Unlocking Best Practices in Blockchain: Insights from the European Blockchain Sandbox

Author: Marianna Zaccaro, Dublin City University, marianna.zaccaro2@mail.dcu.ie

Blockchain technology is rapidly evolving, offering innovative solutions across industries. To foster responsible innovation, the European Blockchain Sandbox provides a structured environment where blockchain solutions can be tested in collaboration with regulators. Launched by the European Commission, the sandbox facilitates dialogue between innovators and policymakers, helping to identify regulatory obstacles and promote legal clarity for blockchain applications.
The recently published *European Blockchain Sandboxes Best Practices Reports (2023) – 1st Cohort, Part A and Part B* offer valuable insights into how blockchain solutions are being implemented across different sectors. This article aims to identify and highlight the best practices that characterize successful blockchain applications by analyzing the use cases presented in the reports, in order to better understand the factors that contribute to effective and compliant blockchain adoption in Europe. The best practices outlined in Annex 3 of Report A highlight key aspects of their application. Below is a detailed exploration of these principles, grouped into essential themes.

Digital Transformation in Logistics: A New Era of Efficiency and Security[1]

In today's rapidly evolving world, the logistics industry is experiencing a profound digital transformation. Through innovative technologies, processes are becoming faster, more efficient, and secure.

1. **Digitization of Logistics Documentation[2]**

Implementing end-to-end digitization of shipping and logistics documents, such as the Electronic Consignment Note (e-CMR), is essential for enhancing efficiency and traceability. Blockchain technology ensures that all shipping-related information remains immutable and traceable, offering unparalleled transparency throughout the supply chain. By digitizing documents, the process becomes smoother and more reliable, with each step recorded and verified.

2. **Interoperability Between Public and Private Entities**

Seamless communication among various stakeholders, including exporters, customs agencies, freight forwarders, and port authorities, is crucial for an efficient logistics process. Standardized digital protocols like AIDA and Port Community Systems (PCS) are key enablers of this interoperability. These systems, when integrated with blockchain, allow real-time data exchange, ensuring that everyone involved is on the same page and can operate in sync, regardless of their role in the process.

[1] European Commission, *European Blockchain Sandbox Best Practices Report (2023): 1st Cohort, Part A* (Publications Office of the European Union 2024) pag. 35-36 https://doi.org/10.2759/841857.

[2] European Blockchain Sandbox, *Best Practices Report: 1st Cohort, Part B* (Publications Office of the European Union 2024) page 37 ss. https://doi.org/10.2759/76203

Funded by the European Union

3. **Two-Factor Authentication for Identity Verification**

Ensuring the security and authenticity of all participants in the logistics chain is paramount. Two-factor authentication (2FA) is used to verify the identities of individuals involved in the shipment process. This added layer of security helps prevent fraud and ensures that the data exchanged remains accurate and trustworthy, supporting the overall integrity of the system.

4. **Geolocation and Signature Authentication**

Incorporating geolocated signatures and related transactional data onto the blockchain guarantees that all actions are fully traceable. This practice not only preserves the immutability of the information but also ensures that the actions of all involved parties are verifiable, reinforcing the transparency and reliability of the logistics operations.

5. **Use of Permissioned Blockchain**[3]

By utilizing a permissioned blockchain, such as Hyperledger Fabric, hosted by trusted service providers like AgID-certified entities, only authorized participants can access the network. This creates a highly secure and verifiable system for managing logistics processes. The permissioned nature of the blockchain ensures that all transactions are protected, fostering trust among participants and enhancing the security of the entire operation.

6. Trusted Service Providers and Regulatory Compliance

Adhering to regulatory frameworks like eIDAS[4] ensures that digital processes are not only secure but legally binding. By using trusted service providers, logistics operations meet necessary standards for security and legal validity, ensuring compliance with industry regulations.

Top Strategies for Ensuring Secure and Transparent Digital Documentation[5]

7. Timestamping and Ownership Certification

Use of blockchain notarization to provide tamper-proof evidence of asset existence and integrity. This method ensures that once a document or asset is registered, its authenticity cannot be altered.

8. **API Model for Seamless Integration**[6]

Implementing standardized APIs allows for the easy integration of blockchain solutions into existing IT infrastructures, ensuring smooth adoption across different systems.

9. **Support for Multiple Blockchains**

To ensure compatibility and flexibility, blockchain systems should support integration with widely used platforms such as Ethereum and Bitcoin, allowing users to leverage the strengths of multiple blockchain networks.

Identity Verification and Secure Digital Identities[7]

10. **Secure Digital Identities (SSDIDs)**

Both individuals (e.g., business directors) and organizations have their own SSDIDs, which are encrypted and tied to their private keys. These identities are tamper-proof and blockchain-based,

[3] European Blockchain Sandbox, *Best Practices Report: 1st Cohort, Part B* (Publications Office of the European Union 2024) pag. 20

[4] Idem pag. 61 ss.

[5] European Commission, *European Blockchain Sandbox Best Practices Report (2023): 1st Cohort, Part A* (Publications Office of the European Union 2024) ALMAVIVA, BLOCKCHAIN ITALIA, COMMISSARIAT À L'ÉNERGIE ATOMIQUE, deltaDAO use cases from page 37.

[6] European Blockchain Sandbox, *Best Practices Report: 1st Cohort, Part B* (Publications Office of the European Union 2024) pag. 47

[7] European Commission, *European Blockchain Sandbox Best Practices Report (2023): 1st Cohort, Part A* (Publications Office of the European Union 2024), pag. 60-61.

Funded by the European Union

ensuring no Personally Identifiable Information (PII) is stored on-chain. SSDIDs contain essential information like public keys and credentials, providing secure identity validation without compromising privacy.

11. **Ownership and Control with SSDIDs**

SSDIDs grant full ownership and control over digital identities to individuals and organizations, allowing the business owner and suppliers to manage their own identity credentials. This enhances security, privacy, and flexibility, offering significant advantages over traditional, centralized identity systems.

12. **Biometric Verification**

By integrating biometric data with SSDIDs, businesses can ensure that only the authentic individuals (such as business owners and suppliers) can access or perform actions like receiving or initiating payments. This multi-factor security adds an extra layer of protection against identity theft**,** fraud, and unauthorized access.

13. **Secure Communication with DIDComm**

The business owner and supplier can engage in secure and private communications via DIDComm, a messaging protocol based on Decentralized Identifiers (DIDs)**.** DIDComm encrypts messages end-to-end, preventing man-in-the-middle attacks and ensuring that only the intended recipient can decrypt and read the message.

14. **Privacy and Prevention of Tracking with PeerDIDs**

To enhance privacy and prevent the tracking or correlation of identities, users adopt peerDIDs, which are pairwise DIDs generated specifically for a relationship between two entities. These blind signatures help ensure secure, private communication, minimizing exposure to unauthorized parties.

15. **Integration of W3C Verifiable Credentials (VCs)**

Using W3C Verifiable Credentials within the SSDID and payments system ensures cross-border transaction efficiency. Benefits include enhanced security**,** improved privacy**,** increased trust**,** interoperability**,** simplified compliance, and cost-effectiveness.

16. **Auditable Nuggets**

Auditable Nuggets are encrypted pieces of information that are provided only to authorized participants. These nuggets, encrypted with private keys, are time-restricted and used for regulatory compliance and auditing purposes, enabling transparency without the need for storing PII data in centralized systems.

Blockchain for Intellectual Property and Creative Industries[8]

17. **NFTs Representing Ownership Rights**

Non-Fungible Tokens (NFTs) enable fractional ownership of creative assets, such as music rights. This technology makes it easier for a broader audience to invest in and access ownership of valuable intellectual property.

18. **Smart Contracts for Clarity and Security**[9]

These self-executing contracts, written in code, automatically enforce the agreed-upon terms once conditions are met, eliminating the need for intermediaries. They provide clear, transparent terms, reducing the risk of misinterpretation or disputes. Additionally, smart contracts streamline processes

[8] European Commission, *European Blockchain Sandbox Best Practices Report (2023): 1st Cohort, Part A* (Publications Office of the European Union 2024) pag.39.

[9] European Blockchain Sandbox, *Best Practices Report: 1st Cohort, Part B* (Publications Office of the European Union 2024) pag. 31

Funded by the European Union

like royalty distribution, ensuring timely and accurate payments. By automating these functions, smart contracts enhance trust, reduce costs and offer an efficient solution for creators and investors.

Enhancing Cybersecurity[10]

19. Defending Against Quantum Threats

Implementing quantum-resistant encryption is critical to future-proofing blockchain systems. As quantum computing advances, this encryption ensures that sensitive data remains secure from both current cyber threats and potential future quantum attacks, protecting critical infrastructure from risks like "Harvest Now, Decrypt Later" attacks.

20. Combining Encryption Techniques

Layered encryption strategies combine multiple encryption methods to enhance security. This approach ensures that even if one layer is compromised, other layers continue to provide protection. By integrating both classical and quantum-resistant encryption methods, organizations can safeguard data against both present ransomware and future quantum computing threats.

21. Non-Disruptive Deployment

Security updates and new features should be deployed with minimal downtime to avoid disrupting business operations. This ensures business continuity while improving security. Tools like modular blockchain designs allow for upgrades and patches to be implemented quickly and without the need for extensive downtime or system reconfigurations.

22. Adaptable, Modular Design

Blockchain solutions should feature an adaptable, modular design that can evolve with emerging threats. By making it easy to update cryptography libraries and algorithms, organizations can quickly integrate new security measures to stay ahead of cyber threats. This flexibility also simplifies compliance and audit processes, ensuring systems remain robust without requiring disruptive updates.

Sustainability and Ethical Applications[11]

23. Choose Energy-Efficient Consensus Mechanisms

Blockchain solutions must balance security with energy consumption. Proof-of-Stake (PoS) and Proof-of-Authority (PoA) are excellent choices for reducing energy usage while maintaining reliable transaction validation. These consensus algorithms are designed to be energy-efficient compared to traditional Proof-of-Work (PoW) systems, making them ideal for sustainable blockchain applications.

24. Use Cryptographic Techniques for Data Integrity[12]

Ensuring the authenticity and immutability of data is essential, particularly when handling sensitive or critical information. Cryptographic fingerprints, such as hashes, can be used to create tamper-proof records of data transactions, ensuring that the original data remains unchanged throughout its lifecycle. This practice is especially valuable when sharing information across decentralized networks.

25. Integrate Blockchain with Existing Systems

Rather than overhauling traditional systems, blockchain can be integrated with existing electronic platforms to enhance digitalization. Blockchain technology can improve interoperability, streamline

[10] European Commission, *European Blockchain Sandbox Best Practices Report (2023): 1st Cohort, Part A* (Publications Office of the European Union 2024) pag. 42.

[11] European Commission, *European Blockchain Sandbox Best Practices Report (2023): 1st Cohort, Part A* (Publications Office of the European Union 2024) COMMISSARIAT À L'ÉNERGIE ATOMIQUE + COMPELLIO (UNI SYSTEMS) from page 44.

[12] European Blockchain Sandbox, *Best Practices Report: 1st Cohort, Part B* (Publications Office of the European Union 2024) pag. 23

data transfers, and provide secure management of assets, making it a powerful tool for industries that need secure, real-time data sharing.

26. **Implement Transparent Data Dashboards**

Providing public access to data visualizations, especially for critical sectors like environmental monitoring, can foster trust and engagement. A public dashboard that displays data in an understandable way not only increases transparency but also enables third parties to audit and verify the accuracy of the information, ensuring that data collection and processing are done correctly.

27. **Optimize Blockchain for Low-Cost Sensor Integration**

Blockchain technology can be deployed alongside low-cost sensors to collect real-time data, such as environmental or climate information. These sensors, integrated with blockchain, can ensure data integrity and transparency. Using blockchain to notarize sensor data allows for decentralized data collection while maintaining accuracy and preventing tampering, all while keeping energy consumption low.

28. **Focus on Sustainability**

Blockchain should not only serve technological needs but also align with sustainability goals[13]. Whether it's for green energy or eco-responsible industry, blockchain solutions should prioritize energy efficiency. Selecting blockchain protocols and design choices that minimize energy consumption ensures that these technologies are sustainable and fit within the growing demand for eco-conscious business practices.

Highlight on Best Practices gaps

The examined section consists of behaviors that have not yet been standardized, which the European Blockchain Sandbox has identified in certain use cases and considers as potential solutions to specific challenges in the current application of blockchain technologies for improved regulation. However, there are certain aspects that remain unaddressed in the reports, which can be defined as gaps. The team working on the SEEBLOCKS.eu project has set out to tackle these gaps and to broaden the best practices definition, aiming to contribute to the improvement of the regulatory framework and ensure a more comprehensive approach to blockchain governance.

The primary gaps identified in the examined reports pertain to the role of blockchain technology in key areas such as digital identity, document certification and tokenized assets.

Integration of Blockchain in Digital Identity Frameworks: There is a lack of harmonization at the European level regarding digital identity, with multiple recognition methods coexisting. One key challenge is integrating the European Digital Identity (EUDI) Wallet within the regulatory framework and defining the necessary requirements to initiate this process. Addressing this gap requires structured dialogue with regulators to ensure that blockchain solutions align with the European Union’s digital identity strategies, facilitating secure and standardized authentication mechanisms.

Blockchain for Notarization and Document Signing: Another critical gap concerns the use of blockchain for notarization and document signing. While blockchain has the potential to supplement traditional signature tools and expand certification processes, there is no clear regulatory and technical framework for its full integration under the eIDAS regulation. It is essential to determine the legal and technical requirements for the seamless adoption of blockchain-based certification,

[13] European Blockchain Sandbox, *Best Practices Report: 1st Cohort, Part B* (Publications Office of the European Union 2024) pag. 41.

ensuring compliance with European legislation and resolving conflicts related to certification, data storage, and privacy.

Bridging the Gap Between Pre-Production and Real-Life Adoption: While blockchain-based solutions have been tested in controlled environments, there is still a significant challenge in scaling these implementations for real-world applications. It is important to support the integration of blockchain technologies in critical sectors such as social security, educational credentials and the European Self-Sovereign Identity Framework (ESSIF). Extending the paradigm of self-sovereignty and decentralized verifiable credentials, would ensure that blockchain-based identity and credentialing systems can be effectively deployed across different countries and in cross-border interactions.

Enhancing the EUDI Development through EBSI: Another major gap concerns the need to align the European Digital Identity (EUDI) initiative with the capabilities of the European Blockchain Services Infrastructure (EBSI). Working to elaborate on both existing and new EBSI functionalities could ensure an effective support of decentralized identity ecosystems. A key aspect of this effort involves engaging a broader range of stakeholders to drive adoption and facilitate interoperability between national and cross-border identity verification systems.

Ensuring Interoperability, Trust and Accountability in Digital Organizations: While decentralized digital organizations present an innovative alternative to traditional structures, a significant gap remains in establishing interoperability between these new models. For such organizations to function effectively, they must integrate with regulatory environments while preserving their decentralized nature. Additionally, trust and accountability mechanisms need to be clearly defined to ensure transparent and verifiable decision-making, governance structures and smart contract implementations. Addressing these challenges requires developing models that promote seamless interaction between decentralized and conventional entities while upholding high standards of security, compliance, and operational reliability.

Regulatory Clarity on Tokenized Securities and Stablecoin Integration: There is a huge potential for tokenizing financial securities, but there is still legal uncertainty[14] regarding the classification and treatment of tokenized assets under existing financial regulations, such as MiFID II. Additionally, the integration of stablecoins for payments introduces challenges related to compliance with European financial and payment regulations. It is crucial to establish clear guidelines on how tokenized securities and stablecoins can operate within the EU's regulatory framework, ensuring investor protection, legal certainty and adherence to anti-money laundering (AML) and financial oversight requirements.

Cross-Border Transactions and Ownership Recognition: Since the ownership of tokenized securities is represented through NFTs and investors may reside in different EU Member States, there are challenges related to cross-border transactions, taxation and legal recognition of ownership. Ensuring that blockchain-based proof of ownership is legally binding across jurisdictions is essential for the adoption of tokenized assets. Furthermore, stablecoin-based payments must be seamlessly

[14] European Blockchain Sandbox, *Best Practices Report: 1st Cohort, Part B* (Publications Office of the European Union 2024) pag. 70

Funded by the European Union

integrated into existing financial infrastructures, ensuring compliance with SEPA regulations and providing legal certainty for cross-border dividend distributions and securities transactions.

Conclusion

Guided by the objective to deliver a targeted, democratic, and industry-driven initiative to support European interests in standardization within the Blockchain/DLT domain, the SEEBLOCKS.eu team has embraced the challenge of identifying best practices that will make it easier for companies to comply with current regulations.

Given that existing regulations often provide only broad guidelines on desired behaviors, leaving significant room for interpretation and uncertainty in practical implementation, the team has focused on addressing this challenge. Specifically, they have identified six key areas of interest (Sustainability, Scalability, Accountability, Privacy, Security and Trust) in which best practices have been developed to bridge the gap between abstract regulatory principles and concrete technical solutions. In doing so, SEEBLOCKS.eu aims to establish a standardized and compliant blockchain ecosystem that not only aligns with European regulatory frameworks but also promotes innovation, while ensuring security, transparency and trust.

Funded by the European Union