BLOCKSTAND

Feasibility and Market Analysis Report on Integrating Blockchain Technology into Qualified Trust Service Provider (QTSP) Frameworks

P. Soumplis

Abstract

Blockchain technology has emerged as a promising solution for digital identity management and authentication within the European Union. This deliverable provides a comprehensive overview of how blockchain and distributed identity systems (DIDs) enhance the security and decentralization of digital identity frameworks. We examine the integration of DIDs into trust service infrastructures, addressing key challenges such as interoperability, scalability, security, and regulatory compliance. Additionally, the analysis explores emerging market trends and includes a SWOT analysis to assess the strategic position of Qualified Trust Service Providers (QTSPs) in a blockchain-enabled market. The study also highlights opportunities for improving digital identity systems and outlines the potential impact on trust services, ultimately offering insights into the future landscape of secure and decentralized digital identities in the EU.

Contents

Abbreviations

- **eID**: Electronic Identification
- **eIDAS**: Electronic Identification, Authentication and Trust Services
- **EU**: European Union
- **TSP**: Trust Service Provider
- **QTSP**: Qualified Trust Service Provider
- **DLT**: Distributed Ledger Technology
- **EUDI**: European Digital Identity
- **EUDIW**: European Digital Identity Wallet
- **GDPR**: General Data Protection Regulation
- **PKI**: Public Key Infrastructure
- **CAB**: Conformity Assessment Body
- **CA**: Certificate Authority
- **ETSI**: European Telecommunications Standards Institute
- **ISO**: International Organization for Standardization
- **HSM**: Hardware Security Module
- **QSCD**: Qualified Signature Creation Device
- **SSI**: Self-Sovereign Identity
- **DID**: Decentralized Identifier
- **VC**: Verifiable Credential
- **W3C**: World Wide Web Consortium
- **PII**: Personally Identifiable Information
- **ISMS**: Information Security Management System
- **PoS**: Proof of Stake
- **BFT**: Byzantine Fault Tolerance

- **ZKP**: Zero-Knowledge Proof
- **ROI**: Return on Investment
- **SME**: Small and Medium-sized Enterprise
- **TPS**: Transactions Per Second
- **PoW**: Proof of Work
- **DPoS**: Delegated Proof of Stake
- **IoT**: Internet of Things
- **AI**: Artificial Intelligence

Executive Summary

The European Union (EU) has advanced electronic identification (eID) and trust services to improve digital transaction security, efficiency, and interoperability. Initially, the Electronic Signature Directive (1999) provided a legal foundation for secure electronic signatures. However, it encountered challenges due to the lack of technical standardization and the reliance on high-security devices, limiting its effectiveness and cross-border compatibility.

To address these limitations, the EU introduced the eIDAS Regulation in 2016, expanding its scope to include various trust services beyond electronic signatures. eIDAS established Qualified Trust Service Providers (QTSPs) to ensure secure and legally recognized electronic transactions throughout the EU. These QTSPs enable digital signatures and other trust services that comply with rigorous legal and technical standards, supporting the EU's digital identity ecosystem.

Despite these advancements, eIDAS 1.0 faced challenges related to low interoperability, limited electronic attribute coverage, and insufficient user control over personal data. The proposed eIDAS 2.0 aims to address these issues with enhancements in security, interoperability, and user-centered identity management. In particular, it integrates blockchain and Distributed Ledger Technologies (DLTs), which offer decentralized identity management, immutable audit trails, and smart contract automation, strengthening QTSP operations to better align with ETSI and ISO standards.

The demand for blockchain-enhanced trust services is growing, driven by the need for secure, transparent digital interactions in sectors such as finance, healthcare, and public administration. Blockchain enables better security for complex transactions, identity management, and regulatory compliance, which is beneficial to large enterprises, governments, and SMEs alike. For SMEs, blockchain-integrated trust services provide affordable and scalable security solutions, enhancing their competitiveness.

However, blockchain integration presents challenges, such as regulatory compliance, scalability, and infrastructure costs. Solutions such as standardized architectures, Layer 2 scaling, and permissioned blockchain networks help mitigate these concerns. Despite upfront investments, blockchain integration offers substantial ROI by improving security, reducing fraud risks, and improving operational efficiency through smart contracts. These efficiencies position QTSPs as innovators in the digital trust market, able to attract more clients and expand their offerings.

1 Introduction

1.1 Evolution of Electronic Identification and Trust Services in the European Union

The adoption of electronic identification (eID) and trust services for authentication and digital signatures has been an important target within the European Union (EU) [28], [29]. The vision is to integrate these technologies into daily transactions and enhance security, efficiency, and interoperability. Nevertheless, realizing this vision is a complex task, as it involves a combination of technologies and legislative frameworks to ensure seamless and secure cross-border functionality. The EU's initial efforts to establish a legal framework for electronic signatures started with the Electronic Signature Directive [26] in 1999. This directive aimed to recognize electronic signatures as legally equivalent to handwritten signatures, laying the groundwork for secure electronic transactions. More importantly it established the legal framework for such services. This enabled EU countries to adopt similar frameworks in order to bridge the gap between digital and traditional forms of authentication. However, it encountered significant challenges that limited its effectiveness. A primary issue was the absence of common technical standards across the different member states. Instead of following a common mechanism, each one implemented its own for electronic signatures, which lead to incompatibilities that hindered cross-border electronic transactions - a core objective of the directive. This fragmentation undermined the directive's potential to facilitate seamless digital interactions across the EU. Additionally, the directive focused on high-security devices such as smart cards and USB cryptographic tokens, which were state-of-the-art at the time. These devices required specialized drivers and were not user-friendly, especially with the rise of mobile devices. The reliance on such hardware impeded widespread adoption due to accessibility and usability issues, as users found it challenging to integrate these technologies into their routines. Notably, the directive introduced the concept of Trust Service Providers (TSPs), initially referred to as "certification-service providers," who are important authorities providing non-repudiation in regulated electronic signing procedures. Recognizing the shortcomings of the Electronic Signature Directive, the EU introduced the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation (EU) No 910/2014 [28], which came into effect in 2016. eIDAS aimed to create an interoperability framework for national electronic identification schemes and extended beyond electronic signatures to include various trust services. This regulation aimed to enhance cross-border digital interactions between citizens, businesses,

and public authorities by establishing guidelines for mutual recognition of eID schemes across member states. A significant innovation in eIDAS was the formalization and expansion of TSPs into Qualified Trust Service Providers (QTSPs). QTSPs are entities that provide one or more qualified trust services and have been granted qualified status by a supervisory body in an EU member state. Their role is pivotal in the digital identity ecosystem, as they offer services that meet strict legal and technical requirements set by the regulation. Hence, QTSPs ensure their services are recognized across all EU member states, facilitating seamless cross-border digital transactions. The services they deliver covers a wide range of trust services, including issuing qualified certificates for electronic signatures and seals, time-stamping services, electronic registered delivery services, and website authentication certificates. The introduction and formalization of QTSPs was essential in establishing a trustworthy environment for electronic transactions, where both individuals and businesses can operate confidently. Aiming to facilitate more flexible and accessible digital signing methods, in eIDAS 1.0 were also defined different levels of authentication and identification mechanisms with specific guidance on cloud-based signatures and remote signing. Despite these advancements, eIDAS 1.0 faced challenges. The main was the low interoperability due to varying national implementations and local interpretations of the law, which limited the use of foreign services in the different markets. Furthermore, eIDAS 1.0 did not adequately covered electronic attributes such as proof of residence, medical certificates, or professional qualifications, which are often required in comprehensive remote onboarding processes. This omission hindered the utility of eID services in various sectors. Additionally, the regulation did not place the user at the center of the identity and trust services ecosystem. Users lacked control over their personal data during verification and onboarding processes, impacting trust and adoption. Relying parties, such as banks and other organizations, were slow to adopt eIDAS-compliant processes due to operational complexities and the substantial infrastructural changes required to accept qualified electronic signatures. In response to these limitations, the EU recently proposed eIDAS 2.0 [29], aiming to increase security, interoperability, and user-centricity in electronic identification and trust services. Security became a core aspect of eIDAS 2.0, benefiting both citizens engaging in online transactions and businesses offering services online. This regulation aims to introduce a unified technical architecture with clear standards to ensure consistency across member states, thereby reducing fragmentation and fostering a robust digital ecosystem. One of the significant enhancements in eIDAS 2.0 is the expansion of trust services. It includes electronic archiving, electronic ledgers, management of remote electronic signing devices, and creation of electronic seals. This expansion enables

QTSPs to offer a broader range of services, catering to the evolving needs of digital transactions. Additionally, the European Digital Identity Wallet (EUDI) [10] is introduced, allowing citizens to control their digital identity via mobile devices. This wallet can store personal identification data and electronic attributes securely, empowering users with control over when and how their data is shared during authentication and onboarding processes. The inclusion of attributes such as addresses, driver's licenses, bank account proofs, health information, and academic qualifications significantly enhances the utility of eID services across various sectors. With the aforementioned changes, eIDAS 2.0 places the user at the heart of the digital identity ecosystem while addressing previous shortcomings related to user control and trust. Users can now participate more actively in managing their identities, which can lead to mass adoption. The regulation also sets standards for providers of identity services and trust services, pushing up the overall level of security available to businesses and organizations. QTSPs play a crucial role in this ecosystem by ensuring that the trust services provided meet the stringent requirements of the regulation, thus fostering confidence among users and relying parties. Moreover, for businesses and relying parties, eIDAS 2.0 offers numerous benefits including improved interoperability simplifies cross-border transactions and the recognition of digital identities and signatures. With clear standards and a unified architecture, organizations can adopt eIDAS-compliant processes with greater confidence, knowing that they align with EU-wide regulations. Enhanced security measures reduce risks associated with digital transactions, allowing businesses to rely on authentication mechanisms.

1.2 Role of QTSPs

In this context, QTSPs play a key role in the European Union's digital infrastructure by delivering trust services that enable secure and legally recognized electronic transactions. Under the eIDAS Regulation, QTSPs are entities that provide qualified trust services and have been granted qualified status by a supervisory body in an EU Member State. Their services are essential for establishing trust in digital interactions, ensuring that electronic transactions are as secure and reliable as traditional paper-based processes. They enable the creation of qualified electronic signatures and seals that are legally equivalent to handwritten signatures and physical seals [11]. In this way, the identity of signatories is verified by the QTSP and also link their signatures to their identities. This ensures the authenticity and integrity of electronic documents. Additionally, time stamping services guarantee the existence of data at a specific point in time [2], which is essential for legal and compliance purposes, as it provides verifiable evidence

that the electronic document or transaction existed at a certain moment. QTSPs also offer Qualified Electronic Registered Delivery Services (QERDS) that allow for the secure transmission of electronic documents, providing evidence of sending and receiving similar to registered mail [14]. This service ensures that both the sender and recipient are authenticated and that the contents of the communication are protected against unauthorized access or alteration, enhancing users' trust in online services. Regarding their role in electronic identification schemes, they provide authentication mechanisms in order to verify the identities of individuals and entities in digital transactions [1]. Moreover, by collaborating with national eID provides, the security and reliability of electronic identification systems is enhanced. This can facilitate the secure access to online services across the EU QTSPs are also needed for realizing the upcoming European Digital Identity Wallet as proposed in eIDAS 2.0. Their role will enhance security and users' control over their personal data that is they will contribute in securely storing and managing their digital identities and credentials on mobile devices. Given their critical role in providing security among users, QTSPs are responsible for maintaining high security standards in the digital ecosystem. They implement cryptographic techniques to protect sensitive information and establish procedures for detecting, reporting, and responding to security incidents [13]. This includes the secure management and storage of cryptographic keys, employing advanced key management systems to prevent unauthorized access. QTSPs are also committed to data protection and privacy, adhering to regulations such as the General Data Protection Regulation (GDPR) [27]. QTSPs undergo regular audits and certifications by designated conformity assessment bodies. These assessments ensure continuous compliance with eIDAS requirements, security standards, and operational best practices, reinforcing their reliability and trustworthiness. QTSPs also provide comprehensive customer support and education, assisting users in understanding and effectively utilizing trust services. This includes offering guidance on the proper use of electronic signatures, addressing user inquiries, and providing training to ensure stakeholders can confidently engage in digital transactions. Ensuring that their services are recognized across all EU Member States, QTSPs facilitate secure and interoperable digital interactions among member states. This enables seamless cross-border electronic transactions within the EU, supporting the objectives of the Digital Single Market. However, QTSPs face several challenges and keeping up with new technologies, such as blockchain, AI, and quantum computing, with the latter one expected to impact trust services, is a significant concern. Their ongoing efforts are required to enhance security, support digital identity initiatives, and adapt to technological changes. This is critical for advancing the EU's objectives of a unified and secure digital single market.

1.3 QTSP Frameworks Overview Standards and regulations

1.3.1 Regulatory Framework and Standards

Central to this regulatory framework is the EN 319 series of standards developed by the European Telecommunications Standards Institute (ETSI), which define the technical and operational requirements for trust service providers [26]. Key role have the following standards: (i) EN 319 401, (ii) EN 319 411-1 and (iii) EN 319 411-2. EN 319 401 specifies general policy requirements for trust service providers setting the foundational principles and practices that QTSPs must implement, including security management, operational controls, and organizational policies. EN 319 411-1 outlines the general policy and security requirements for trust service providers issuing certificates. It focuses on ensuring that QTSPs implement well-defined security practices, maintain comprehensive documentation, and undergo regular audits to verify compliance. EN 319 411-2 builds upon this by detailing specific requirements for trust service providers issuing EU qualified certificates. These standards require stringent controls on cryptographic key management, incident response protocols, and regular security assessments to protect against potential threats. In addition to these, the EN 319 102 series provides guidelines for the creation and validation of Advanced Electronic Signatures (AdES), ensuring interoperability across different systems and platforms. EN 319 102-1 specifies the processes and technical specifications required for generating and verifying digital signatures to guarantee their authenticity and integrity. EN 319 102-2 defines the structure and content of signature validation reports, which are essential to verify the validity and reliability of digital signatures over time. These reports play a crucial role in maintaining the trustworthiness of digital transactions, particularly in long-term scenarios where certificates may expire or be revoked.

1.3.2 Infrastructure and Technologies

The QTSP infrastructure encompasses a range of technologies and processes designed to deliver services with high security and reliability. A central component of this infrastructure is the QSCDs, responsible for generating and managing the cryptographic keys used in digital signatures [11]. There are two primary types of QSCDs: (i) Hardware-Based Devices: e.g., smart cards or USB tokens used on-premises. These devices provide a secure environment for key storage and signature creation, physically held by users to prevent unauthorized access, (ii) Hardware Security Modules (HSMs) Offered as a Service: Integrated into secure environments within the QTSP's infrastructure and typically provided through a cloud-based subscription model. HSMs enable remote signing ca-

pabilities while ensuring the security of cryptographic keys in a controlled environment. Trust Lists are another critical component of the QTSP infrastructure. These are XML-formatted lists maintained by EU Member States, cataloging all qualified trust service providers and their respective services. Trust Lists serve as official registers that users and relying parties can consult to verify the authenticity and status of trust services, such as digital signatures, electronic seals, and timestamping services. By referencing these Trust Lists, stakeholders can ensure they are interacting with legitimate and compliant QTSPs. Integral to the issuance of qualified certificates are Identity Proofing Systems. These systems are responsible for verifying the identities of individuals or entities before issuing digital certificates, thereby preventing fraud and ensuring that only legitimate users receive trust services. Identity proofing typically involves a combination of in person verification, document authentication, and digital verification methods, adhering to the stringent requirements set forth by the eIDAS Regulation and the EN 319 standards. QTSPs are subject to regular audits conducted by accredited Conformity Assessment Bodies (CABs) to ensure ongoing compliance with regulatory standards. These audits assess various aspects of QTSP operations, including security measures, operational procedures, and adherence to documentation requirements. The audit process involves both document reviews and on-site evaluations, providing a comprehensive assessment of QTSP compliance with the required standards. Successful audits result in certification reports that confirm the compliance of QTSP and eligibility for inclusion in Trust Lists.

1.3.3 Integration of Blockchain Technology and eIDAS 2.0 Enhancements

The proposed eIDAS 2.0 regulation introduces significant enhancements, expanding the role of QTSPs and integrating emerging technologies like blockchain (Distributed Ledger Technology, DLT) into the trust services framework. Firstly, eIDAS 2.0 introduces trust services for electronic ledgers, recognizing DLT/blockchain technologies as legally admissible mechanisms to ensure the integrity and authenticity of data. QTSPs can provide qualified electronic ledger services, offering legally recognized proof of data integrity, timestamping, and sequencing of transactions without reliance on a centralized authority. This integration enables the creation of tamper-proof records and enhances transparency in digital transactions. Furthermore, QTSPs can offer qualified electronic archiving services, ensuring the long-term preservation and integrity of electronic data and documents. This is crucial for compliance with regulatory requirements that mandate the retention of records over extended periods. Using advanced cryptographic techniques and secure storage solutions, QTSPs can guarantee the authenticity

and availability of archived data. eIDAS 2.0 emphasizes the use of remote signature creation devices managed by QTSPs, facilitating the widespread adoption of electronic signatures without the need for physical devices. This aligns with the growing demand for user-friendly, mobile, and remote signing solutions. QTSPs ensure that remote signature services meet the same security and legal standards as traditional hardware-based signatures. QTSPs will also play a key role in supporting the EUDIW, a secure and user-centric digital wallet that allows citizens to store and manage their electronic identities and credentials on mobile devices. QTSPs may provide services related to identity verification, issuance of digital attributes, and authentication mechanisms compliant with the requirements of eIDAS and GDPR. This empowers users with greater control over their personal data and improves privacy.

1.3.4 Compliance with Additional Standards and Regulations

Beyond the ETSI EN 319 series, QTSPs must also consider other relevant standards and regulations that impact their operations. In this direction, compliance with GDPR is essential, as QTSPs handle personal data during identity verification and certificate issuance processes. QTSPs must implement appropriate technical and organizational measures to protect personal data, ensure lawful processing, and uphold the rights of data subjects. This includes data minimization, obtaining explicit consent, and ensuring data portability and erasure where applicable. Also, adoption of the ISO/IEC 27001 standard for Information Security Management Systems (ISMS) is common practice among QTSPs to ensure a robust security posture. This standard helps QTSPs implement comprehensive security controls and processes to protect sensitive information and manage risks effectively, aligning with eIDAS requirements for security and reliability. The European Committee for Standardization (CEN) develops standards that complement ETSI's work, particularly in areas like secure signature creation devices, decentralized identity management, and archiving services. Collaboration with international standardization efforts, such as those by the International Organization for Standardization (ISO), ensures global interoperability and adherence to best practices.

1.4 Opportunities and Challenges of Blockchain-Based Systems

Blockchain technology has emerged as a transformative solution that can enhance the security of the offered services in various sectors. Providing security for identity management can be no exception. The integration of blockchain-based identity management systems presents a plethora of opportunities while also introduces a set of challenges.

Understanding these is crucial for all the stakeholders in order to leverage blockchain's potential within the framework of the revised eIDAS 2.0 regulation. One of the foremost opportunities that blockchain-based identity management systems offer is enhanced security and trust. Blockchain's inherent characteristics - immutability, decentralization, and cryptographic security can provide a foundation for protecting digital identities against fraud and unauthorized access, while at the same time they can increase the scalability and automation of the process in a seamless way across different parties for various use-cases in different countries in the EU and worldwide. In the EU context particularly, where data protection and privacy are paramount under regulations (e.g., GDPR), blockchain can ensure that personal data is securely stored and managed. The decentralized nature of blockchain eliminates single points of failure, making it significantly more resistant to cyber-attacks compared to traditional centralized systems. Furthermore, the transparent and verifiable nature of blockchain transactions can enhance the trust among users and service providers, as all identity-related actions are recorded in an immutable ledger that can be audited independently. Another significant opportunity lies in the facilitation of interoperability and cross-border recognition of digital identities. The EU's digital single market initiative [23] aims to enable seamless digital interactions across member states. An identity system that is based on blockchain can bridge the gaps between the heterogeneous national eID schemes and provide a unified and interoperable platform for identity verification. This is crucial as it simplifies the administrative process for individuals and businesses across EU, which can enhance the digital economy. More importantly, users can have greater control of their personal data, managing their own digital identities without relying on centralized authorities. This is needed in WEB 3.0/ WEB 4.0 targets which emphasizes on user empowerment and data sovereignty. Through blockchain, the creation of Decentralized Identifiers (DIDs) [24] can be facilitated. This enhances privacy and reduces the risk of data exposure, as the owner of the DID selects what exactly information to share and with whom. In their systematic review, the authors of [9] highlight the evolution of digital identity management from centralized to decentralized approaches. They emphasize the emergence of Self-Sovereign Identity (SSI) systems that leverage DIDs and Verifiable Credentials (VCs), standardized by the World Wide Web Consortium (W3C). This review provides a comprehensive overview of how blockchain and DIDs contribute to more secure and decentralized digital identity systems, which significantly strengthen the security of communications involving distributed participants. Additionally, the scope of DIDs and VCs extends beyond individuals to include a broad range of entities such as cloud services, edge computing resources, and Internet of Things (IoT) de-

vices. However, due to their novelty, existing literature lacks a comprehensive survey on the application of DIDs and VCs across different domains beyond SSI systems. Despite these promising opportunities, blockchain-based identity management systems in the EU face several challenges that must be addressed to realize their full potential. One of the primary challenges is ensuring compliance with eIDAS 2.0 and GDPR. While blockchain offers enhanced security and privacy features, aligning these with the stringent EU regulations requires careful consideration of data protection mechanisms. The immutability of blockchain records poses a particular challenge in this regard, as it conflicts with GDPR's requirement to allow individuals to request the deletion or rectification of their personal data. Solutions, such as off-chain storage combined with on-chain references or advanced cryptographic techniques, are necessary to reconcile blockchain's permanence with regulatory demands for data erasure and correction. Additionally, the eIDAS Regulation is closely related to SSI and DIDs within the European Union's digital ecosystem. SSI is an innovative approach that allows users to create and manage their own digital identities independently of centralized authorities, utilizing DIDs as unique, user-controlled identifiers [5]. These DIDs, as defined by the W3C, are fully under the control of the DID subject and are not dependent on any centralized registry, identity provider, or certificate authority. By leveraging VCs, SSI enables users to selectively disclose specific pieces of information to third parties, thereby enhancing privacy and reinforcing personal data protection [6]. The eIDAS Regulation facilitates this decentralized identity management by providing a robust trust framework that ensures cross-border interoperability and legal recognition of digital identities and electronic documents [28]. This integration allows DIDs to be linked with traditional electronic identification methods, such as notified eID schemes and qualified electronic certificates, thereby enabling secure and seamless electronic interactions across EU member states. Furthermore, eIDAS supports the implementation of Distributed Ledgers and blockchain technologies to maintain the registry of DIDs, as proposed by the Decentralised Identity Foundation (DIF). However, the convergence of DIDs with the eIDAS framework introduces challenges, including technical limitations related to scalability and interoperability, as well as privacy concerns regarding the linkage between DIDs and electronic certificates. The eIDAS-supported SSI framework addresses these issues by establishing standardized protocols and leveraging trusted service providers and identity providers to create secure and verifiable identity assertions without necessitating prior relationships between parties [9]. Overall, the eIDAS Regulation significantly advances the goals of user empowerment and data sovereignty, fostering a more secure, private, and legally enforceable digital identity ecosystem within the EU. Another significant challenge is how

to achieve interoperability between blockchain-based identity systems and existing national eID schemes. The diversity of technologies, standards, and protocols employed across EU member states complicate the seamless integration of blockchain solutions. Therefore, it is essential to establish unified and technological agnostic technical standards and frameworks to facilitate the interoperability in a concrete way. Additionally, the scalability of blockchain networks to handle the vast number of identity transactions required across the EU is a critical concern. Ensuring that blockchain systems can operate efficiently and cost-effectively at scale without compromising security or performance is vital for their adoption. While blockchain-based identity management systems offer enhanced security and user control, attracting people and widespread acceptance required a lot of steps. Education and transparent communication so as people familiarize with the way these new technologies work and safeguard their personal data is needed.

2 Technical feasibility

2.1 Blockchain and QTSPs

Blockchain technology can be particularly advantageous for QTSPs, which by integrating blockchain technology into the existing frameworks can offer enhanced services that improve the security, transparency, and operational efficiency of trust services [20]. Blockchain's decentralized architecture and intrinsic characteristics such as immutability, and ability to facilitate trustless transactions make it a compelling addition to traditional QTSP infrastructure [31]. QTSPs can leverage the decentralize nature of blockchains to enhance their processes regarding the availability and security of their services. Offering trust services and relying on a few selected (computing) nodes can be a central point of failure which can impact the security and the availability of the offered services [7]. Leveraging a blockchain network with many nodes this risk can be significantly eliminated, while at the same time the security of the enhanced services especially against cyber-attacks is enhanced. What is more, in the current system, certificate issuance, verification, and revocation are managed by a central entity. If these processes are performed in a decentralized manner through the use of blockchain, each certificate issuance event will be recorded as an immutable transaction on the blockchain. This will increase the trustworthiness and reliability of the digital signature process with a transparent and tamper-proof history of all issued certificates. One other advantage of relying on blockchain is the automation through the use of Smart Contracts which improve the efficiency and

trustworthiness of the process. Smart Contracts are self-executing contracts with the terms directly written into code, can handle certificate issuance upon successful identity verification, automate renewal processes, and manage certificate revocation in real-time. This automation minimizes human error, ensures consistent adherence to predefined policies, and accelerates the certificate management lifecycle. Furthermore, by performing continuous audits on smart contracts on publicly available (open-source code) enhances the trustworthiness and familiarization of the users through on chain transparency. Another critical enhancement provided by blockchain is the creation of immutable audit trails. Blockchain's inherent immutability ensures that all digital signature transactions are permanently recorded and cannot be altered retroactively. This feature provides a reliable and verifiable audit trail for compliance purposes, simplifying regulatory reporting and enhancing accountability. Auditors and stakeholders can independently verify the authenticity and integrity of digital signatures without relying solely on QTSP-provided records, thereby increasing further the transparency and trust in the system. The transparent nature of blockchain hence makes easier the detection of fraudulent activities, as any unauthorized changes to digital signatures can be quickly identified and addressed, which can be performed in automated manner leveraging Machine Learning and creating automated tools that can detect such evens. This software could operate in the same way the antivirus is used in the PC to protect from viruses. Moreover, blockchain inherently employs cryptographic techniques to secure data, which can be leveraged to enhance the security of private key management within QTSP frameworks [21]. In traditional systems, private keys are typically stored in centralized repositories, making them vulnerable to breaches and unauthorized access. In contrast, blockchain enables distributed key management, where private keys can be securely stored across multiple nodes, significantly reducing the risk of a single point of compromise. This distributed approach not only enhances the security of private keys but also allows for the implementation of multi-signature schemes. Multi-signature schemes require multiple approvals for sensitive operations, thereby further strengthening security and ensuring that no single entity has unilateral control over critical processes. This key management approach mitigates the risks associated with centralized storage and provides an additional layer of security against potential attacks. Blockchain can also enhance the services offered through Public Key Infrastructure (PKI) as both pivotal technologies in the realm of digital trust [21], each addressing distinct aspects of security and authentication. PKI is fundamentally designed to encrypt communications and authenticate the origin of digital messages through asymmetric encryption, utilizing a pair of public and private keys. This makes PKI highly effective for securing email communications,

digital signatures, and establishing trusted connections between entities and is used by QTSPs. However, PKI relies on centralized Certificate Authorities (CAs), which can be single points of failure and targets for cyberattacks. In contrast, blockchain offers a decentralized and immutable ledger for recording transactions, ensuring that once data is entered, it cannot be altered or deleted. This characteristic makes blockchain ideal for applications requiring transparent and tamper-proof record-keeping, such as digital identity verification, supply chain tracking, and smart contracts. Unlike PKI, blockchain does not necessitate a centralized authority, reducing the risks associated with single points of failure and enhancing system resilience. While PKI excels in securing communications and providing authenticated identities, blockchain enhances transparency and immutability, making it suitable for decentralized trust systems. This complementary approach enables QTSPs to offer comprehensive security solutions that address a broader spectrum of digital trust needs, from secure communications to transparent and decentralized identity management [16]. Incorporating blockchain into QTSP infrastructures presents numerous challenges that must be effectively resolved. The primary issue to address is the interoperability between blockchain platforms and current QTSP systems. For seamless integration, it is crucial to develop standardized APIs and middleware solutions that enable effective communication between various systems, thus allowing blockchain to effectively augment conventional certificate management processes. Additionally, scalability and performance are vital considerations, as blockchain networks need to handle the high transaction volumes typical in digital signature operations without degrading performance. Strategies such as implementing Layer 2 scaling solutions, including state channels or sidechains, and optimizing consensus mechanisms are critical to improving blockchain scalability and maintaining efficient performance. Regulatory and compliance issues introduce additional complexity. Blockchain's unchangeable nature can conflict with regulations like GDPR, which requires personal data to be deleted or anonymized upon request. To address this, QTSPs can utilize hybrid solutions that integrate both on-chain and off-chain data storage, allowing personal data to be erased or anonymized while preserving the blockchain ledger's integrity. Achieving this balance is crucial for staying compliant while harnessing blockchain's security advantages. Furthermore, public blockchain systems are not immune to security risks such as 51% attacks or smart contract exploits. Implementing robust security measures, including regular security audits, secure smart contract development practices, and consensus mechanism enhancements, is essential to protect against these vulnerabilities. Continuous monitoring and updating of security protocols can help QTSPs stay ahead of potential threats and maintain the integrity of their

blockchain-integrated digital signature management systems. Despite these challenges, the integration of blockchain technology into QTSP frameworks offers a transformative opportunity to enhance the security, transparency, and efficiency of digital signature management. By addressing technical, regulatory, and operational challenges through strategic planning, security measures, and adherence to regulatory standards, QTSPs can leverage blockchain technology to meet the evolving demands of the digital economy, ensuring secure, transparent, and efficient digital signature services across the European Union.

2.2 Alignment with ETSI Standards

The integration of blockchain technology into QTSP frameworks requires adherence to standards to ensure compliance, interoperability, and security. Aligning with these standards not only ensures that blockchain-based trust services meet stringent regulatory requirements but also leverages the inherent strengths of blockchain technology to enhance the overall reliability and efficiency of QTSP operations. This section identifies the relevant standards, corrects any inaccuracies, and explains how blockchain integration aligns with these standards, highlighting compliance measures and the added value brought about by blockchain technologies.

2.2.1 Overview of Relevant ETSI Standards

Several standards are relevant for the operation and integration of trust services within the EU framework, especially with respect to blockchain integration into QTSPs. The key standards are as follows:

ETSI EN 319 401 [ref35] *Electronic Signatures and Infrastructures; General Policy Requirements for Trust Service Providers.*

This standard specifies general policy requirements for TSPs. It establishes the foundational principles and practices that TSPs must implement to ensure the trustworthiness of their services. It covers aspects such as organizational structure, information security management, operational controls, and risk assessment. It serves as a baseline for TSPs to align their policies and procedures with recognized criteria, fostering trust among users and relying parties.

ETSI EN 319 411-1 [ref5] *Electronic Signatures and Infrastructures; Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 1: General Requirements.*

This standard outlines the policy and security requirements for TSPs issuing certificates, focusing on general requirements applicable to all types of certificates. It addresses aspects such as Certificate Authority (CA) management, certificate lifecycle operations, repository and database security, and environmental controls. The standard ensures that TSPs maintain high levels of security and reliability in their certificate issuance processes, thereby supporting trust in electronic transactions.

ETSI EN 319 411-2 [ref6] *Electronic Signatures and Infrastructures; Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 2: Requirements for Trust Service Providers Issuing EU Qualified Certificates.*

Building upon Part 1, this standard specifies additional policy and security requirements for TSPs issuing qualified certificates in accordance with the eIDAS Regulation. It includes stringent controls on identity verification, certificate issuance and management, cryptographic key generation and protection, and the use of Qualified Signature Creation Devices (QSCDs). The standard ensures that qualified certificates meet the highest legal and security requirements within the EU.

ETSI EN 319 412 Series [ref36, ref37, ref38] *Electronic Signatures and Infrastructures; Certificate Profiles.*

The EN 319 412 series defines profiles for public key certificates issued by TSPs. The series comprises several parts:

(i) **Part 1**: Overview and Common Data Structures.

(ii) **Part 2**: Certificate Profile for Certificates Issued to Natural Persons.

(iii) **Part 3**: Certificate Profile for Certificates Issued to Legal Persons.

(iv) **Part 4**: Certificate Profile for Web Site Certificates.

(v) **Part 5**: QCStatements, which includes the Qualified Certificate Statements indicating compliance with eIDAS requirements.

These profiles ensure interoperability and compliance with regulatory requirements across different types of certificates.

ETSI EN 319 102-1 [ref39] *Electronic Signatures and Infrastructures; Procedures for Creation and Validation of Advanced Electronic Signatures (AdES); Part 1: Creation and Validation.*

This Technical Specification specifies procedures for the creation and validation of Advanced Electronic Signatures (AdES) and Advanced Electronic Seals (AdES) that are compliant with the eIDAS Regulation. It covers various signature formats such as XAdES (XML Advanced Electronic Signatures), CAdES (CMS Advanced Electronic Signatures), PAdES (PDF Advanced Electronic Signatures), and ASiC (Associated Signature Containers). The standard provides guidelines on how to produce and validate digital signatures to ensure their legal validity and technical interoperability.

ETSI EN 319 102-2 [ref40] *Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of Advanced Electronic Signatures (AdES); Part 2: Signature Validation Reports.*

This specification defines the structure and content of signature validation reports, which are essential for verifying the validity and reliability of digital signatures over time. These reports play a crucial role in maintaining the trustworthiness of digital transactions, particularly in long-term scenarios where certificates may expire or be revoked.

ETSI TS 119 461 [ref41] *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Electronic Registered Delivery Service Providers.*

This standard specifies policy and security requirements for providers of Electronic Registered Delivery Services (ERDS). It ensures that such services offer reliable and secure methods for the transmission of electronic data between parties, with legal equivalence to traditional registered mail.

ETSI TS 119 495 [ref40] *Electronic Signatures and Infrastructures; Sector Specific Requirements; Identity Proofing.*

This Technical Specification outlines requirements for TSPs that provide identity proofing services as part of remote or face-to-face identity verification processes. It details methods for verifying the identity of individuals or legal entities before issuing certificates or other trust services. The standard emphasizes security and reliability in identity proofing, including procedures for document verification, biometric checks, and data validation, ensuring compliance with legal obligations and reducing the risk of fraud.

ETSI TS 119 512 [ref42] *Electronic Signatures and Infrastructures; Cryptographic Suites.*

This standard specifies cryptographic suites for securing trust services, including

digital signatures, seals, and timestamps. It ensures that cryptographic algorithms and key lengths meet current security requirements and are resistant to known attacks.

ISO 22739:2020 [ref43] *Blockchain and Distributed Ledger Technologies — Vocabulary.*

This International Standard defines a set of terms and definitions for blockchain and Distributed Ledger Technologies. Establishing a common vocabulary ensures consistent understanding and communication among stakeholders, including developers, regulators, and users.

ISO 23257:2022 [ref44] *Blockchain and Distributed Ledger Technologies — Reference Architecture.*

This International Standard specifies a reference architecture for blockchain and DLT systems. It provides a generic framework that describes the components, functionalities, and relationships within a blockchain network. The standard assists organizations in designing and evaluating blockchain solutions by offering a structured approach to architecture development, ensuring interoperability and alignment with business requirements.

ISO/TR 23455:2019 [ref45] *Blockchain and Distributed Ledger Technologies — Overview of and Interactions Between Smart Contracts in Blockchain and Distributed Ledger Technology Systems.*

This Technical Report provides an overview of smart contracts in blockchain systems, including their characteristics, interactions, and potential use cases. It assists in understanding how smart contracts can be utilized within trust services to automate processes and enforce agreements.

ISO/TR 23244:2020 [ref46] *Blockchain and Distributed Ledger Technologies — Privacy and Personally Identifiable Information Protection Considerations.*

This Technical Report addresses privacy and Personally Identifiable Information (PII) protection in the context of blockchain and DLTs. It analyzes how blockchain technologies interact with privacy regulations like the GDPR. The report provides guidance on designing and implementing blockchain systems that comply with privacy requirements.

ISO/TR 23576:2020 [ref47] *Blockchain and Distributed Ledger Technologies — Security Management of Digital Asset Custodians.*

This Technical Report provides guidance on the security management of digital asset custodians operating in blockchain environments. It outlines best practices for safeguarding digital assets, focusing on risk management, access control, key management, and incident response.

DIN TS 31648:2021 [ref48] *Criteria for Trusted Transactions—Records Management and Preservation of Evidence in DLT/Blockchain.*

This German Technical Specification provides criteria for trustworthy digital transactions using blockchain technology, focusing on records management and the preservation of evidence. It outlines requirements for ensuring the authenticity, integrity, and reliability of records stored on DLT systems, aligning with legal and regulatory obligations.

2.2.2 Mapping Blockchain Integration to ETSI Standards

Table 1 provides a detailed mapping of the proposed blockchain integration strategies to the relevant ETSI standards, demonstrating compliance and improvement of the functionality of trust services.

Table 1. Mapping Blockchain Integration to ETSI and ISO Standards

Document Section	Relevant Standards	Alignment Description
Policy and Security Requirements	**ETSI Standards:** - ETSI EN 319 401 [**ref35**] - ETSI EN 319 411-1 [**ref5**] - ETSI EN 319 411-2 [**ref6**] **ISO Standards:** - ISO/IEC 27001 [**ref43**] - ISO 22739:2020 [**ref44**]	**ETSI EN 319 401**: Blockchain's immutable ledger can enhance trustworthiness, aligning with general policy requirements for TSPs. **ETSI EN 319 411-1/2**: Ensuring that blockchain-based services comply with security requirements for certificate issuance and management. **ISO/IEC 27001**: Integration of blockchain within an Information Security Management System (ISMS) ensures effective risk management and security controls. **ISO 22739:2020**: Utilizing standardized blockchain terminology ensures clarity and consistency in policy documentation and communications.
Certificate Issuance and Management	**ETSI Standards:** - ETSI EN 319 411-1 [**ref5**] - ETSI EN 319 411-2 [**ref6**] - ETSI EN 319 412 series [**ref36**, **ref37**, **ref38**] **ISO Standards:** - ISO 23257:2022 [**ref45**]	**ETSI EN 319 411-1/2**: Blockchain can enhance the integrity and transparency of certificate issuance and management processes, ensuring compliance with general and specific requirements. **ETSI EN 319 412 series**: Certificates issued via blockchain can conform to standardized profiles, ensuring interoperability and legal recognition. **ISO 23257:2022**: Provides a reference architecture for integrating blockchain into certificate management systems, aiding in designing effective QTSP architectures that incorporate DLTs.

Continued on next page

Table 1 – Continued from previous page

Document Section	Relevant Standards	Alignment Description
Electronic Signatures and Seals	**ETSI Standards:** - ETSI EN 319 102-1 [**ref39**] - ETSI EN 319 102-2 [**ref40**] - ETSI EN 319 411-1 [**ref5**] - ETSI EN 319 411-2 [**ref6**] **ISO Standards:** - ISO/TR 23455:2019 [**ref46**]	**ETSI EN 319 102-1/2**: Blockchain supports the creation and validation of AdES and Seals by providing tamper-evident storage and verification mechanisms. **ETSI EN 319 411-1/2**: Enhances security measures for electronic signatures and seals through blockchain's cryptographic capabilities. **ISO/TR 23455:2019**: Offers guidance on smart contracts, which can automate signature validation processes within blockchain, enhancing efficiency while maintaining compliance with legal and technical standards.
Identity Proofing and Verification	**ETSI Standards:** - ETSI TS 119 495 [**ref47**] **ISO Standards:** - ISO/TR 23244:2020 [**ref48**]	**ETSI TS 119 495**: Blockchain-based decentralized identity solutions can align with identity proofing requirements, enhancing security and user control. **ISO/TR 23244:2020**: Addresses privacy and PII protection in blockchain systems, ensuring compliance with GDPR when integrating blockchain into identity proofing processes.
Time-Stamping Services	**ETSI Standards:** - ETSI EN 319 421 [**ref49**] **ISO Standards:** - ISO 22739:2020 [**ref44**]	**ETSI EN 319 421**: Blockchain's inherent timestamping capabilities align with requirements for trusted time-stamping services, providing immutable and verifiable timestamps. **ISO 22739:2020**: Standardized blockchain terminology ensures clarity in documenting time-stamping services and related processes.

Continued on next page

Table 1 – Continued from previous page

Document Section	Relevant Standards	Alignment Description
Privacy and Identity Management	**ETSI Standards:** - ETSI TS 119 495 [**ref47**] **ISO Standards:** - ISO/TR 23244:2020 [**ref48**]	**ETSI TS 119 495**: Emphasizes security and reliability in identity proofing, which can be enhanced by blockchain's features. **ISO/TR 23244:2020**: Addresses privacy and PII protection in blockchain systems, ensuring GDPR compliance when integrating blockchain into identity proofing processes.
Security Framework and Controls for DLT	**ISO Standards:** - ISO/IEC 27001 [**ref43**]	**ISO/IEC 27001**: Implementing blockchain must align with established Information Security Management System standards, ensuring effective risk management, access control, and security measures for blockchain implementations within QTSP infrastructures.
Certificate Profiles	**ETSI Standards:** - ETSI EN 319 412 series [**ref36**, **ref37**, **ref38**] **ISO Standards:** - ISO 22739:2020 [**ref44**]	**ETSI EN 319 412 series**: Ensures that blockchain-based certificates conform to standardized profiles for interoperability and compliance. **ISO 22739:2020**: Utilizing standardized blockchain terminology ensures clarity in certificate profiles and related documentation within blockchain environments, promoting consistency among stakeholders.
Records Management and Preservation	**ISO Standards:** - DIN TS 31648:2021 [**ref50**]	**DIN TS 31648:2021**: Provides criteria for trustworthy digital transactions using blockchain, focusing on records management and preservation of evidence. Integrating blockchain enhances the authenticity, integrity, and reliability of records, aligning with legal and regulatory obligations.

2.2.3 Detailed Alignment with Key Standards

The integration of blockchain technology into QTSPs requires meticulous alignment with established policy and security standards to ensure the delivery of secure, reliable and compliant trust services. In this section, we present the primary integration points where the blockchain technology can be embedded within QTSP frameworks with regard to the eIDAS use cases and showing how blockchain integration aligns with ETSI and ISO standards presented in Table 1.

Policy and Security Requirements Integrating blockchain technology into QTSPs necessitates adherence to established policy and security standards to ensure secure, reliable, and compliant trust services. Key standards governing these requirements include ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ISO/IEC 27001, and ISO/IEC 27002. ETSI EN 319 401 sets the general policy requirements for TSPs, emphasizing robust security measures, effective risk management, and strict regulatory compliance. It outlines essential organizational and technical measures, such as information security management, operational controls, incident management, and business continuity, establishing a foundational framework for TSPs to foster trust among users and relying parties. Building upon these general requirements, ETSI EN 319 411-1 and ETSI EN 319 411-2 specify the policy and security requirements for TSPs issuing digital certificates, including EU Qualified Certificates. ETSI EN 319 411-1 addresses general requirements applicable to all certificates, ensuring high levels of security and reliability in certificate issuance processes. ETSI EN 319 411-2 extends these requirements specifically for EU Qualified Certificates, introducing additional controls on identity verification, certificate management, cryptographic key protection, and the use of QSCDs, ensuring compliance with the eIDAS Regulation. Complementing the ETSI standards, ISO/IEC 27001 provides a comprehensive framework for establishing, implementing, maintaining, and continuously improving an Information Security Management System. ISO/IEC 27002 offers detailed guidelines for information security controls, assisting organizations in selecting and implementing appropriate security measures based on their specific risk environments. Blockchain integration enhances these policy and security requirements in several ways. The decentralized and immutable nature of blockchain introduces robust security measures by ensuring that all transactions are secure, tamper-proof, and verifiable, aligning with the stringent security controls mandated by ETSI and ISO standards. Additionally, blockchain's architecture reduces single points of failure, significantly lowering the risk of data breaches and unauthorized alterations, which aligns with the risk management protocols outlined in ISO/IEC 27001. Furthermore, blockchain's

transparent and immutable records facilitate detailed audit trails, crucial for compliance with regulatory standards and security examinations as specified in ETSI EN 319 401 and ISO/IEC 27002. This transparency enhances accountability and trustworthiness, enabling QTSPs to demonstrate compliance and maintain high standards of security and reliability.

Certificate Issuance and Management Blockchain technology necessitates strict alignment with established standards to ensure secure, reliable, and interoperable certificate issuance and management. Key standards governing this area include ETSI EN 319 411-1, ETSI EN 319 411-2, the ETSI EN 319 412 Series, and ISO/IEC 9594-8:2017. ETSI EN 319 411-1 and ETSI EN 319 411-2 outline comprehensive policy and security requirements for TSPs issuing digital certificates, with Part 1 addressing general requirements applicable to all certificate types and Part 2 specifying additional requirements for issuing EU Qualified Certificates in compliance with the eIDAS Regulation. The ETSI EN 319 412 Series defines standardized profiles for public key certificates, ensuring uniform formats and interoperability across different systems and jurisdictions. Meanwhile, ISO/IEC 9594-8:2017 provides frameworks for public-key and attribute certificates, supporting the structural integrity and interoperability of digital certificates within global directories. Blockchain integration enhances these standards by enabling decentralized and automated certificate management through smart contracts. This automation streamlines processes such as issuance, renewal, and revocation, eliminating the need for intermediary intervention and reducing potential points of failure. Each certificate transaction is immutably recorded on the blockchain ledger, ensuring a tamper-proof audit trail that enhances trust and accountability. Furthermore, smart contracts enforce compliance with the certificate profiles defined in the ETSI EN 319 412 Series and ISO/IEC 9594-8:2017, ensuring that all certificates adhere to standardized formats and regulatory requirements. This alignment facilitates mutual recognition of digital trust services across EU member states and internationally, promoting seamless interoperability and enhancing the reliability of digital transactions. By leveraging blockchain technology, QTSPs can not only comply with stringent policy and security standards but also improve the efficiency and resilience of their certificate issuance and management processes, thereby fostering greater confidence among users and relying parties within the European Union's digital ecosystem.

Electronic Signatures and Seals QTSPs that leverage blockchain technology can enhance the creation, validation, and long-term management of electronic signatures and seals by aligning with key standards such as ETSI EN 319 102-1, ETSI EN 319 102-2, and the

ISO 14533 Series. ETSI EN 319 102-1 and ETSI EN 319 102-2 establish the procedures for creating and validating Advanced Electronic Signatures and Advanced Electronic Seals, ensuring their legal validity and technical interoperability. The ISO 14533 Series further defines processes for long-term authentication, crucial for maintaining the integrity and validity of electronic signatures over extended periods. Blockchain technology significantly enhances these standards through several key mechanisms: First it provides a decentralized and immutable ledger for storing electronic signatures and seals. Each signature is time-stamped and cryptographically linked within the blockchain, ensuring that signatures are tamper-proof and easily verifiable. This secure storage aligns with the procedural requirements of ETSI EN 319 102-1 and ETSI EN 319 102-2, guaranteeing the authenticity and integrity of electronic signatures. The permanent and unalterable nature of blockchain records supports long-term validation of electronic signatures. By preserving verification data in a tamper-proof manner, blockchain ensures that signatures remain valid and trustworthy over time, fulfilling the requirements set forth by the ISO 14533 Series for maintaining signature integrity and reliability. Also blockchain eliminates the need for centralized validation authorities by distributing trust across a network of nodes. This decentralization enhances resilience against cyberattacks and unauthorized access, ensuring continuous and reliable validation of electronic signatures. Such distributed validation aligns with the security measures advocated by ETSI EN 319 102-1, reinforcing the robustness and trustworthiness of electronic signature services.

Identity Proofing and Verification Integrating blockchain technology into QTSPs aligns seamlessly with key standards such as ETSI TS 119 495 and ISO/IEC 29003:2018, which establish comprehensive requirements and guidelines for secure and reliable identity proofing processes. These standards emphasize the necessity of robust verification methods and the stringent protection of personal data, ensuring that identity proofing services are both secure and compliant with regulatory frameworks. Blockchain enhances identity proofing and verification through decentralized identity management by utilizing DIDs and VCs. This decentralized approach empowers individuals to control their digital identities without relying on centralized authorities, thereby reducing vulnerabilities associated with centralized identity repositories. Additionally, blockchain technology supports privacy enhancement through cryptographic proofs, such as zero-knowledge proofs. These techniques allow individuals to prove specific identity attributes without revealing sensitive personal data, ensuring compliance with the GDPR and other privacy standards. Moreover, blockchain facilitates secure attribute verification by ensuring that identity attributes are securely stored and easily verifiable on the

blockchain. This guarantees the integrity and authenticity of identity information, fully complying with the requirements set forth by ETSI TS 119 495 and ISO/IEC 29003:2018. The immutable and transparent nature of blockchain records ensures that all identity verification processes are tamper-proof and auditable, thereby enhancing the overall reliability and trustworthiness of identity proofing services.

Time-Stamping Services The blockchain technology can enhance time-stamping services by aligning with key standards such as ETSI EN 319 421 and the ISO/IEC 18014 Series. ETSI EN 319 421 outlines the policy and security requirements for Trust Service Providers issuing time-stamps, emphasizing the need for accurate time synchronization, protection against forgery and manipulation, and robust audit and verification capabilities. The ISO/IEC 18014 Series complements these requirements by providing a comprehensive framework for time-stamping services, detailing mechanisms for generating independent and linked time-stamp tokens and establishing traceable time sources to ensure the integrity and precision of time-stamps in electronic transactions. Blockchain integration enhances these time-stamping services through several key mechanisms. Each blockchain transaction is inherently time-stamped and recorded immutably on the blockchain ledger, ensuring that records are both accurate and tamper-proof. This immutability aligns with the stringent requirements of ETSI EN 319 421 and the ISO/IEC 18014 Series, guaranteeing that time-stamps cannot be altered or falsified once recorded. Additionally, the consensus mechanisms employed by blockchain networks ensure synchronization across all participating nodes, maintaining consistent and reliable time-stamping across the entire network. This synchronization is crucial for meeting the accuracy and reliability standards specified by both ETSI and ISO. Furthermore, the transparent nature of blockchain ledgers facilitates comprehensive auditability. Each time-stamp can be independently verified by any authorized party, enhancing the trustworthiness of the time-stamping services provided by QTSPs. The ability to independently audit and verify time-stamps without relying on a centralized authority ensures that the integrity of time-stamped records is maintained, thereby fulfilling the audit and compliance requirements outlined in ETSI EN 319 421 and the ISO/IEC 18014 Series. By leveraging blockchain technology, QTSPs can deliver time-stamping services that are not only compliant with established standards but also offer enhanced security, accuracy, and transparency.

Privacy and Identity Management Integrating blockchain technology into QTSPs requires strict adherence to established privacy standards to ensure the protection of Personally Identifiable Information (PII). The relevant standards in this context include

ISO/IEC 29100:2011, which establishes a comprehensive privacy framework for PII protection, and ISO/TR 23244:2020, which specifically addresses privacy considerations within blockchain and Distributed Ledger Technologies (DLT) environments. ISO/IEC 29100:2011 outlines fundamental privacy principles and guidelines for implementing effective privacy controls, ensuring that organizations handle PII in a manner that respects individuals' privacy rights. ISO/TR 23244:2020 further refines these principles by focusing on the unique privacy challenges and considerations associated with blockchain technologies, providing guidance on how to protect PII within decentralized and immutable ledger systems. Blockchain integration enhances privacy and identity management through the implementation of privacy-preserving techniques such as zero-knowledge proofs and selective disclosure. These methods enable the verification of identity attributes without exposing sensitive personal data, thereby aligning with privacy principles and regulatory requirements like the GDPR. Additionally, decentralized identity solutions empowered by blockchain technology allow users to have greater control over their personal data, enabling them to manage and share their information securely and selectively. This user-centric approach not only enhances data privacy but also ensures compliance with stringent data protection laws by minimizing data exposure and increasing transparency in data handling processes.

Security Framework and Controls for DLT A security framework is also required to address the unique risks and vulnerabilities associated with DLTs. Key standards guiding this integration include ISO/TR 23245:2021 and ISO/IEC 27001. ISO/TR 23245:2021 provides comprehensive guidance on identifying and mitigating security risks, threats, and vulnerabilities specific to blockchain environments. It outlines best practices for securing blockchain implementations, addressing areas such as cryptographic security, network protection, and safeguarding against common DLT threats like 51% attacks and smart contract exploits. ISO/IEC 27001 complements this by establishing the requirements for an effective Information Security Management System. This standard ensures that organizations implement systematic processes for managing sensitive information, maintaining confidentiality, integrity, and availability through a risk-based approach. Blockchain integration enhances the security framework and controls for QTSPs by implementing advanced cryptographic algorithms and secure consensus mechanisms. These measures are fundamental in protecting against common DLT threats, ensuring that data transactions are both secure and verifiable. The use of robust cryptographic techniques, such as elliptic curve cryptography and hashing algorithms, safeguards the integrity and confidentiality of data stored on the blockchain. Additionally, secure consensus mechanisms like Proof of Stake (PoS) or Byzantine Fault Tolerance

(BFT) enhance the resilience of the blockchain network, preventing unauthorized transaction validations and ensuring network stability. Risk management is further strengthened through regular security assessments and continuous monitoring, aligning with the practices outlined in ISO/IEC 27001. By conducting periodic vulnerability assessments and penetration testing, QTSPs can proactively identify and mitigate potential security weaknesses within their blockchain implementations. Continuous monitoring tools enable real-time detection of suspicious activities and potential breaches, facilitating swift incident response and minimizing the impact of security threats. This proactive approach to risk management ensures that QTSPs maintain a high level of security posture, adhering to both ISO/TR 23245:2021 and ISO/IEC 27001 standards. Furthermore, the integration of blockchain technologies into the organization's overall ISMS framework ensures a cohesive and comprehensive approach to information security. By embedding blockchain security measures within the ISMS, QTSPs can ensure that all aspects of their blockchain operations are governed by standardized security policies and procedures. This integration supports the alignment of blockchain-specific security controls with the broader organizational security objectives, fostering a unified strategy for managing information security risks. As a result, QTSPs can achieve enhanced protection of their digital trust services, ensuring compliance with international best practices and maintaining the trust of their stakeholders.

Interoperability Framework The key standard governing this area is ISO 23257:2022, which provides a comprehensive reference architecture for blockchain and DLTs. This standard promotes interoperability and standardization by outlining the essential components, functionalities, and relationships within blockchain systems, thereby facilitating the design of compatible and scalable blockchain solutions. Blockchain integration aligns with ISO 23257:2022 by adopting a standardized design approach, which ensures that blockchain solutions are developed based on recognized architectural frameworks. This standardized design guarantees compatibility with existing systems and networks, enabling QTSPs to integrate blockchain technologies without disrupting their current operations. Furthermore, the creation of standardized Application Programming Interfaces (APIs) and middleware solutions is critical for enabling effective communication across different blockchain platforms and legacy systems. By establishing uniform interfaces, QTSPs can facilitate smooth data exchange and interoperability, reducing integration complexities and enhancing overall system efficiency. Additionally, blockchain technology supports the development of cross-border services, which is essential for the harmonization of digital trust services within the European Union and on a global scale. The standardized reference architecture provided by ISO 23257:2022 ensures that

blockchain-enabled trust services are scalable and flexible, capable of adapting to varying regulatory and operational requirements across different jurisdictions. This harmonization not only enhances the scalability and flexibility of QTSP operations but also promotes mutual recognition of digital trust services, thereby fostering a more unified and efficient Digital Single Market. Using standardized architectures, APIs, and middleware solutions, QTSPs can effectively implement blockchain technologies that are interoperable, scalable, and compliant with international standards, thus supporting the seamless operation of digital trust services across borders.

Certificate Profiles: The relevant standards in this context are the ETSI EN 319 412 Series and ISO/IEC 9594-8:2017. The ETSI EN 319 412 Series defines comprehensive profiles for certificates issued by TSPs ensuring that these certificates meet uniform formats and interoperability requirements essential for seamless integration within the European Union's digital ecosystem. This series covers various aspects of certificate profiles, including the structure, data elements, and validation mechanisms necessary for maintaining consistency and reliability in digital trust services. Complementing the ETSI standards, ISO/IEC 9594-8:2017 provides a robust framework for public-key and attribute certificates, outlining the foundational structures and protocols required for effective certificate management. This standard ensures that PKIs and attribute-based access controls are implemented consistently, facilitating the secure issuance, management, and validation of digital certificates across different platforms and organizations. Blockchain integration enhances compliance with these certificate profiling standards by enabling the design of blockchain-based certificates that conform to the standardized profiles defined in the ETSI EN 319 412 Series and ISO/IEC 9594-8:2017. By adhering to these profiles, blockchain-based certificates gain recognition and acceptance across EU member states and internationally, promoting mutual recognition and trust in digital transactions. Furthermore, blockchain technology leverages standardized data structures and terminology as outlined in these standards, ensuring that certificate data remains compatible and easily interpretable within blockchain environments. This standardized approach not only enhances the compatibility of blockchain solutions with existing systems but also simplifies the integration process for QTSPs. Additionally, the immutable and transparent nature of blockchain facilitates facilitated validation of certificates. By aligning certificate issuance and management processes with the ETSI EN 319 412 Series and ISO/IEC 9594-8:2017, blockchain-enabled certificates can be seamlessly recognized and validated across different systems and networks. The decentralized ledger ensures that all certificate transactions are recorded in a tamper-proof manner, providing a reliable audit trail that supports the verification processes mandated

by these standards. This alignment ensures that blockchain-based certificates maintain their integrity and trustworthiness, thereby enhancing the overall reliability and efficiency of digital trust services provided by QTSPs.

Technology Analysis of DLT The relevant standard in this context is ISO/TR 23455:2019, titled Blockchain and Distributed Ledger Technologies —Overview of and Interactions Between Smart Contracts in Blockchain and Distributed Ledger Technology Systems. This technical report provides a comprehensive overview of smart contracts within blockchain systems, detailing their characteristics, functionalities, and potential use cases. It serves as a critical resource for QTSPs seeking to leverage smart contracts to enhance their trust service operations. Informed Decision-Making is a fundamental aspect of integrating blockchain technology into QTSP frameworks. ISO/TR 23455:2019 offers valuable technical analysis that aids QTSPs in selecting appropriate blockchain solutions that best fit their operational needs and compliance requirements. By understanding the various types of smart contracts and their interactions within different blockchain environments, QTSPs can make informed decisions about which blockchain platforms and smart contract functionalities will optimize their trust services. This ensures that the chosen blockchain solutions are not only technologically sound but also strategically aligned with the goals of the QTSPs. Smart Contract Implementation is another critical area where blockchain integration significantly benefits QTSPs. Smart contracts, as detailed in ISO/TR 23455:2019, are self-executing agreements with the terms directly written into code. By leveraging smart contracts, QTSPs can automate various trust service processes, such as certificate issuance, renewal, and revocation. This automation enhances operational efficiency by reducing the need for manual intervention, minimizing the potential for human error, and speeding up service delivery. In addition, smart contracts ensure compliance with legal and technical standards by embedding regulatory requirements directly into the contract code, thereby maintaining adherence to established protocols without additional oversight. Performance Optimization is essential for maintaining the security and efficiency of trust service operations within QTSPs. Understanding the interactions and dependencies within blockchain systems, as outlined in ISO/TR 23455:2019, enables QTSPs to optimize both the performance and security of their blockchain implementations. By analyzing how smart contracts interact with the underlying blockchain infrastructure, QTSPs can identify and address potential bottlenecks, enhance transaction throughput, and ensure robust security measures are in place. This proactive approach to performance optimization ensures that blockchain-based trust services remain scalable, resilient, and capable of meeting the growing demands of digital transactions within the European Union's digital ecosystem.

2.3 Interoperability and Scalability Considerations

Interoperability is a cornerstone of ETSI standards, ensuring that trust services can seamlessly integrate across different systems and jurisdictions within the EU. Blockchain technology inherently supports interoperability through standardized protocols and decentralized architectures, which facilitate seamless data exchange and interaction with various trust service providers and digital identity systems. To enhance interoperability, QTSPs can adopt blockchain platforms that support standardized APIs and middleware solutions, enabling effective communication between blockchain networks and existing IT infrastructures. This ensures that blockchain-enhanced trust services can operate cohesively with other digital trust frameworks, fostering a unified and interoperable digital trust ecosystem as envisioned by ETSI EN 319 401. Scalability is another critical consideration outlined in ETSI standards, requiring trust services to handle large volumes of transactions efficiently. Blockchain integration addresses scalability challenges through the adoption of Layer 2 solutions, sharding, and permissioned blockchain architectures. These technical strategies enhance blockchain's capacity to process high transaction volumes without compromising performance or security, ensuring that QTSPs can meet the scalability requirements specified in ETSI standards.

Table 2 summarizes the key scalability solutions and their alignment with ETSI standards.

2.4 Compliance Management and Auditability

Compliance with regulatory standards is a fundamental aspect of ETSI EN 319 401, which mandates trust service providers to implement comprehensive compliance management systems. Blockchain integration enhances compliance and auditability through its transparent and immutable ledger system. Blockchain's immutable ledger provides a tamper-proof audit trail of all trust service transactions. Every action, from certificate issuance to revocation, is recorded on the blockchain, ensuring that all transactions are traceable and verifiable. This aligns with ETSI EN 319 401's requirements for detailed audit trails and supports efficient and effective compliance audits. The decentralized and transparent nature of blockchain allows for real-time monitoring of trust service operations. QTSPs can leverage blockchain's built-in transparency to continuously monitor transaction activities, detect anomalies, and ensure compliance with regulatory standards. This proactive monitoring capability aligns with ETSI's emphasis on maintaining ongoing compliance and swiftly addressing any deviations from estab-

Table 2. Scalability solutions and their alignment with ETSI standards

Scalability Solution	ETSI Standard Alignment
Layer 2 solutions	Enhance transaction throughput and reduce latency, aligning with ETSI EN 319 401's scalability requirements by ensuring efficient handling of high-volume trust service transactions without compromising security or interoperability.
Sharding	Distributes the blockchain network into smaller partitions (shards), enabling parallel processing of transactions. This aligns with ETSI EN 319 401's emphasis on scalable trust service infrastructures capable of supporting growing transaction volumes.
Permissioned Blockchains	Offer higher transaction throughput and lower latency by restricting network participation to authorized entities. This aligns with ETSI EN 319 401's requirements for secure and scalable trust service operations, ensuring compliance with regulatory standards while enhancing performance.
Consensus Mechanism Optimization	Adopting efficient consensus algorithms like PoS and BFT aligns with ETSI EN 319 401's security and performance standards, ensuring scalable and secure transaction processing within trust service frameworks.

lished protocols. ETSI EN 319 401 requires trust service providers to conduct regular security audits to identify and mitigate vulnerabilities. Blockchain integration supports this requirement by providing a secure and transparent platform that is inherently resistant to tampering and unauthorized alterations. Additionally, the use of smart contracts for automated processes reduces the risk of human error, further enhancing the security posture of trust services. Aligning with GDPR requirements, blockchain integration ensures that personal data is handled in compliance with data protection regulations. By implementing off-chain storage solutions and using encryption and pseudonymization techniques, QTSPs can protect sensitive personal data while maintaining the integrity and auditability of blockchain transactions. This dual approach ensures that blockchain-enhanced trust services adhere to both ETSI and GDPR standards, mitigating legal and compliance risks.

3 Market Analysis

The integration of blockchain technology into QTSPs will represents a significant shift in the digital trust services industry. In this section an evaluation of the demand for

blockchain-enhanced trust services is provided along with an assessment of the competitive environment. In the end the trends of this emerging market are presented and a SWOT analysis is conducted to better understand the position of QTSPs in a blockchain-enabled market.

3.1 Evaluation of the demand for blockchain-enhanced trust services

The demand for blockchain-integrated trust services is driven by the increasing need for secure, transparent, and efficient digital transactions across various sectors. The proliferation of digital technologies, coupled with rising cybersecurity threats, has heightened the emphasis on trust services that can assure the integrity and authenticity of digital interactions. This demand is segmented into three primary categories: the enterprise sector, government and public services, and small and medium-sized enterprises. In the enterprise sector, large corporations are adopting blockchain-enhanced trust services to secure complex transactions, manage digital identities, and protect sensitive data [8]. Industries such as finance, healthcare, supply chain, and legal services are particularly inclined in leveraging blockchain technology in order to enhance their operational integrity and compliance [25]. In the financial sector particularly, institutions require secure digital signatures and timestamping services to adhere to the regulatory standards and prevent fraudulent activities. Blockchain's immutable ledger ensures that transactions are tamper-proof, thereby increasing trust and reducing the risk of fraud. Similarly, in healthcare, blockchain facilitates the secure sharing of patient data across different entities, ensuring data integrity and compliance with data protection regulations like the GDPR. The ability to maintain a transparent and immutable record of patient interactions enhances data security and operational efficiency, making blockchain an invaluable tool for large enterprises. Additionally, supply chain companies utilize blockchain to track the provenance of goods, ensuring transparency and accountability from origin to destination, and thus mitigating risks associated with counterfeit products and enhancing the supply chain integrity. Legal services benefit from blockchain through the secure management of digital contracts and the verification of legal documents, ensuring their authenticity and reducing the likelihood of disputes. These applications underscore the significant demand within the enterprise sector for scalable and secure blockchain solutions that can handle high transaction volumes without compromising on security or efficiency. Governments worldwide are increasingly adopting digital platforms to deliver a wide range of public services, necessitating digital trust services to ensure security and transparency [19]. Leveraging blockchain helps in offering

enhanced trust services including secure identity verification, document authentication, and transparent record-keeping, which are critical for maintaining public trust and administrative efficiency. The European Union's eGovernment initiatives, for instance, emphasize the integration of reliable trust services to enhance citizen engagement and streamline administrative processes [22]. Blockchain technology enables governments to create tamper-proof records of public transactions, ensuring that citizen data is securely managed and accessible only to authorized personnel. This not only enhances data security but also improves the efficiency of public service delivery by reducing bureaucratic delays and minimizing the risk of data breaches. Moreover, blockchain facilitates the implementation of decentralized public service platforms, allowing for greater transparency and accountability in government operations. For example, blockchain can be used to secure voting systems, ensuring the integrity of electoral processes and increasing voter confidence. The ability to provide transparent and immutable records of public transactions fosters trust among citizens, making blockchain an essential component of modern eGovernment frameworks. SMEs also are increasingly recognizing the transformative potential of blockchain technology in order to enhance security. Access to affordable and scalable trust services enables SMEs to compete more effectively in the digital marketplace by providing secure transaction processing, efficient identity management, and transparent record-keeping. Blockchain-integrated trust services offer SMEs the ability to implement secure digital signatures and identity verification systems without the need for extensive technical expertise or significant financial investment. This democratization of advanced trust services allows SMEs to enhance their operational security, reduce the risk of fraud, and ensure compliance with regulatory requirements. Additionally, the scalability of blockchain solutions ensures that SMEs can grow without being hindered by technological limitations, thereby supporting their long-term sustainability and competitiveness. The demand for user-friendly blockchain services that offer seamless integration with existing business processes is on the rise, as SMEs seek to leverage technology to improve their operational efficiency and customer trust. The above-described cases collectively illustrate the demand for blockchain-enhanced trust services within the digital trust services industry. The enterprise sector, government and public services, and SMEs each present unique opportunities for QTSPs to deploy scalable and secure blockchain solutions that address specific needs, thereby driving the overall market growth for blockchain-integrated trust services. The projected demand for blockchain-integrated trust services is poised for substantial growth, driven by multiple factors including technological advancements, regulatory developments, and increasing awareness of data security and transparency among organizations and con-

sumers alike. According to recent market research, the global blockchain market is expected to grow from approximately 18 billion in 2024 to over 200 billion EUR by 2029, exhibiting a compound annual growth rate (CAGR) of around 65% during this period [25]. This exponential growth underscores the expanding recognition of blockchain's potential to revolutionize trust services by enhancing security, efficiency, and transparency. It also underlines the need for the EU to be at the forefront of this technological evolution to ensure that it harnesses blockchain's full potential while maintaining regulatory oversight and fostering a secure digital environment for its citizens and businesses. Leading the adoption of blockchain-integrated trust services will enable the EU to position itself as a global leader in digital innovation, attracting significant investments and fostering the growth of a blockchain ecosystem within the EU region that will automate and increase the security of the offered services also minimizing the cross-border complexities. Particularly, integrating blockchain technology with the eIDAS Regulation enables the creation of a standardized and secure digital identity infrastructure that facilitates seamless cross-border digital interactions, essential for the functioning of the digital single market. Moreover, the EU's proactive stance on blockchain ensures the development of interoperable solutions that meet stringent regulatory standards, thereby enhancing trust and confidence among users and service providers. This leadership not only promotes economic growth and technological advancement but also ensures that digital identity solutions are resilient, privacy-preserving, and aligned with the EU's commitment to data protection and sustainability. Consequently, the EU's strategic integration of blockchain within its digital identity framework is crucial for driving secure, efficient, and trustworthy digital interactions, reinforcing its role as a pioneer in the global digital trust services landscape. Continuous advancements in the blockchain technology are a primary driver of the projected demand for blockchain-enhanced trust services. Innovations such as interoperability solutions, scalable consensus mechanisms, and privacy-preserving technologies like Zero-Knowledge Proofs (ZKPs) are making blockchain more practical for enterprise applications. For instance, developments in Layer 2 scaling solutions, including Rollups and Sidechains, significantly increase transaction throughput and reduce latency, enabling blockchain to support high-volume trust service operations more effectively. In [32], the authors explore how ZKPs can address GDPR compliance challenges within blockchain projects, providing a framework for managing privacy while maintaining blockchain's decentralized benefits. Their findings highlight the importance of privacy-preserving technologies for regulatory alignment, positioning ZKPs as a critical innovation in blockchain's expansion across data-sensitive sectors. Additionally, advancements in smart contract functionality and decentralized identity

frameworks are enabling more sophisticated and secure trust service offerings, further stimulating demand [18]. However, regulatory support and the establishment of clear legal frameworks are crucial factors. Governments and regulatory bodies worldwide are increasingly recognizing the importance of blockchain in enhancing digital trust and security. In the European Union, initiatives such as the European Blockchain Services Infrastructure (EBSI) and the ongoing refinement of the eIDAS Regulation are fostering an environment conducive to blockchain adoption. These regulatory developments provide the necessary assurance to organizations regarding the compliance and legal standing of blockchain-enhanced trust services, thereby encouraging their adoption. The global push towards digital transformation across industries is another significant contributor to the rising demand for blockchain-enhanced trust services. Organizations are increasingly seeking digital solutions to streamline operations, enhance data security, and improve customer trust. Blockchain's inherent features of immutability, decentralization, and transparency align perfectly with these objectives, making it an attractive technology for enterprises undergoing digital transformation. As businesses continue to digitize their operations, the need for reliable and secure trust services will escalate, driving the demand for blockchain-integrated solutions. Growing consumer awareness about data privacy and security is also playing a pivotal role in driving the demand for blockchain-integrated trust services. Consumers are becoming more conscious of how their data is managed and are demanding greater transparency and control over their personal information. Blockchain's ability to provide verifiable and immutable records of data transactions enhances consumer trust, making blockchain-enhanced trust services highly appealing to organizations aiming to meet these consumer expectations. Hence, the adoption rates of blockchain-enhanced trust services are expected to accelerate as organizations recognize the tangible benefits and return on investment (ROI) associated with blockchain integration. Early adopters are setting precedents and demonstrating successful implementations, thereby encouraging broader market penetration. Case studies from leading enterprises illustrate significant improvements in security, efficiency, and trust, further propelling the adoption rates across various industries. As organizations across various sectors seek to enhance their trust services through secure, transparent, and efficient digital solutions, the market for blockchain-enhanced trust services is expected to expand rapidly. QTSPs are well-positioned to capitalize on this growing demand by leveraging blockchain technology to offer innovative and compliant trust service solutions that meet the evolving needs of their clients. The competitive landscape for blockchain-integrated trust services is highly dynamic, marked by established QTSPs expanding their service offerings and new entrants harnessing innovative

blockchain technologies to gain a foothold in the market. GlobalSign, a leading QTSP, exemplifies this trend by actively integrating blockchain solutions to enhance its certificate management and security frameworks. According to their recent insights, PKI and Blockchain serve different yet complementary roles in addressing the social problem of trust. While PKI focuses on encrypting communications and authenticating message originators through asymmetric encryption, Blockchain provides a secure, immutable ledger for recording time-stamped transactions without relying on centralized Certificate Authorities. This differentiation allows to leverage Blockchain for identity verification and secure IoT device management, enhancing the robustness and transparency of their trust services.

3.2 Cost implications

Integrating blockchain technology into QTSP frameworks involves significant financial investments and strategic considerations. The most critical cost factor is the infrastructure and technology required to support blockchain implementation. Upgrading the existing IT infrastructure is essential to accommodate the operational demands of a distributed ledger system. This upgrade necessitates substantial Capital Expenditures (CAPEX) for acquiring high-performance servers and advanced networking equipment capable of handling the increased computational load inherent to blockchain technologies. The decision between deploying a private, public, or consortium blockchain profoundly impacts the overall cost structure. Private blockchains, favored by the European Union for their enhanced control and privacy, typically incur higher costs due to the necessity for dedicated infrastructure and ongoing maintenance. In contrast, public blockchains may offer reduced infrastructure costs by leveraging existing public networks but come with challenges related to scalability and transaction fees [4]. The EU' s current strategic direction leans towards the implementation of private blockchains to ensure compliance with stringent regulatory standards and data protection requirements. Another substantial expenditure arises from software development and acquisition. Customizing blockchain platforms to align seamlessly with QTSP operations demands specialized development efforts. This customization involves creating smart contracts tailored to automate processes such as certificate issuance and revocation, developing application programming interfaces (APIs) to ensure interoperability with existing systems, and designing user interfaces that facilitate seamless interactions for both administrators and end-users [3]. The complexity of integrating blockchain with legacy systems may necessitate bespoke middleware solutions, further escalating de-

velopment costs. Additionally, opting for proprietary blockchain platforms or middleware introduces recurring licensing fees, adding to the long-term financial commitment. Ongoing maintenance, including software updates and security patches, is essential to ensure the blockchain network remains secure and functional, thereby requiring continuous budget allocation. Operational and maintenance costs also play a pivotal role in the overall financial implications of blockchain integration. Regular maintenance is crucial for the sustained performance and security of the blockchain infrastructure. This includes routine software updates, security patches, and system optimizations to protect against emerging threats and vulnerabilities. Moreover, robust security management practices must be implemented to safeguard the blockchain network from cyberattacks, unauthorized access, and operational anomalies. This often necessitates investing in advanced security solutions and employing specialized personnel to manage and monitor the blockchain system effectively. Additionally, staff training is imperative to equip personnel with the necessary skills to operate and manage the new blockchain systems, ensuring smooth adoption and minimizing disruptions to existing workflows. Despite the significant upfront and ongoing costs, the potential Return on Investment (ROI) from integrating blockchain technology into QTSP frameworks is considerable. Enhanced security and trust are primary drivers of ROI, as blockchain's immutable ledger and decentralized architecture significantly reduce the risk of data breaches and unauthorized alterations, thereby lowering costs associated with fraud prevention and compliance violations. Furthermore, the automation of trust service processes through smart contracts increases operational efficiency, reducing the need for manual interventions and minimizing human errors. This automation not only accelerates transaction processing but also lowers operational costs, contributing to a favorable ROI. Additionally, compliance with regulatory standards such as the eIDAS Regulation and GDPR is streamlined through blockchain's transparent and immutable records, potentially reducing costs related to audits and legal liabilities. The ability to offer secure, transparent, and efficient trust services can also enhance the competitive advantage of QTSPs, attracting more clients and expanding market share, which further contributes to the overall ROI. Scalability considerations are paramount when integrating blockchain technology into QTSP frameworks. The blockchain infrastructure must be capable of handling high transaction volumes without compromising performance or security. Implementing scalability solutions such as Layer 2 protocols, sharding, and adopting more efficient consensus mechanisms like Proof of Stake (PoS) or Byzantine Fault Tolerance (BFT) is essential to ensure that the blockchain network can grow in tandem with the increasing demands of trust service operations. These scalability measures not only en-

hance transaction throughput and reduce latency but also ensure that the blockchain system remains cost-effective and efficient as the volume of transactions scales. Additionally, the infrastructure should be designed to accommodate future growth, allowing QTSPs to expand their services without necessitating significant re-engineering or additional investments. Risk assessment is another critical aspect of the cost implications associated with blockchain integration. Technical risks, such as scalability limitations, interoperability issues with existing systems, and the maturity level of blockchain platforms, can lead to project delays, increased costs, or system vulnerabilities. Addressing these technical challenges requires thorough planning, robust testing, and the adoption of best practices in blockchain deployment. Regulatory risks also pose significant concerns, as compliance with regulations like eIDAS and GDPR is complex and evolving. Misalignment with these regulations can result in legal penalties, reputational damage, and financial losses. Therefore, QTSPs must ensure that their blockchain implementations are fully compliant with all relevant regulatory requirements through continuous monitoring and adaptation. Security risks, including 51% attacks, smart contract vulnerabilities, and key management issues, must be mitigated through the implementation of advanced security measures, regular security audits, and the adoption of secure consensus protocols. Furthermore, adoption risks, such as user resistance to new technologies and the slow pace of acceptance, can impact the realization of anticipated ROI. To mitigate these risks, QTSPs should invest in comprehensive training programs, engage in user education initiatives, and adopt a phased implementation approach to facilitate smoother transitions and higher adoption rates.

In conclusion, the integration of blockchain technology into QTSP frameworks involves significant cost implications, encompassing infrastructure upgrades, software development, and ongoing maintenance. However, the potential ROI, driven by enhanced security, operational efficiency, regulatory compliance, and competitive advantage, justifies the initial and ongoing investments. Scalability and risk assessment are critical factors that must be meticulously managed to ensure the successful and sustainable integration of blockchain technology. By strategically addressing these cost implications and associated risks, QTSPs can leverage blockchain to deliver secure, transparent, and efficient trust services, thereby positioning themselves advantageously in the evolving digital trust services market.

3.3 Return on Investment (ROI) and Cost-Benefit Analysis

One of the most significant benefits of blockchain integration is the enhancement of operational efficiencies through automation. Smart contracts, which are self-executing contracts with the terms directly written into code, can automate various processes such as certificate issuance, renewal, and revocation. This automation reduces the need for manual intervention, thereby decreasing administrative overhead and minimizing the potential for human error. For instance, the automation of certificate renewal processes ensures timely renewals without the delays typically associated with manual processes, thereby maintaining uninterrupted service for clients. The reduction in administrative tasks not only lowers labor costs but also allows QTSPs to allocate resources more strategically towards innovation and service improvement. Enhanced security is another critical advantage that directly contributes to ROI. Blockchain's decentralized and immutable ledger significantly reduces the risk of data breaches and fraudulent activities, which are prevalent concerns in centralized systems. By mitigating these risks, QTSPs can avert the substantial financial losses associated with cybersecurity incidents, including costs related to breach remediation, legal liabilities, and reputational damage. Furthermore, the implementation of multi-signature schemes and decentralized key management enhances the overall security infrastructure, providing an additional layer of protection against unauthorized access and ensuring the integrity of digital signatures. The reduction in security-related incidents translates into direct cost savings and preserves the financial stability of the organization. Operational efficiency gains from blockchain integration also contribute to ROI. The automation capabilities of smart contracts streamline certificate management workflows, accelerating processes and reducing turnaround times. This increased efficiency not only enhances service delivery but also improves customer satisfaction, potentially leading to higher client retention rates and the attraction of new clients seeking reliable and efficient trust services. Additionally, the scalability offered by blockchain technology allows QTSPs to handle a larger volume of transactions without a proportional increase in operational costs, thereby supporting business growth and expanding market reach [11]. Market differentiation and competitive advantage are intangible yet substantial benefits that positively impact ROI. By adopting blockchain technology, QTSPs position themselves at the forefront of technological innovation within the digital trust services market. This differentiation can attract clients who prioritize advanced security measures and transparency, thereby expanding the client base and increasing market share [7]. Moreover, the ability to offer blockchain-enhanced trust services can open up new revenue streams, such as pre-

mium services for clients requiring higher levels of security and transparency, further contributing to the financial returns of the integration. Long-term cost savings represent another pivotal aspect of the cost-benefit analysis. Decentralized systems reduce the need for extensive centralized infrastructure, leading to lower maintenance and operational costs over time. The immutable nature of blockchain eliminates the need for costly data reconciliation processes, as all transactions are permanently recorded and easily verifiable. Additionally, the reduction in fraud and error-related losses contributes to sustained cost savings, enhancing the overall financial health of the organization.

3.4 Scalability and Long-Term Economic Implications

One of the critical technical and economic considerations for QTSPs is the scalability of blockchain systems and their long-term economic implications. This section provides an analysis of the scalability challenges associated with blockchain integration, explores potential solutions, and examines how these factors influence the long-term economic viability of blockchain adoption within QTSP operations. Since the inception of blockchain technology, there has been ongoing discussion regarding its ability to handle a continuously growing number of transactions and accommodate sustained growth. Scalability challenges in blockchain arise due to limitations in transaction throughput, latency, and resource consumption [33]. QTSPs process high volumes of transactions related to digital signature issuance, verification, and certificate management. Integrating blockchain technology into these operations necessitates a blockchain infrastructure capable of efficiently handling such transactional loads. It is well-known that public blockchains like Bitcoin and Ethereum have limited transaction throughput. Bitcoin processes approximately 7 transactions per second (TPS), while Ethereum initially handled around 15 TPS. However, with the implementation of PoS and sharding in Ethereum 2.0, this number is expected to increase significantly. In contrast, traditional payment systems like Visa can process up to 24,000 TPS [30]. The low throughput of public blockchains is primarily due to their consensus mechanisms, which prioritize security and decentralization over scalability. For QTSPs, utilizing a public blockchain with low transaction throughput can lead to processing delays and affect operational efficiency. A significant challenge is the inability of current public blockchain networks to offer deterministic latencies; the upper bound of the expected time for a transaction to be confirmed is non-deterministic. Transaction confirmation times depend on network utilization and the transaction fees users are willing to pay. As the number of transactions increases, network congestion can lead to higher transaction fees and slower confir-

mation times, impacting the cost-effectiveness of blockchain integration [12]. Furthermore, blockchain networks require nodes to store the entire ledger, which continuously grows as new transactions are added. This increasing data size poses storage challenges and increases resource consumption. Nodes participating in the network must allocate computational power and storage capacity, leading to higher operational costs. For QTSPs, efficiently managing these resources is crucial to maintain cost-effectiveness and sustainability in the long term. To address the aforementioned scalability challenges, several technical solutions and approaches have been proposed and implemented in various blockchain platforms. QTSPs considering blockchain integration can leverage these solutions to enhance scalability and optimize long-term economic outcomes. Layer 2 solutions encompass a variety of architectural approaches that involve building protocols on top of existing blockchains to offload transactions from the main chain, thereby increasing throughput and reducing congestion. (i) State channels enable two parties to conduct numerous transactions off-chain, with only the initial and final states recorded on the blockchain. This significantly reduces the number of on-chain transactions and improves scalability. (ii) Sidechains are independent blockchains running in parallel to the main chain, connected via a two-way peg. They allow the transfer of assets between chains, enabling specialized processing without burdening the main chain. (iii) Techniques like Plasma and rollups bundle multiple transactions into a single on-chain transaction, reducing the load on the main chain. Rollups execute transactions off-chain and submit compressed transaction data to the main chain for verification. Implementing Layer 2 solutions can enhance the scalability of blockchain networks used by QTSPs, allowing them to handle higher transaction volumes without compromising security or decentralization. Another technique is sharding, which divides the blockchain network into smaller partitions called shards, each capable of processing its own transactions and smart contracts. By distributing the workload across multiple shards, the network can achieve higher throughput and scalability. For QTSPs, sharding can enable parallel processing of transactions related to digital signatures and certificates, improving efficiency and reducing latency. However, implementing sharding introduces complexity in maintaining network security and consistency across shards. Protocols like Ethereum 2.0 are actively developing sharding solutions to enhance scalability. Consensus mechanisms play a crucial role in determining the scalability of a blockchain network. Selecting a blockchain platform with an optimized consensus mechanism can significantly impact scalability and the long-term economic implications for QTSPs. (i) Proof of Stake (PoS): Validators stake an amount of cryptocurrency as collateral to participate in the consensus process. PoS reduces computational resource requirements and increases

transaction throughput compared to Proof of Work (PoW). (ii) Delegated Proof of Stake (DPoS): Stakeholders elect a limited number of delegates to validate transactions, enhancing efficiency and scalability. Permissioned blockchains restrict network participation to authorized entities, reducing the number of nodes required to reach consensus. This controlled environment allows for higher transaction throughput and lower latency compared to public blockchains. For QTSPs, permissioned blockchains provide a scalable solution tailored to their operational needs, enabling efficient processing of trust services while maintaining necessary security and privacy controls. Additionally, permissioned blockchains can be optimized to meet specific regulatory requirements and integrate seamlessly with existing enterprise systems. Scalability solutions have significant long-term economic implications for QTSPs integrating blockchain technology, as they can affect operational costs, system performance, and the ability to adapt to future growth. Reducing resource consumption and improving transaction efficiency, scalability solutions can lead to substantial cost savings. Layer 2 solutions and optimized consensus mechanisms lower computational and energy requirements, translating to reduced expenses on hardware, energy consumption, and maintenance. Also, higher transaction throughput and lower latency enhance service quality, potentially attracting more clients and increasing revenue. Efficient scalability ensures that the blockchain infrastructure can support growing transaction volumes without proportional increases in operational costs, contributing to favorable economies of scale. As demand for digital trust services grows, the blockchain system must accommodate increased transaction volumes and more complex operations. Investing in scalable blockchain solutions future-proofs the technological infrastructure of QTSPs, ensuring the system remains robust and performant over time, avoiding the need for costly overhauls or migrations to new platforms. Note that scalable systems are better positioned to integrate emerging technologies, such as the Internet of Things (IoT) and Artificial Intelligence (AI), which may introduce new transaction types and data processing requirements. By adopting scalable blockchain architectures, QTSPs can remain agile and responsive to technological advancements. Scalability enhances the ability of QTSPs to offer reliable and efficient services, strengthening their competitive position in the market. Clients increasingly demand fast, secure, and scalable trust services, and the ability to meet these expectations can differentiate QTSPs from competitors. Furthermore, scalable blockchain solutions enable QTSPs to expand their service offerings, such as real-time transaction processing, high-volume data validation, and support for global operations. Scalability issues can lead to system bottlenecks, service disruptions, and security vulnerabilities. Proactively addressing scalability, QTSPs mitigate risks associated with system overloads

and performance degradation. Scalable systems are more resilient to attacks that exploit network congestion or transaction delays, enhancing overall security.

3.5 SWOT Analysis

Conducting a SWOT analysis can help QTSPs to evaluate their strengths, weaknesses, opportunities, and threats within the blockchain-enhanced trust services market. This analysis not only highlights the internal and external factors influencing QTSPs but also guides them in leveraging their strengths, addressing weaknesses, capitalizing on opportunities, and mitigating threats to maintain a competitive edge in the evolving digital trust landscape.

3.5.1 Strengths

QTSPs possess inherent strengths that uniquely position them to integrate blockchain technology effectively into their service offerings. One of the primary strengths is their established expertise in delivering trust services, including the secure issuance, management, and verification of digital certificates and signatures. This expertise is grounded in a deep understanding of cryptographic principles, secure key management, and compliance with stringent security standards, which are fundamental to blockchain technology. For instance, their proficiency in asymmetric cryptography and digital signature algorithms aligns closely with the cryptographic mechanisms employed in blockchain systems, facilitating a smoother integration process. Moreover, QTSPs have extensive experience navigating complex regulatory frameworks such as the eIDAS Regulation and the GDPR. This regulatory compliance proficiency enables QTSPs to design and implement blockchain solutions that meet stringent legal requirements, providing a competitive advantage over less regulated entities. Their ability to ensure that blockchain implementations adhere to data protection and electronic identification standards is crucial, given the immutable nature of blockchain records and the importance of protecting personal data. For example, QTSPs can implement privacy-preserving techniques like zero-knowledge proofs to comply with GDPR while leveraging blockchain's transparency. Additionally, QTSPs have established trust and strong relationships with clients across various sectors, including finance, healthcare, and government. This trust is built on a track record of reliability, security, and compliance, making clients more receptive to adopting new blockchain-based services offered by QTSPs. For instance, InfoCert, one of Europe' s largest QTSPs, has successfully integrated blockchain technology to enhance its digital identity verification and document authentication services, reinforcing

client trust and expanding its service offerings. Furthermore, QTSPs' reputable brand and demonstrated commitment to security can alleviate client concerns regarding the adoption of new technologies. Their proven ability to deliver secure and compliant trust services positions them as credible providers of blockchain-enhanced solutions. This credibility is critical in an industry where trust and reliability are paramount.

3.5.2 Weaknesses

Despite their strengths, QTSPs may face several internal challenges that could impede the effective integration of blockchain technology. A significant weakness is the potential technological lag, where QTSPs may lack the necessary expertise in blockchain technology, leading to slower adoption and implementation. Blockchain systems require specialized technical skills, including proficiency in distributed ledger technologies, smart contract development, and consensus mechanisms. The shortage of in-house blockchain experts can hinder QTSPs from swiftly capitalizing on blockchain's benefits and may necessitate substantial investment in training or hiring skilled personnel. Another notable weakness is the challenge of integrating the blockchain with existing legacy systems. Many QTSPs operate on established infrastructures that may not be inherently compatible with blockchain technologies. For example, traditional PKI systems used by QTSPs rely on centralized architectures, whereas blockchain operates on decentralized principles. Reconciling these differences may require significant modifications or complete overhauls of current systems, leading to increased implementation costs and extended timelines. The complexity of integration can also introduce technical risks, such as system incompatibilities and data migration challenges. Organizational inertia and resistance to change within traditional QTSPs can further impede innovation and adaptation to new technological paradigms. Employees accustomed to legacy systems and processes may be hesitant to embrace blockchain integration due to uncertainties about its benefits, potential disruptions, or job security concerns. This resistance necessitates comprehensive change management initiatives to foster a culture of innovation and adaptability. Without a supportive organizational environment, QTSPs may struggle to implement blockchain solutions effectively. Additionally, resource constraints, such as limited financial budgets and competing priorities, can limit the ability of QTSPs to invest in blockchain technology. The substantial capital expenditures required for infrastructure upgrades, software development, and ongoing maintenance may strain resources, particularly for smaller QTSPs. Balancing these investments with other operational demands is a significant challenge that must be carefully managed.

3.5.3 Opportunities

The expanding market for blockchain-enhanced trust services presents numerous opportunities for QTSPs to innovate and diversify their service offerings. There is a growing demand for secure digital transactions, decentralized identity management, and automated compliance solutions. According to Market Research Future, the global blockchain identity management market is expected to reach USD 19.0 billion by 2027, growing at a CAGR of 85% from 2020 to 2027 [23]. This surge is driven by increasing cybersecurity threats, regulatory compliance requirements, and the need for efficient identity verification processes. By leveraging blockchain's decentralized and immutable ledger capabilities, QTSPs can offer enhanced security features, such as tamper-proof digital certificates, real-time verification processes, and self-sovereign identity solutions. For example, blockchain-based DIDs and VCs enable users to control their personal data, aligning with GDPR requirements and improving user trust [5]. QTSPs can capitalize on this trend by developing blockchain-integrated identity verification services that meet evolving client needs. Furthermore, strategic partnerships with technology providers, blockchain startups, and regulatory bodies can enhance QTSPs' capabilities and accelerate blockchain adoption. Collaborations with blockchain innovators can provide QTSPs with access to cutting-edge technologies and expertise. For example, Belgian Mobile ID partnered with major banks and telecom operators to launch the itsme® platform [17], a digital identity solution recognized under eIDAS, which utilizes blockchain components to provide secure and user-friendly services. The rise of new applications, such as blockchain-based supply chain transparency, smart contract-driven trust services, and IoT security, offers QTSPs the potential to tap into emerging markets. By offering blockchain-enhanced trust services in these areas, QTSPs can expand their market reach and establish themselves as leaders in innovative trust solutions. Furthermore, favorable regulatory developments, such as the European Commission's support for blockchain through the European Blockchain Services Infrastructure (EBSI) initiative, provide an encouraging environment for QTSPs to innovate [15].

3.5.4 Threats

The external environment presents several threats that QTSPs must navigate to successfully integrate blockchain technology. Competition from technology giants and innovative startups poses a significant threat. Companies like IBM, Microsoft, and Accenture are investing heavily in blockchain technology and offer comprehensive blockchain solutions, including trust services. These organizations possess advanced technological capabilities, substantial resources, and established client networks, potentially over-

shadowing QTSPs' offerings. The rapid pace of technological advancements in the blockchain space can render existing solutions obsolete. New blockchain platforms, consensus mechanisms, and cryptographic techniques are continually emerging. QTSPs risk investing in technologies that may become outdated or unsupported, necessitating continuous investment in research and development to stay current. Failure to keep pace with these advancements can result in QTSPs losing their competitive edge and market share. Regulatory uncertainty and evolving compliance requirements also pose challenges. The legal landscape for blockchain technology is still developing, with varying regulations across jurisdictions. Uncertainties regarding how existing laws apply to blockchain, such as issues around data immutability conflicting with the GDPR's "right to be forgotten," can introduce complexities and increase operational risks. QTSPs must remain agile to adapt to new laws and standards, necessitating ongoing compliance assessments and adjustments to trust service operations. Technological vulnerabilities inherent in blockchain technology can undermine the trust and reliability of blockchain-enhanced trust services. Risks such as smart contract flaws, 51% attacks, and emerging threats from quantum computing can compromise security. For example, vulnerabilities in smart contracts can lead to unauthorized access or manipulation of trust services. These vulnerabilities not only pose security risks but also have the potential to damage QTSPs' reputations and erode client trust. Economic factors, such as budget constraints or economic downturns, could limit investments in blockchain technology, hindering QTSPs' ability to innovate and maintain competitive services. Additionally, as more QTSPs adopt blockchain, the market may become saturated, leading to increased competition and potentially reduced profit margins. Dependency on third-party blockchain platforms or service providers introduces additional risks, including service outages, vendor lock-in, and data privacy concerns. QTSPs must carefully assess these dependencies and develop strategies to mitigate associated risks.

4 Conclusion

The integration of blockchain technology into Qualified Trust Service Provider frameworks represents a significant advancement in enhancing the security, efficiency, and interoperability of trust services within the European Union's digital ecosystem. By leveraging blockchain's inherent features—decentralization, immutability, and cryptographic security—QTSPs can address existing challenges associated with centralized trust models and improve compliance with regulations.

Technical feasibility studies indicate that blockchain can be effectively aligned with ETSI standards, such as ETSI EN 319 401 and EN 319 411, ensuring that blockchain-based trust services meet stringent regulatory requirements. Interoperability and scalability considerations can be managed through the adoption of standardized APIs, Layer 2 scaling solutions, and optimized consensus mechanisms, enabling the seamless integration with existing systems and accommodating high transaction volumes.

Analysis of the market indicates an increasing demand for trust services powered by blockchain technology in numerous industries. This trend is fueled by the necessity for secure and transparent digital exchanges. Despite the substantial initial costs associated with infrastructure upgrades, software creation, and operational outlays, the potential returns on investment are substantial. Advantages comprise heightened security, efficiency gains through automation, and a bolstered competitive edge.

In conclusion, integrating blockchain technology within QTSP frameworks is both technically feasible and economically advantageous. Addressing technical challenges and leveraging their expertise in trust services, QTSPs can lead the way in delivering secure, efficient, and compliant trust services. This integration not only aligns with the European Union's vision for a unified digital single market but also fosters a resilient and trustworthy digital ecosystem for all stakeholders.

References

[1] European Telecommunications Standards Institute (ETSI). Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements. Standard EN 319-411-1 V1.2.2. ETSI EN 319 411-1 V1.2.2. ETSI, July 2018.

[2] European Telecommunications Standards Institute (ETSI). Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers providing Time-Stamping Services. Standard EN 319 421 V1.1.1. ETSI EN 319 421 V1.1.1. ETSI, Apr. 2016.

[3] European Telecommunications Standards Institute (ETSI). Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Identity Proofing. Tech. rep. ETSI TS 119 495 V1.5.1. 2020.

[4] European Telecommunications Standards Institute (ETSI). Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation. https://cdn.standards.iteh.ai/samples/63929/de245340712d411485196cb98a427bea/ETSI-EN-319-102-1-V1-4-0-2020-03-.pdf. ETSI EN 319 102-1 V1.4.0. 2020.

[5] World Wide Web Consortium (W3C). Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/. W3C Recommendation, Jul. 2022. 2022.

[6] World Wide Web Consortium (W3C). Verifiable Credentials Data Model 1.0. http://www.w3.org/TR/verifiable-claims-data-model/. W3C Recommendation, Jan. 2019. 2019.

[7] A. Dorri, S. S. Kanhere, and R. Jurdak. Blockchain in Internet of Things: Challenges and Solutions. arXiv preprint arXiv:1608.05187. 2016.

[8] C. Laroiya, D. Saxena, and C. Komalavalli. "Applications of Blockchain Technology". In: *Handbook of Research on Blockchain Technology*. Ed. by S. Krishnan et al. Academic Press, 2020, pp. 213–243.

[9] C. Mazzocca et al. A Survey on Decentralized Identifiers and Verifiable Credentials. arXiv preprint arXiv:2302.14016. 2023.

[10] European Commission. European Digital Identity. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en. 2021.

[11] European Commission. Qualified Electronic Signatures and Seals under eIDAS. https://ec.europa.eu/digital-single-market/en/trust-services-and-eid.

[12] K. Croman et al. "On Scaling Decentralized Blockchains". In: *International Conference on Financial Cryptography and Data Security*. 2016.

[13] European Union Agency for Cybersecurity (ENISA). Recommendations for the implementation of trust services. https://www.enisa.europa.eu/topics/cybersecurity-policy/trust-services/technical-guidance-on-qualified-trust-services.

[14] European Union Agency for Cybersecurity (ENISA). Security guidelines on the appropriate use of qualified electronic registered delivery services. https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-registered-delivery-services. ENISA, 2017. 2017.

[15] European Commission. European Blockchain Services Infrastructure (EBSI). n.d. URL: https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure.

[16] H. Halpin and M. Piekarska. "Introduction to Security and Privacy on the Blockchain". In: *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Paris, France, 2017, pp. 1–3.

[17] itsme®. itsme®. n.d. URL: https://itsme-id.com/.

[18] Y. Liu et al. "SS-DID: A Secure and Scalable Web3 Decentralized Identity Utilizing Multilayer Sharding Blockchain". In: *IEEE Internet of Things Journal* 11.15 (Aug. 2024), pp. 25694–25705.

[19] M. Kassen. "Blockchain and e-government innovation: Automation of public information processes". In: *Information Systems* 103 (2022).

[20] M. Swan. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.

[21] M. Turkanović and B. Podgorelec. "Signing Blockchain Transactions Using Qualified Certificates". In: *IEEE Internet Computing* 24.6 (Nov. 2020), pp. 37–43.

[22] M.-V. Vladucu et al. "E-Voting Meets Blockchain: A Survey". In: *IEEE Access* 11 (2023), pp. 23293–23308.

[23] Market Research Future. Blockchain Identity Management Market Research Report - Global Forecast till 2027. Available online: https://www.marketresearchfuture.com/reports/blockchain-identity-management-market-forecast-2027. 2021.

[24] O. Avellaneda et al. "Decentralized Identity: Where Did It Come From and Where Is It Going?" In: *IEEE Communications Standards Magazine* 3.4 (2019), pp. 10–13. DOI: 10.1109/MCOMSTD.2019.9031542.

[25] Statista. Blockchain use cases in financial services 2021. https://www.statista.com/statistics/1279848/blockchain-use-in-financial-services/. 2021.

[26] European Union. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A31999L0093. Official Journal of the European Communities, L 343, pp. 1–16. 1999.

[27] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj. Official Journal of the European Union, L 119, pp. 1–88. 2016.

[28] European Union. Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32014R0910. Official Journal of the European Union. 2014.

[29] European Union. Regulation on European Digital Identity (eIDAS 2.0). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52021PC0206. Official Journal of the European Union. 2021.

[30] Visa Inc. Visa Acceptance for Retailers. Available: https://usa.visa.com/run-your-business/accept-visa-payments/visa-acceptance-for-retailers.html. 2021.

[31] X. Xu et al. A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017 IEEE International Conference on Software Architecture (ICSA). 2017.

[32] D. Zein and W. Pinkwart. Leveraging Zero-Knowledge Proofs for GDPR Compliance in Blockchain Projects. Position Paper. INATBA, 2024.

[33] Z. Zheng et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”. In: *2017 IEEE International Congress on Big Data*. 2017.