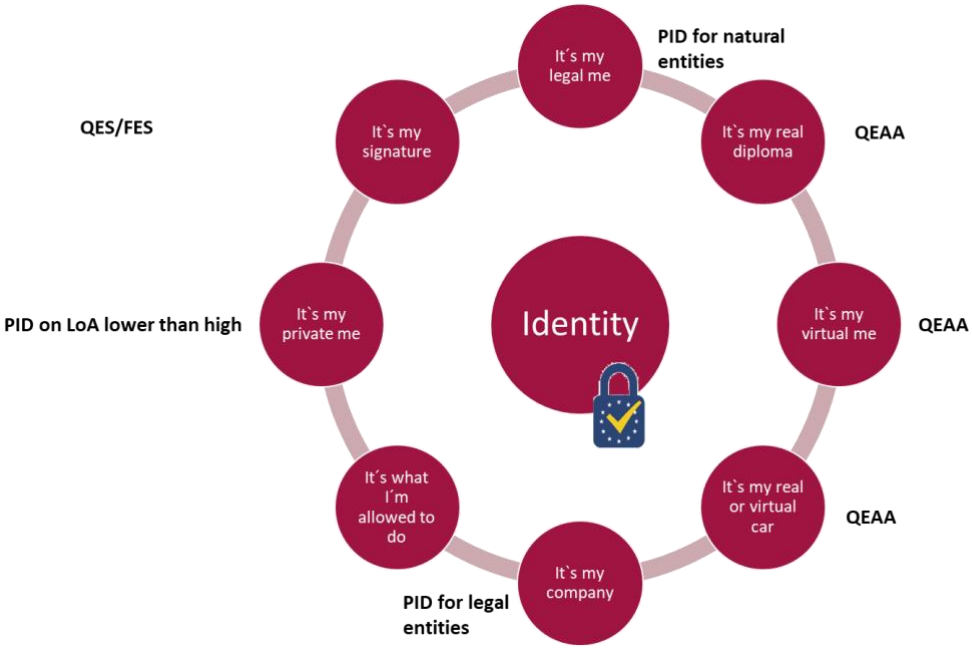

Figure 2: 360 degrees identity with eIDAS 2.0

The focus in European standardisation should be especially on the relationship between identities of natural/legal entities and their real and virtual characteristics. The harmonisation of technical framework so existing Web 3 applications, payment wallets and the upcoming eIDAS 2.0 ecosystem including the worldwide interoperability.

Especially the portfolio definition of QTSP for Ledger and in this context the adjustment of EBSI regarding eIDAS 2.0 seem to be the most important issues to be solved in order to create European trusted DLT infrastructure for the Metaverse. In this context also the standardisation on decentralised identity management so especially DID have to be mentioned. In summary the integration of those technologies in the eIDAS framework through European Standards in ETSI in CEN can be mentioned as essential for legally compliant transactions in the Metaverse as those standards are the technical fundament of eIDAS 2.0.

Bibliography

Alamillo, I., 'SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market' (2020).

Alamillo, I. and Schwalm, S., 'Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0' (European Review of Digital Administration & Law – Erdal, 2021, Volume 2, Issue 2, pp. 89-100).

Alamillo, I. and Schwalm, S., 'Decentralised Digital Identity in the Metaverse under eIDAS 2' (Webinar of Chair for the Responsible Development of the Metaverse, Alicante 2023).

Alamillo, I. and others, 'Qualified Ledgers: Bridging the Gap between Blockchain Technology and Legal Compliance' (2024) *Open Identity Summit 2024*, 10.18420/OID2024_19

Allen, C., 'Self-Sovereign Identity Principles' (WebOfTrustInfo, 2016) <https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md>

Antin, D., 'The Technology of the Metaverse, It's Not Just VR' (The Startup, 5 May 2020).

Anke, J. and others, 'Self-Sovereign Identity as the Basis for Universally Applicable Digital Identities' (2021) 58 HMD 247.

Bernal Bernabe, J. and others, 'An Overview on ARIES: Reliable European Identity Ecosystem' in Challenges in Cybersecurity and Privacy - the European Research Landscape (2019), River Publishers.

Dwivedi, Y. K. and others, 'Metaverse Beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy' (66 International Journal of Information Management, 2022) <https://doi.org/10.1016/j.ijinfomgt.2022.102542>

Du Seuil, D., 'European Self Sovereign Identity Framework' (European Economic and Social Committee, 2019).

Hellwig, D., Karlic, G. and Huchzermeier, A., Build Your Own Blockchain (Springer International Publishing 2020).

Korte, U. and others, 'Criteria for Trustworthy Digital Transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation' (Open Identity Summit 2020, Lecture Notes in Informatics (LNI), 2020), 49, 60.

Kubach, M. and others, 'Self-Sovereign and Decentralized Identity as the Future of Identity

Management?' in Heiko Roßnagel, Christoph Schunck and Sebastian Mödersheim (eds), (Open Identity Summit 2020), 35.

Kusber, T. and others, 'Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain' (DACH-Security, 2018), 177.

Kusber, T. and others, 'Records Management and Long-Term Preservation of Evidence in DLT' (Open Identity Summit, 2021), 131.

Marr, B., 'The Important Difference Between Web3 and The Metaverse' (Forbes Magazine, 22 February 2022) <https://www.forbes.com/sites/bernardmarr/2022/02/22/the-important-difference-between-web3-and-the-Metaverse/?sh=3d02677e5af3>

Merkle, R., 'Protocols for Public Key Cryptosystems' (IEEE Symposium on Security and Privacy, 1980) 122-134.

Rieger, A. and others, 'Digital Identities and Verifiable Credentials' (2021) 63 Business & Information Systems Engineering.

Sato, M. and Matsuo, S., 'Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography' in ICCCN: 26th International Conference on Computer Communications and Networks (IEEE, 2017) 1, 8.

Schwalm, S., 'The (not only) social impact of the eIDAS 2.0 digital identity approach in Germany and Europe' in CRYPTOASSETS, DEFI REGULATION AND DLT: Proceedings of the II Token World Conference - Derecho de Blockchain y Digitalización de la Sociedad (First Edition, Madrid 2021) 23–38.

Schwalm, S., 'The possible impacts of the eIDAS 2.0 digital identity approach in Germany and Europe' in Open Identity Summit 2023 (Gesellschaft für Informatik eV 2023) 109–120.

Schwalm, S., 'EU-Digital Wallet – Chances and challenges for EU Digital Identity – a German perspective' (My Data Conference, Helsinki, 2023).

Schwalm, S., 'eIDAS 2 and the role of identity standards: an outlook of current activities' (La propuesta de Reglamento eIDAS 2: contexto y visión general, Universidad de Murcia, Murcia, 23 November 2023).

Strüker, J. and others, 'Self-Sovereign Identity - Foundations, Applications, and Potentials of Portable Digital Identities' (Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, Bayreuth 2021)

Weber, M., Schwalm, S., Vogt, T. and Krogel, W., 'Records Management acc. ISO 15489: Introduction and Guideline' (Berlin 2018)

Werbach, K., The Blockchain and the New Architecture of Trust (MIT Press 2018)

Xu, X., Weber, I. and Staples, M., Architecture for Blockchain Applications (Springer 2019)

Yaga, D., Mell, P., Roby, N. and Scarfone, K., Blockchain Technology Overview (NIST Interagency/Internal Report, National Institute of Standards and Technology 2018)

Yildiz, H. and others, 'Connecting Self-Sovereign Identity with Federated and User-centric Identities via SAML Integration' in 2021 IEEE Symposium on Computers and Communications (ISCC) (IEEE 2021) 1.