BLOCKSTAND

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

P. Soumplis

Abstract

This document explores the viability and market potential of integrating blockchain technology within Qualified Trust Service Provider (QTSP) frameworks to aid small and medium enterprises (SMEs). Through examining current standards, regulatory mandates, and technological trends, the analysis identifies the benefits and challenges associated with this integration. Key advantages are highlighted, such as increased data security, more efficient operations, and better compliance with European regulations like eIDAS and GDPR. Conversely, the report notes challenges such as technical complexity and the need for significant initial investment. Concluding with a practical guide for SMEs to adopt blockchain-based QTSP solutions, it emphasizes the importance of collaboration, financial strategy, and support networks for a successful rollout. This evaluation provides SMEs with actionable insights to utilize digital trust services and boost their competitive edge in the market.

Keywords: blockchain, QTSP, SME, eIDAS, GDPR, decentralized identity, digital trust services

Contents

Abbreviations

- **ABAC** – Attribute-Based Access Control
- **API** – Application Programming Interface
- **AWS** – Amazon Web Services
- **BaaS** – Blockchain as a Service
- **CAdES** – CMS Advanced Electronic Signatures
- **CapEx** – Capital Expenditures
- **CBA** – Cost-Benefit Analysis
- **CI/CD** – Continuous Integration/Continuous Deployment
- **CMS** – Cryptographic Message Syntax (implied in CAdES context)
- **DDoS** – Distributed Denial of Service
- **DLT** – Distributed Ledger Technology
- **DPIA** – Data Protection Impact Assessment
- **EBSI** – European Blockchain Services Infrastructure
- **EBP** – European Blockchain Partnership
- **EC** – European Commission
- **EIB** – European Investment Bank
- **eIDAS** – Electronic Identification, Authentication and Trust Services
- **ERP** – Enterprise Resource Planning
- **EU** – European Union
- **EUDI** – European Digital Identity (Wallet)
- **FIPS** – Federal Information Processing Standards
- **FTE** – Full-Time Equivalent
- **GDPR** – General Data Protection Regulation
- **HSM** – Hardware Security Module

- **IP** – Intellectual Property
- **IPFS** – InterPlanetary File System
- **IR** – Incident Response
- **ISO** – International Organization for Standardization
- **IT** – Information Technology
- **IEC** – International Electrotechnical Commission
- **L2** – Layer 2
- **NPV** – Net Present Value
- **OpEx** – Operational Expenditures
- **PAdES** – PDF Advanced Electronic Signatures
- **PBFT** – Practical Byzantine Fault Tolerance
- **PDF** – Portable Document Format (implied in PAdES context)
- **PKI** – Public Key Infrastructure
- **PPP** – Public-Private Partnership
- **PSD2** – Payment Services Directive 2
- **QSCD** – Qualified Signature Creation Device
- **QTSP** – Qualified Trust Service Provider
- **R&D** – Research and Development
- **ROI** – Return on Investment
- **SHA** – Secure Hash Algorithm (e.g., SHA-256)
- **SME** – Small and Medium-Sized Enterprise
- **TLS** – Transport Layer Security
- **TPS** – Transactions Per Second
- **XAdES** – XML Advanced Electronic Signatures
- **XML** – Extensible Markup Language (implied in XAdES context)
- **zk-SNARK** – Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

Executive Summary

This report examines the feasibility and market potential of integrating blockchain technology into Qualified Trust Service Provider (QTSP) frameworks, with a particular focus on addressing the needs of small and medium-sized enterprises (SMEs). In the current digital economy, SMEs often grapple with limited resources, the need for regulatory compliance, and heightened cybersecurity risks. Blockchain-enabled QTSP solutions offer a transformative way to address these challenges by delivering secure, efficient, and legally compliant digital services that empower SMEs.

The relevance of blockchain-integrated QTSPs for SMEs lies in their ability to increase security and streamline operations while aligning with key EU regulations such as eIDAS and GDPR. Through the use of decentralized ledgers, cryptographic validation, and smart contracts, these solutions enable SMEs to optimize trust services such as digital signatures, certificate issuance, and identity verification. This not only reduces operational costs and minimizes errors, but also provides a competitive advantage by facilitating participation in cross-border transactions and meeting evolving market expectations.

A cornerstone of successfully implementing these solutions is the adhesion to established technical and regulatory standards. Frameworks such as the ETSI EN 319 series and ISO/IEC 27001 ensure the integrity, authenticity, and legal credibility of trust services. By complying with these standards, SMEs can achieve interoperability across systems and secure cross-border recognition of their digital transactions, a critical factor for operating within the EU's single market and building trust with partners and clients.

To guide SMEs through the adoption process, the report advocates a phased approach. It starts with a readiness assessment to assess the current infrastructure and organizational capabilities. This is followed by pilot projects that allow SMEs to test specific use cases and refine their strategies based on real-world data. Subsequently, resource allocation, including budgeting, staffing, and partnerships, sets the stage for full deployment, which is executed according to a well-defined timeline with clear milestones. This methodical progression helps SMEs smoothly transition while keeping risks to a minimum.

Practical implementation guidelines further support SMEs by addressing the technical complexities of adoption. These recommendations cover choosing an appropriate architecture, such as cloud-based or on-premise systems, and ensuring seamless integration with existing setups. Security remains a priority, with an emphasis on practices like

secure key management and data minimization to meet GDPR and eIDAS requirements. Scalability is also considered, with technologies like Layer 2 solutions and permissioned networks enabling the system to expand in line with business growth without sacrificing performance.

Risk management is another critical focus area. The report highlights potential challenges such as technical failures, data breaches, and vulnerabilities in smart contracts. To counteract these, it suggests regular audits, robust incident response protocols, and continuous system monitoring. These proactive measures safeguard the resilience and compliance of the QTSP framework, allowing SMEs to maintain secure and efficient operations in a digital landscape.

Financially, the adoption of blockchain-integrated QTSP solutions requires an upfront investment, but the long-term rewards are substantial. Benefits include lower compliance costs, improved operational efficiency, and a stronger market presence. To ease the financial burden, SMEs can tap into EU grants and public-private partnerships, which provide crucial support and make the transition more accessible.

Finally, through collaboration in consortiums and knowledge networks, SMEs can pool resources, share expertise, and adopt best practices of peers. These cooperative efforts not only speed up the implementation process, but also drive innovation, positioning SMEs as leaders in digital transformation.

1 Introduction

The global economy is undergoing a transformation driven by rapid digitization that redefines how businesses operate, communicate, and engage with their stakeholders. In this dynamic environment, trust services, such as electronic signatures, seals, and time stamping, have emerged as critical tools to ensure the security, authenticity, and legal validity of digital transactions. Within the European Union (EU), Qualified Trust Service Providers (QTSPs) are entrusted with delivering these services, adhering to the rigorous standards outlined in the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation. Although these services are vital for all businesses, SMEs that are the cornerstone of the EU economy, often struggle to adopt them. Challenges such as limited financial resources, complex regulatory requirements, and growing cybersecurity threats can prevent small businesses from embracing these digital solutions, ultimately affecting their ability to compete in a highly interconnected market.

The integration of blockchain technology into QTSP frameworks offers a transformative opportunity to address these barriers. Known for its decentralized structure, cryptographic security, and tamper-proof recordkeeping, the blockchain provides a reliable and efficient foundation to improve trust services. For SMEs, blockchain-enabled QTSP solutions promise to simplify processes, lower costs, and ensure compliance with key EU regulations, including eIDAS and the General Data Protection Regulation (GDPR). Beyond operational benefits, these solutions can enable SMEs to participate confidently in cross-border transactions, unlocking new avenues for growth and innovation in a digital first world.

This report delivers a detailed feasibility and market analysis of integrating blockchain technology into QTSP frameworks, with a particular emphasis on the unique needs and constraints of SMEs. Explores the potential of blockchain-based trust services to empower smaller enterprises, assesses relevant standards and regulatory landscapes, and provides a clear roadmap for adoption. In addition, the report includes actionable implementation guidelines, risk management strategies, and financial insights to guide SMEs through their digital transformation journey. By addressing both technical and practical considerations, this analysis aims to equip SMEs with the knowledge and resources needed to successfully adopt blockchain-enabled QTSP solutions.

The report is organized into the following sections.

- **Section 2: Blockchain-Integrated QTSPs: Relevance for SMEs** This section ex-

plains why blockchain is a game-changer for SMEs, addressing their specific challenges and outlining the legal and regulatory factors they must consider.

- **Section 3: Standards and Frameworks for Blockchain-Enabled Trust Services** Here, we review the essential technical and regulatory standards—such as the ETSI EN 319 series and ISO/IEC 27001—that support blockchain integration into QTSP frameworks.
- **Section 4: Roadmap for Adopting Blockchain-Enabled QTSP Solutions** A step-by-step adoption plan is provided, covering readiness assessments, pilot projects, resource planning, and full-scale deployment.
- **Section 5: Implementation Guidelines and Best Practices** Practical recommendations are offered on technical design, security measures, and scalability to ensure a smooth implementation process.
- **Section 6: Risk Management and Compliance** This section identifies potential risks—like technical issues or regulatory violations—and provides strategies to mitigate them effectively.
- **Section 7: Financial Considerations and Funding Opportunities** The financial aspects of adoption are analyzed, including a cost-benefit breakdown and information on funding options such as EU grants.
- **Section 8: Support Framework and Ecosystem Building** The value of collaboration through consortia and knowledge-sharing networks is highlighted, showing how SMEs can tap into collective resources and expertise.

2 Blockchain-Integrated QTSPs: Relevance for SMEs

SMEs are vital to the economic framework of the European Union, representing more 99% of all businesses and employing approximately 100 million people [1]. Despite their importance, SMEs encounter significant challenges, including limited financial and human resources, the complexity of complying with strict regulations, and competition from larger firms with greater capabilities. In this environment, trust and security are essential for electronic transactions, requiring SMEs to adopt cost-effective solutions that improve efficiency while ensuring compliance. Blockchain-integrated QTSP solutions offer a powerful approach to overcoming these hurdles.

Blockchain technology provides a decentralized, immutable, and transparent ledger that

enhances security by maintaining tamper-evident records. Once a transaction is recorded, it cannot be altered, fostering trust in digital interactions [2]. This feature is particularly valuable for SMEs, which often lack the resources to implement robust security measures independently. Additionally, blockchain streamlines processes like certificate issuance, verification, and revocation through automation, addressing operational inefficiencies that disproportionately burden smaller businesses. For example, traditional certificate management can be slow and error-prone, but blockchain's use of smart contracts reduces manual effort and minimizes errors [3], as supported by studies on blockchain's impact on SMEs [4].

Legal compliance is another critical area where blockchain-integrated QTSPs benefit SMEs. The EU's Electronic Identification, Authentication, and Trust Services (eIDAS) Regulation [5] and General Data Protection Regulation (GDPR) [6] set stringent standards for data security, privacy, and cross-border transactions. Blockchain's cryptographic validation ensures the authenticity and integrity of digital signatures and seals, meeting eIDAS requirements [5]. Its decentralized structure also supports GDPR compliance by enabling distributed data storage, addressing data sovereignty concerns [6]. This results in a system that delivers legally recognized trust services efficiently, with a transparent audit trail that simplifies compliance reporting and risk management—key advantages in trust-sensitive sectors like finance and healthcare [7].

Furthermore, blockchain-enabled QTSPs provide SMEs with a competitive edge by facilitating innovative, secure, and compliant digital services. For instance, self-sovereign identity frameworks allow users to control their personal data via verifiable credentials, enhancing trust with clients and partners [8]. This capability differentiates SMEs in competitive markets, particularly as privacy concerns grow. Enhanced transparency and streamlined processes also empower SMEs to meet market demands, expand their customer base, and engage in international trade more effectively [9].

In summary, blockchain-integrated QTSP solutions equip SMEs with tools to address their unique challenges. By leveraging blockchain's decentralized framework, SMEs can achieve secure, efficient, and compliant digital transactions, positioning them to compete with larger enterprises and thrive in the digital economy.

2.1 Why Should SMEs Adopt Blockchain-Enabled QTSP?

Blockchain-enabled trust frameworks improve the security of digital transactions by distributing trust across a decentralized network of nodes. This approach eliminates the

single point of failure typical in centralized systems, thereby reducing the risk of data manipulation and unauthorized access. The immutability of distributed ledgers, combined with cryptographic techniques, ensures that sensitive records, electronic signatures, and time-stamped transactions remain tamper-proof. These characteristics are critical not only for the protection of information, but also for the construction of a transparent, verifiable audit trail that supports regulatory compliance [5, 6]. Beyond security, integrating blockchain into QTSP operations enables SMEs to achieve a level of legal certainty and compliance that is traditionally accessible only to larger enterprises. Regulations such as the eIDAS Regulation and the GDPR impose stringent standards on digital trust services and data protection. By automating processes such as certificate issuance, verification, and revocation through smart contracts, blockchain-based QTSP solutions streamline workflows, reduce manual errors, and lower the overhead associated with maintaining compliance. This level of automation not only simplifies internal operations, but also significantly reduces the risk of non-compliance, thus mitigating potential legal and financial penalties [5, 6].

Furthermore, the decentralized nature of blockchain supports seamless interoperability between different jurisdictions and systems. For SMEs operating in a global market, this means that cross-border digital transactions can be executed with greater transparency and mutual trust. The nature of blockchain transactions fosters confidence among international partners and regulatory bodies, helping SMEs expand their reach without the typical barriers imposed by heterogeneous national standards. Studies have shown that such innovations can lead to improved operational efficiency and lower long-term costs, positioning SMEs as agile competitors in a rapidly digitizing economy [10, 9]. Integrating blockchain-enabled QTSP solutions boosts the competitiveness of SMEs. Using cutting-edge technologies, small and medium enterprises demonstrate their dedication to innovation and strong security protocols, attracting clients interested in data integrity and privacy. This move also creates new growth opportunities in industries where trust and compliance are essential. Essentially, strategically embedding blockchain within QTSP frameworks provides SMEs with the resources needed to tackle limited assets, navigate regulatory hurdles, and compete with larger enterprises.

2.2 Typical Pain Points and How Blockchain-Integrated QTSP Addresses Them

SMEs encounter a range of operational and strategic barriers that impede their digital transformation efforts. A primary challenge is their limited financial and human re-

sources, which restrict their ability to deploy advanced cryptographic services and identity management systems critical for secure digital transactions. For instance, implementing traditional Public Key Infrastructure (PKI) systems often requires significant upfront investment in hardware security modules (HSMs) and specialized IT personnel—costs that can exceed €50,000 annually for even basic setups [11]. SMEs, typically operating with constrained budgets and lacking in-house expertise, find these expenses prohibitive. Additionally, the shortage of skilled staff exacerbates the difficulty of maintaining these systems, leaving SMEs vulnerable to inefficiencies and security gaps.

Beyond resource constraints, SMEs must navigate a complex regulatory landscape, including the eIDAS Regulation [5] and the General Data Protection Regulation (GDPR) [6]. These frameworks impose stringent requirements for electronic signatures, data privacy, and interoperability between-border trust services. Compliance requires detailed documentation, regular audits, and adherence to standards such as ETSI EN 319 411-1 [12], which can overwhelm SMEs without dedicated legal or compliance teams. A single misstep, such as failing to secure a qualified electronic signature, can result in legal penalties, reputational damage, or exclusion from EU tenders, compromising your competitive position [10]. In addition, cybersecurity poses a persistent threat. SMEs relying on centralized databases are prime targets for cyberattacks, with 43% experiencing data breaches in 2022 alone [13]. Limited resources hinder the implementation of robust intrusion detection, disaster recovery plans, or regular security audits, amplifying their exposure to risks like ransomware or phishing.

Blockchain-enabled Qualified Trust Service Provider solutions offer advantages to address these challenges by delivering auditable, cost-efficient, and automated processes that eliminate the need for SMEs to develop complex cryptographic infrastructure from scratch. Unlike traditional systems that require substantial capital expenditures, such as standalone HSMs costing upward of €5,000 per unit [11], blockchain-based QTSPs provide a modular service-based approach. Through pay-as-you-go or subscription models, SMEs can access tailored functionalities like certificate issuance, time-stamping, or identity verification, scaling services dynamically to match operational needs [9]. For example, a logistics SME could adopt a blockchain-based electronic seal service for €500 annually, avoiding the high cost of an in-house solution (€10,000 or more)[10]. This flexibility reduces financial strain and allows SMEs to redirect resources to core business activities.

Compliance is also simplified through the unified and tamper-evident ledger on the blockchain. Each transaction is automatically recorded and secured with cryptographic

proofs, creating a transparent audit trail that aligns with eIDAS and GDPR requirements [5, 6]. This automation streamlines periodic regulatory checks, reducing audit preparation time by up to 30% according to industry estimates [4] and minimizes the burden of GDPR documentation by embedding data minimization principles into the system design. Furthermore, the immutability of the ledger allows immediate detection of inconsistencies or unauthorized changes, enhancing accountability and trust [2]. SMEs can thus meet regulatory demands without the overhead of extensive compliance staff, leveling the playing field with larger competitors.

Cybersecurity risks are significantly mitigated by the decentralized architecture of the blockchain. Unlike centralized databases vulnerable to single-point failures, the blockchain distributes transaction records and validation processes between multiple network nodes, reducing the risk of catastrophic outages or breaches [14]. When paired with QTSP certification standards, such as the use of Qualified Signature Creation Devices (QSCD), this structure provides SMEs with robust legal and technical assurance [12]. For instance, a 2023 pilot in Spain's Alastria network demonstrated that blockchain-based identity verification cut breach-related losses by 20% for participating SMEs [9]. This resilience empowers SMEs to engage confidently in secure, cross-border transactions, knowing their electronic signatures and sensitive data are protected in line with EU standards.

In a global marketplace increasingly defined by digital trust and regulatory rigor, blockchain-integrated QTSP solutions provide SMEs with a strategic advantage. By addressing financial, compliance, and security pain points, these technologies enable smaller firms to improve operational resilience, reduce costs, and compete effectively. The combination of affordability, automation, and robust protection positions SMEs to thrive in the digital economy, meeting the demands of clients, regulators, and partners alike.

2.3 Legal and Regulatory Considerations

Operating within the European Union imposes a multifaceted legal framework on SMEs, governing electronic trust services and data protection. The *Electronic Identification, Authentication, and Trust Services* (eIDAS) Regulation [5] serves as the cornerstone, standardizing mutual recognition of electronic identification and trust services across Member States. This framework grants qualified electronic signatures and seals legal equivalence to their physical counterparts, facilitating seamless digital transactions throughout the EU. For SMEs leveraging blockchain-based QTSP solutions, eIDAS ensures that adherence to its technical specifications—such as secure certificate issuance and key management—guarantees the legal validity of their digital interactions. This harmo-

nized approach reduces barriers to cross-border commerce, enabling SMEs to engage confidently with partners in diverse jurisdictions without navigating disparate national rules [15].

Simultaneously, the *General Data Protection Regulation* (GDPR) [6] imposes rigorous obligations on personal data handling, challenging blockchain's inherent immutability. Principles like data minimization and the right to erasure require innovative adaptations. SMEs can address these by storing sensitive data off-chain, using zero-knowledge proofs for verification without disclosure, or employing cryptographic hashing to anonymize records on-chain [16]. These strategies balance GDPR compliance with blockchain's security benefits, ensuring privacy while preserving an auditable ledger. Such designs demand careful planning but enable SMEs to meet legal expectations without sacrificing technological advantages [17].

Beyond eIDAS and GDPR, SMEs must contend with sector-specific mandates and national variations. In finance, healthcare, and logistics, additional directives—such as the EU's Payment Services Directive (PSD2) [18] or Germany's e-Invoicing laws—layer further requirements onto digital transactions. Compliance with international standards like ISO/IEC 27001 [19] or the ETSI EN 319 series [12] can streamline these obligations, enhancing credibility with regulators and clients. Partnering with pre-certified QTSPs allows SMEs to adopt blockchain solutions that inherently meet these benchmarks, minimizing the need for internal expertise [20].

A pivotal development is the proposed *eIDAS 2.0* framework, introducing the *European Digital Identity Wallet* (EUDI Wallet) to bolster user control and interoperability [21]. Set to expand the scope of digital identities and verifiable credentials, eIDAS 2.0 will likely influence blockchain system design by prioritizing privacy-by-design and cross-border functionality. SMEs adopting these solutions must anticipate these shifts, as compliance could unlock access to broader markets and strengthen customer trust [22]. Proactive alignment with this evolving regulation positions SMEs to capitalize on emerging opportunities, such as streamlined public sector interactions or enhanced e-commerce capabilities.

In essence, blockchain-integrated QTSP solutions enable SMEs to navigate this regulatory landscape effectively. By embedding eIDAS-compliant processes and privacy-focused innovations, these systems reduce legal risks, foster trust with stakeholders, and support expansion into EU markets under a cohesive digital framework. Staying attuned to legislative updates ensures SMEs remain agile and competitive in a regulated digital

economy.

3 Standards and Frameworks for Blockchain-Enabled Trust Services

The integration of blockchain technology into QTSP frameworks is based on a set of technical and regulatory standards. At the core of this ecosystem is the ETSI EN 319 series, which establishes a comprehensive foundation for digital trust services within the EU. ETSI EN 319 401 delineates general policy requirements for trust service providers, emphasizing governance, risk management, and operational integrity [23]. Based on this, ETSI EN 319 411-1 and 411-2 specify detailed security and operational protocols for issuing digital certificates and qualified electronic signatures, ensuring their legal validity under the eIDAS Regulation [12, 5]. These standards collectively safeguard the authenticity and interoperability of trust services, enabling seamless cross-border recognition of digital transactions.

Further refining these capabilities, ETSI EN 319 102-1 and 102-2 outline precise procedures for the creation and validation of advanced electronic signatures and seals, critical for blockchain-based implementations [24]. Furthermore, ETSI TS 119 495 addresses identity proofing, providing secure methodologies to authenticate identities before credential issuance, a key step in maintaining trust in decentralized systems [25]. This ETSI framework ensures that blockchain-enabled QTSP solutions deliver consistent, secure, and legally compliant services, aligning with eIDAS mandates and supporting GDPR's data protection goals without redundant technical overlap.

On the international stage, standards such as ISO / IEC 27001 bolster blockchain trust services by offering a systematic approach to managing cybersecurity risks [19]. Updated in 2022, it addresses modern threats like quantum computing risks, ensuring resilience across both blockchain and conventional IT environments. ISO 22739:2020 standardizes the blockchain terminology, fostering a common language for global adoption, while ISO 23257:2022 provides a reference architecture for scalable and interoperable blockchain systems [26, 27]. These ISO standards complement the ETSI EN 319 412 series, which defines certificate profiles to ensure uniformity and reliability in credential issuance and verification [28]. Together, they create a cohesive framework that bridges technical innovation with regulatory compliance.

For SMEs, aligning blockchain-enabled QTSP solutions with these standards offers dual

benefits: It offers increased security and simplified integration into existing digital ecosystems. Compliance with ETSI and ISO benchmarks not only meets EU legal requirements but also enhances system transparency and auditability, critical for regulatory oversight [20]. This alignment empowers SMEs to deploy scalable and trustworthy solutions that compete in a global digital marketplace, leveraging standardized protocols to reduce development costs and ensure interoperability with partners and public infrastructures.

4 Roadmap for Adopting Blockchain-Enabled QTSP Solutions

For SMEs, adopting blockchain-enabled Qualified Trust Service Provider (QTSP) solutions requires a structured roadmap to navigate the shift from centralized trust frameworks to decentralized, blockchain-based systems. This transition introduces unique technical and operational demands—such as consensus mechanisms and cryptographic protocols—that differ from traditional setups. The roadmap outlined here provides a phased approach, balancing feasibility with scalability, to help SMEs integrate these solutions effectively. It addresses key challenges, including resource constraints and regulatory alignment, while offering practical steps to enhance digital trust capabilities.

4.1 Roadmap Overview

The adoption process unfolds in four interconnected phases: readiness assessment, pilot project, resource allocation, and full deployment with milestones. The *readiness assessment* evaluates an SME's digital infrastructure, staff skills, and compliance baseline, identifying gaps that could impede blockchain integration. Next, a *pilot project* tests a specific use case—like certificate issuance—allowing SMEs to refine their approach with minimal risk. The *resource allocation* phase secures budget, personnel, and partnerships to scale the pilot into a production system. Finally, *full deployment* integrates the solution across operations, guided by a timeline with clear milestones. This phased strategy ensures SMEs can adapt to technical complexities and regulatory shifts, such as eIDAS 2.0 [21], while optimizing resource use [**EIB_Whitepaper2021**].

4.2 Readiness Assessment for SMEs

Before embarking on blockchain adoption, SMEs must assess their operational and technical preparedness. This phase examines network resilience, data management prac-

tices, and compliance with standards like ETSI EN 319 411-1 [12]. For example, an SME with outdated servers may struggle with blockchain's computational demands, necessitating upgrades or cloud solutions. Workflow analysis can pinpoint inefficiencies—such as manual certificate renewals—that blockchain could streamline, providing a clear value proposition [9].

4.2.1 Organizational Maturity and Digital Infrastructure

Organizational maturity hinges on governance, risk management, and digital adoption levels. SMEs with existing tools for secure data exchange or electronic signatures are better positioned, as these systems share foundational elements like key management with blockchain [20]. Where deficiencies exist, incremental enhancements—such as adopting cloud-based encryption—can bridge gaps without overwhelming resources. Aligning leadership and staff with decentralized trust concepts is equally critical, requiring a shift from traditional control models to collaborative frameworks suited for blockchain's multi-node structure.

4.2.2 Skills and Training Requirements

Blockchain's technical nuances demand specialized skills, from smart contract coding to node management. SMEs must train IT staff in these areas, while compliance teams need grounding in blockchain's regulatory implications [14]. Short, targeted programs e.g., online courses from platforms like Coursera or consortia workshops—can upskill employees cost-effectively, reducing reliance on external experts. Cross-functional training ensures broader organizational buy-in, minimizing risks of missteps during deployment.

4.3 Step-by-Step Adoption Path

A phased adoption path mitigates risks and optimizes resource use, unfolding across three key stages namely (i) pilot project, (ii) resource allocation, and (iii) timeline with milestones.

4.3.1 Pilot Project Identification and Feasibility

Starting with a pilot project limits exposure while proving the value of the blockchain. SMEs should select a high impact, contained use case, such as automating supplier credential verification, to test integration with QTSP services. A sandbox environment allows teams to assess performance (e.g., transaction speed) and interoperability with ex-

isting systems, improving the solution before scaling [4]. Stakeholder feedback during this stage ensures that the pilot aligns with business needs and regulatory requirements.

4.3.2 Resource Allocation (Budget, Staff, Partnerships)

Scaling from pilot to production requires deliberate resource planning. Budgets must cover platform licensing (e.g., €1,000-€5,000 annually for cloud-based blockchain services [**EIB_Whitepaper2021**]), hardware (if on-premise), and staff training. SMEs can opt for modular platforms like Hyperledger Fabric, adding features incrementally to manage costs. Partnerships with certified QTSPs or blockchain consortiums (e.g., Alastria) provide expertise and shared infrastructure, compensating for initial investments [9]. Due diligence on vendors, focusing on security certifications and scalability, ensures long-term viability.

4.3.3 Timeline and Milestones

A defined timeline with milestones drives the deployment. Short-term goals (3 to 6 months) include pilot completion and infrastructure setup, while medium-term goals (6 to 12 months) expand features such as multisignature approvals. Long-term milestones (12–24 months) aim for full integration and compliance with evolving standards, such as the EUDI Wallet eIDAS 2.0 [22]. Regular audits at each stage, assessing throughput, security, and user adoption, enable course corrections, ensuring the solution scales without compromising reliability.

4.4 Benefits of the Phased Approach

This roadmap offers SMEs a practical and low-risk path to adoption. By starting with a readiness assessment, companies pinpoint critical upgrades early, avoiding costly upgrades later. Pilot projects validate feasibility in real-world conditions, building confidence before broader rollout. Resource allocation balances investment with benefits such as efficiency gains (e.g., 20% cost reduction in certificate management [9]), while milestones provide flexibility to adapt to regulatory changes. Ultimately, this approach equips SMEs with secure, compliant trust services, enhancing their competitiveness in the European digital market.

5 Implementation Guidelines and Best Practices

Incorporating a blockchain-enabled QTSP framework involves balancing technical feasibility, regulatory compliance, and organizational preparedness. SMEs need more than strategic direction; they need detailed implementation guidance to address the specifics of designing, deploying, and maintaining trust services. Such guidance should cover the intricacies of system architecture, including the interactions between the chosen infrastructure, whether cloud-based, on-premises, or hybrid, and both existing legacy systems and new blockchain components. In addition, organizations need to focus on operational best practices, from storing and managing cryptographic keys to coordinating technical upgrades between internal teams without disrupting service continuity. Properly addressing these factors helps SMEs achieve an effective blend of cost efficiency, security, and interoperability. Consistent documentation, clear change management procedures, and rigorous testing are also crucial to maintaining the stability of the deployment. The sections that follow highlight critical considerations for building a secure technical architecture and illustrate how to integrate legacy applications with blockchain technology.

5.1 Technical Architecture Overview for SMEs

The technical architecture supporting a blockchain-enabled QTSP environment should serve as the backbone for secure, scalable, and legally compliant trust operations. For smaller companies, this requires strategic design choices that take advantage of decentralized features, such as distributed consensus and smart contract automation, while still aligning with the constraints imposed by limited IT budgets and regulatory rules such as GDPR or eIDAS. It is often beneficial for SMEs to begin with a modular architecture in which trust services, such as digital signatures and certificate management, are kept distinct from auxiliary blockchain features. Through this way, organizations can maintain flexibility as their requirements evolve, adding or removing modules without overhauling the entire system. Equally important is ensuring that the technical stack supports interoperability across various blockchain protocols and can seamlessly handle the concurrent operation of multiple nodes. Clear considerations should be given to load balancing, failover mechanisms, and monitoring solutions, as blockchain networks operate continuously and require robust fault tolerance. In addition, employing standardized interfaces and open APIs can ease integration with both internal applications and external services, allowing the trust service layer to interact smoothly with cloud

environments, identity verification systems, or specialized data analytics platforms. Ultimately, the objective is to establish a framework that respects the limitations of SME resources and is adaptable enough to meet the security and reliability standards inherent to QTSP operations.

5.1.1 Cloud vs. On-Premise Options

When selecting an infrastructure model for hosting a blockchain-integrated QTSP solution, the choice often narrows to cloud-based versus on-premise deployment, each offering distinct advantages and trade-offs. Cloud platforms appeal to many SMEs because they facilitate rapid scalability and straightforward resource provisioning, often at a predictable cost. The availability of managed blockchain services further reduces the burden of network management and allows smaller IT teams to focus on building and maintaining the trust layer rather than operating and securing blockchain nodes. In addition, cloud vendors typically provide specialized security features, such as hardware security modules for key protection, that align well with eIDAS-compliant workflows. However, cloud adoption can raise data sovereignty concerns, especially for SMEs handling sensitive client information or operating in heavily regulated industries. In these cases, on-premise setups may be preferable for retaining direct control over data storage and network access. Although on-premise models grant a higher degree of autonomy, they also impose a more substantial requirement for internal expertise in infrastructure configuration, maintenance, and security monitoring. Additionally, on-premise implementations may be less elastic in handling peak loads or sudden spikes in certificate issuance requests, making capacity planning and redundancy strategies critical to avoid performance bottlenecks. A third option involves hybrid approaches that combine on-premise nodes for sensitive operations with cloud-based redundancy for failover scenarios or less sensitive data storage, thus offering a level of flexibility that may be especially appealing to risk-averse SMEs exploring blockchain technologies for the first time.

5.1.2 Integrating with Legacy Systems

For many SMEs, the transition to blockchain-based trust services must coexist with older software assets that still play crucial roles in daily operations, such as enterprise resource planning modules, document management solutions, or customer relationship management tools. Integrating blockchain features with these legacy systems can be challenging because their data formats, authentication models, or processing workflows may not align with the decentralized consensus and cryptographic methods employed by blockchain networks. Consequently, SMEs often benefit from a layered integration

strategy, where a middleware component acts as a gateway between blockchain nodes and conventional back-end applications. This middleware not only translates data structures and coordinates identity checks but also manages transaction throughput by queuing and batching requests, ensuring that the blockchain network is neither overwhelmed nor underutilized. Another pivotal aspect of integration involves the establishment of application programming interfaces (APIs) that define how legacy systems communicate with the blockchain layer, including how certificates are requested, issued, or revoked. These APIs must incorporate eIDAS-compliant security controls, covering encryption of data in transit and the proper handling of cryptographic keys, to maintain high levels of trust. Furthermore, integration planning should account for the potential need to migrate select data sets to or off the blockchain, particularly where there are concerns about GDPR compliance or data retention rules. Such migrations might involve hashing or tokenizing personally identifiable information, so that detailed records are held in more conventional databases while only secure references reside on-chain. Ensuring all of these facets—APIs, middleware, encryption, data migration strategies—are both well-documented and regularly tested can help SMEs mitigate risk, sustain performance, and continue leveraging their legacy systems as they evolve toward a decentralized trust model.

5.2 Security and Privacy Best Practices

Effective privacy and security safeguards are crucial for SMEs adopting blockchain-based QTSP solutions. Despite the advantages of decentralization and immutability, blockchain alone does not guarantee protection from threats such as unauthorized access, cryptographic key misuse, or non-compliance with data protection directives. To maintain trust and legal standing, SMEs must systematically incorporate preventive and detective controls into every layer of the blockchain-integrated architecture. This is especially important given the mixed environment in which blockchain services often operate: legacy back-ends, cloud-based front-ends, and multiple external data processors. By adhering to stringent security protocols and industry-aligned privacy methods, SMEs can limit their vulnerability to breaches and ensure conformance with existing regulations. Furthermore, organizations that can demonstrate robust security and privacy postures can benefit from accelerated onboarding of new clients, particularly in sectors such as healthcare, finance, and government contracting that prioritize strong data protection standards. The following sub-points detail specific considerations around certificate and key management practices, as well as overarching compliance measures

related to GDPR, eIDAS, and similar regulatory frameworks.

5.2.1 Handling Certificates, Signatures, and Private Keys

A cornerstone of any QTSP operation lies in the careful generation, management, and storage of cryptographic keys and certificates. Blockchain does not diminish the need for meticulous key lifecycle handling; in fact, the distributed nature of the technology can amplify the risks if a private key is lost or compromised. SMEs should maintain a strict policy that dictates the secure generation of private keys using hardware security modules (HSMs) or equivalent certified appliances that meet recognized security standards. Ideally, the creation of digital certificates and signatures should be integrated with tamper-resistant modules to prevent accidental or malicious key disclosure. This step is crucial to preserving the integrity of trust services, especially when used for legal documents or cross-border transactions. In addition to secure key creation, ongoing rotation and revocation practices are vital. Private keys should be rotated at predefined intervals to reduce the window of exposure if a key is compromised. Likewise, certificate revocation processes should be designed to quickly alert relevant stakeholders and invalidate credentials when misuse or key compromise is detected. Complementing these measures, employing multisignature configurations and granular role-based access controls can further limit the potential impact of unauthorized access. SMEs can also leverage blockchain-based revocation registries, which provide immediate and transparent evidence of certificate changes. All these layers of security ensure that the trust conferred by blockchain-enabled services remains intact under a variety of threat scenarios.

5.2.2 Ensuring Compliance (GDPR, eIDAS)

Compliance with GDPR, eIDAS, and other regulations extends beyond cryptographic rigor to include processes such as data minimization, consent management, and lawful data handling practices. Under GDPR, data controllers must collect only necessary personal data, document the legal basis for each processing activity, and ensure that individuals can exercise rights such as data access or erasure requests. For SMEs integrating blockchain, reconciling the inherent immutability of distributed ledgers with requirements for data deletion poses a particular challenge. Strategies to reconcile these contrasts include storing personal data off-chain while keeping only hashed or tokenized references on the ledger, or using advanced cryptographic techniques like zero-knowledge proofs to validate attributes without revealing underlying data. Adherence to the eIDAS requirements is equally significant, as these rules specify the procedures and qualifications for issuing and recognizing digital signatures and time stamps. Specifically, the reg-

ulation sets high expectations around the legal validity of electronic signatures and seals, mandating that solutions be auditable and tamper-evident. By adopting best practices such as embedding standardized signature formats, such as XAdES, CAdES, or PAdES, SMEs can present their electronic documents in a manner that aligns with recognized technical standards. Organizations should also ensure that each step in their blockchain workflows, from certificate issuance to user authentication, is documented to facilitate periodic audits. Automated compliance checks, smart contracts that encode data retention rules, and continuous monitoring of transaction patterns help SMEs stay within the bounds of ever-evolving regulations.

5.3 Scalability, Performance, and Maintenance Considerations

Designing a blockchain-integrated system for long-term reliability and cost effectiveness requires careful consideration regarding scalability, performance, and operational maintenance. Although a blockchain can theoretically accommodate increasing volumes of transactions, in practice, there are architectural and consensus-based constraints that can limit throughput or significantly raise transaction costs. A successful SME deployment avoids performance bottlenecks by anticipating growth in transactions and participants, ensuring that system resources, whether cloud-based or on-premise, are tuned to handle peak demand without sacrificing service responsiveness or legal compliance. Meanwhile, systematic maintenance routines, ranging from periodic software updates and security patches to regular consensus mechanism audits, allow an enterprise to stay current with the constantly evolving nature of distributed ledger platforms. Keeping a proactive eye on performance metrics, such as block confirmation times or network latency, helps SMEs identify emerging issues before they escalate, thus preserving service continuity and user trust.

5.3.1 Layer 2 Solutions, Permissioned Networks, etc.

Various architectural choices enable SMEs to tackle scalability and performance more effectively. Layer 2 (L2) solutions, for example, are built on top of an existing blockchain, offering additional transaction capacity and faster confirmations without modifying the core protocol. Techniques such as payment channels or rollups can help decongest the main chain, making them well suited for scenarios where an SME's trust services generate a high volume of chain events. Another approach involves adopting permissioned blockchains, in which network validators must be preapproved or meet certain criteria. By reducing the open, anonymous nature of typical public chains, permissioned net-

works often achieve superior throughput and predictable latency levels. These qualities can be particularly advantageous for SMEs that require more controlled governance and data visibility. Additionally, a permissioned environment aligns more naturally with the eIDAS requirement that trust service providers maintain full accountability for the integrity of issued signatures and time stamps. In all cases, a sustainable balance must be struck between decentralization (and the corresponding benefits of fault tolerance and transparency) and manageability (which relates to performance overhead, day-to-day operation, and compliance). SMEs that prioritize efficiency and controlled access might converge on a permissioned setup augmented by L2 mechanisms, thus achieving both strong security and operational agility. Ongoing capacity planning is crucial: As transaction loads fluctuate or new parties join the blockchain network, it may be necessary to adjust consensus parameters, node hardware, or the frequency of off-chain batch settlements. Consistent reviews of system logs, smart contract behavior, and node health can prevent minor performance issues from snowballing into disruptive outages. Through such careful stewardship, SMEs can deliver trust services that are scalable, fully poised to grow alongside their business operations.

6 Risk Management and Compliance

The deployment of blockchain-enabled QTSP solutions introduces a unique risk profile, blending the intricacies of distributed ledger technology (DLT) with the stringent demands of EU regulations such as eIDAS [5] and GDPR [6]. Unlike centralized trust systems, blockchain's reliance on cryptographic key management, smart contract execution, and multi-node coordination amplifies technical vulnerabilities while elevating compliance stakes. Failures, whether due to system outages, cyberattacks, or regulatory lapses, can erode legal validity, incur penalties, and damage the reputation of SME. Thus, a robust risk management framework is critical, integrating proactive threat identification, mitigation, and continuous oversight across technical and regulatory domains. This section details key risks, technical countermeasures, and an advanced monitoring approach to ensure that SMEs maintain secure, compliant operations.

6.1 Common Risks in Blockchain-Enabled QTSP Deployments

SMEs face a convergence of technical and regulatory risks when integrating blockchain into QTSP frameworks, each threatening the core trust service functionality: digital signatures, seals, and time stamping.

6.1.1 Technical Failures, Data Breaches, and Smart Contract Vulnerabilities

The distributed nature of the blockchain demands high availability and integrity between nodes, but technical failures remain a risk. Network partitions or consensus failures (e.g. Byzantine faults) can delay or invalidate transactions, disrupting QTSP services such as certificate issuance [29]. For example, a 51% attack on a permissionless blockchain could compromise ledger integrity, though permissioned networks common in QTSP deployments mitigate this through restricted access [30]. Hardware failures, such as disk corruption in the validator nodes, further threaten uptime, with recovery complicated by the append-only structure of the blockchain.

Data breaches target private keys and off-chain repositories, compromising cryptographic security. A 2023 ENISA report notes that 30% of blockchain-related incidents stem from key mismanagement [31]. Smart contracts—automating trust processes like signature validation—introduce additional vulnerabilities. Reentrancy attacks, integer overflows, or logic errors (e.g., unhandled exceptions) can enable unauthorized fund transfers or lock assets, as seen in the 2016 DAO hack [32]. For SMEs, such incidents could invalidate legal trust services, triggering disputes or regulatory scrutiny.

6.1.2 Regulatory Non-Compliance Risks

Compliance with eIDAS and GDPR poses distinct challenges. eIDAS requires rigorous identity proofing (ETSI TS 119 495 [25]) and lifecycle management for qualified certificates, with non-compliance risking legal nullification of signatures. The GDPR right to erasure clashes with blockchain immutability, while decentralized storage complicates the accountability of the data controller [16]. A 2022 study found 25% of blockchain implementations struggled with GDPR alignment due to inadequate off-chain strategies [17]. SMEs, often resource-constrained, face increased exposure to fines (up to €20M under GDPR) or operational bans if audits reveal lapses.

6.2 Mitigation Strategies and Incident Response

A multilayered mitigation framework is essential to address these risks, leveraging advanced tools and protocols tailored to blockchain-QTSP integration.

6.2.1 Technical Safeguards

Preventing technical failures requires redundant node deployment and consensus optimization. Using Practical Byzantine Fault Tolerance (PBFT) ensures resilience against

up to one-third of node failures, suitable for permissioned QTSP networks [33]. Regular stress testing - simulating 1000+ transactions per second (TPS) - validates throughput and latency under load. For data breaches, Hardware Security Modules (HSMs) with FIPS 140-2 Level 3 certification secure private keys, reducing theft risk by 90

Smart contract security requires rigorous development practices. Static analysis tools such as Mythril detect vulnerabilities (e.g. reentry), while formal verification with tools such as Isabelle / HOL proves the contract conformity to specifications [34]. Multisignature (multisig) wallets for critical operations requiring 2-of-3 approvals prevent single-point compromises. Post-deployment, run-time monitoring with invariants (e.g., balance checks) flags anomalies in real time.

6.2.2 Regulatory Compliance Measures

To align with eIDAS, SMEs should implement workflows compliant with ETSI EN 319 411-1, automating certificate life cycle tracking through smart contracts [12]. GDPR compliance requires hybrid storage: Personal data reside off-chain in encrypted vaults, with only hashes on-chain, enabling erasure without ledger conflicts [16]. Zero-knowledge proofs (e.g., zk-SNARKs) verify identity attributes without exposing raw data, satisfying data minimization [35]. Regular conformance testing against eIDAS CAB audits ensures ongoing adherence.

6.2.3 Incident Response Protocols

A structured incident response (IR) plan is vital. Upon detecting a breach, for example, through anomaly detection tools such as Splunk, SMEs must isolate affected nodes, revoke compromised keys using QTSP revocation lists, and inform stakeholders within the 72-hour window of GDPR [6]. A predefined escalation path (IT - compliance - legal) ensures swift action, while post-incident forensics leverages immutable logs for root cause analysis. Training drills - simulating a key leak - enhance staff readiness, reducing downtime by up to 40

6.3 Ongoing Audit and Monitoring Framework

Continuous oversight ensures resilience and compliance. SMEs should implement blockchain-specific monitoring tools such as Hyperledger Explorer to track node health, TPS, and consensus latency, with thresholds (e.g., <5% packet loss) triggering alerts. Smart contract auditing platforms (for example, OpenZeppelin Defender) automate invariant checks,

ensuring signature issuance aligns with ETSI standards [24]. Off-chain logs, mirrored on IPFS with SHA-256 hashing, provide tamper-proof audit trails for GDPR reporting [36].

Regular audits - quarterly internal and annual external by eIDAS-accredited bodies - assess configurations against ISO / IEC 27001 [19]. Penetration testing, targeting smart contract exploits and node DDoS vulnerabilities, identifies weaknesses (e.g., gas limit overflows). Automated compliance scripts, integrated via CI/CD pipelines (e.g., GitLab), verify adherence to eIDAS and GDPR at each update, reducing human error by 85% [4]. This framework fosters a proactive security culture, ensuring SMEs' QTSP solutions remain robust, compliant, and adaptable to emerging threats like quantum decryption [37].

7 Financial Considerations and Funding Opportunities

Blockchain-enabled QTSP solutions promise SMEs enhanced security, operational efficiency, and regulatory compliance, but their deployment demands a meticulous financial strategy. The transition to distributed ledger technology involves both substantial initial investment and ongoing operational costs, which can be particularly burdensome for organizations with limited capital reserves or narrow profit margins. Despite these challenges, empirical data derived from pilot projects and economic models indicate that a well-executed approach can produce substantial long-term benefits, including cost reductions, revenue growth, and improved market positioning [10]. In what follows, this section offers a technical framework for financial planning by detailing typical expenses, potential returns on investment (ROI), and mechanisms for securing external funding. By integrating analytical tools such as Net Present Value (NPV) alongside publicly available EU grant programs, SMEs can optimize resource allocation and gain competitive advantages within a rapidly evolving digital trust ecosystem.

7.1 Cost-Benefit Analysis for SMEs

A structured Cost-Benefit Analysis (CBA) is critical for SMEs operating under tight resource constraints to determine whether blockchain-based QTSP solutions are financially viable. Although it is common to separate expenditures into capital (CapEx) and operational (OpEx) categories, a thorough approach requires granularity when estimating hardware upgrades, integration services, and training. CapEx frequently includes fees associated with permissioned blockchain platforms such as Hyperledger Fabric, which may be licensed annually depending on the number of network nodes and trans-

action volumes [10]. Additional costs often arise from the purchase or upgrade of Hardware Security Modules (HSMs) that comply with standards such as FIPS 140-2 Level 3, particularly for storing and managing cryptographic keys. Spending may also occur in areas such as middleware deployment, where hourly developer rates range significantly, reflecting the complexity of linking blockchain ledgers to existing enterprise resource planning (ERP) systems.

OpEx typically emerges as recurring expenses for cloud-based services such as AWS or Azure, where subscription fees scale according to throughput and storage usage [9]. Continuous training in areas such as Solidity coding or node administration can also represent a nontrivial operational cost. Maintenance requirements, including node monitoring and security patch deployment, commonly demand a fraction of a full-time position, but that role must be carefully budgeted to ensure uninterrupted operations. Empirical studies indicate that pilot projects should ideally limit initial spending to around one-fifth of the projected total cost to control financial risk before larger-scale implementation [38].

Although the adoption of blockchain-enabled trust services may appear expensive at first, the associated benefits can significantly offset these expenditures. Automating certificate issuance through self-executing smart contracts can substantially reduce manual labor. Such efficiencies often translate into saved staff hours, which is consequently freed up resources for higher value tasks. Improvements in transaction throughput and cross-border recognition of e-signatures further reduce administrative and legal overhead [10], enhancing the attractiveness of these solutions in multiple sectors. By minimizing compliance breaches through cryptographically verifiable logs, organizations also mitigate the likelihood of incurring sanctions under regulations such as GDPR [6], further improving the cost-benefit profile.

7.2 Potential ROI and Long-Term Savings

Robust ROI potential becomes evident once SMEs precisely target operational inefficiencies and fully exploit the technical advantages offered by decentralized ledgers. Pilot studies suggest that within one year of deployment, many organizations achieve operational cost savings of 20 to 35 percent [9], thus reducing the repayment period. These efficiencies stem from automating processes, reducing paper-based workflows, and integrating trust services directly into existing enterprise software. The use of smart contracts often eliminates time-consuming tasks related to dispute resolution or document authentication, thereby reducing transactional friction. Some firms report substantial

decreases in cybersecurity insurance premiums, given the audit trails and tamper-evident nature of blockchain-based systems [31]. Incremental revenue gains can also materialize when the improved reliability and trustworthiness of certified digital signatures expand an SME's market share or enable more cross-border transactions.

Long-term technical savings typically accrue over a three- to five-year horizon. As reliance on proprietary infrastructure for Public Key Infrastructure (PKI) diminishes, organizations can reallocate maintenance budgets to strategic expansions in blockchain-based services. In some cases, harnessing open-source platforms like Hyperledger Fabric can reduce annual operating costs, particularly compared to investments in on-premise servers [38]. Scalability emerges as a strategic advantage: blockchains configured for 500 to 1,000 transactions per second can handle growth in user demand without necessitating costly hardware upgrades. Data show that additional benefits arise when automation replaces a significant portion of manual tasks, potentially saving thousands of euros per year in labor. Compliance enhancements that facilitate cross-border recognition of eIDAS can further increase contract volumes for regulated sectors, effectively doubling or tripling the overall ROI by the end of a five-year period [10].

7.3 Funding Opportunities and Optimization

External financing can soften the impact of upfront spending and accelerate the timeline of a blockchain project. EU grants, such as those offered under the Digital Europe Program, commonly range from fifty to 200 thousand euros for pilot initiatives and can cover a substantial fraction of the deployment cost [39]. Horizon Europe also serves as a conduit for research and development funding, often favoring consortia that demonstrate groundbreaking trust service capabilities [40]. Innovation loans from institutions like the European Investment Bank (EIB) support SMEs at competitive interest rates, helping them hedge risk while adopting cutting-edge technologies [10].

Collaborative ventures also reduce capital expenditures by pooling resources among multiple participants, often cutting up-front costs by thirty to forty percent [9]. A phased approach that begins with a pilot project and subsequently broadens deployment avoids immediate overextension and allows for the gradual refinement of key performance indicators. Many SMEs opt for cloud-based environments for their pilot phases and a selective on-premise model for sensitive operations, balancing cost efficiency with security needs. This hybrid approach can shorten breakeven periods by an estimated 12 to 18 months [38]. Because many of these financial arrangements and deployment strategies must also conform to governance standards like ETSI EN 319 401, forward-thinking

SMEs will plan meticulously to ensure that each choice, from vendor selection to financing, aligns with broader compliance requirements and risk management priorities.

By synthesizing cost modeling, ROI analytics, and multiple funding avenues, SMEs can adopt blockchain-based QTSP solutions with minimal risk and maximum returns. Successful strategies hinge on continuous monitoring of the financial landscape, careful selection of funding partners, and timely updates to the underlying technical infrastructure. When executed in alignment with ETSI regulations and broader European directives, these deployments can secure a resilient and cost-effective foothold in an increasingly digital marketplace.

8 Support Framework and Ecosystem Building

Adopting blockchain-integrated QTSP solutions extends beyond technical implementation, requiring SMEs to engage a robust support ecosystem. With limited internal resources compared to larger firms, SMEs benefit from collaborative networks that provide shared infrastructure, technical expertise, and regulatory alignment. This ecosystem—spanning EU-wide consortia, knowledge hubs, and standardized tools—addresses challenges like node management, cryptographic integration, and cross-border interoperability. By leveraging these frameworks, SMEs can accelerate deployment, optimize resilience, and ensure compliance with standards like ETSI EN 319 411-1 [12] and eIDAS 2.0 [21]. This section explores technical collaboration models, knowledge-sharing platforms, and resource toolkits, emphasizing their role in building a scalable, SME-friendly trust service landscape.

8.1 Collaborative Approaches: Consortia and Public-Private Partnerships

Collaboration via consortia and public-private partnerships (PPPs) offers SMEs access to advanced blockchain infrastructure and expertise, reducing individual deployment burdens.

8.1.1 Consortia Models

Consortia like Alastria or the European Blockchain Partnership (EBP) operate permissioned networks (e.g., Hyperledger Fabric, Quorum), where SMEs share governance of validator nodes—typically 5–10 nodes handling 500–1,000 TPS [30]. This distributes

costs (e.g., €10,000–€20,000/year for node upkeep [10]) and maintenance tasks (e.g., consensus upgrades, security patches). Technical benefits include pre-built APIs for eIDAS-compliant signatures and standardized smart contracts (e.g., OpenZeppelin libraries), achieving 99.9% uptime and <1-second latency [9]. Consortia also refine interoperability protocols—like EBP's EBSI, supporting 100+ cross-border use cases—ensuring seamless QTSP integration across EU jurisdictions [41].

8.1.2 Public-Private Partnerships

PPPs, such as those under the Digital Europe Programme, pair SMEs with public entities and tech firms to pilot QTSP solutions. For instance, a 2023 PPP in Spain deployed a blockchain-based credential system, reducing identity verification costs by 30% (€3,000–€5,000/year) via shared HSMs and cloud nodes [39]. These partnerships provide regulatory sandboxes—e.g., testing EUDI Wallet integration under eIDAS 2.0—mitigating legal risks during development [22]. SMEs gain access to subsidized R&D (e.g., €50,000–€200,000 grants) and pre-audited frameworks, cutting deployment timelines by 6–12 months [40].

8.2 Creating and Leveraging SME-Focused Knowledge Networks

Knowledge networks bridge technical and domain expertise, enabling SMEs to optimize blockchain-QTSP deployments through peer learning and expert guidance.

8.2.1 Network Structure and Technical Exchange

Platforms like the European Digital SME Alliance or regional hubs (e.g., Blockchain4Europe) connect SMEs with 50–200 members, hosting repositories of Solidity smart contracts, node configuration scripts, and ETSI-compliant workflows [24]. Technical workshops - offering hands-on training in PBFT consensus or zk-SNARKs integration—enhance skills for <€500/participant [14]. SMEs contribute to use case insights (e.g., agri-food provenance tracking at 1,000 transactions/day), while tech partners provide scalable solutions (e.g., 10 MB / s throughput nodes) [4]. This exchange reduces R&D costs by 20–30% (€5,000–€15,000) via shared IP [9].

8.2.2 Sector-Specific Adaptations

Networks tailor blockchain applications to SME sectors. In logistics, shared frameworks for time-stamping (e.g., 100,000 timestamps/year at <€0.01 each) cut verification latency by 90% [10]. Healthcare SMEs leverage consortia like MyHealthMyData for GDPR-compliant data hashing, processing 500+ patient records daily with zero-knowledge proofs

[17]. These adaptations - supported by 50 to 100 annual case studies - enable SMEs to deploy sector-optimized QTSPs, increasing adoption rates by 15 to 25% [20].

8.3 Essential Tools and Resources

Standardized tools and resources streamline blockchain-QTSP integration, minimizing technical overhead and ensuring compliance.

8.3.1 Technical Toolkits

EBSI or ENISA Toolkits include:

- **Smart Contract Templates**: Pre-verified Solidity code for certificate issuance (e.g., 1,000 certificates / hour) with gas costs <0.01 ETH [42].
- **Node Setup Scripts**: Ansible playbooks for the deployment of Hyperledger nodes, achieving 99.95% uptime on AWS EC2 (t3.medium, €0.04/hour) [31].
- **HSM Integration**: APIs for Thales nShield HSMs, securing 10,000+ keys with <1ms latency [11].

These reduce the setup time by 40 to 60% (2 to 4 weeks vs. 6 to 8) and cut costs by € 2,000 to € 5,000 [38].

8.3.2 Compliance Templates and Checklists

Templates include:

- **DPIAs**: GDPR-ready assessments for off-chain storage, processing 1 GB/day with SHA-256 hashing [36].
- **eIDAS Blueprints**: ETSI EN 319 412-compliant workflows for 500+ signatures/day [28].

Checklists cover:

- **Node Security**: 20-point audit (e.g., TLS 1.3, <5% packet loss) [19].
- **Compliance**: 15-step eIDAS/GDPR validation (e.g., <1% error rate in identity proofing) [25].

These tools, updated quarterly through EU repositories, ensure that SMEs meet regulatory thresholds with 95% audit pass rates, saving €3,000–€7,000/year in consulting fees [20].

8.4 Ecosystem Benefits

This framework accelerates adoption by 12 to 18 months, with consortiums cutting CapEx by 30 to 40% (€ 10,000 to € 15,000) and networks increasing technical capacity by 20 to 30% (for example, 500 TPS) [9]. The tools ensure 99. 9% compliance uptime, improve the resilience of SMEs and enable scalable trust services throughout the EU digital market [41].

Collaboration through consortia and knowledge networks is vital for SMEs. These ecosystems enable resource sharing, expertise exchange, and innovation, accelerating the adoption of QTSP solutions enabled by blockchain [9].

Conclusion

The integration of blockchain technology into QTSP frameworks represents a paradigm shift for SMEs within the European Union's digital economy. This feasibility and market analysis underscores that blockchain-enabled QTSP solutions are not merely an incremental enhancement but a transformative enabler, addressing SMEs' perennial challenges of resource scarcity, regulatory complexity, and cybersecurity exposure. THrough the use of distributed ledger technology (DLT), SMEs can achieve a confluence of operational efficiency, legal compliance, and competitive differentiation, positioning them to thrive in an increasingly digitized marketplace.

From a technical point of view, the decentralized architecture of the blockchain - backed by cryptographic immutability and smart contract automation - provides robust security and transparency that traditional centralized systems struggle to replicate. The ETSI EN 319 series, ISO/IEC 27001, and emerging eIDAS 2.0 standards provide a rigorous framework, ensuring that blockchain-based trust services meet stringent requirements for certificate issuance, identity proofing, and cross-border interoperability [12, 19, 21]. For SMEs, this alignment translates into a tamper-evident audit trail and automated compliance workflows, reducing the operational overhead of manual processes by up to 30% and mitigating the risks of GDPR fines exceeding € 20M [4, 6]. Moreover, permissioned networks and Layer 2 solutions enable scalability - handling 500–1,000 transactions per second - without compromising latency or cost, a critical factor for resource-constrained firms [30].

Financially, the adoption of these solutions demands a strategic approach to balance upfront capital expenditures (CapEx) of €30,000–€50,000 against long-term returns. Pilot

data indicate a robust return on investment (ROI) in 2 to 5 years, driven by operational savings (20 to 35%) and revenue growth (10 to 25%) from increased trust and market access [9, 10]. EU funding mechanisms, further alleviate initial burdens, enabling SMEs to implement phased implementations that break even earlier [39]. This economic viability, paired with technical resilience, positions blockchain-QTSP integration as a feasible investment rather than a speculative venture.

The ecosystem support framework amplifies these benefits, with consortiums like Alastria and the EBSI, reducing CapEx by 30–40% through shared infrastructure and preverified tools [41]. Knowledge networks and technical toolkits, including Solidity templates and ETSI-compliant workflows, reduce deployment timelines by 40 to 60%, empowering SMEs to bridge skill gaps and sector-specific needs (e.g., 100,000 timestamps/year at <€0.01 each in logistics) [**EIBWhitepaper2021]**, 42]. This collaborative backbone not only accelerates adoption but fosters innovation, as SMEs leverage peer insights to refine use cases such as self-sovereign identity or GDPR-compliant data hashing [17].

However, risks remain: technical failures, vulnerabilities in smart contracts, and regulatory missteps could undermine trust and legal standing. A proactive risk management framework, integrating PBFT consensus, HSM-secured keys, and continuous monitoring via tools like Hyperledger Explorer, mitigates these threats, achieving 99.9% uptime and 95% audit pass rates [**ENISA2023]**, 33]. SMEs must also anticipate future challenges, such as quantum decryption threats, by adopting post-quantum cryptography as standards evolve [37].

In conclusion, blockchain-integrated QTSP solutions offer SMEs a strategic pathway to digital transformation, harmonizing security, compliance, and economic pragmatism. The roadmap—spanning readiness assessments, pilot testing, and full deployment—provides a practical blueprint, while consortia and funding optimize execution. As eIDAS 2.0 and the European Digital Identity Wallet reshape the trust landscape, early adopters will gain a first-mover advantage, cementing their role as agile innovators in the EU's digital single market [22]. For SMEs, the question is no longer whether to adopt, but how swiftly and effectively they can harness this technology to redefine their competitive edge.

References

[1] Eurostat. Small and Medium-Sized Enterprises (SMEs) in the EU. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Small_and_medium-sized_enterprises_(SMEs)_in_the_EU. 2023.

[2] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: *Cryptography Mailing List* (2008).

[3] Nick Szabo. "Smart Contracts: Building Blocks for Digital Markets". In: *Extropy* (1996).

[4] Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues". In: *Telematics and Informatics* 36 (2019), pp. 55–81. DOI: 10.1016/j.tele.2018.11.006.

[5] European Union. Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv\%3AOJ.L_.2014.257.01.0073.01.ENG. 2014.

[6] European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/eli/reg/2016/679/oj. 2016.

[7] Yan Wang et al. "Blockchain Technology in the Food Industry: A Review of Potentials, Challenges and Future Research Directions". In: *Logistics* 4.4 (2020), p. 27. DOI: 10.3390/logistics4040027.

[8] Christopher Allen. "The Path to Self-Sovereign Identity". In: *Rebooting the Web of Trust* (2016).

[9] OECD. Digital Strategies for SME Growth. Report. 2023.

[10] European Investment Bank. Blockchain for SMEs: Financing and Roadmaps. Whitepaper. 2021.

[11] ENISA. Hardware Security Modules: Guidelines for Secure Use and Management. https://www.enisa.europa.eu/publications/hardware-security-modules. 2020.

[12] ETSI. ETSI EN 319 411-1 V3.1.1 (2021-03): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/03.01.01_60/en_31941101v030101p.pdf. 2021.

[13] Verizon. 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/2022-data-breach-investigations-report-dbir.pdf. 2022.

[14] Melanie Swan. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015. ISBN: 978-1491920497.

[15] Pierre Dumont. "eIDAS Regulation and Its Impact on Digital Trust Services in the EU". In: *Journal of European Law and Technology* 12.3 (2021), pp. 45–62.

[16] Michèle Finck. "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?" In: *European Parliament Policy Department Study* (2018).

[17] Roman Beck and Christoph Müller-Bloch. "Blockchain as a Privacy-Enabling Technology". In: *Business Information Systems Engineering* 60.5 (2018), pp. 381–395. DOI: 10.1007/s12599-018-0552-3.

[18] European Union. Directive (EU) 2015/2366 on payment services in the internal market. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32015L2366. 2015.

[19] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001. Accessed: 2025-03-08. 2022.

[20] ENISA. Trust Services Security: Best Practices for SMEs. https://www.enisa.europa.eu/publications/trust-services-security-best-practices. 2021.

[21] European Commission. Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52021PC0281. Accessed: 2025-03-08. 2021.

[22] European Commission. eIDAS 2.0 Pilot Progress Report. Report. 2024.

[23] ETSI. ETSI EN 319 401 V3.1.1 (2020-09): General Policy Requirements for Trust Service Providers. https://www.etsi.org/deliver/etsi_en/319400_319499/319401/03.01.01_60/en_319401v030101p.pdf. 2020.

[24] ETSI. ETSI EN 319 102-1 V1.3.1 (2020-12): Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation. https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.03.01_60/en_31910201v010301p.pdf. 2020.

[25] ETSI. ETSI TS 119 495 V1.5.1 (2020-11): Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under Regulation (EU) No 910/2014. https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.05.01_60/ts_119495v010501p.pdf. 2020.

[26] International Organization for Standardization. ISO 22739:2020 Blockchain and distributed ledger technologies — Terminology. https://www.iso.org/standard/73771.html. Accessed: 2025-03-08. 2020.

[27] International Organization for Standardization. ISO/TS 23257:2022 Blockchain and distributed ledger technologies — Reference architecture. https://www.iso.org/standard/75093.html. 2022.

[28] ETSI. ETSI EN 319 412-1 V1.4.1 (2020-06): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.04.01_60/en_31941201v010401p.pdf. 2020.

[29] Leslie Lamport, Robert Shostak, and Marshall Pease. "The Byzantine Generals Problem". In: *ACM Transactions on Programming Languages and Systems* 4.3 (1982), pp. 382–401. DOI: 10.1145/357172.357176.

[30] Christian Cachin and Marko Vukolić. Blockchain Consensus Protocols in the Wild. https://arxiv.org/abs/1707.01873. 2017.

[31] ENISA. Blockchain Security Report 2023. https://www.enisa.europa.eu/publications/blockchain-security-report-2023. 2023.

[32] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. "A Survey of Attacks on Ethereum Smart Contracts (SoK)". In: *Principles of Security and Trust* (2017), pp. 164–186. DOI: 10.1007/978-3-662-54455-6_8.

[33] Miguel Castro and Barbara Liskov. "Practical Byzantine Fault Tolerance". In: *Proceedings of OSDI* (1999), pp. 173–186.

[34] Yoichi Hirai. "Formal Verification of Smart Contracts Using Isabelle/HOL". In: *Ethereum Research* (2017).

[35] Jens Groth. “On the Size of Pairing-Based Non-Interactive Arguments”. In: *Advances in Cryptology – EUROCRYPT 2016* (2016), pp. 305–326. DOI: 10.1007/978-3-662-49896-5_11.

[36] Juan Benet. IPFS - Content Addressed, Versioned, P2P File System. https://arxiv.org/abs/1407.3561. 2014.

[37] Daniel J. Bernstein and Tanja Lange. “Post-Quantum Cryptography”. In: *Nature* 549 (2017), pp. 188–194. DOI: 10.1038/nature23461.

[38] European Commission. Digital Transformation of SMEs: A Practical Guide. https://ec.europa.eu/docsroom/documents/46002. 2021.

[39] European Commission. Digital Europe Programme. https://digital-strategy.ec.europa.eu/en/activities/digital-programme. 2021.

[40] European Commission. Horizon Europe. https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en. 2021.

[41] European Commission. European Blockchain Services Infrastructure: 2023 Progress Report. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI. Accessed: 2025-03-08. 2023.

[42] OpenZeppelin Community. OpenZeppelin Contracts Library. https://github.com/OpenZeppelin/openzeppelin-contracts. Accessed: 2025-03-08. 2023.