Journal Pre-proof

Consumer-Controlled Digital Twin Architecture: How blockchain technology gives consumers control over their smart devices' digital twins and data

Filipe Pinto , Catarina Ferreira da Silva , Sergio Moro , Pedro Aquino

PII: S2096-7209(25)00069-7
DOI: https://doi.org/10.1016/j.bcra.2025.100342
Reference: BCRA 100342

To appear in: *Blockchain: Research and Applications*

Received date: 24 January 2024
Revised date: 14 June 2025
Accepted date: 16 June 2025

Please cite this article as: Filipe Pinto , Catarina Ferreira da Silva , Sergio Moro , Pedro Aquino , Consumer-Controlled Digital Twin Architecture: How blockchain technology gives consumers control over their smart devices' digital twins and data, *Blockchain: Research and Applications* (2025), doi: https://doi.org/10.1016/j.bcra.2025.100342

Highlights

- Introduces the Consumer-Controlled Digital Twin Architecture
- Systematic review of digital twins, self-sovereign identity & blockchain convergence
- Integrates DIDs, VCs, DIDComm, Hyperledger Fabric / Indy & IPFS in Eclipse Ditto
- Case study validates secure P2P data exchange across the full smartwatch lifecycle
- Benchmarks show low latency; future work targets integrating personalized AI

Consumer-Controlled Digital Twin Architecture: How blockchain technology gives consumers control over their smart devices' digital twins and data

Filipe Pinto [a,*] 0000-0002-4447-6903, Catarina Ferreira da Silva [a,*] 0000-0003-3222-081X, Sergio Moro 0000-0002-4861-6686 [a,b,*], Pedro Aquino [a] 0009-0001-9780-6152

[a] Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR, Lisboa, 1649-026, Portugal
[b] University of Jordan, School of Tourism and Hospitality/Aqaba, 77110, Jordan

* Corresponding authors.
filipe@filipe-pinto.com (Filipe Pinto)
Catarina.Ferreira.Silva@iscte-iul.pt (Catarina Ferreira da Silva)
Sergio.Moro@iscte-iul.pt (Sergio Moro)

Abstract

This article presents Consumer-Controlled Digital Twin Architecture (C2DTA), a novel architecture that aims to empower consumers in the Personal Data Ecosystem (PDE). The hallmark of the architecture is the transfer of the smart device Digital Twin (DT) to the consumer domain, granting consumers *de facto* control over their data. This paradigm shift hinges on multiple decentralized technologies, chiefly Self-Sovereign Identity (SSI). C2DTA leverages blockchain to manage ecosystem transactions, assets, decentralized identifiers (DIDs), and verifiable credentials (VCs) while enabling decentralized storage. The evolved PDE allows stakeholders to engage in trustworthy and secure peer-to-peer transactions atop DIDs. We present a literature review on the convergence of DT and SSI, including GAIA-X. We provide a comprehensive architecture analysis detailing the integrated technologies and present informed predictions for the market dynamics poised to facilitate the adoption of C2DTA and its impacts on the PDE. The architecture is implemented using Eclipse Ditto and Eclipse Mosquitto as the DT platform, Hyperledger Fabric as the transaction ledger, Hyperledger Indy as the identity ledger, Hyperledger Aries to build decentralized identity software agents, and the InterPlanetary File System for decentralized storage, showcasing a business scenario that tracks the lifecycle of a smartwatch equipped with a heartbeat sensor, from manufacture to purchase, twinning, and resale. Feasibility testing confirms that C2DTA effectively empowers consumers to manage their smart device DTs and associated data. Our evaluation, although limited by the scale of our tests, suggests that the performance impacts of the decentralized infrastructure are within acceptable parameters. Finally, we discuss future research areas.

Keywords: Digital twin, Blockchain, Decentralized identifiers, Verifiable credentials, DIDComm, Personal data ecosystem

1 Introduction

The International Data Corporation (IDC) [1] estimates that by 2025, IoT devices, encompassing machines, sensors, and cameras, will collectively generate 79.4 zettabytes of data. Although Smart Devices (SDs) can increase consumer well-being [2], they also present challenges. Sensors invade the consumer privacy sphere, capturing data stored in silos that attract cybercriminals [3], while Original Equipment Manufacturers (OEMs) often exploit the data

for their benefit [4], leaving consumers without tangible rewards [5]. The framework governing the collection and use of personal data involving consumers and OEMs to create economic value, known as the Personal Data Ecosystem (PDE) [6], is unbalanced [7]. It allows OEMs to monopolize data flow profits while consumers bear the system's externalities and is therefore associated with a loss of control over personal information [8]. To address this, industry and academia are exploring blockchain-based Internet of Things (IoT) solutions (BIoT) for people-centered architectures [9].

Blockchain's strong cryptographic foundation, immutable and tamper-proof nature, decentralization, and smart contract support allow for critical mechanisms that, when integrated with user-centered architectures, elevate consumer status in the PDE [10]. By leveraging blockchain decentralized ledger technologies, it is possible to establish a network of trustless peers that collectively agree on an immutable, auditable, and cryptographically secure shared version of the truth [11]. This network offers support for decentralized identifiers that link users with their data without the need for third parties [12]. When combined with Personal Data Stores (PDSs), frameworks that allow users to collect, store, manage, and share their data according to their preferences [13], this identity mechanism, referred to as Self-Sovereign Identity (SSI) [14], gives consumers sovereign control over their data. When used within a user-centered framework that allows consumers to control and leverage their data, this mechanism transforms them from passive data subjects to active participants in the PDE. This shift underscores the critical role of maintaining data rights, such as access, usage, and sharing, which are firmly in the hands of consumers. The decentralized nature of SSI and the PDS, supported by technologies such as blockchain, facilitates secure, transparent, and user-centric data management, leading to a more equitable, trustworthy, and innovative user-empowered PDE [15].

The Digital Twin (DT) concept originated at NASA and became publicly recognized in 2003 [16]. It refers to a virtual representation or digital counterpart of a physical object, system, or process [17]. Since its introduction, the concept has evolved and matured, reaching a significant growth stage by 2014 [18]. Although projections on growth rates vary, multiple sources agree that the healthcare sector stands out as a key industry for DT adoption [19, 20]. Transforma Insights [21] forecasts a market size of 24.1 billion devices and a reach of $1.5 trillion, with the consumer sector accounting for 65% of all connections. DT reflects the inevitable trend toward cyber-physical integration[1] [17], enabling human interaction to transcend the boundaries of the physical realm, where inherent spatial and temporal constraints can limit efficiency.

DT reframes much of the early efforts to develop connected device solutions, initially based on telemetry and Machine-to-Machine (M2M) communications and later enhanced with IoT technologies [23]. This evolution has produced a more structured, multifaceted development framework supporting services and Artificial Intelligence (AI) [17]. For instance, a smartwatch with a DT extends beyond basic data collection, as it continuously gathers and analyzes detailed data to update and refine its virtual model, creating a comprehensive understanding of the user's behaviors, activities, and potentially even physiological states. As DT crosses into the consumer realm, it is reasonable to surmise that some OEMs may exploit the

[1] Cyber-physical integration can be seen as a transformation from "bits to atoms," which is a concept that dates back at least to 1997 when Ishii and colleagues introduced the concept of "tangible bits" [22].

concept of product personalization [24] or other features with a disproportionately lower impact or benefit for consumers to gain further consumer insights with DT-based solutions. Therefore, it is vital to develop mechanisms that enable consumers to control their devices' DTs [25]. While incumbent OEMs may oppose it, new market entrants could seize this as a strategic competitive advantage.

This paper introduces the Consumer-Controlled Digital Twin Architecture (C2DTA). The main objective of C2DTA is to empower consumers in the PDE. We achieve this goal by shifting the DT from the cloud under OEM control to the edge under consumer control. This shift makes consumers *de facto* controllers—meaning they have actual control in practice [26]—as opposed to controllers versus *de jure* controllers—meaning they have legally recognized control [27]—of their SD data by giving them effective control over the DT and its associated data [28].

The motivation behind C2DTA is the need to empower consumers in the AI era when data are a fundamental commodity [29]. C2DTA addresses two key challenges: achieving economic fairness through the control of DTs and bridging a critical technical gap in leveraging edge computing and federated learning to improve consumer control. By addressing these interconnected issues, C2DTA provides a foundation for consumer-centered data practices in the AI era.

The economic fairness in controlling DTs arises from the current cloud-based approach, where OEMs retain *de facto* control over the DT and the associated consumer-generated data [30]. As consumers become more aware of the growing value of data, they are likely to demand solutions that restore control and ensure equitable participation. Tesla is a paradigmatic example of the urgent need for mechanisms that empower consumers to reclaim sovereignty over their own data, as its trillion-dollar valuation [31] is supported by its ability to leverage DTs to train its Full Self-Driving (FSD)[2] feature [32, 33].

By providing a practical framework for secure, self-sovereign edge-based data management, C2DTA also closes the gap among proponents of edge computing, federated learning, and privacy-preservation methods, such as homomorphic encryption, as a mechanism to improve the privacy and security of AI training data within IoT contexts [29, 34–37]. While these works emphasize the benefits of storing and processing data at the edge, they often overlook the critical step of ensuring that data are kept at the edge in a self-sovereign manner under consumer control. C2DTA provides the practical foundation necessary to make these principles actionable.

The novelty of this research lies in developing a solution that is both consumer- and digital-twin-centered. As shown in Section 2, the integration of DT and decentralized identity technology is an underexplored topic, with most existing efforts being theoretical. Our approach establishes a foundational framework for the consumer-controlled Personal Digital Twin (PDT), discussed further in Section 5, this framework positions consumer-controlled PDT as pivotal in empowering individuals in the AI era.

[2] At the Matroid 2020 conference Andrej Karpathy from Tesla explained how they use the data collected by their customers' cars to train their self-driving neural network, https://www.youtube.com/watch?v=hx7BXih7zx8

Additionally, our research introduces a dual blockchain approach, which is detailed in Section 3.1 and strengthens data security and provenance. This further empowers consumers by enabling them to be sovereign providers of trustworthy data to the AI ecosystem. Finally, although a detailed exploration is beyond the scope of this paper, we consider data property rights issues [38] and discuss how C2DTA may help mitigate these challenges by securely maintaining data at the edge.

Our study establishes the viability of C2DTA through an exhaustive evaluation of eight use cases that track the lifecycle of a smartwatch equipped with a heartbeat sensor, from manufacture to purchase, twinning, untwinning, and resale. To further test the architecture's functionality, C2DTA was implemented via Eclipse Ditto for DT management [39], Eclipse Mosquitto [40] for sensor data transmission, Hyperledger Indy for decentralized identity and verifiable credentials management, the ACA-Py Hyperledger Aries framework to develop software agents and DIDComm communication protocols [41, 42], Hyperledger Fabric for anchoring ecosystem transactions [43], and the InterPlanetary File System (IPFS) [44] as the decentralized data storage mechanism.

Following an analysis of the state of the art, we believe our work introduces the following novel contributions:

1) **Self-sovereign DT ecosystem architecture.** —We propose an architecture that enables stakeholders of the digital-twinned SD ecosystem to securely manage DTs and leverage their data. In this architecture, those who own devices control the associated DTs at the edge, and stakeholders transact in a decentralized, self-sovereign, and secure manner. We further explore the impact of the architecture on the PDE and the business strategies to support the architecture.
2) **DT, SSI, and blockchain integration taxonomy.** —We propose a structured framework for consistently evaluating conceptual and practical implementations, enabling clear classification, identifying research gaps, and guiding future development in decentralized systems.
3) **Fabric, Indy and Aries with ACA-Py integration.** —We propose an architecture that integrates Hyperledger Fabric for managing SDs and datasets with Hyperledger Aries for overseeing stakeholder identifiers, verifiable credentials, and secure communication protocols through ACA-Py. This integration ensures reliable ecosystem operations across the lifecycle of SDs, encompassing manufacturing, sale, ownership transfer, and processes such as twinning and untwinning. Our analysis encompasses eight detailed scenarios, seven rigorously tested across 88 steps. Furthermore, we introduce mechanisms, including automation, to safeguard the integrity of an ecosystem and ensure its operational reliability.
4) **Future innovation for consumer empowerment.** —We introduce several concepts emerging from our architecture and underscore its role in fostering consumer agency and trust. We explore how "data-only DTs" and the aggregation of several C2DTs can lead to the "Consumer-Controlled Personal Digital Twin (C2PDT)."

The structure of this paper is as follows: Section 2 discusses the state of the art in DT and SSI implementations in the context of enabling consumer control of their SD data via blockchain. Section 3 introduces the concept of C2DTA, elucidating its principles, benefits, and functionalities. Section 4 presents and discusses the results of our research. Section 5 outlines pro-

spective future work, pinpointing opportunities for further C2DTA exploration and applications. Finally, Section 6 concludes by summarizing the findings and their implications for the future of the PDE.

2 Current trends and challenges in SSI and digital twin integration

DT technology offers formidable capabilities derived from its support for three of the most powerful tools in terms of human knowledge capabilities: conceptualization, comparison, and collaboration [16]. In addition, DT concepts, abstractions, properties, and functionalities are exceptionally intuitive, effortlessly adapting to various application areas [45]. When integrated with decentralized ledger technology, such as blockchain, these DT capabilities are further enhanced in terms of security, transparency, and operational efficiency. Our work leverages these combined technologies, the key among which is the integration of DT and the SSI standard, to empower consumers in the PDE.

SSI emerged as a response to the limitations of user/password internet identity management, which transformed the internet into a "patchwork of identity one-offs" [46] governed by feudal-like contracts of adhesion [47]. Efforts to improve user experience and privacy included the 2001 LinkTank initiative [48], the 2004 Identity Gang [49], and Cameron's 2005 [46] claims-based architecture. The concept of sovereignty emerged in 2011 with Loffreto's [50] proposal for sovereign source authority, which argues for the right to an identity at birth. Around this period, decentralized naming systems such as Namecoin and Blockstack [51, 52] triggered the discussion of blockchain-based identity systems. By 2016, the U.S. Department of Homeland Security had backed the first SSI implementation [53, 54], contributing to the Web Consortium (W3C) Credentials Community Group and the W3C DID Working Group[3].

C2DTA makes full use of SSI standards, as discussed in detail in Section 3, and technologies, which include the following:

- **Decentralized Identifiers (DIDs)**[4] are permanent, globally resolvable, decentralized, and cryptographically verifiable identifiers anchored in a Verifiable Data Registry (VDR) that leverages decentralized ledgers such as blockchain. DIDs rely on a private/public key. The ID owner manages the private key with a digital wallet, while the public key and other metadata are anchored to the blockchain as a JSON structure named DIDDoc [55]. As DID matured, SSI architects realized that in peer-to-peer interactions, DIDs and DID documents can be generated and exchanged directly between the peers needing to identify and authenticate without the need to register them in a blockchain. This approach, supported by self-certifying DIDs [54], offers massively better scalability and performance than ledger-based DIDs without compromising security [56].
- **Verifiable Credentials (VCs)**[5] are assertions about a DID that can be independently verified via cryptographic methods to ensure their integrity and authenticity. Issuers authenticate VCs with private keys, holders store them in digital wallets, and verifiers use the issuer's public key to verify their authenticity [57].

[3] https://www.w3.org/2019/did-wg/
[4] https://www.w3.org/TR/did-core/
[5] https://www.w3.org/2017/vc/WG/

- **Decentralized Identifier Communication (DIDComm)**[6] enables DIDs and VCs to be exchanged by software agents that represent and act on behalf of an identity owner who has entrusted them with specific responsibilities and powers to act in the best interest of the identity owner. Agents hold DIDs, cryptographic keys, and verifiable credentials and interact with other agents via DIDComm [58]. DIDComm is a framework for safe, structured interactions built atop DIDs [59]. It uses a message-based architecture that enables transport-agnostic operation, supporting synchronous, asynchronous, online, and offline scenarios.

Together, DIDs, VCs, and DIDComm enable individuals to take control and manage data about them [60] by fostering an owner-centric, decentralized, standard-based approach to personal data management [61].

To provide a comprehensive understanding of the state-of-the-art integration of DT with SSI and Blockchain, a systematic approach was adopted for the literature review. The research question is as follows: “How are DTs integrated with the SSI and blockchain” guided the analysis. Ultimately, the objective was to identify similar implementations for a comparative analysis with C2DTA. To this end, we used the search criteria below, excluding non-English publications and research efforts that, while mentioning the terms, do not discuss, at a minimum, the integration of DTs and SSI, following the PRISMA [62] literature review process outlined in Fig. 1.

"Digital Twin" AND Blockchain AND ("self-sovereign" OR "decentralized identity" OR "verifiable credential")

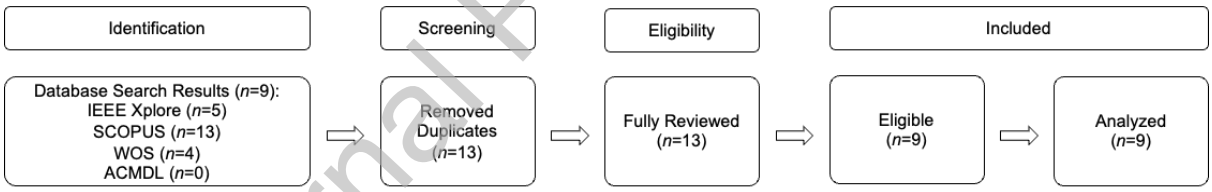


Fig. 1. Literature review process workflow diagram.

The selected papers were categorized based on the classification system presented in Fig. 2.

[6] https://identity.foundation/

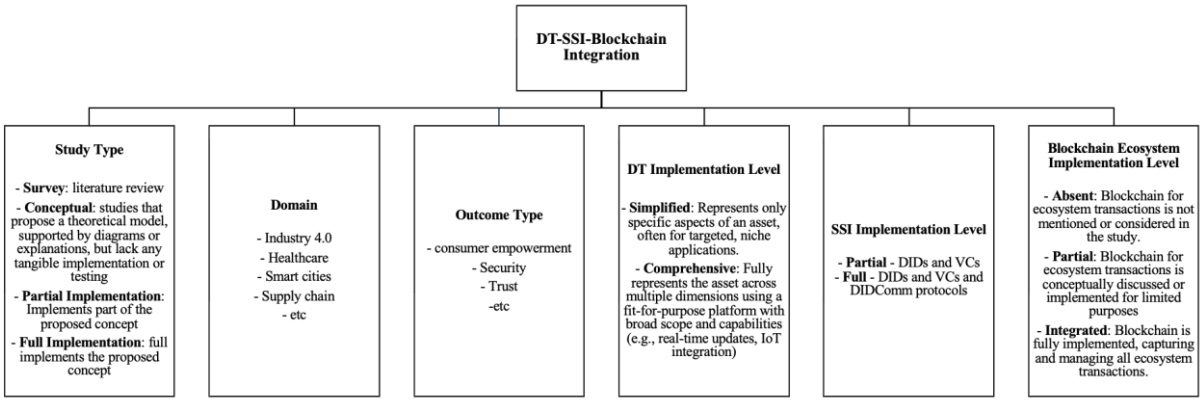


Fig. 2. Integration Maturity Taxonomy of DT-SSI-blockchain systems. DT: Digital twin, SSI: Self-sovereign identity, DIDs: Decentralized identifiers, VCs: Verifiable credentials, DIDComm: Decentralized identifier communication.

This taxonomy evaluates the DT, SSI, and blockchain integration levels within decentralized systems that leverage DTs to represent assets, systems, or processes; SSI to ensure stakeholder identity and trustworthiness; and blockchain to track stakeholder interactions. Blockchain inclusion emerges naturally with the adoption of SSI, as DIDs and VCs enable a decentralized framework of verifiable and secure exchanges, fostering trust among stakeholders and establishing an ecosystem of inherently trustworthy interactions, recorded and ensured by blockchain. The "DT Implementation Level" distinguishes between "Simplified" strategies, which represent only specific aspects of an asset or system for niche applications, and "Comprehensive" strategies, which fully represent assets across multiple dimensions via fit-for-purpose platforms capable of IoT integration for assets, or in the case of systems, real-time updates. Similarly, the "SSI Implementation Level" differentiates between "Partial," which uses only DIDs, or DIDs and VCs, and "Full," which integrates DIDComm protocols for stakeholder communication. Finally, the "Blockchain Ecosystem Implementation Level" evaluates the extent to which blockchain manages ecosystem transactions, with values ranging from "Absent," where blockchain is not mentioned, to "Partial," where it is implemented for limited purposes, and "Integrated," where blockchain fully captures and manages all ecosystem transactions.

Table 1 was compiled on the basis of a study analysis of the six eligible publications.

Table 1 Literature review results.

Reference	Study type	Domain	Outcome type	DT (Digital Twin) implementation level	SSI (Self-Sovereign Identity) implementation level	Blockchain implementation level
This study	Implementation	Consumer Smart Devices	**Consumer empowerment**: Consumers are given *de facto* control of the smart device's DT, which runs at the edge	**Comprehensive**: A DT of the smart device is implemented using Eclipse Ditto, a fit-for-purpose DT platform that integrates IoT	**Full**: Hyperledger Aries is used for Decentralized Identifiers (DIDs) used for ecosystem stakeholders, and Verifiable Credentials (VCs) track manufacturing and ownership proofs. ACA-py is used to implement complex Decentralized Identifier Communication (DIDComm) communication protocols among stakeholders, and stakeholders and devices (twin/untwin)	**Integrated**: Hyperledger Fabric is used to track smart devices and smart devices datasets hashes, stored off-chain (IPFS), throughout their lifecycle
[63]	Conceptual	Building Information Modeling	**Trust**: Enhances transparency in the management of building information across the lifecycle	**Simplified**: Discusses a DT of the building lifecycle stores slow-moving data primarily acting as a holder of notarized data	**Partial**: Discusses DIDs and VCs as stakeholder trust mechanism but does not fully implement DIDComm protocols	**Partial**: Blockchain is discussed for data notarization but does not manage all ecosystem transactions comprehensively
[64]	Implementation	Digital Identity Management	**User Empowerment**: Empowers users with control over their digital identities and ensures data privacy	**Simplified**: The Digital Twin is represented by Soulbound Tokens that tokenize user attributes	**Partial**: Incorporates DIDs and VCs but does not provide evidence of a DIDComm protocol implementation	**Integrated**: Blockchain is fully utilized to manage Soulbound Tokens (ERC-4671)
[65]	Conceptual	General	**General Purpose**: Highlights transparent governance, improving AI and data models for better insights and audits	**Comprehensive**: Discusses theoretical applications and possibilities of integrating DT, IoT, AI, and Blockchain	**Partial**: SSI is discussed, without concrete details about DIDs, VCs, or DIDComm protocols	**Partial**: Blockchain is discussed for enhancing security and smart contracts
[66]	Implementation	Mobility	**Trust**: Enhances transparency and trust in vehicle sales	**Simplified**: DT is represented conceptually as a token (ERC-721) holding vehicle-related information, but no telematics (no IoT)	**Partial**: Used for both the user and the vehicle but does not provide evidence of a DIDComm protocol implementation	**Integrated**: Ethereum blockchain is used to manage transactions, store hashes for off-chain data (IPFS), and ensure system integrity

Reference	Study type	Domain	Outcome type	DT (Digital Twin) implementation level	SSI (Self-Sovereign Identity) implementation level	Blockchain implementation level
[67]	Conceptual	Industry 4.0	**Trust**: Enhances security in computing environments in the context of Cloud-to-Edge Computing Continuum	**Comprehensive**: DT discussed as representing specific computing resources, updated in realtime and with predictive feedback loop	**Partial**: DIDs and VCs are discussed but the paper does not address DIDComm protocol for secure communication	**Absent**: Blockchain is not considered to enable communications among the computer resources
[68]	Conceptual	Metaverse	**Trust and Interoperability:** Enhances trust between entities and facilitates interoperability of identities and data across virtual environments	**Simplified**: The DT is discussed solely to hold identity data or other data related to individuals but lacks any dynamic behavior	**Partial**: DIDs and VCs are discussed but the paper does not address DIDComm protocol for secure communication	**Absent**: Blockchain is not discussed for managing ecosystem transactions or interactions
[69]	Review paper	Generic	**Landscape Mapping**: Identifies key research streams and future research paths, and technological integration of DT, SSI, and Blockchain	**Simplified**: DTs are discussed without dynamic or operational aspects	**Partial**: SSI is discussed, without concrete details about DIDs, VCs, or DIDComm protocols	**Partial**: Blockchain is discussed in relation to secure data management and smart contracts
[70]	Conceptual	Industry 4.0 and metaverse	**Trust and Security**: Focuses on applying decentralized identity and secure data management within virtualized industrial environments	**Comprehensive:** The DT is positioned to manage identity, operational, and lifecycle data across interconnected industrial systems	**Partial**: DIDs and VCs are discussed but the paper does not address DIDComm protocol for secure communication	**Absent**: Blockchain is not discussed for managing ecosystem transactions or interactions

Reference	Study type	Domain	Outcome type	DT (Digital Twin) implementation level	SSI (Self-Sovereign Identity) implementation level	Blockchain implementation level
[71]	Conceptual	Industry 4.0	**Trust**: Focuses on applying blockchain, SSI, and smart contracts to build trust in a manufacturing environment while ensuring scalability and interoperability	**Comprehensive**: DTs are discussed as virtualizing physical assets and processes in the context of IoT	**Partial**: DIDs and VCs are discussed for identity and reputation management, but the paper does not address DIDComm protocol for secure communication	**Integrated**: Blockchain is discussed as being central to the system, managing trust, transactions, smart contracts, and interoperability through scalable solutions like Layer 2 and sidechains.

The current state of the art in DT, SSI, and blockchain integration reflects a landscape primarily dominated by conceptual models and partial implementations. Most studies explore the potential of these technologies but fall short in delivering comprehensive, integrated solutions. DTs often serve as static data holders without dynamic interaction or real-time updates. SSI implementations are typically incomplete, discussing DIDs and VCs without leveraging DIDComm protocols for secure communication, which implies that ecosystem interactions have not been fully considered. As a result, blockchain is sometimes absent or not fully integrated with full lifecycle management and transaction handling. These limitations reveal a gap between theoretical advancements and practical, scalable solutions that can fully harness the combined potential of DT, SSI, and blockchain technologies.

C2DTA advances the state of the art by delivering a fully integrated, operational system that directly empowers consumers with full control over their SDs' DTs. Unlike the studies that offer fragmented or conceptual solutions, our architecture implements a comprehensive DT using Eclipse Ditto, ensuring real-time, dynamic interaction at the edge, where data privacy and user autonomy are maximized. The system achieves full SSI integration through Hyperledger Aries and ACA-py, supporting sophisticated DIDComm protocols for secure, seamless communication between stakeholders and devices and enabling consumers, among others, to perform twin and untwin operations. Furthermore, Hyperledger Fabric is fully integrated to manage the lifecycle of SDs by securely tracking dataset hashes off-chain via IPFS, ensuring integrity, transparency, and trust across the ecosystem. This cohesive and advanced integration of DT, SSI, and blockchain technologies sets a new standard for practical, scalable solutions, delivering unprecedented consumer empowerment and end-to-end system security.

Despite the embryonic status of DT integration with SSI and blockchain, existing frameworks such as the International Data Spaces (IDSs)[7] Reference Architecture Model (RAM)[8] offer promising pathways for advancing their integration. The IDS RAM emerged from the need to protect data sovereignty and ownership in the industrial context [72]. It provides a framework that allows a person or organization to unambiguously define the terms and conditions related to data sovereignty, such as data usage, pricing, payment entitlements, and validity periods when sharing data [73]. It is at the core of the GAIA-X[9] initiative to develop a federated data and service infrastructure for Europe [74]. This initiative is influenced by and bound by the Data Governance Act (DGA) [75]. The DGA relies on "neutral data intermediaries" who promote data sharing by matching supply and demand [27]. These intermediaries include data marketplaces, platforms, trusts, and personal data intermediaries to facilitate effective data exchange and collaboration [76].

C2DTA champions a distinct viewpoint. Rather than moving data from "cloud silos" to even larger "data space silos," it proposes anchoring personal data at the edge, where a decentralized computing grid can leverage federated learning and privacy-preserving technologies such as homomorphic encryption [77] to train AI models. With this approach, C2DTA can enable a highly private AI infrastructure where AI models, rather than consumer data, are exchanged. This approach significantly simplifies the privacy and legal challenges associated with data property rights [26, 78, 79], the classification of personal data [80], and the complexities of consent [81, 82]. These challenges are particularly pertinent within the European

[7] https://internationaldataspaces.org/

[8] https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0

[9] https://gaia-x.eu/

legal context, which has been resistant to the concept of data property rights [83] and, in the face of the growth of AI, sees itself torn between obstructing personal data flows to safeguard privacy, as mandated by the General Data Protection Regulation (GDPR) [84], and promoting data sharing to spur data-driven economic expansion, as defined in the DGA [76].

3 Consumer-controlled digital twin architecture (C2DTA)

This section provides a detailed overview of C2DTA, which is divided into two parts. Part one presents a persuasive argument for the C2DTA, exploring its core concepts and providing a detailed description of their implications. Part two is devoted to a detailed analysis of the architecture's functionalities, focusing on eight use case scenarios. Notably, the diagrams follow the Unified Modeling Language (UML) association notation, in which an arrow indicates the direction of the communication flow, and its absence implies bidirectionality.

3.1 Overview

Motivation: The business-takes-all, vertically integrated, cloud-based [30] approach to asset DTs in which OEMs have *de facto* control of the DT may not be the most important consumer concern. Unbeknownst to many, OEMs extensively collect data from the SDs they sell, monetizing it through value-added services and selling it to third-party Data Purchasers (DP) (Fig. 3). However, consumers may reconsider their stance as they become aware of the importance of data for AI, which, according to IDC projections, is projected to add $19.9 trillion to the global economy through 2030 and drive 3.5% of the global GDP in 2030 [85]. One well-documented example is Tesla, a company that creates a DT for each car it produces [33] and is poised to generate billions of dollars in revenue with FSD[10] [32, 33].

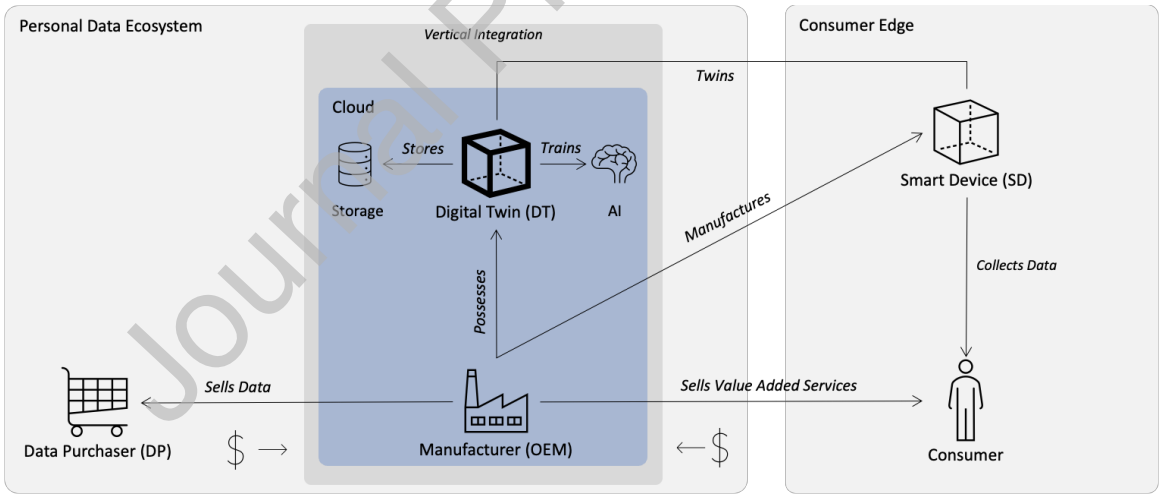


Fig. 3. – Business-takes-all/vertically integrated/cloud-based digital twin personal data ecosystem.

Our core proposition: C2DTA empowers consumers in the PDE by shifting the DT away from the cloud towards the edge under *de facto* consumer control (Fig. 4). This shift introduces several changes to the PDE. First, consumers become responsible for supporting DT capability and storage. Second, the ecosystem welcomes three new providers: the Data Storage Provider (DSP), the AI Algorithm Provider (AAP), which the consumer pays for access

[10] See note 2

to their models (e.g., "Heart attack predictor," "Device failure predictor")[11], and the Federated Learning Provider (FLP), which provides the federated learning infrastructure and pays consumers to train AI models using their data. The incentives and foundational strategies that facilitate these changes are discussed in the "Market Strategy" topic at the end of this section. Third, OEMs must design and manufacture SDs to ensure seamless integration into the ecosystem. Finally, and most importantly, data remain anchored at the consumer edge and do not move. Instead of data, AI models are now exchanged.

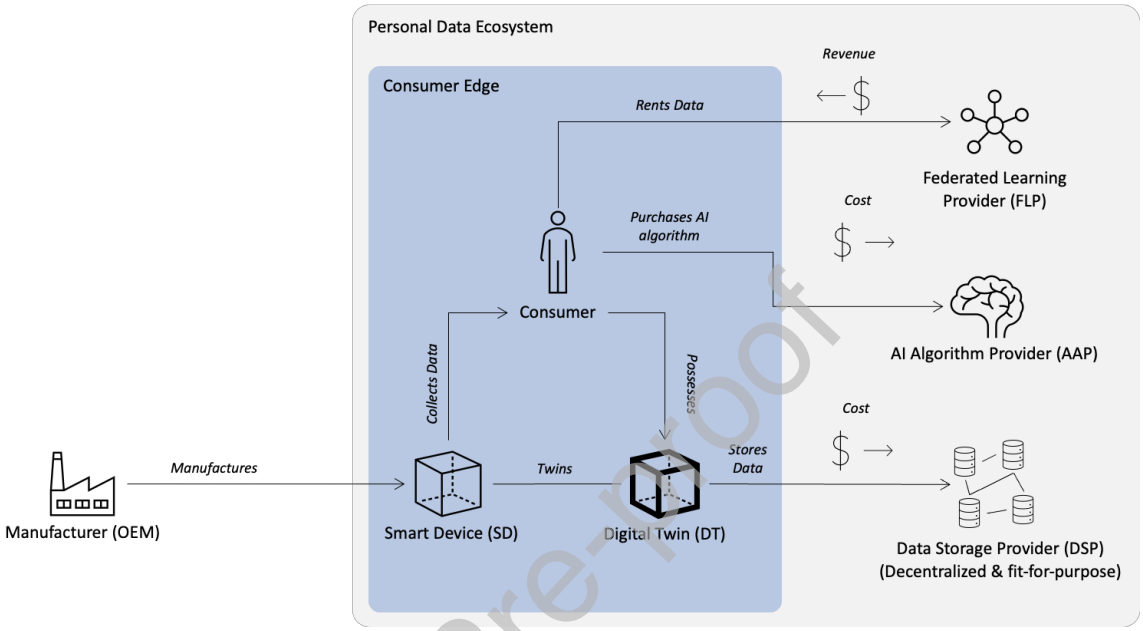


Fig.4. Consumer-centered personal data ecosystem.

Dual blockchain: C2DTA operates with two blockchains in tandem, namely, the ecosystem ledger and the identity ledger (Fig. 5). On the one hand, the ecosystem ledger allows organizations interested in creating a consumer-controlled DT ecosystem to codify their consumer-centered principles and operate a consortium in a highly efficient, secure, and trustworthy manner [86, 87]. In addition, the ecosystem ledger ensures the traceability and integrity of all ecosystem artifacts and the history of transactions and states within the ecosystem by tracking device lifecycles[12] (see "Device Status" topic), DT associations, and datasets. On the other hand, the identity ledger enhances the trust architecture by anchoring VCs that establish the provenance of important events, such as consortia organization enrollment and manufacturing and ownership of a device. Furthermore, DIDComm, facilitated by the identity ledger, provides a secure communication channel for stakeholders, allowing for encrypted, peer-to-peer messaging that resists tampering and eavesdropping. Fig. 5 shows the Hyperledger Fabric structures and the attributes that enable the ecosystem ledger to track the ecosystem devices (Section 3.2 discusses how they work). Permissioned blockchains such as Hyperledger Fabric have performance, cost, and privacy characteristics [88] that make them ideal for consortia, while solutions for identity ledger choices are discussed in the next section. In addition, the C2DTA's VC and its attributes are represented. VCs include the "Enrollment VC,"

[11] Consumers may be interested to pay AI providers for advanced models for data they don't have, for instance, a consumer can rent a cardiovascular-risk model that analyzes routine exam results.

[12] Different ecosystems may support different transactions such as sharing or even fractional ownership.

which documents the organizations' consortium membership; the "Genesis VC," which records the SD provenance; and the "Ownership VC," which verifies a user's control over a given SD.

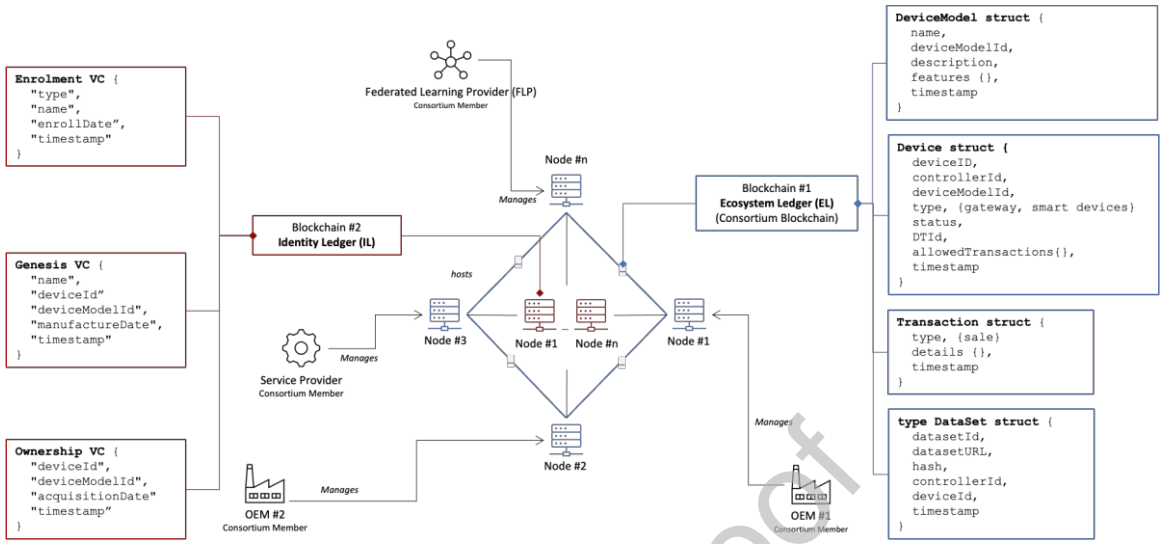


Fig. 5. Consumer-Controlled Digital Twin Architecture (C2DTA) dual blockchain strategy with an Identity ledger for Decentralized identifiers (DIDs), Verifiable credentials (VCs), and an ecosystem ledger for transactions tracking.

Agents: Each stakeholder within the C2DTA is represented by an SSI agent responsible for executing all operational functions (Fig. 6). Agents connect, request, and issue credentials to prove things and discover things via DIDComm protocols, a "recipe for a stateful interaction" [89]. Many devices can host agents. For example, consumers can host their agents in mobile digital wallets, businesses can use cloud servers, and devices can operate their agents autonomously. Agents rely on digital wallets to provide secure storage for stakeholders' cryptographic materials, such as keys and VCs. Agents that do not have stable internet endpoints—typical consumers and devices—require mediation services [90] provided by SSI-as-a-Service (SSIaaS) providers[13] such as mediator service providers[14] and mobile wallet providers[15]. These service providers offer cloud agents with stable internet endpoints and act as intermediaries, receiving messages on behalf of the agent and holding them until the agent can retrieve them. Our work represents agents that use the Aries RFC 0006: SSI Notation[16]. For instance, the consortium's agent is represented by 1@C, in which "1" signifies the first agent within the consortium's domain and "C" denotes the C2DTA consortium as a "self-sovereign entity" with its identity domain. In the case of devices, which the notation considers "non-self-sovereign," they are represented in lowercase. For example, the SD agent is represented by "1@sd", while its mediator agent is represented by "2@sd".

[13] SSI-as-a-Service (SSIaaS), such as the examples currently offered by Danube Tech (e.g., godiddy.com), is bound to emerge as adoption of the SSI ecosystem increases.
[14] Indicio.Tech offers a mediator agent, with open-source code available in the ACA-Py library
[15] Examples include Trinsic (https://trinsic.id/), TNO EASSI (https://www.tno.nl/)
[16] https://github.com/hyperledger/aries-rfcs/tree/main/concepts/0006-ssi-notation

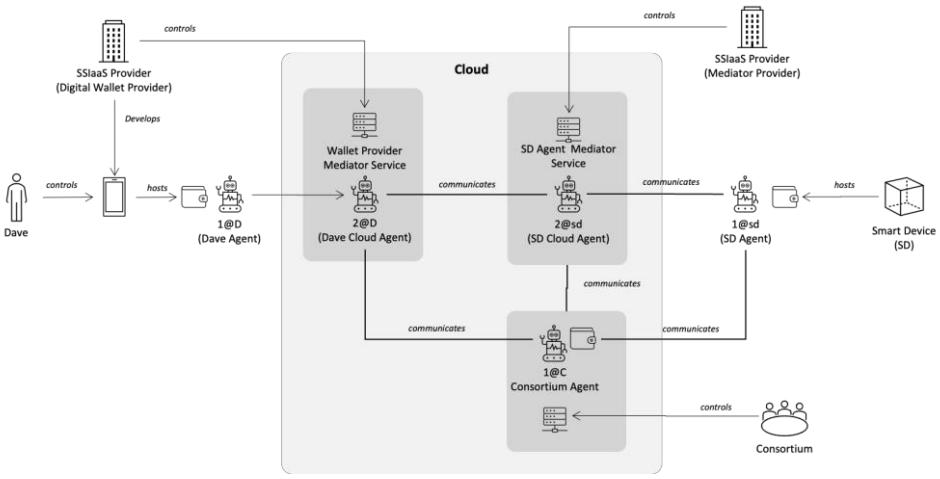


Fig. 6. Consumer-Controlled Digital Twin Architecture (C2DTA) Self-Sovereign Identity (SSI) agents.

Device: C2DTA distinguishes between two device types: the Edge Gateway (EGW) and a SD. Each has a "device model" providing metadata that support integration into the device ecosystem, such as features and images common to that model. For SDs, this "device model" is vital, linking the SD to its DT definition, which uses the Web of Things (WoT) standard. This W3C [91] standard uses the Thing Description (TD) meta-model and supports JSON-LD[17] for enhanced DT discoverability [92]. Furthermore, each device has a Quick Response (QR) code with the Out-of-Band (OOB) communication Uniform Resource Identifier (URI) for its agent. This QR code, when scanned by human stakeholders, opens mobile app digital wallets via a deep link [93], allowing them to establish a connection with the device.

Device identity: Both EGW and SDs generate their own identities. A self-generated identity improves trustworthiness by mitigating the risks of identity theft and unauthorized access, as preset manufacturers' IDs can be duplicated or stolen. The EGW generates a public DID, and the SD generates a Universally Unique Identifier (UUID). Both these identities are generated during the first boot. The EGW needs a public DID because it creates VCs, for example, when a consumer sells an SD and is a trust anchor of the ecosystem.

Edge gateway: The EGW is an indispensable and multifunctional component of C2DTA (Fig. 7). First, it serves as a connectivity hub at the consumer edge, linking the SDs and their controllers' agents with the broader ecosystem through DIDComm protocols. Second, the EGW hosts the DT platform that facilitates the SD twins. Third, it interfaces with the ecosystem ledger to track SD status updates (see the Device Status topic below) and with the identity ledger for credential verification and issuance. Finally, the EGW regularly transfers historical data from the DT platform to decentralized storage. An EGW can support multiple SDs or focus on a single SD, such as a smart car. The EGW controller is tasked with authorizing the onboarding of SDs, after which SD controllers may initiate the twinning and untwinning processes. Ultimately, by decentralizing computing power currently concentrated in the cloud by incumbent PDE entities (e.g., OEMs, data purchasers), the EGW gives consumers *de facto* control over their data and provides them with a trustworthy and safe mechanism to engage with other ecosystem stakeholders. While the EGW is a single point of failure in C2DTA, its primary role is to safeguard data integrity and privacy. If the PDE experiences a failure or disruption, consumer data remain secure and inaccessible to unauthorized entities.

[17] https://www.w3.org/TR/json-ld11/

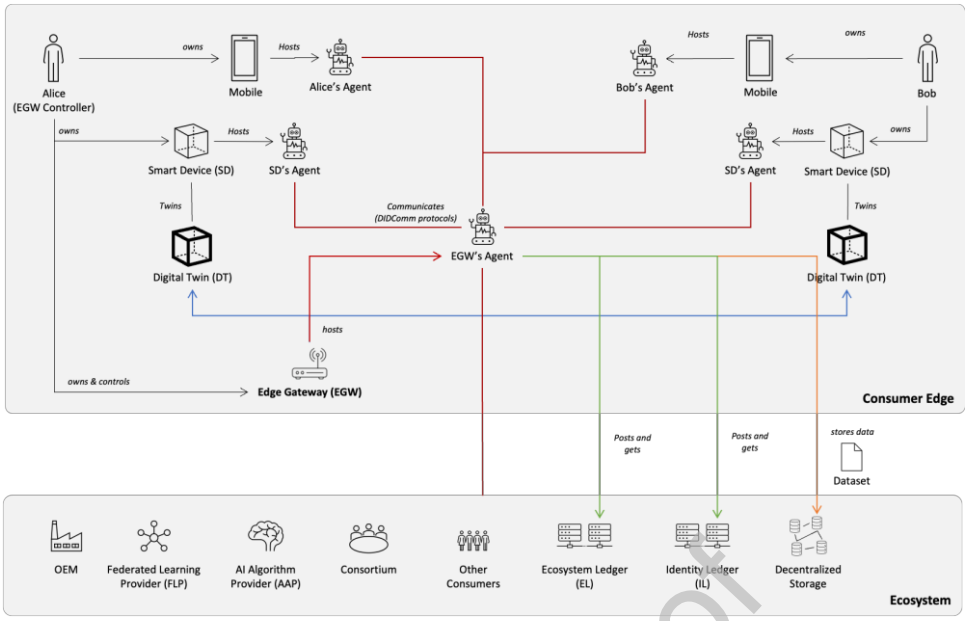


Fig. 7. The role of the Edge Gateway (EGW) in the ecosystem as a consumer-side hub for connectivity, Digital-twin hosting, ledger integration, and data stewardship.

Device status: C2DTA is an asset-centric solution that uses a six-state model to track devices from cradle to grave (Fig. 8). In the case of device and data provenance, these statuses are registered in the ecosystem ledger as follows:

1. **Manufactured.** —Establishes the SD's readiness for its initial boot-up at the factory. On powering up, the SD agent automatically connects with the OEM agent, who creates and sends a "Genesis VC." Subsequently, the OEM registers the SD in the DT ledger, setting its state to "Available" and setting the OEM as its controller.
2. **Available.** —When an SD state changes to "Available," it triggers a process that lists the device for sale on the consortium's decentralized eCommerce site. When a sale is completed, the OEM sends an "Ownership VC" to the consumer and updates the SD status in the ledger to "In-Transit."
3. **In-transit.** —After buying the SD, it is assumed that the new controller does not immediately take physical possession of it. This state reflects a situation in which the new consumer has an "ownership VC" but has not yet taken possession of the SD.
4. **Claimed**. —Upon receiving the SD, the consumer can "claim" the device[18]. The EGW acts as an ecosystem policy enforcer by matching the "Ownership VC" and "Genesis VC." If both VCs refer to the same SD, the EGW updates the ledger, marking the SD's state as "Claimed."
5. **Twinned**. After "claiming" an SD, the consumer can "twin" it. To do so, the consumer connects to the EGW agent to request twinning. The EGW agent downloads the DT definition file (WoT) from the consortium repository and then creates the DT. The EGW then sends a message to the SD agent instructing it to start collecting data. When the process is complete, the EGW agent updates the SD state to "Twinned."
6. **Decommissioned.** —When the SD reaches the end of its lifecycle, the DT ledger is updated to reflect its decommissioning status.

[18] For clarity we will assume here that the consumer has access to an EGW. In the next section both cases are considered in detail.

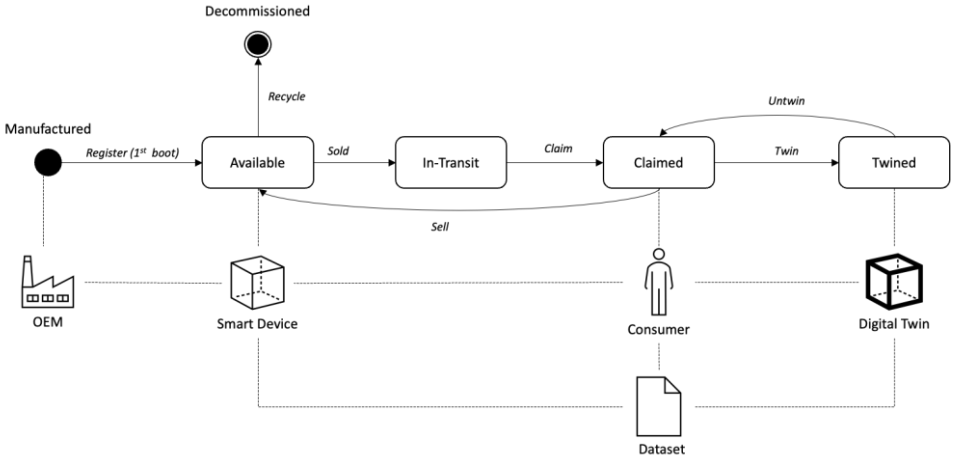


Fig. 8. Smart device (SD) state diagram.

Device storage: Even though we propose using the IPFS to store DT data in addition to the system provided by the DT platform, consumers should be able to choose from different storage solutions (e.g., AWS S3). Since consumers are financially responsible for this capability, consortia should provide alternatives. We propose using decentralized storage, such as IPFS, given its ability to scale, resist censorship, and prevent data centralization under a single operator [94]. Notably, the data storage field is developing rapidly, with organizations such as MyData.org [60] and the Decentralized Identity Foundation (DIF) Foundation's Secure Data Storage Working Group[19] focusing on personal data storage standards.

SD twinning: This capability is arguably at the core of C2DTA. Once the consumer decides to twin an SD, the system automatically creates the DT in the DT platform, initiating sensor data transmission to the twin and regularly pushing DT data to decentralized storage. The DT creation process leverages the W3C WoT standard. With respect to sensor data transmission, while DIDComm could have been a valid choice, we strategically opted for Message Queuing Telemetry Transport (MQTT) to optimize performance.

Transaction control: Transactions that involve actions from multiple SSI agents must have their state preserved. One example is OEM enrollment into the consortium initiated by an employee, who must communicate with the OEM agent to finish the enrollment. C2DTA uses a key-pair table to implement this functionality. While we have not used time limits to complete this operation, it could be implemented in the future and become a setup configuration for the consortium.

Automation: To ensure scalability, accountability, and ease of use, C2DTA utilizes automated procedures whenever feasible. One of the strategies involves using "goal codes"[20] in agents' communications, thus enabling effective communication between various parties by providing a means to express their intentions comprehensibly to humans and automated software. For example, when an introduction is made between two agents, the architecture uses goal codes to further contextualize the requests, allowing agents to make automated decisions. Another area of automation is device registration. All devices are self-registered in the

[19] https://identity.foundation/working-groups/secure-data-storage.html
[20] https://github.com/hyperledger/aries-rfcs/tree/main/concepts/0519-goal-codes

ecosystem ledger and are responsible for generating their own identities, which requires access to the identity ledger in the case of the EGW.

Organization representatives: Each organization must place trust in one or more of its employees to act on its behalf within the ecosystem. The consortium's agent maintains the list of allowed organizations' representatives in the agent table.

Architectural blueprint: The architecture comprises the consumer and business edges and the ecosystem, peer-to-peer communications, and record layers (Fig. 9). The "consumer edge" is where the EGW, SD, and DT operate. The "business edge" encompasses the consortium that manages the C2DTA implementation, the EGW, and the SD OEMs. To enroll in the consortium, OEMs must identify an ecosystem manager that establishes the initial connection to the consortium agent and then introduce it to the OEM agents. Through its marketing website, the ecosystem layer furnishes potential stakeholders with insights into the consortium's advantages. Moreover, this layer enables stakeholders to conduct transactions, buying and selling devices[21], for example, using the consortium's decentralized marketplace[22]. In addition, it allows stakeholders to buy and sell devices via a consortium decentralized marketplace app. The peer-to-peer layer allows stakeholders to communicate in a safe and structured way via DIDComm protocols. The third layer is the Records Layer, which anchors the ecosystem transactions and identity ledgers.

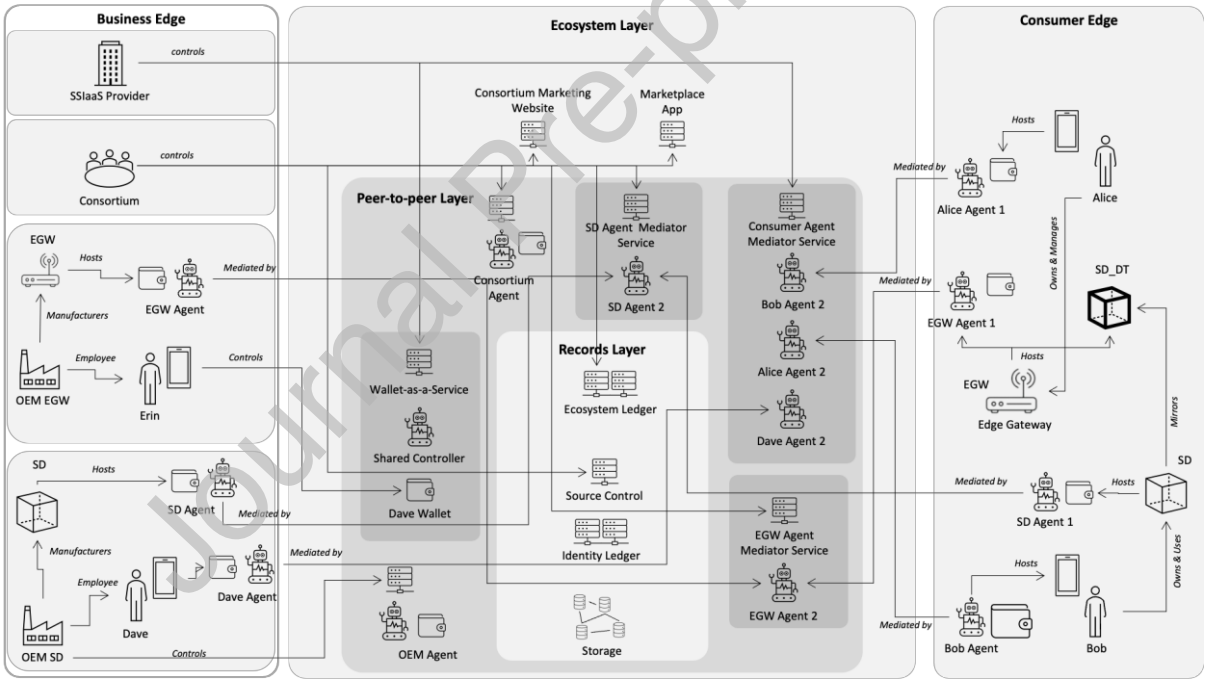


Fig. 9. Consumer-Controlled Digital Twin Architecture (C2DTA) five layers: business, ecosystem, peer-to-peer, records, and consumer edge layers.

[21] This research only considers the sale of an SD, although, it is expected that the marketplace will support other operations in the future, such as sharing and fractional ownership.

[22] Implementation of these apps is beyond of the scope of this paper.

Open source: C2DTA was designed to be an open-source initiative managed by a consortium potentially made up of universities, SSI service providers (e.g., wallet providers, software developers), and other stakeholders interested in developing a consumer-centered PDE (Fig. 10). Specific C2DTA-based consortia could focus on specific SD types and geographical locations and operate under different business and operational governance models [87]. At a minimum, a C2DTA-based consortium must include one or more OEMs willing to build C2DTA-enabled SDs and several AAPs to deliver value to consumers.

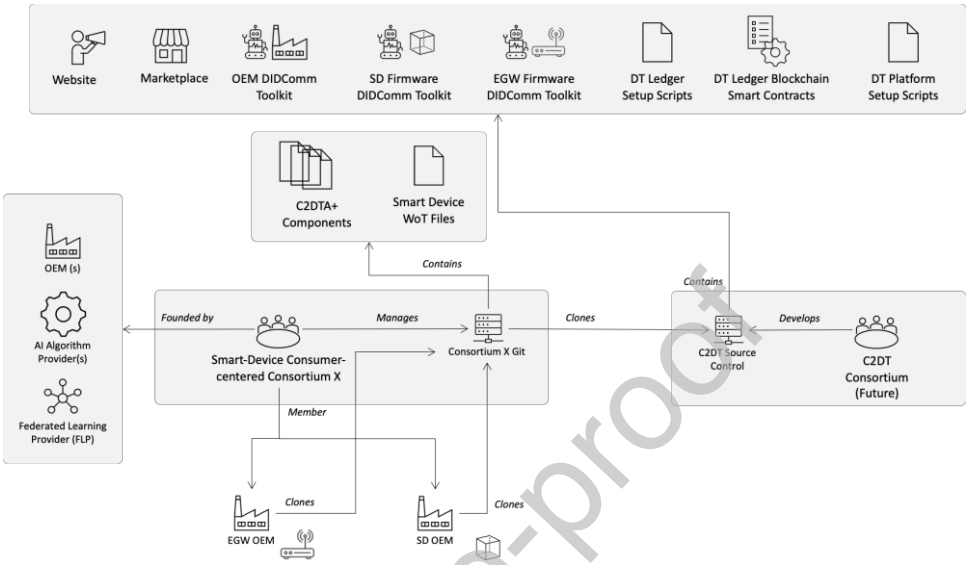


Fig. 10. Consumer-Controlled Digital Twin Architecture (C2DTA) component cloning framework for launching consumer-centered Smart device (SD) consortia.

Market strategy: In the absence of a legal framework, there is no incentive for incumbent OEMs with well-established DT or Industrial IoT capabilities to participate in the new ecosystem that empowers consumers. Yet, four forces still drive C2DTA adoption as represented in Fig.11. First, emerging manufacturers, especially those exploring 3D printing and social manufacturing [95, 96], can reduce capital expenditure by offloading DT infrastructure to C2DTA. Second, the same shift allows them to foster consumer trust by giving consumers *de facto* control over their DTs. Third, C2DTA's asset-centric, dual-blockchain architecture records each smart device, its datasets, and their interrelationships on-chain, securing data provenance and thereby improving opportunities for consumer data monetization. Fourth, C2DTA facilitates the aggregation of multiple DTs into a single personal digital twin, a concept further discussed in Section 5.

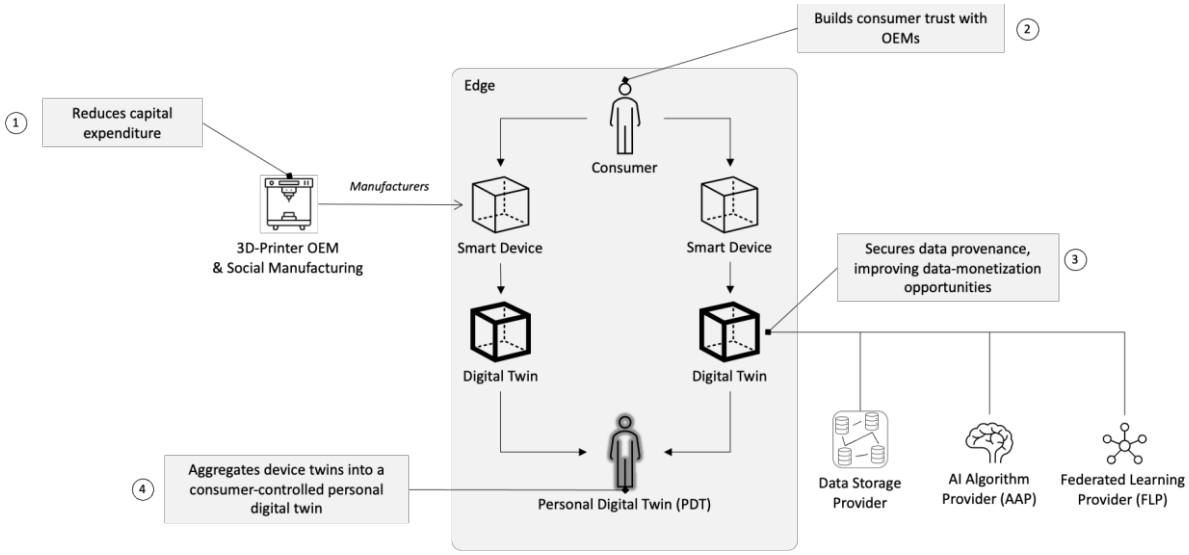


Fig. 11. Consumer-Controlled Digital Twin Architecture (C2DTA) market drivers.

Transaction fees: While not discussed in detail as it is beyond the scope of this paper, fees are associated with various aspects, such as issuing DIDs, credentials, digital wallet usage, DIDComm mediators, and others [97]. The specific costs and payment mechanisms will depend on whether the consortium deploys its blockchains or utilizes third-party networks. In the latter case, the consortium may act as an intermediary to provide a single invoice to its members or require members to have direct accounts with third-party providers.

3.2 Functional description

This section provides a detailed functional description of the C2DTA using eight sequenced business scenarios (Fig. 12), each represented in its unique sub-section. The eight scenarios are as follows:

1. An OEM enrolls in a C2DTA-based consortium (Section 3.2.1).
2. The OEM registers a device type in the ecosystem ledger (Section 3.2.2).
3. A device manufactured by the OEM self-registers in the ecosystem ledger (Section 3.2.3).
4. A consumer buys a device from the OEM (Section 3.2.4).
5. The consumer claims a device (Section 3.2.5).
6. The consumer twins the SD (Section 3.2.6).
7. The consumer untwins the SD (Section 3.2.7).
8. The consumer sells the SD to another consumer (Section 3.2.8).

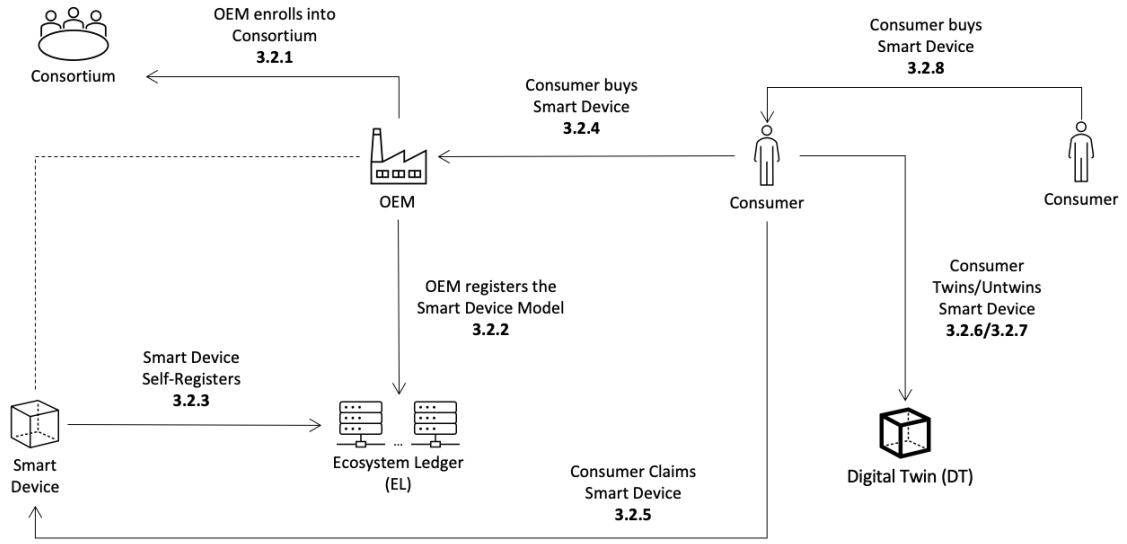


Fig. 12. Consumer-Controlled Digital Twin Architecture (C2DTA) high-level lifecycle and transaction flow covering Original Equipment Manufacturing (OEM) enrollment, device registration, consumer ownership, twinning/untwinning, and secondary-market transfer.

This scenario makes the following assumptions and decisions:

- The existence of a viable consortium.
- The OEM devices are C2DTA compliant and correctly leverage the consortium's firmware libraries.
- The existence of a smart-wallet provider with support for Hyperledger Aries RFC 0509[23] , 0028[24].
- The OEM deploys and sustains its own SSI agent server on the cloud.
- The EGW uses firmware information to connect with the factory's Wi-Fi network and incorporates a basic interface that enables the controller to input the Wi-Fi's SSID and password.
- The EGW supports a DIDComm protocol that allows consumers to connect an SD to Wi-Fi. When a consumer initiates the protocol, the EGW starts a Bluetooth server that the SD searches for during boot. This Bluetooth server is known via firmware to all devices and uses Secure Simple Pairing (SSP) to pair the EGW and the SD. Once paired, the EGW sends the SSID and password via the Serial Port Profile (SPP) protocol.
- The consortium operates a marketing website and a decentralized marketplace (see Section 3.1, subsection Architectural Blueprint) composed of a sustainable group of organizations that jointly host the ecosystem ledger and an identity ledger.
- While most operations in C2DTA are automated, scenarios requiring human interaction assume that consumers' digital wallets support the Aries RFC 0509 Action Menu protocol[25].
- Since Aries RFC 0028[26] is not implemented, simple messages were used to enable agent introductions.

[23] https://github.com/hyperledger/aries-rfcs/blob/main/features/0509-action-menu/README.md
[24] https://github.com/hyperledger/aries-rfcs/blob/main/features/0028-introduce/README.md
[25] https://github.com/hyperledger/aries-rfcs/tree/main/features/0509-action-menu
[26] https://github.com/hyperledger/aries-framework-go/issues/269

To enhance clarity and provide a holistic perspective of each use case scenario, we have opted for informal diagrams over the more complex UML sequence diagrams.

3.2.1 OEM enrollment

This scenario has two phases. During phase one (Fig. 13), an OEM employee named Dave uses the consortium's marketing website to enroll the OEM in the organization. Upon receiving the enrollment request, the Consortium's agent (1@C) sends instructions for the deployment of the OEM's agent (1@O), an Out-of-Band (OOB) URI[27] to enable DIDComm communications, and the goal code. To ensure system integrity, 1@C assigns a transaction UUID stored in the transaction table. Once 1@O is operational, Dave resolves the OOB URI, opening his digital wallet. This allows agent (1@D) to connect with 1@C. To validate the transaction and goal, 1@C uses the agent table to record Dave's role[28]. After this, 1@D uses an implicit invitation[29] to connect with 1@O with a public DID known to him. The corresponding pseudocode is as follows:

```
1. Dave->marketingWebsite.EnrollOEM()
2. marketingWebsite->1@C.RequestOOB_URI()
3. 1@C.TransactionStart(createUUID())
4. 1@C.createOOB(c2dt.consortium.enroll.OEM UUID)->marketingWebsite
5. marketingWebsite.Display(OOBInstructions,OOB_URI)
6. OEM.AgentBoot() – after OEM Staff deploys server
7. If 1@O.isFirstBoot() then 1@O.CreatePublicDID()
8. Dave->marketingWebsiteGet(OOB_URI)
9. 1@D.AgentConnect(OOB_URI, goal)->1@C
10. If 1@C.goal(ENROLL) AND 1@C.GetTransaction(UUID) then 1@C.CreateConsortiumAgent()
11. 1@D.AgentConnect(OOB_URI,goal)->1@O – Implicit invitation
```


[27] https://github.com/hyperledger/aries-rfcs/blob/main/features/0434-outofband/README.md

[28] Although we did not implement this, a given consortium may opt to have the OEM issue a "power delegation" VC to Dave.

[29] https://github.com/hyperledger/aries-rfcs/blob/main/features/0160-connection-protocol/README.md

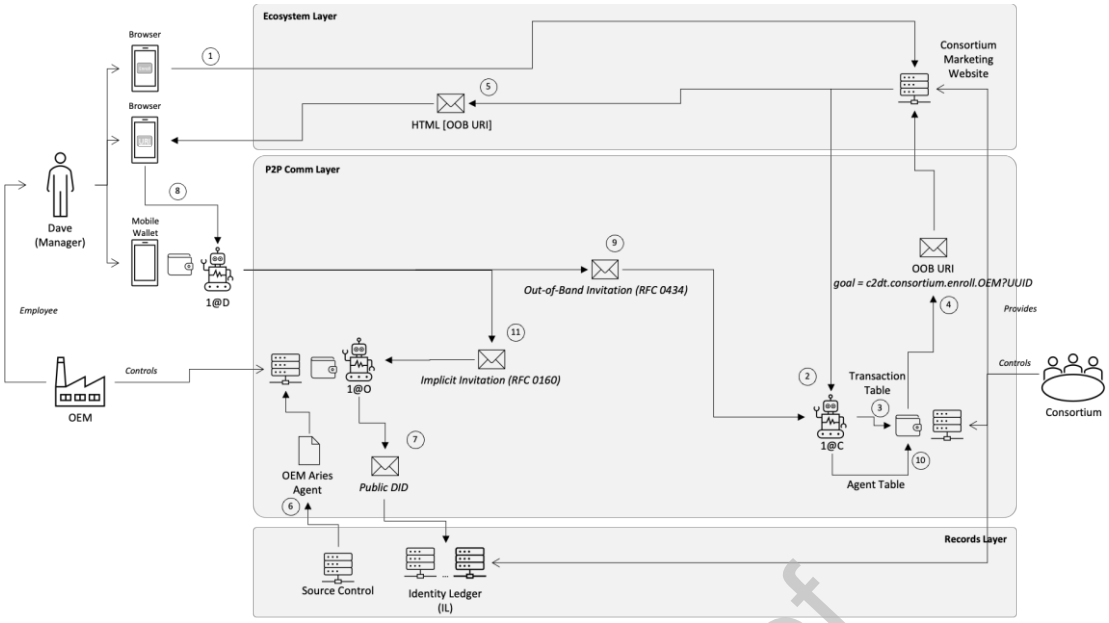


Fig. 13. Phase 1 of Original Equipment Manufacturer (OEM) enrollment via Out-of-Band (OOB) URI.

In phase two (Fig. 14), 1@D introduces 1@O to 1@C, facilitating their connection[30]. Once connected, 1@C updates the agent table with the OEM's public DID. To ensure trustworthiness, 1@C proposes the Enrollment VC[31] to 1@O, requesting specific documents. After the documents are validated, 1@C messages[32] 1@O are used to generate the digital certificate, which allows 1@O to post information about the devices it manufactures to the ecosystem ledger. Once the certificate is generated, 1@O notifies 1@C, completing the process and resulting in the issue of the Enrollment VC to 1@O.

```
1. 1@D.Introduction(OOB_URI,goal code)->1@O
2. 1@O.AgentConnect(OOB_URI, goal)->1@C
3. If 1@C.goal(ENROLL) AND 1@C.GetTransaction(UUID) then UpdateA-
   gent(OEM_DID)
4. 1@C.CredentialPropose(ENROLLMENT)->1@O
5. 1@O.SubmitDocProof()->1@C
6. If 1@C.isValidProofs() then 1@C.Message("Generate_Credentials")->1@O
7. 1@O->1@C.GenerateX.509()
8. 1@O.EcosystemLedgerEnroll()
9. 1@O.Message("CA_ACK")->1@O
10. 1@C.CredentialIssue("Enrollment")->1@O
```

[30] https://github.com/hyperledger/aries-rfcs/blob/main/features/0028-introduce/README.md
[31] https://github.com/hyperledger/aries-rfcs/blob/main/features/0453-issue-credential-v2/README.md
[32] https://github.com/hyperledger/aries-rfcs/blob/main/features/0095-basic-message/README.md

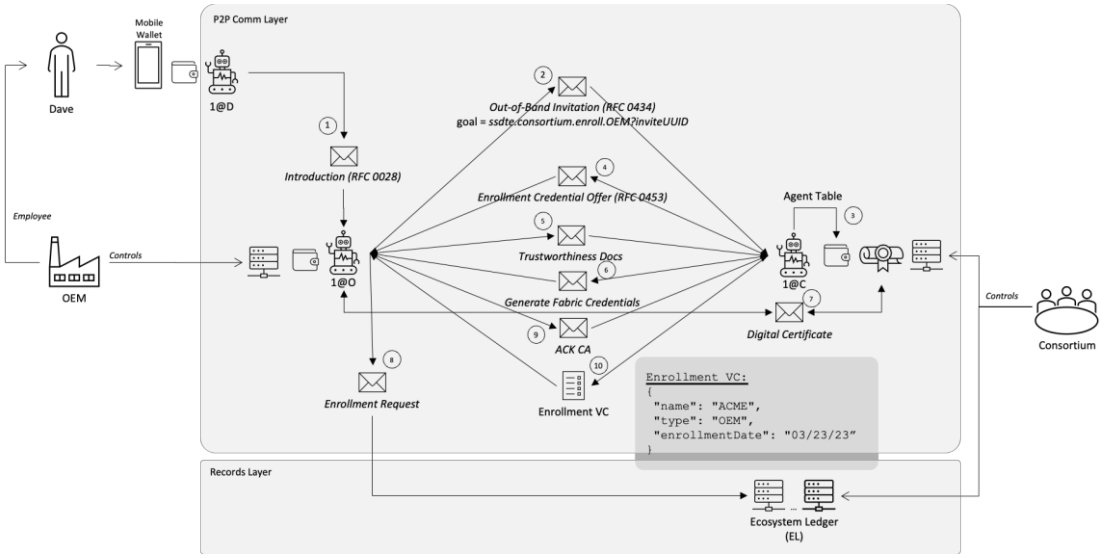


Fig. 14. Phase 2 of Original Equipment Manufacturer (OEM) enrollment.

3.2.2 Device model registration

To register the device model (Fig. 15), Dave uses his digital wallet to have 1@D request the action menu from 1@C[33]. He then selects the "Register Model" providing the necessary information. Upon receiving the information, 1@C generates a unique identifier for the model and posts a transaction to the ecosystem ledger. In addition, 1@C uploads the WoT file to the consortium's source control, enabling consumers to associate their devices with the model, and posts the images and feature information to the Marketplace App, allowing consumers to purchase them. Subsequently, 1@C messages 1@O the *deviceModelID*, thus completing the process.

1. `1@D.ActionMenuGet()->1@C`
2. `1@D.DeviceModelRegister(Name,Description,[Feature_info],[Images],WoT_file)->1@C`
3. `1@C.EcosystemLedgerStore(Device_metadata)`
4. `1@C.SourceControlStore(WoT)`
5. `1@C.MarketAppStore(Metadata,[feature_info],[images])`
6. `1@C.Message(deviceModelID,DeviceName)->1@O`

[33] https://github.com/hyperledger/aries-rfcs/blob/main/features/0509-action-menu/README.md

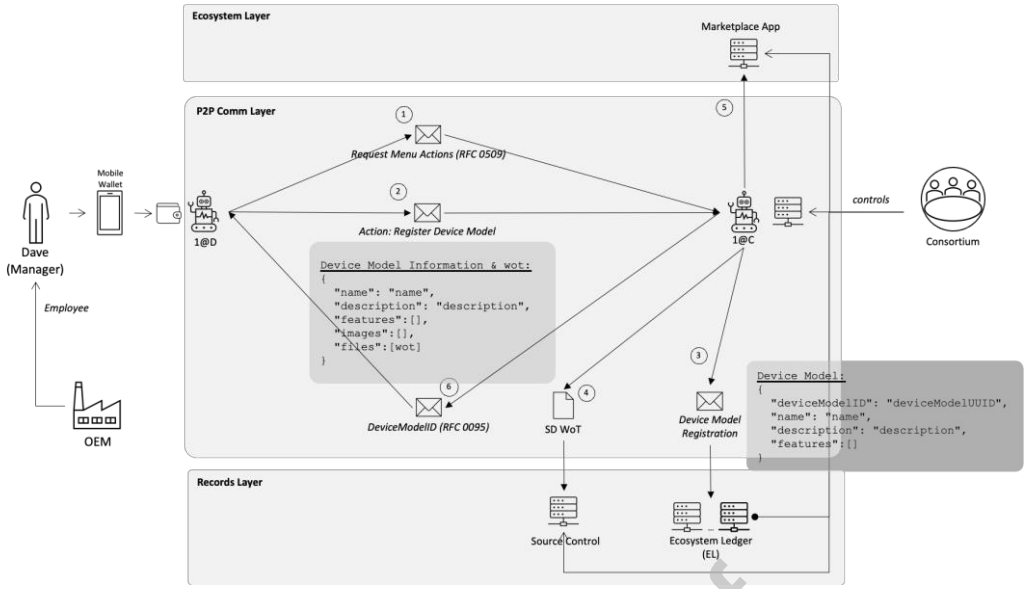


Fig. 15. Device model registration from Original Equipment Manufacturer (OEM) manager wallet invocation to Web-of-Things (WoT) file upload in source control.

3.2.3 Device self-registration

C2DTA-enabled devices automatically register in the ecosystem ledger during the first boot (Fig. 16). Given that the EGW and the SD have slightly different processes, we analyze both. Although we did not implement this, during self-registration, the OEM can define a "sale array" with a list of attributes that assist the sale, such as price, currency, whether it is negotiable, any discounts, etc. To simplify the diagram, the EGW steps to obtain the digital certificate and enroll in the ecosystem ledger demonstrated in phase 2 of OEM enrollment (see Fig. 12) were omitted. Importantly, 1@egw obtains the OEM's public DID for the connection via the firmware. Additionally, when 1@O lists the EGW for sale in the Marketplace App, the "buy" button URL is associated with the OEM's OOB URI and the goal *c2dt.consortium.buydevice*, along with the "sale array" information.

EGW self-registration encompasses the following steps:

1. (OEM integrates the EGW with the required consortium's firmware libraries)
2. 1@egw.Boot()
3. If 1@egw.FirstBoot() then 1@egw.CreatePublicDID()
4. 1@egw.AgentConnect(PublicDID,*c2dt.consortium.registerdevice DID*)->1@O
5. 1@O.CredentialProposal(GENESIS)->1@egw
6. 1@O.EcosystemLedgerStore(EGW_metadata)
7. 1@O.MarketStore()
8. 1@O.CredentialIssue(GENESIS)->1@egw

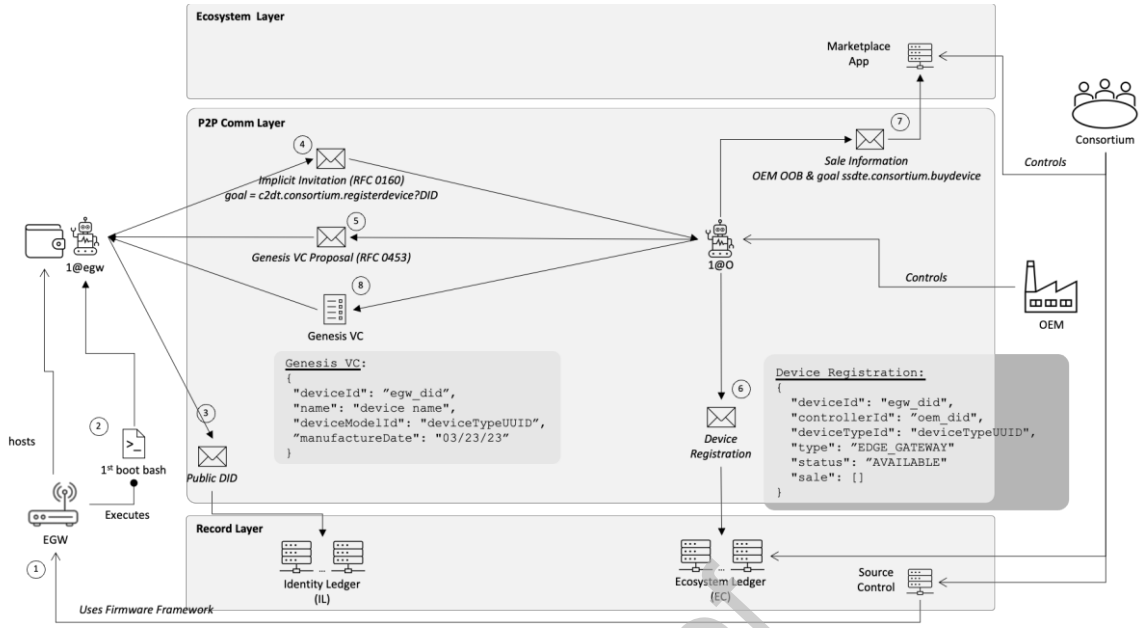


Fig. 16. Edge Gateway (EGW) self-registration from first boot, public Decentralized identifier (DID) and genesis Verifiable credential (VC) generation, to ecosystem ledger entry and marketplace listing.

SD self-registration (Fig. 17) involves the following steps:

1. (The OEM integrates the SD with the required consortium firmware libraries)
2. 1@sd.Boot()
3. If 1@sd.FirstBoot() then 1@sd.GenerateUUID()
4. 1@egw.AgentConnect(PublicDID, c2dt.consortium.registerdevice UUID)->1@O
5. 1@O.CredentialProposal(GENESIS)->1@sd
6. 1@O.EcosystemLedgerStore(SD_metadata)
7. 1@O.MarketplaceStore()
8. 1@O.CredentialIssue(GENESIS)->1@sd

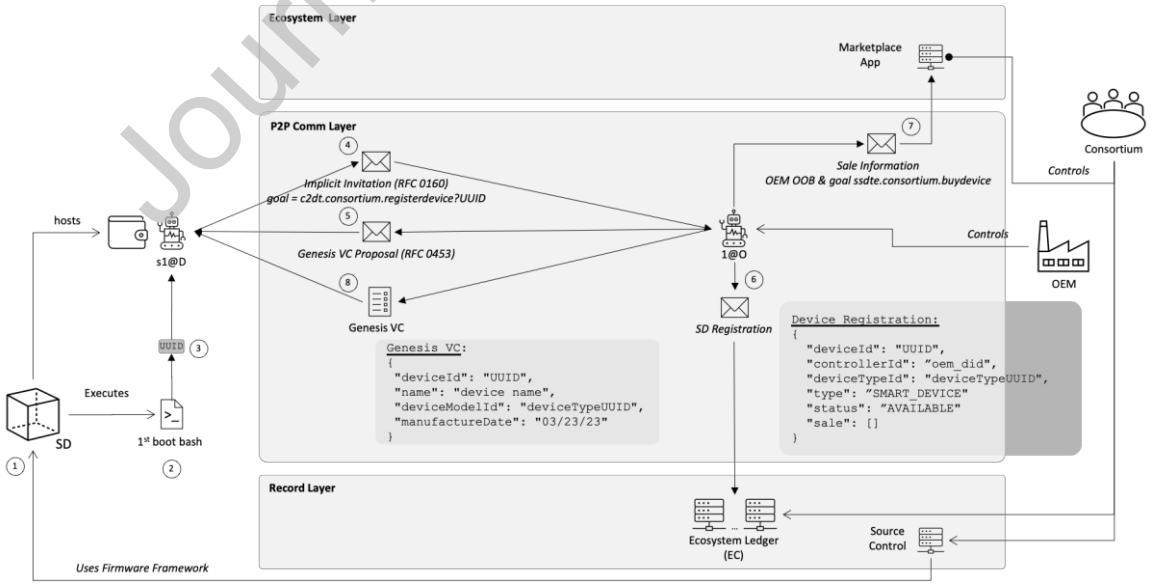


Fig. 17. Smart Device (SD) self-registration from first boot, identifier and genesis Verifiable credential (VC) generation, to ecosystem ledger entry and marketplace listing.

3.2.4 Consumer buys device

The process for purchasing a device (Fig. 18) is identical for both the EGW and the SD, although consumers must first acquire an EGW to join a C2DT ecosystem. Only after an EGW is obtained can a consumer own SDs. As detailed in Section 3.2.3, Alice's agent (1@A) connects with 1@O because the "Buy" link is associated with the OEM's OOB_URI and goal. With this information, the 1@O knows that it should propose an "Ownership VC" with a price. The following list outlines this process.

1. `Alice.MarketplaceSearch()`
2. `Alice.MarketplaceBuy()`
3. `1@A.AgentConnect(OOB_URI, goal)->1@C`
4. `1@O.CredentialProposal(OWNERSHIP,price)->1@A`
5. `1@A.Bank.Pay() – out of scope`
6. `1@O.EcosystemLedgerUpdate(IN-TRANSIT)`

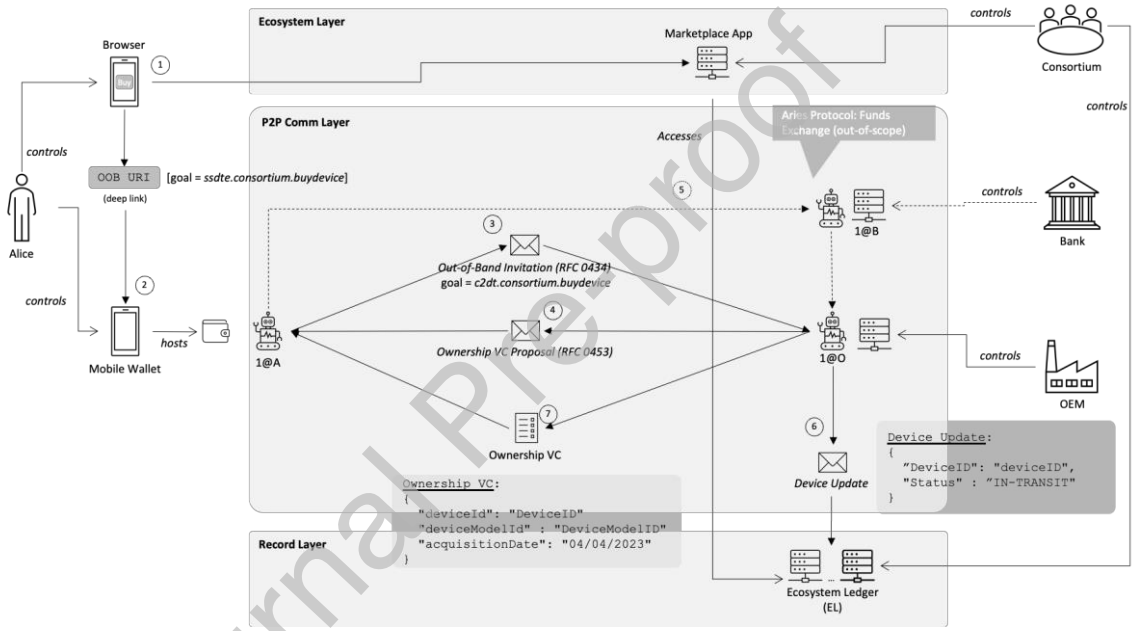


Fig. 18. Device Buy from marketplace Out-of-band (OOB) "Buy" link invocation to ownership Verifiable credential (VC) issuance and ecosystem ledger status update.

3.2.5 Device claiming

This section describes the process for claiming an EGW and an SD (Fig. 19). Claiming an SD is more complex because it requires establishing an association with an EGW. In this scenario, Alice owns an EGW, and Bob owns an SD. After Alice claims the EGW, Bob must request permission onboard his SD. The EGW claiming process is described below. Importantly, the ecosystem ledger transaction *ControllerId* is set to the self-certifying DID Alice uses in communication with EGW. This establishes Alice's control over the EGW without compromising her privacy.

1. `Alice.Scans(EGW_OOB_QR)`
2. `1@A.AgentConnect(EGW_OOB_URI, c2dt.consortium.claim)->1@egw`
3. `1@egw.CredentialRequest("OWNERSHIP")->1@A`
4. `1@A.CredentialPresentation(OWNERSHIP)`

5. If (1@egw.ValidatesProof(EGW_Ownership,EGW_Genesis) then 1@O.Ecosys-temLedgerUpdate(CLAIMED,A.did@A:egw)

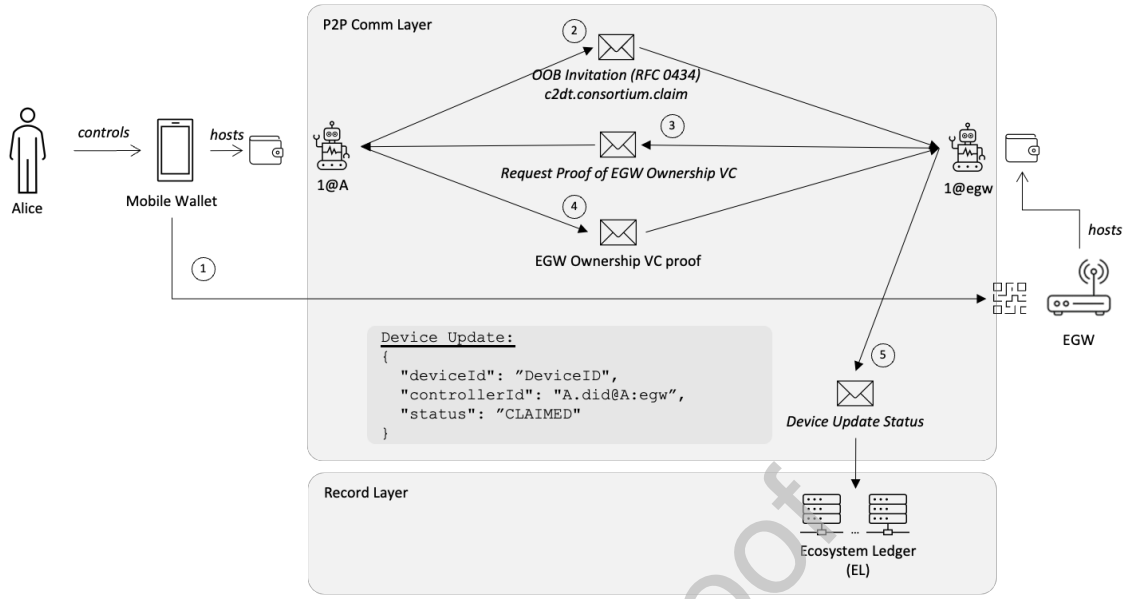


Fig. 19. Edge Gateway (EGW) claiming from device OOut-of-band (OOB) URI scanning, to ownership Verifiable credential (VC) assertion, controller identification assignment, and ecosystem ledger update.

The SD claiming process (Fig. 20) is described below. Given its additional complexity, the process is carried out within the context of a transaction. The SD also connects to the EGW via RFC 0214[34] and RFC 0228[35].

1. 1@B.ActionMenuGet()->1@egw
2. 1@B.SDClaim()
3. 1@egw.CredentialRequest(OWNERSHIP)
4. 1@B.CredentialPresentation(OWNERSHIP)
5. 1@egw.TransactionStart(DeviceID)
6. (Bob scans the SD QR code along with the *c2dt.consortium.claim* goal)
7. 1@B.Connect(SD_OOB_URI, goal)->1@sd
8. If 1@sd.isClaimGoallCode() then 1@sd.Request(EGW_standing_invitation)
9. 1@B.Submits(EGW_standing_invitation)
10. 1@sd.AgentConnect(EGW_OOB_URI,goal)->1@egw
11. 1@egw.CredentialRequest(GENESIS)
12. 1@sd.CredentialPresentation(GENESIS)
13. 1@egw.Message(APPROVE_ONBOARDING)->1@A
14. If 1@egw.ValidatesProof(SD_Ownership,SD_Genesis) AND 1@egw.isAp-proved() then 1@egw.DeviceAdd(B.did@egw.did,device ID)[36]
15. 1@egw.EcosystemLedgerUpdate(CLAIMED,EGW_DID)

[34] https://github.com/hyperledger/aries-rfcs/tree/main/features/0214-help-me-discover
[35] https://github.com/hyperledger/aries-rfcs/blob/main/features/0028-introduce/README.md
[36] The Device table enables 1@egw to know which agents own which SDs.

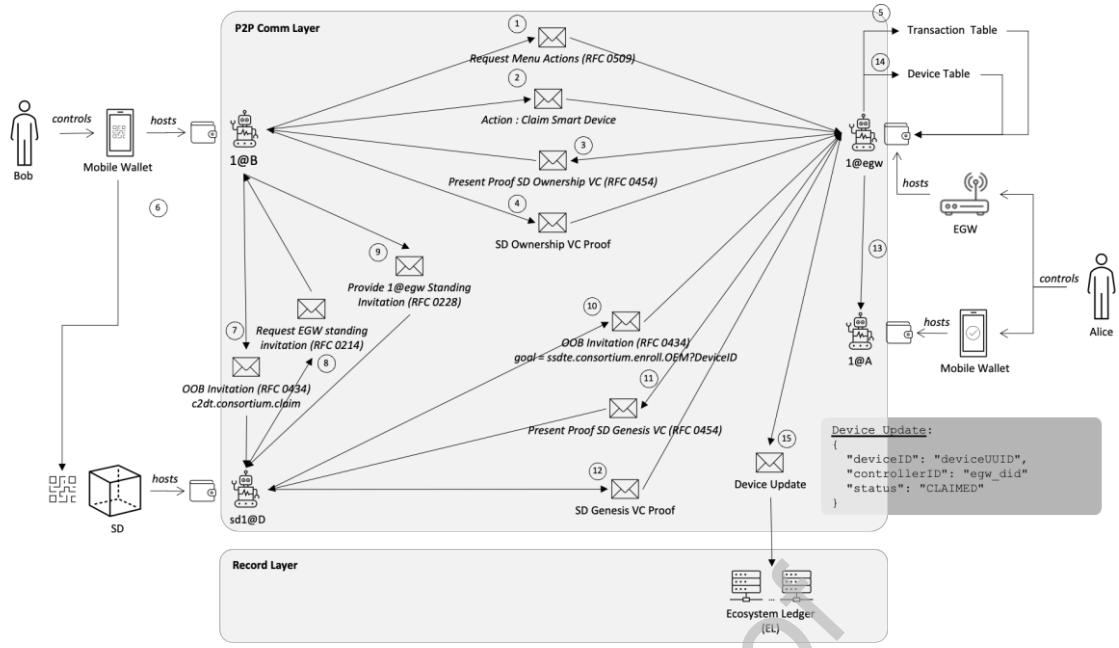


Fig. 20. Smart Device (SD) consumer claiming from action-menu invocation through ownership & genesis credential exchange to ecosystem ledger "claimed" update.

3.2.6 SD twinning

The SD twinning process (Fig. 21) is described below. Importantly, metadata from each dataset generated by the DT are anchored in the ecosystem ledger, which establishes its provenance and significantly increases trustworthiness.

1. 1@B.ActionMenuGet()->1@egw
2. 1@B.Twin(SD_deviceID[37], Twin_configuration[38])
3. 1@egw.Message(APPROVE_TWINNING)->1@A
4. 1@egw.DeviceUpdate(Twin_configuration)
5. 1@egw. Get(WoT) – first getting the *DeviceModelID* from the SD table stored during the "SD claim" action
6. 1@egw.StartDT(WoT) – assumes the DT platform has been running
7. 1@egw.Message(STREAM)->1@sd.StartStreaming(MQTT_TOPIC)
8. 1@sd.MQTTClientConfigure()
9. 1@egw.EcosystemLedgerUpdate(DeviceId,TWINNED)
10. (SD starts sending data sensor data via MQTT, and on regular intervals 1@egw creates datasets)
11. 1@egw.EcosystemLedgerCreate(dataset_metadata)
12. 1@egw.DecentralizedStorageStore(dataset)

[37] Created by the SD during the first boot.

[38] In our implementation, the *twin_configuration* defines the frequency with which files are written to decentralized storage (e.g., 24 h). Other implementations may define other parameters.

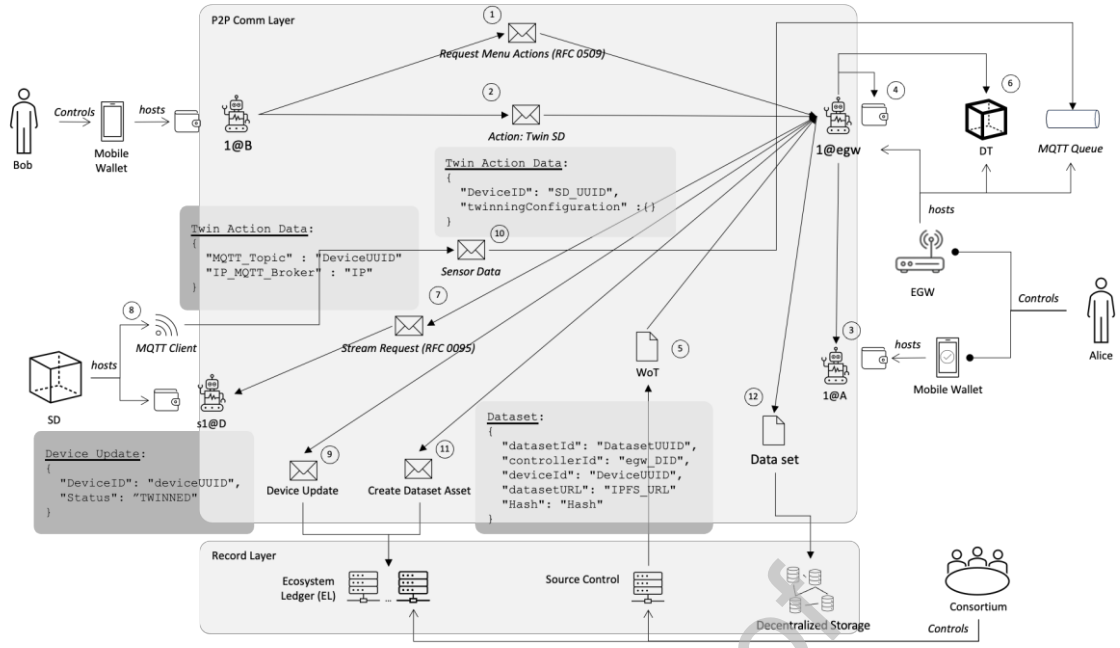


Fig. 21. Smart Device (SD) twining from twin request and Web of Things (WoT) retrieval to MQTT streaming, dataset creation, and ecosystem ledger "twinned" update.

3.2.7 SD untwinning

The SD untwinning process (Fig. 22) allows consumers to stop the SD data collection. This action is crucial for data trustworthiness, as no datasets can be linked to the device once it is untwinned.

1. `1@B.ActionMenuGet()->1@egw`
2. `1@B.Untwin(SD_deviceID, Untwin_configuration`[39]`)`
3. `1@egw.Message("StopStreaming")->1@sd`
4. `1@egw.DeviceDelete(SD_deviceID)`
5. `1@egw.DigitalTwinDelete()`
6. `1@egw.Untwin(untwin_configuration)`
7. `1@egw.EcosystemLedgerUpdate(CLAIMED)`

[39] Although this is beyond the scope of this article, in the future, C2DTA could use a configuration file to define specific actions on untwinning (e.g., unpin DT files, move to deep storage). This is particularly important when consumers do not host their IPFS nodes and rely on third-party providers that charge based on the storage used (e.g., https://www.pinata.cloud/pricing). Untwinning does not require approval from Alice because the SD owner is Bob.

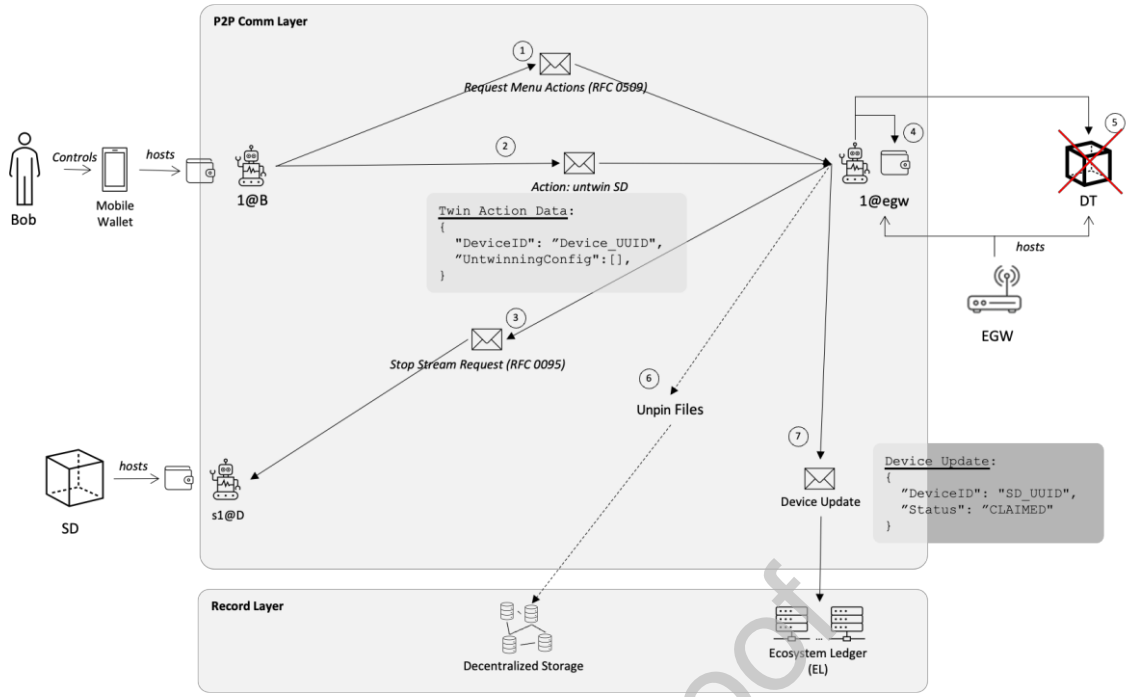


Fig. 22. Smart Device (SD) untwining from untwin request and streaming termination to digital twin (DT) and ecosystem ledger reversion to "claimed."

3.2.8 SD selling

To sell an SD (Fig. 23), the SD must be untwinned before being transferred to another consumer with access to an EGW. The following steps illustrate this process, where Bob sells the SD to Eve. Bob's EGW facilitates transactions because it possesses a public DID and ecosystem ledger access. This allows it to request revocation of the existing ownership VC, generate a new one, and update the status of the SD on the ecosystem ledger. Bob's EGW forwards the sale configuration to 1@C, including its OOB URI and the sell goal[40]. These elements are associated with the "buy" button, allowing Eve (or any other future buyers) to establish the connection.

1. 1@B.ActionMenuGet()->1@egw
2. 1@B.SDSell(SD_deviceID, Sale_configuration,Untwin_configuration)
3. 1@egw.ActionMenuGet()->1@C
4. 1@egw.Sell(Sale_Configuration)()->1@C
5. 1@C.MarketplaceStore(Sale_Configuration)
6. Eve.MarketplaceBuy(Bob's SD)
7. 1@E.Boot()
8. 1@E.AgentConnect("OOB URI",goal_code)->1@egw
9. If goal= "buy device" then 1@egw.CredentialPropose("Ownership")
10. 1@egw.CredentialRevoke(Ownership)->1@O
11. 1@egw.CredentialIssue("Ownership")->1@E[41]
12. 1@egw.EcosystemLedgerUpdate("IN-TRANSIT")
13. 1@E.ClaimSD()->1@egw_e – the process would continue as seen above, with Eve eventually twinning the SD again

[40] The sale configuration can include price, photos, or even automated negotiation procedures.
[41] At this point, Eve would initiate the money transfer protocol (which is beyond the scope of this research).

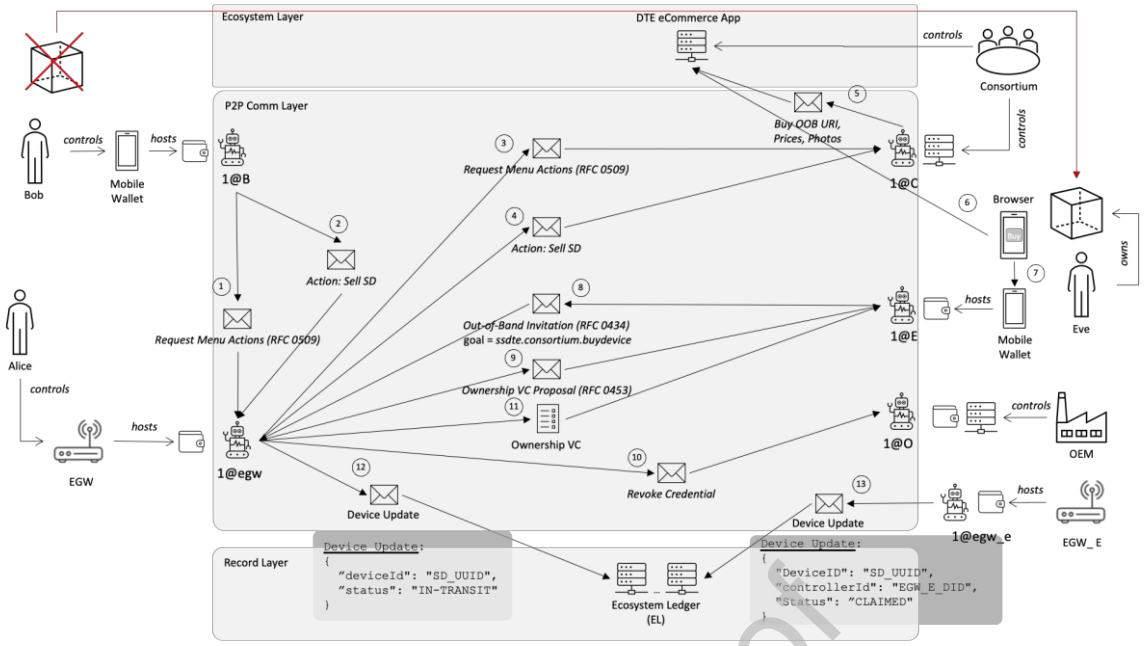


Fig. 23. Smart Device (SD) selling from sale configuration and marketplace listing to ownership revocation, ecosystem ledger "in-transit" update, and buyer reclaiming.

4 Evaluation and discussion

C2DTA was evaluated via the first seven use case scenarios for the business case delineated in Section 3.2. They include:

1) OEM enrollment in the consortium,
2) device type registration,
3) device self-registration,
4) consumer buys a device from the OEM,
5) consumer claims the device,
6) consumer twins SD,
7) consumer untwins SD.

Gherkin-based test scripts and the ACA-py Test Harness[42] were employed to execute the use case scenarios required to achieve this. The system's response time for each scenario step was documented, providing preliminary data on potential latency and scalability issues. Docker was deployed on a Proxmox/QEMU/KVM-based virtual machine (VM) on an Asus server with 16 GB of RAM and 32 CPUs (Fig. 24).

Our C2DTA implementation uses Hyperledger Fabric, the British Columbia Test Indy Network,[43] Eclipse Ditto, and IPFS. Hyperledger Fabric, a permissioned blockchain, was chosen for its commendable performance, scalability [98], and capacity to offer the consortium enhanced control over member enrollment [99]. An existing Hyperledger Indy network was selected, given its status as a highly interoperable, fit-for-purpose, public permissioned blockchain platform with robust privacy features and improved trustworthiness, and Eclipse Ditto because it is the most widely adopted open-source DT platform [100, 101].

[42] https://github.com/hyperledger/aries-agent-test-harness
[43] http://dev.greenlight.bcovrin.vonx.io/

Our evaluation focuses on testing the feasibility of our architecture, with an emphasis on identity management strategies, blockchain infrastructures, chaincodes and transaction control mechanisms, the SD status lifecycle, the automated twinning and untwinning processes and their integration with the WoT. In addition, we assess the transmission and storage of sensor data via in-transit and at-rest encryption, DIDComm protocols, and the generation and decentralized storage of datasets.

The test environment also reflects this focus. Minimal viable networks were utilized for Hyperledger Fabric and IPFS, with each Hyperledger Fabric node using one container to host the ledger (with CouchDB) and one to support the runtime services. The Ordering and Certificate Authority (CA) functions were deployed on their respective nodes. In addition, we established a two-node IPFS network in which each node utilized two containers, the first to host the ledger (with CouchDB) and the second to support the runtime services. The Ordering and CA functions were deployed on their respective nodes. A two-node IPFS network was also established.

Every actor in our test scenario (the orange nodes in Fig. 24) was assigned a container containing the ACA-py controller and the digital wallet. We developed a Python-based simulator for the smartwatch, which was placed in a dedicated container (light orange) responsible for generating a dataset comprising a heartbeat, geolocation, and timestamp at a 1 Hz frequency. These data were submitted to the DT infrastructure via MQTT over the Secure Sockets Layer (SSL).

The DT infrastructure leverages Eclipse Mosquitto[44] 2.0.1.5 and Eclipse Ditto 3.0.0, with each Ditto service deployed on its container. The services included the following: the “nginx server” responsible for routing requests and load balancing; the “Gateway” responsible for handling API requests and routing them to appropriate internal services; the “Connectivity” service responsible for managing external connections and integrations; the “Things” responsible for managing the state and data of individual DTs; the “Policies” service responsible for managing access control for DT; the “Things-search” responsible for providing search capabilities over DT; and the “database” responsible for persisting data related to DT, policies, and other service states. Since the Eclipse community edition was used, encryption was implemented at the operating system level[45] to encrypt data at rest. The EGW agent creates the DT infrastructure when it receives the request to twin the first SD. In other words, as long as the consumer does not twin an SD, the DT infrastructure does not exist.

[44] https://mosquitto.org/

[45] https://pentera.io/blog/how-to-achieve-data-at-rest-encryption-for-mongodb-community-edition-container-using-ecryptfs/

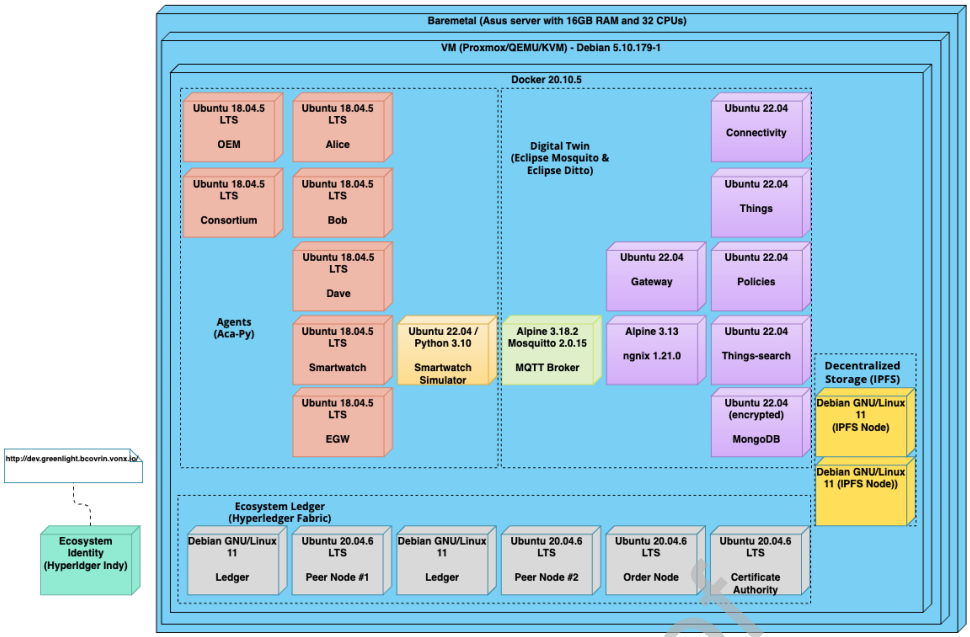
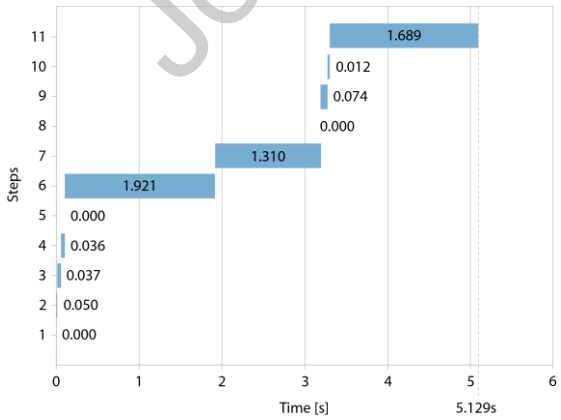


Fig. 24. Consumer-Controlled Digital Twin Architecture (C2DTA) containerized experimental setup: agent nodes with digital wallets and a smartwatch simulator streaming 1 Hz sensor data over MQTT/SSL to the Edge gateway (EGW) hosting the Digital twin (DT).

Our test results are shown below. Steps that have zero-time durations are associated with actions involving user interface selection, software deployment, or operations involving systems that were not developed as part of this research (e.g., the consortium website). The numbers on the list of actions described on the right-hand side correspond to the step numbers on the ordinate axis of the figures.

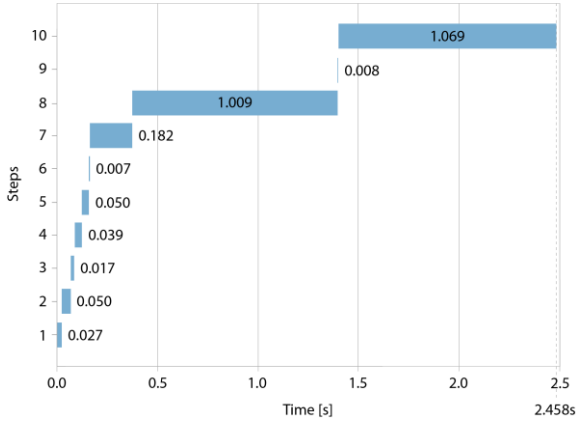
The lengthiest action is the OEM agent boot (6) (Fig. 25), followed by the implicit connection between the OEM and the Consortium (11), which is 94% slower than the OOB connection from Dave with the Consortium (9). This difference results from the fact that the invitee must retrieve the DIDDoc from the ledger. The other lengthy transaction is the creation of the OEM public DID (7), which also involves ledger access. These results also demonstrate that the DIDComm transactions are relatively efficient under minimal load and do not introduce a toll from a usability standpoint.




```
1.  Dave->marketingWebsite.EnrollOEM()
2.  marketingWebsite->1@C.RequestOOB_URI()
3.  1@C.TransactionStart(createUUID())
4.  1@C.createOOB(c2dt.consortium.enroll.OEM)
    ->marketingWebsite
5.  marketingWebsite.Display(OOBInstruc-
    tions,OOB_URI)
6.  OEM.AgentBoot()
7.  If 1@O.isFirstBoot() then 1@O.CreatePub-
    licDID()
8.  Dave->marketingWebsite.Get(OOB_URI)
9.  1@D.AgentConnectAgent(OOB_URI,goal)->1@C
10. If 1@C.goal("enroll") AND 1@C.Transac-
    tionGet(UUID) then 1@C.CreateConsorti-
    umAgent()
11. 1@D.AgentConnectAgent(OOB_URI) ->1@O
```

Fig. 25. Dave Connects with consortium (Original Equipment Manufacturer (OEM) Enrollment Phase 1) test results.

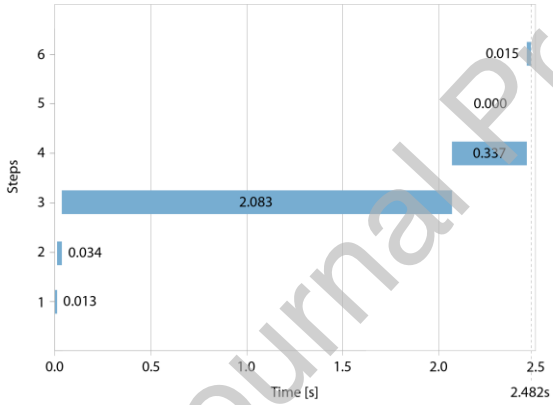
In phase 2 of OEM enrollment (Fig. 26), three operations are significantly slower: the OEM's Fabric network onboarding (8), which requires ledger access; (10) the creation and signing of the VC, which requires the digital signature; and (7) the generation of the OEM Fabric X.509 certificate (7), which also involves cryptographic operations.




```
1. 1@D.Introduction(OOB_URI,goal)->1@O
2. 1@O.AgentConnect(OOB_URI,goal)->1@C
3. If 1@C.goal(ENROLL) AND 1@C.GetTransac-
   tion(UUID) then UpdateAgent(OEM_DID)
4. 1@C.CredentialPropose(ENROLLMENT)->1@O
5. 1@O.SubmitDocProof()->1@C.
6. If 1@C.isValidProofs() then 1@C.Mes-
   sage("Generate_Credentials")->1@O
7. 1@O->1@C.GenerateX.509()
8. 1@O.EcosystemLedgerEnroll()
9. 1@O.Message("CA_ACK")->1@O
10.1@C.CredentialIssue(ENROLLMENT)->1@O
```

Fig. 26. Original Equipment Manufacturer (OEM) connection with consortium (OEM enrollment Phase 2) test results.

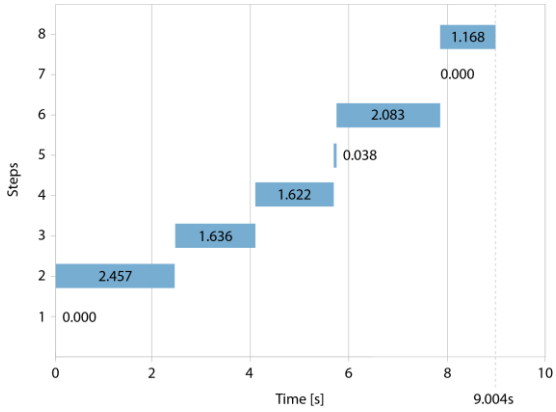
In the "device model" registration use case (Fig. 27), the longest operation involves posting the smartwatch device model metadata into the ecosystem ledger (3), which requires ledger access. This is in line with previous tests.




```
1. 1@D.ActionMenuGet()->1@C
2. 1@D.DeviceModelRegister(Name,Descrip-
   tion,[Feature_info],[Images],WoT_file)->1@C
3. 1@C.EcosystemLedgerStore(Device_metadata)
4. 1@C.SourceControlStore(WoT)
5. 1@C.MarketAppStore(Metadata,[fea-
   ture_info],[images])
6. 1@C.Message(deviceModelID ,DeviceName)->1@O
```

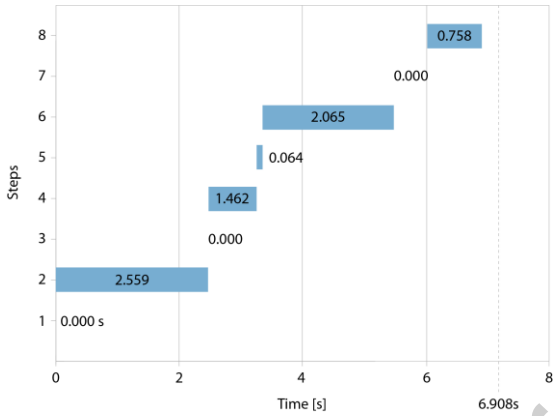
Fig. 27. "Device Model" registration.

The EGW and smartwatch self-registration use case tests are highlighted in Fig. 28 and Fig. 29, which show the slow booting time of the ACA-py agents. This metric gains particular significance when the agents operate on constrained computational devices. The test results show that the time required to establish implicit connections between agents aligns with previously recorded data in step 11 of scenario 1 (Fig. 25). However, the process of creating device Verifiable Credentials demonstrated an unexplained variation between the EGW step 8 and the SD step 8. This discrepancy warrants further study to understand the underlying reasons.



1. (OEM integrates the EGW with the required consortium's firmware libraries)
2. 1@egw.Boot()
3. If 1@egw.FirstBoot() then 1@egw.CreatePublicDID()
4. 1@egw.AgentConnect(PublicDID, *c2dt.consortium.registerdevice DID)*->1@O
5. 1@O.CredentialProposal(GENESIS)->1@egw
6. 1@O.EcosystemLedgerStore(EGW_metadata)
7. 1@O.MarketStore()
8. 1@O.CredentialIssue(GENESIS)->1@egw

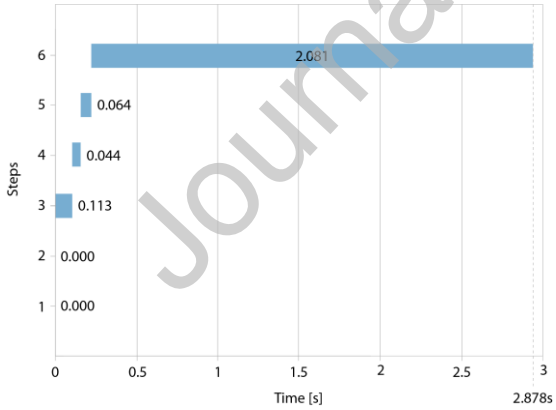
Fig. 28. Edge Gateway (EGW) self-registration.



1. (The OEM integrates the SD with the required consortium firmware libraries)
2. 1@sd.Boot()
3. If 1@sd.FirstBoot() then 1@sd.GenerateUUID()
4. 1@egw.AgentConnect(PublicDID,c2dt.consortium.registerdevice UUID)->1@O
5. 1@O.CredentialProposal("Genesis")->1@sd
6. 1@O.EcosystemLedgerStore(SD_metadata)
7. 1@O.MarketplaceStore()
8. 1@O.CredentialIssue(GENESIS)->1@sd

Fig. 29. Smart Device (SD) self-registration.

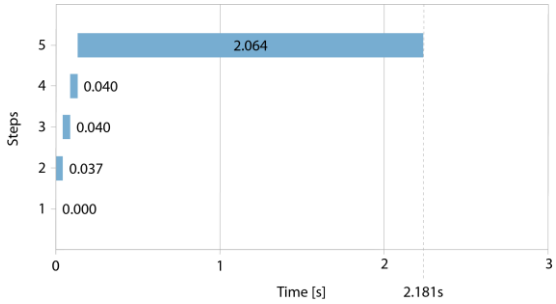
Once more, the penalty involved in updating the SD's status in the ecosystem ledger is confirmed, as shown by the length of step 6 (Fig. 30).



1. Alice.MarketplaceSearch()
2. Alice.MarketplaceBuy()
3. 1@A.AgentConnect(OOB_URI, goal)->1@C
4. 1@O.CredentialProposal(OWNERSHIP,price)->1@A
5. 1@A.Bank.Pay() – out of scope
6. 1@O.EcosystemLedgerUpdate(IN-TRANSIT)

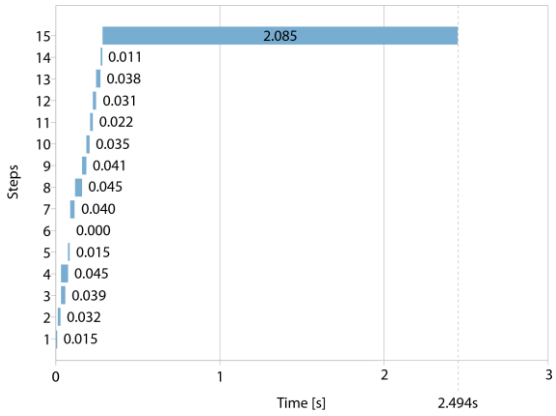
Fig. 30. Consumer buys a smart device.

Once again, the device claiming scenario (Fig. 31 and Fig. 32) confirms the results above, in which the slowest transactions are the ecosystem ledger SD status update, as these involve ledger access and data registry.




```
1. Alice.Scans(EGW_OOB_QR)
2. 1@A.AgentConnect(EGW_OOB_URI, c2dt.con-
   sortium.claim)->1@egw
3. 1@egw.CredentialRequest("OWNERSHIP")->1@A
4. 1@A.CredentialPresentation(OWNERSHIP)
5. If 1@egw.Vali-
   datesProof(EGW_Ownership,EGW_Genesis)
   then 1@O.EcosystemLedg-
   erUpdate(CLAIMED,A.did@A:egw)
```

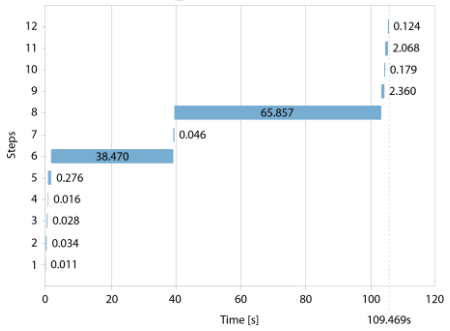
Fig. 31. Edge Gateway (EGW) claiming.




```
1. 1@B.ActionMenuGet()->1@egw
2. 1@B.SDClaim()
3. 1@egw.CredentialRequest(OWNERSHIP)
4. 1@B.CredentialPresentation(OWNERSHIP)
5. 1@egw.TransactionStart(DeviceID)
6. (Bob scans the SD QR code along with the
   c2dt.consortium.claim goal)
7. 1@B.Connect(SD_OOB_URI, goal)->1@sd
8. If 1@sd.isClaimGoalCode() then 1@sd.Re-
   quest(EGW_standing_invitation)
9. 1@B.Submits(EGW_standing_invitation)
10. 1@sd.AgentConnect(EGW_OOB_URI,goal)-
    >1@egw
11. 1@egw.CredentialRequest(GENESIS)
12. 1@sd.CredentialPresentation(GENESIS)
13. 1@egw.Message(APPROVE_ONBOARDING)->1@A
14. If 1@egw.Vali-
    datesProof(SD_Ownership,SD_Genesis) AND
    1@egw.isApproved() then 1@egw.De-
    viceAdd(B.did@egw.did, device ID)
15. 1@egw.EcosystemLedg-
    erUpdate(CLAIMED,EGW_DID)
```

Fig. 32. Smart Device (SD) claiming.

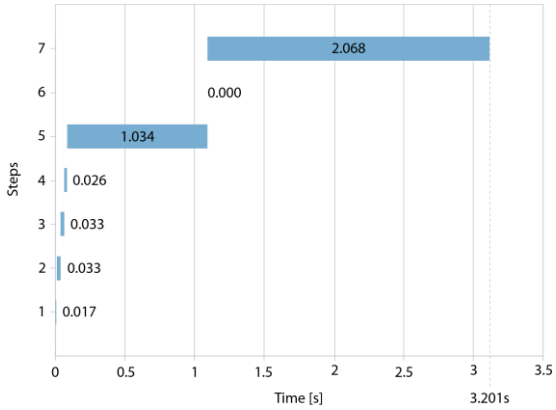
The smartwatch twinning (Fig. 33) test interfaces with the DT platform, which must be booted. As expected, the Eclipse Ditto boot (6) and the configuration of the MQTT client (8) are lengthy operations. However, this only occurs the first time an SD is twinned on an EGW. Creating the dataset's status record on the ecosystem ledger aligns with similar operations, such as step 15 of SD claiming or step 6 of EGW claiming.




```
1. 1@B.ActionMenuGet()->1@egw
2. 1@B.Twin(SD_deviceID, Twin_configura-
   tion)
3. 1@egw.Message(APPROVE_TWINNING)->1@A
4. 1@egw.DeviceUpdate(Twin_configuration)
5. 1@egw. Get(WoT)  - first getting the De-
   viceModelID from the SD table stored
   during the "SD claim" action
6. 1@egw.StartDT(WoT) – assumes the DT
   platform is already running
7. 1@egw.Message(STREAM) ->1@sd.Start-
   Streaming(MQTT_TOPIC)
8. 1@sd.MQTTClientConfigure()
9. 1@egw.EcosystemLedgerUpdate(De-
   viceId,TWINNED)
10. (SD starts sending sensor data via MQTT,
    and on regular intervals 1@egw creates
    datasets)
11. 1@egw.EcosystemLedgerCreate(da-
    taset_metadata)
12. 1@egw.DecentralizedStorageStore(dataset)
```

Fig. 33. Smartwatch twinning.

The untwinning test results (Fig. 34) demonstrate that deleting a twin from Eclipse Ditto is quick, as expected. Ecosystem ledger access is also in line with previous results.



1. 1@B.ActionMenuGet()->1@egw
2. 1@B.Untwin(SD_deviceID, Untwin_configuration)
3. 1@egw.Message("StopStreaming")->1@sd
4. 1@egw.DeviceDelete(SD_deviceID)
5. 1@egw.DigitalTwinDelete()
6. 1@egw.Untwin(untwin_configuration)
7. 1@egw.EcosystemLedgerUpdate(CLAIMED)

Fig. 34. Smartwatch untwinning.

In summary, our tests confirm the feasibility of C2DTA, specifically the consumer's ability to control the DT and its associated data. Furthermore, the tests validate our initial expectations regarding the performance impact of writing on identity and ecosystem ledgers and cryptographic operations. Since the added latency never exceeded two seconds, we find that consumer interactions with SDs are acceptable. Finally, the results indicate that while DIDComm protocols reduce performance, the overall effect remains minimal, especially considering their importance to consumer empowerment.

Finally, adopting architectures that enable consumers to control their SD data relies on developing performance benchmarks that will allow them to choose the best solution. These benchmarks should evaluate several factors, including the following:

- **Consumer-centeredness:**—The level of control that consumers have over their data. For example, C2DTA is designed to maximize consumer control, whereas GAIA-X opts to use "data spaces" controlled by third parties (see Section 2).
- **Resilience:**— The ability of the system to withstand attacks on its infrastructure (e.g., denial of service, eavesdropping, malware) and data (e.g., data tampering, identity fraud, data theft). In the case of C2DTA, data are protected by several measures, such as a dual ledger, self-generating device ID, and reliance on a private blockchain.
- **Sustainability:**— The ability of an ecosystem to maintain its functionalities and support stakeholders over the long term by balancing benefits and costs. In the case of C2DTA, we highlight potential market strategies that could influence sustainability.
- **Scalability:** —The ability of the system to support operations at scale with potentially thousands of users and millions of devices, each with terabytes of information. This is impacted by the performance of hardware, ledger(s), secure communications, digital wallets, cryptographic operations, etc. Architectures such as C2DTA, which further decentralize the PDE by leveraging edge devices, must also assess their scalability, which we plan to address in future work.
- **Ease of use:** The ability of the average user to operate within the ecosystem. In the case of C2DTA, the consumer manages DTs, which are intuitive and open up vast possibilities, as discussed in Section 5.

- **Legal compliance:**— The ability to comply with relevant data protection laws and regulations (e.g., GDPR, CCPA).

Although this benchmark analysis is critically important, it falls outside the scope of the current study because of its extensive and multifaceted nature.

5 Future work

Our research points to several tactical and strategic areas for further exploration.

At a tactical level, testing C2DTA at scale is imperative. Simulating thousands of devices engaging with the ledger through frequent SD status updates, creating and retrieving DIDs and VCs, and optimizing DIDComm protocol performance will provide further insights into the architecture's scalability. Concurrently, it is vital to push the boundaries of edge computing to understand how the architecture handles a deluge of data from many devices and evaluate Federated Learning performance and the efficacy of privacy-preserving methods such as homomorphic encryption. These tests should emulate real-world hardware components, leveraging tools such as the ARM cloud infrastructure[46]. Finally, refining the user interface for digital wallets will be a crucial area of focus, ensuring a seamless and intuitive experience for consumers leveraging emerging initiatives such as the Open Wallet Foundation (OWF)[47].

At the strategic level, C2DTA reveals exciting concepts. For example, the data-only DT (DoDT) is a concept that allows consumers to create twins of third-party-owned SDs, such as medical devices, for the sole purpose of being able to claim their data (Fig. 35). The C2PDT concept [102, 103] aggregates the information from many contributing C2DTA-based DTs to create consumer-controlled PDT. It is possible to envision that consumers use C2PDT to navigate the metaverse [104]. At this point, the C2PDT aggregates digital and analog data on individual consumers. This notion of "Unified Consumer-Controlled Digital Posture" (UC2DP) would allow for the training of AI models without compromising consumer privacy or security, taking the concept of Personal AI to a brand-new level.

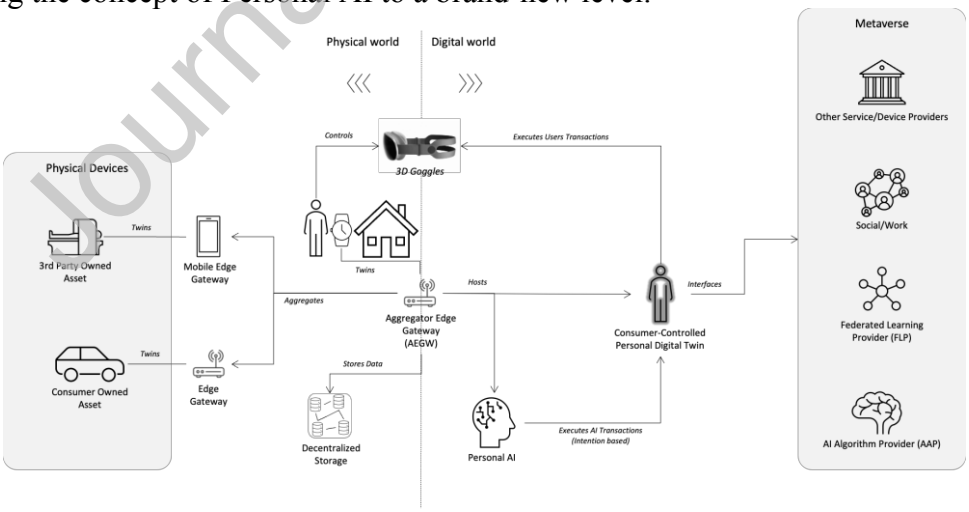


Fig. 35. Unified Consumer-Controlled Digital Posture (UC2DP).

[46] https://www.arm.com/markets/computing-infrastructure

[47] https://openwallet.foundation/

6 Conclusions

C2DTA represents a significant improvement in redefining the dynamics of the PDE. Our findings demonstrate its potential to increase consumers' control over their data. Our dual blockchain approach, combined with SSI technologies and the EGW device, lays a robust foundation for a more advanced PDE.

This new PDE is founded on security, privacy, transparency, and consumer-centeredness. It relies on the collaboration of stakeholders such as OEMs, AI Algorithm Providers, and FLPs organized in consortia, which prioritize the exchange of AI models over raw data. We argue that this model mitigates further privacy risks and aligns with certain trends, including 3D printing and social manufacturing.

These tests demonstrate the feasibility of our model and highlight areas ripe for future exploration.

In the near term, critical research will focus on the scalability of C2DTA, enhancements in the performance of DIDComm protocols, advancements in edge computing for real-time data processing and analytics, and the development of user-friendly digital wallet interfaces. In the long term, we aim to explore the C2PDT concept, its intersection with the multiverse, the emergence of the "Unified Consumer-Controlled Digital Posture" (UC2DP), and the opportunity to give consumers control over both analog and digital data.

Ultimately, our work is not only a technical journey but also a step towards reshaping the use of consumer data, ensuring that consumers are central figures in the data economy of the twenty-first century.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author contributions

Filipe Pinto: Conceptualization, Methodology, Validation, Formal Analysis, Writing – Original Draft, Visualization **Catarina Ferreira da Silva**: Supervision, Writing – Review & Editing, Funding Acquisition **Sergio Moro**: Supervision, Writing – Review & Editing, Funding Acquisition **Pedro Aquino**: Software, Visualization

Funding

This work was supported by the Fundação para a Ciência e Tecnologia (FCT) within projects UIDB/04466/2020 and UIDP/04466/2020 and in part by the project Blockchain.PT – Agenda Decentralize Portugal with Blockchain, (Project No 51), WP 7: Interoperability, call No 02/C05-i01.01/2022, funded by the Portuguese Recovery and Resilience Program (PPR), the Portuguese Republic and the European Union (EU) under the framework of the Next Generation EU Program.

During the preparation of this work, the authors used ChatGPT to improve language and readability. After using this tool/service, they reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

[1] D. Reinsel, How You Contribute to Today's Growing DataSphere and Its Enterprise Impact, https://blogs.idc.com/2019/11/04/how-you-contribute-to-todays-growing-datasphere-and-its-enterprise-impact/. 2019. (Accessed: 01 Jan 2025).

[2] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, et al., Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future, J. Clean. Prod. 274 (2020) 122877, https://doi.org/10.1016/j.jclepro.2020.122877.

[3] R. Soltani, U. Trang Nguyen, A. An, A new approach to client onboarding using self-sovereign identity and distributed ledger, in: Proceedings of the 2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1129–1136, https://doi.org/10.1109/Cybermatics_2018.2018.00205.

[4] A. Kumari, A. Golyan, R. Shah, et al., Introduction to data analytics, in: Recent Trends and Future Direction for Data Analytics, IGI Global Scientific Publishing, New York, 2024, pp. 1–14. https://doi.org/10.4018/979-8-3693-3609-0.ch001

[5] M. Paiola, H. Gebauer, Internet of Things technologies, digital servitization and business model innovation in BtoB manufacturing firms, Ind. Mark. Manag. 89 (2020) 245–264, https://doi.org/10.1016/j.indmarman.2020.03.009.

[6] J. Rose, D. Dean, and C. Kalapesi, Unlocking the Value of Personal Data: From Collection to Usage, https://www.weforum.org/publications/unlocking-value-personal-data-collection-usage/. 2013. (Accessed: 14 Jun 2025).

[7] J. Koskinen, S. Knaapi-Junnila, M.M. Rantanen, What if we had fair, people-centred data economy ecosystems? in: Proceedings of the 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), IEEE, 2019, pp. 329–334., https://doi.org/10.1109/smartworld-uic-atc-scalcom-iop-sci.2019.00100.

[8] K.C. Laudon, Markets and privacy, Commun. ACM, 39 (9) (1996)92–104. https://doi.org/10.1145/234215.234476.

[9] F. Pinto, C. Ferreira da Silva, S. Moro, People-centered distributed ledger technology-IoT architectures: a systematic literature review, Telematics Inform. 70 (2022) 101812, https://doi.org/10.1016/j.tele.2022.101812.

[10] L. C. Tom Lyons, Convergence of Blockchain, IoT and AI, https://blockchain-observatory.ec.europa.eu/publications/convergence-blockchain-ai-and-iot_en. 2020. (Accessed: 14 Jun 2025).

[11] H. Treiblmaier, C. Sillaber, The impact of blockchain on e-commerce: a framework for salient research topics, Electron. Commer. Res. Appl. 48 (2021) 101054, https://doi.org/10.1016/j.elerap.2021.101054.

[12] L. Stockburger, G. Kokosioulis, A. Mukkamala, et al., Blockchain-enabled

decentralized identity management: the case of self-sovereign identity in public transportation, Blockchain Res. Appl. 2 (2) (2021) 100014. https://doi.org/10.1016/j.bcra.2021.100014.

[13] K.U. Fallatah, M. Barhamgi, C. Perera, Personal data stores (PDS): a review, Sensors 23 (3) (2023) 1477. https://doi.org/10.3390/s23031477.

[14] C. Allen, The Path To Self-Sovereign Identity, https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md. 2016. (Accessed: 04 Jun 2022)

[15] J. Asswad, J. Marx Gómez, Data ownership: a survey, Information, 12 (11) (2021) 465, https://doi.org/10.3390/info12110465.

[16] M. Grieves, Digital twin : manufacturing excellence through virtual factory replication, https://www.researchgate.net/publication/275211047_Digital_Twin_Manufacturing_Excellence_through_Virtual_Factory_Replication. 2015. (Accessed: 14 Jun 2025).

[17] Q. Qi, F. Tao, T. Hu, et al., Enabling technologies and tools for digital twin, J. Manuf. Syst. 58 (2021) 3–21, https://doi.org/10.1016/j.jmsy.2019.10.001.

[18] F. Tao, H. Zhang, A. Liu, et al., Digital twin in industry: state-of-the-art, IEEE Trans. Ind. Inform. 15 (4) (2018) 2405–2415. https://doi.org/10.1109/TII.2018.2873186.

[19] Research and Markets, Digital twin market—growth, trends, COVID-19 impact, and forecasts (2023-2028), https://www.researchandmarkets.com/reports/4787530/digital-twin-market-growth-trends-covid-19, 2023. (Accessed: 07 Jul 2023).

[20] Fortune Business Insights, Digital twin market size, trends, growth & forecast [2030], https://www.fortunebusinessinsights.com/digital-twin-market-106246. 2023. (Accessed: 07 Jul 2023).

[21] Transforma Insights, Global IoT market to grow to 24.1 billion devices in 2030, generating $1.5 trillion annual revenue, https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030. 2020. (Accessed: 07 Jul 2023).

[22] H. Ishii, B. Ullmer, Tangible bits: towards seamless interfaces between people, bits and atoms, in: Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems, ACM, 1997, pp. 234–241, https://doi.org/10.1145/258549.258715.

[23] R. Herrero, Fundamentals of IoT Communication Technologies. Springer, Cham, 2022, https://doi.org/10.1007/978-3-030-70080-5.

[24] S. Aheleroff, R.Y. Zhong, X. Xu, A digital twin reference for mass personalization in industry 4.0, Procedia CIRP 93 (2020) 228–233, https://doi.org/10.1016/j.procir.2020.04.023.

[25] C. Altun, B. Tavli, H. Yanikomeroglu, Liberalization of digital twins of IoT-enabled home appliances via blockchains and absolute ownership rights, IEEE Commun. Mag. 57 (12) (2019)65–71, https://doi.org/10.1109/mcom.001.1900072.

[26] N. Purtova, The illusion of personal data as no one's property, Law Innov. Technol. 7 (1) (2015) 83–111, https://doi.org/10.1080/17579961.2015.1052646.

[27] O. Corchia, E. Simperl, Common European Data Spaces, https://data.europa.eu/sites/default/files/report/EN_data_europa_eu_and_the_European_common_data_spaces_0.pdf, 2022. (Accessed: 13 Jul 2025).

[28] J. Mineraud, O. Mazhelis, X. Su, et al., A gap analysis of Internet-of-Things platforms, Comput. Commun. 89 (2016) 5–16, https://doi.org/10.1016/j.comcom.2016.03.015.

[29] S.H. Alsamhi, R. Myrzashova, A. Hawbani, et al., Federated learning meets blockchain in decentralized data sharing: healthcare use case, IEEE Internet Things J. 11 (11) (2024) 19602–19615. https://doi.org/10.1109/JIOT.2024.3367249.

[30] A. Khan, F. Shahid, C. Maple, et al., Toward smart manufacturing using spiral digital twin framework and twinchain, IEEE Trans. Ind. Inform. 18 (2) (2022) 1359–1366. https://doi.org/10.1109/TII.2020.3047840.

[31] Investing.com, Tesla's SWOT analysis: AI ambitions drive stock amid competition, regulatory hurdles, https://www.investing.com/news/swot-analysis/teslas-swot-analysis-ai-ambitions-drive-stock-amid-competition-regulatory-hurdles-93CH-3794752. 2025. (Accessed: 03 Jan 2025).

[32] E. Fox, "Tesla Full Self-Driving FSD Profitability Remains Underestimated By Analysts & it Will Bring Billions to TSLA in 2021, https://www.tesmanian.com/blogs/tesmanian-blog/fsd-will-bring-billions-to-tesla-in-2021. 2020 (Accessed: 24 Nov 2021).

[33] B. Schleich, N. Anwer, L. Mathieu, et al., Shaping the digital twin for design and production engineering, CIRP Ann. 66 (1) (2017) 141–144, https://doi.org/10.1016/j.cirp.2017.04.040.

[34] H. Sahu, N. K. Joshi, S. V. Chande, Design of secure IoMT networks using a federated learning approach, in: V. Goar, M. Kuri, R. Kumar, et al. (Eds.), Advances in Information Communication Technology and Computing, Springer, Singapore. 2024. pp. 681–695. https://doi.org/10.1007/978-981-97-6106-7_41

[35] F. Piccialli, D. Chiaro, P. Qi, et al., Federated and edge learning for large language models, Inf. Fusion 117 (2025) 102840, https://doi.org/10.1016/j.inffus.2024.102840.

[36] Y. Tang, Y. Liang, Y. Liu, et al., Reliable federated learning based on dual-reputation reverse auction mechanism in Internet of Things, Future Gener. Comput. Syst. 156 (2024) 269–284, https://doi.org/10.1016/j.future.2024.03.019.

[37] Z. Lu, H. Pan, Y. Dai, et al., Federated learning with non-IID data: a survey, IEEE Internet Things J. 11 (11) (2024) 19188–19209. https://doi.org/10.1109/JIOT.2024.3376548.

[38] P. Hummel, M. Braun, P. Dabrock, Own data? Ethical reflections on data ownership, Philos. Technol. 34 (3) (2021) 545–572, https://doi.org/10.1007/s13347-020-00404-9.

[39] T.H. Ko, H.M. Lee, D.H. Noh, et al., Design and implementation of a digital twin platform in vertical farming systems, in: Proceedings of the 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, 2022, pp. 366–368, https://doi.org/10.1109/ICUFN55119.2022.9829694.

[40] Y. Liu, E. Al-Masri, Slow Subscribers: a novel IoT-MQTT based denial of service attack, Clust. Comput. 26 (6) (2023) 3973–3984, https://doi.org/10.1007/s10586-022-03788-9.

[41] M.S. Ferdous, A. Ionita, W. Prinz, SSI4Web: a self-sovereign identity (SSI) framework for the web, in: J. Prieto, F.L. Benítez Martínez, S. Ferretti, et al. (Eds.), Blockchain and Applications, 4th International Congress. Springer, Cham. 2023, pp. 366-379. https://doi.org/10.1007/978-3-031-21229-1_34.

[42] A. Siqueira, A.F. Da Conceição, V. Rocha, Performance evaluation of self-sovereign

identity use cases, in: Proceedings of the 2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), IEEE, 2023, pp. 135–144, https://doi.org/10.1109/DAPPS57946.2023.00026.

[43] M. Antwi, A. Adnane, F. Ahmad, et al., The case of HyperLedger Fabric as a blockchain solution for healthcare applications, Blockchain Res. Appl. 2 (1) (2021) 100012, https://doi.org/10.1016/j.bcra.2021.100012.

[44] M. Alizadeh, K. Andersson, O. Schelén, DHT- and blockchain-based smart identification for video conferencing, Blockchain Res. Appl. 3 (2) (2022) 100066, https://doi.org/10.1016/j.bcra.2022.100066.

[45] R. Minerva, G.M. Lee, N. Crespi, Digital twin in the IoT context: a survey on technical features, scenarios, and architectural models, Proc. IEEE 108 (10) (2020) 1785–1824. https://doi.org/10.1109/JPROC.2020.2998530.

[46] K. Cameron, The Laws of Identity, https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf. 2005. (Accessed: 14 Jun 2025).

[47] D. Searls, The Intention Economy: When Customers Take Charge. Harvard Business Review Press, Boston, MA, 2012.

[48] Planet Work, Augmented social network summary, https://www.planetwork.net/asn, 2003. (Accessed: 04 Jun 2022).

[49] H. Vescent , K. Young , K.H. Duffy et al., A Comprehensive Guide To Self Sovereign Identity, The Purple Tornado, Inc., West Hollywood, CA. 2018.

[50] D. Loffreto, What is 'Sovereign Source Authority', https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html 2012. (Accessed: 16 May 2022).

[51] X. Zhu, Y. Badr, Identity management systems for the Internet of Things: a survey towards blockchain solutions, Sensors, 18 (12) (2018) 4215, https://doi.org/10.3390/s18124215.

[52] P. Dunphy, F.A.P. Petitcolas, A first look at identity management schemes on the blockchain, IEEE Secur. Priv. 16 (4) (2018) 20–29. https://doi.org/10.1109/MSP.2018.3111247

[53] D. Reed, J. Law, D. Hardman, The technical foundations of Sovrin, https://sovrin.org/wp-content/uploads/2018/03/The-Technical-Foundations-of-Sovrin.pdf, 2016. (Accessed: 14 Jun 2025).

[54] A. Preukschat, D. Reed, Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Manning Publications Co., Shelter Island, NY. 2021.

[55] J. Sedlmeir, R. Smethurst, A. Rieger, et al., Digital identities and verifiable credentials, Bus. Inf. Syst. Eng. 63 (5) (2021) 603–613, https://doi.org/10.1007/s12599-021-00722-y.

[56] P.J. Windley, Sovrin: an identity metasystem for self-sovereign identity, Front. Blockchain, 4 (2012) 626726, https://doi.org/10.3389/fbloc.2021.626726.

[57] R. Soltani, U.T. Nguyen, A. An, A survey of self-sovereign identity ecosystem, Secur. Commun. Netw. (2021) 8873429, https://doi.org/10.1155/2021/8873429.

[58] D. Hardman, Aries RFC 0004: Agents, https://github.com/hyperledger/aries-rfcs/tree/main/concepts/0004-agents, 2019. (Accessed: 14 Jun 2025).

[59] D. Hardman, DIDComm v2 Primer, https://docs.google.com/presentation/d/1TBs0ZS6GUTsBGw0Dmogny38_nlpMVYf2_0TgrWBRuDk/edit#slide=id.p, 2022. (Accessed: 11 Jun 2023).

[60] J. Langford, A. Poikola, W. Janssen, et al., Understanding MyData Operators, https://mydata.org/operators/, 2022. (Accessed: 14 Jun 2025).

[61] G. Fedrecheski, J.M. Rabaey, L.C.P. Costa, et al., Self-sovereign identity for IoT environments: a perspective, in: Proceedings of the 2020 Global Internet of Things Summit (GIoTS), IEEE, 2020, pp. 1–6. https://doi.org/10.1109/giots49054.2020.9119664.

[62] D. Moher, A. Liberati, J. Tetzlaff, et al., Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement, Int. J. Surg. 8 (5) (2010) 336–341, https://doi.org/10.1016/j.ijsu.2010.02.007.

[63] L. Cocco, R. Tonelli, Digital transformation in the construction sector: blockchain, BIM and SSI for a more sustainable and transparent system, Future Internet 16 (7) (2024) 232, https://doi.org/10.3390/fi16070232.

[64] M.H. Wen, J. Chun-Wei Lin, Twin3: pluralistic personal digital twins via blockchain, IEEE Access 12 (2024) 178997–179009. https://doi.org/10.1109/ACCESS.2024.3486033.

[65] A. Daniel, S. Sriramulu, N. Partheeban, et al., Digital Twin Technology and Applications. Auerbach Publications, Boca Raton, FL. 2024. https://doi.org/10.1201/9781003469612.

[66] A. M. Thomas, K. V. Lakshmy, R. Ramaguru, et al., A Novel Approach to Build Privacy and Trust in Vehicle Sales Using DID, in: G. Ranganathan, G.A. Papakostas, A. Rocha (Eds.), Inventive Communication and Computational Technologies, Springer, Singapore, 2023, pp. 117–130. https://doi.org/10.1007/978-981-99-5166-6_9

[67] T. Kiss, A. Ullah, G. Terstyanszky, et al., Swarmchestrate: towards a fully decentralised framework for orchestrating applications in the cloud-to-edge continuum, in: Barolli, L. (Eds.), Advanced Information Networking and Applications. Springer, Cham, 2024, pp. 89–100, https://doi.org/10.1007/978-3-031-57931-8_9.

[68] S. Ghirmai, D. Mebrahtom, M. Aloqaily, et al., Self-sovereign identity for trust and interoperability in the metaverse, in: Proceedings of the 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta), IEEE, 2022, pp. 2468–2475, https://doi.org/10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00345.

[69] L. Ante, C. Fischer, E. Strehle, A bibliometric review of research on digital identity: Research streams, influential works and future research paths, J. Manuf. Syst. 62 (2022) 523–538, https://doi.org/10.1016/j.jmsy.2022.01.005.

[70] U. Cali, M.S. Ferdous, E. Karaarslan, et al., SSI meets metaverse for industry 4.0 and beyond, in: Proceedings of the 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), IEEE, 2022, pp. 1–6, https://doi.org/10.1109/iGETblockchain56591.2022.10087134.

[71] J.B. Burgos, M. Pustišek, Tackling trust and scalability of the blockchain-based shared manufacturing concept, in: Proceedings of the 2023 17th International Conference on Telecommunications (ConTEL), IEEE, 2023, pp. 1–7,

https://doi.org/10.1109/ConTEL58387.2023.10199103.

[72] S. Auer, Semantic integration and interoperability, in: B. Otto, M. ten Hompel, S. Wrobel (Eds.), Designing Data Spaces. Springer, Cham. 2022. pp. 195–210, https://doi.org/10.1007/978-3-030-93975-5_12.

[73] B. Otto, S. Steinbuß, A. Teuscher, et al., IDS Reference Architecture Model 3.0, https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/IDS-Reference-Architecture-Model.pdf, 2019. (Accessed: 14 Jun 2025).

[74] D. Beverungen, T. Hess, A. Köster, et al., From private digital platforms to public data spaces: implications for the digital transformation, Electron. Mark. 32 (2) (2022) 493–501, https://doi.org/10.1007/s12525-022-00553-z.

[75] L. Taylor, H. Mukiri-Smith, T. Petročnik, et al., (Re)making data markets: an exploration of the regulatory challenges, Law Innov. Technol. 14 (2) (2022) 355–394, https://doi.org/10.1080/17579961.2022.2113671.

[76] J. Baloup, E. Bayamlıoğlu, A. Benmayor, et al., White paper on the data governance act, SSRN, 2021, preprint. https://doi.org/10.2139/ssrn.3872703.

[77] W. She, Z.H. Gu, X.K. Lyu, et al., Homomorphic consortium blockchain for smart home system sensitive data privacy preserving, IEEE Access 7 (2019) 62058–62070. https://doi.org/10.1109/ACCESS.2019.2916345.

[78] Osborne Clarke LLP, Legal study on Ownership and Access to Data, https://publications.europa.eu/resource/cellar/d0bec895-b603-11e6-9e3c-01aa75ed71a1.0001.01/DOC_1, 2016. (Accessed: 14 Jun 2025).

[79] G. Ishmaev, The ethical limits of blockchain-enabled markets for private IoT data, Philos. Technol. 33 (3) (2020) 411–432, https://doi.org/10.1007/s13347-019-00361-y.

[80] V. Janeček, Ownership of personal data in the Internet of Things, Comput. Law Secur. Rev. 34 (5) (2018) 1039–1052, https://doi.org/10.1016/j.clsr.2018.04.007.

[81] T. Lehtiniemi, Y. Kortesniemi, Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach, Big Data Soc. 4 (2)(2017) 1-11, https://doi.org/10.1177/2053951717721935.

[82] D. J. Solove, Privacy Self-Management and the Consent Dilemma, Harv. Law Rev., 126 (7) (2013) 1880–1903. http://www.jstor.org/stable/23415060.

[83] N. Purtova, Property rights in personal data: Learning from the American discourse, Comput. Law Secur. Rev. 25 (6) (2009) 507–521, https://doi.org/10.1016/j.clsr.2009.09.004.

[84] B. Custers, G. Malgieri, Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data, Comput. Law Secur. Rev. 45 (2022) 105683, https://doi.org/10.1016/j.clsr.2022.105683.

[85] IDC, Artificial Intelligence Will Contribute $19.9 Trillion to the Global Economy through 2030 and Drive 3.5% of Global GDP in 2030, https://www.idc.com/getdoc.jsp containerId=prUS52600524, 2024. (Accessed: 10 Jan 2025).

[86] C. Allenbrand, Smart contract-enabled consortium blockchains for the control of supply chain information distortion, Blockchain Res. Appl. 4 (3) (2023) 100134, https://doi.org/10.1016/j.bcra.2023.100134.

[87] World Economic Forum, Redesigning Trust: Blockchain Deployment Toolkit - Supply Chain Focus, https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment Toolkit.pdf. 2020.

(Accessed: 14 Jun 2025).

[88] T. Lyons, L. Courcelas, K. Timsit, Scalability Interoperability And Sustainability Of Blockchains, https://blockchain-observatory.ec.europa.eu/document/download/58813c3d-95d6-45c1-8ca6-70951e5f5d6d_en filename=report_scalaibility_06_03_2019.pdf. 2019. (Accessed: 14 Jun 2025).

[89] D. Hardman, Aries RFC 0003: Protocols, https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0003-protocols/README.md, 2019. (Accessed: 10 Jan 2024)

[90] D. Hardman, Aries RFC 0046: Mediators and Relays, https://github.com/hyperledger/aries-rfcs/tree/main/concepts/0046-mediators-and-relays, 2018. (Accessed: 14 Jun 2025).

[91] W3C, Web of Things (WoT) Architecture, https://www.w3.org/TR/2020/REC-wot-architecture-20200409/, 2020. (Accessed: 7 Jul 2023).

[92] S. Abburu, A.J. Berre, M. Jacoby, et al., COGNITWIN–hybrid and cognitive digital twins for the process industry, in: Proceedings of the 2020 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), IEEE, 2020, pp. 1–8. https://doi.org/10.1109/ice/itmc49519.2020.9198403.

[93] M. Sabadello, K.D. Hartog, C. Lundkvist, et al., Introduction to DID Auth, https://nbviewer.jupyter.org/github/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/final-documents/did-auth.pdf. 2018. (Accessed: 14 Jun 2025).

[94] N. Sangeeta, S.Y. Nam, Blockchain and interplanetary file system (IPFS)-based data storage system for vehicular networks with keyword search capability, Electronics, 12 (7) (2023)1545, https://doi.org/10.3390/electronics12071545.

[95] M. Li, M. Li, A.R. Harish, et al., Blockchain-based fine-grained digital twin sharing framework for social manufacturing, Adv. Eng. Inform. 58 (2023) 102225, https://doi.org/10.1016/j.aei.2023.102225.

[96] C. Zhang, Z. Wang, G. Zhou, et al., Towards new-generation human-centric smart manufacturing in Industry 5.0: a systematic review, Adv. Eng. Inform. 57 (2023) 102121, https://doi.org/10.1016/j.aei.2023.102121.

[97] Sovrin Foundation, Sovrin Price Plan, https://sovrin.org/sovrin-price-plan/, 2023. (Accessed: 5 Jul 2023).

[98] T. Guggenberger, J. Sedlmeir, G. Fridgen, et al., An in-depth investigation of the performance characteristics of Hyperledger Fabric, Comput. Ind. Eng. 173 (2022) 108716, https://doi.org/10.1016/j.cie.2022.108716.

[99] A.O. Gur, S. Oksuzer, E. Karaarslan, Blockchain based metering and billing system proposal with privacy protection for the electric network, in: Proceedings of the 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), IEEE, 2019, pp. 204–208., https://doi.org/10.1109/sgcf.2019.8782375.

[100] M. Picone, M. Mamei, F. Zambonelli, A flexible and modular architecture for edge digital twin: implementation and evaluation, ACM Trans. Internet Things 4 (1) (2023) 1–32, https://doi.org/10.1145/3573206.

[101] V. Damjanovic-Behrendt, W. Behrendt, An open source approach to the design and implementation of digital twins for smart manufacturing, Int. J. Comput. Integr. Manuf. 32 (4–5) (2019) 366–384, https://doi.org/10.1080/0951192X.2019.1599436.

[102] A. Kopponen, A. Hahto, P. Kettunen, et al., Empowering citizens with digital twins: a

blueprint, IEEE Internet Comput. 26 (5) (2022) 7–16, https://doi.org/10.1109/mic.2022.3159683.

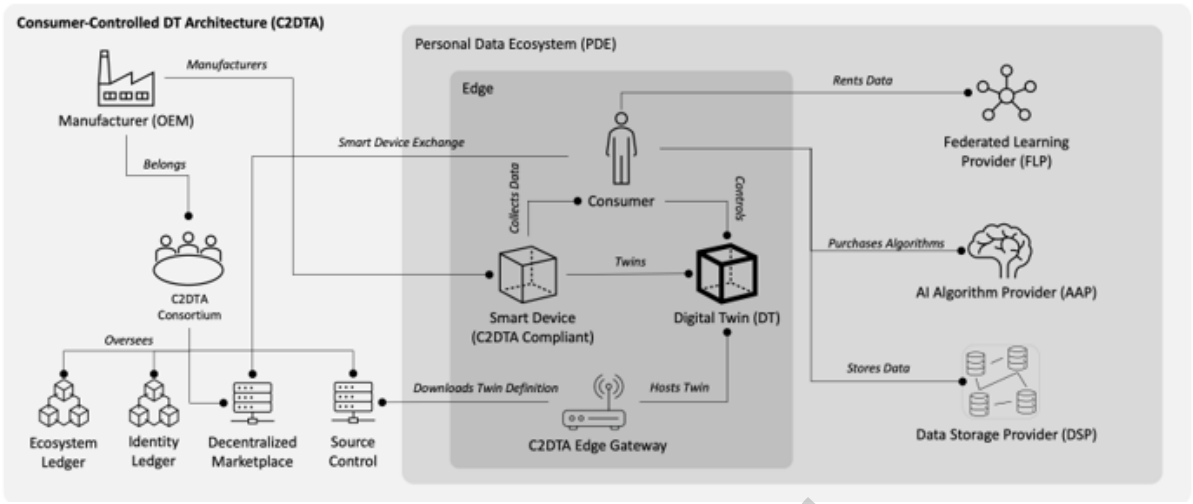
[103] R. Sahal, S.H. Alsamhi, K.N. Brown, Personal digital twin: a close look into the present and a step towards the future of personalised healthcare industry, Sensors, 22 (15) (2022) 5918, https://doi.org/10.3390/s22155918.

[104] T. Huynh-The, T.R. Gadekallu, W. Wang, et al., Blockchain for the metaverse: a review, Future Gener. Comput. Syst. 143(2023) 401–419, https://doi.org/10.1016/j.future.2023.02.008.

Author Contribution Statement

Filipe Pinto: Conceptualization, Methodology, Validation, Formal Analysis, Writing – Original Draft, Visualization **Catarina Ferreira da Silva**: Supervision, Writing – Review & Editing, Funding Acquisition **Sergio Moro**: Supervision, Writing – Review & Editing, Funding Acquisition **Pedro Aquino**: Software, Visualization

Graphical abstract



Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐ The author is an Editorial Board Member/Editor-in-Chief/Associate Editor/Guest Editor for *[Journal name]* and was not involved in the editorial review or the decision to publish this article.

☐ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: