Internet of Products:
Toward a Product Identity Layer of the Digital Economy

A Conceptual Research Paper

Minh Do
Information Technology Institute, Vietnam National University, Hanoi
minhdn@vnu.edu.vn

Keywords: Internet of Products • Product Identity Layer • Digital Infrastructure • 4E Model • Supply Chain Transparency • Tokenization • Real-World Assets • Transaction Cost Theory • Information Asymmetry • Digital Economy

Abstract

In three decades, the internet has undergone successive waves of digitalization that have progressively transformed the global economy. The first wave enabled the digitization of information, creating an environment in which data and content could circulate globally at negligible cost. The second wave extended digital infrastructure to financial assets, enabling monetary value to exist and flow natively through networked systems.

However, a significant portion of the global economy — the physical economy of manufactured goods — remains comparatively under-digitized at the level of individual products. Each year, trillions of dollars of goods move through global supply chains, yet most physical products lose their individual identity once they leave manufacturing environments. This absence creates structural inefficiencies rooted in information asymmetry (Akerlof, 1970) and high transaction costs (Coase, 1937) that pervade global product markets.

This paper proposes the Internet of Products (IoP) as a new digital infrastructure layer in which every physical product possesses a persistent, verifiable, and network-accessible digital identity.

Drawing on transaction cost theory, information asymmetry theory, and digital infrastructure theory, it develops a conceptual framework describing how product identity functions as a new infrastructure layer connecting the physical economy, digital platforms, and financial systems.

The paper introduces the 4E Model of Product Digitization — Encode, Enrich, Exchange, and Execute — with explicit analysis of boundary conditions and failure modes. Six research propositions are refined into testable hypotheses with operationalized constructs. Critical counter-arguments, including the oracle problem, governance failure risks, and privacy-transparency tensions, are examined. An illustrative case analysis across three industries grounds the framework in observable practice.

Theoretical contributions: (1) Positioning IoP as a new digital infrastructure layer analogous to DNS for information; (2) the 4E Model as a staged framework for product digitization with specified boundary conditions; (3) integration of previously fragmented research streams — IoT, supply chain, smart products, DPP, and tokenization — under a unified infrastructure lens. The paper concludes with a structured research agenda targeting empirical validation.

1. Introduction

Over the past three decades, digital technologies have fundamentally reshaped the structure of the global economy through successive expansions of what entities can possess identity within networked systems. The internet initially developed as a communications infrastructure enabling the exchange of information between computers. With the emergence of the World Wide Web in the early 1990s, digital content could be stored, accessed, and shared on a global scale. This phase — widely described as the Internet of Information — established digital identity for informational objects such as documents, web pages, and databases through foundational standards including the Domain Name System (DNS) and Uniform Resource Locators (URLs) (Castells, 2010).

Subsequent technological developments extended digital infrastructure to encompass financial value. Advances in blockchain systems and cryptographic protocols made it possible for financial assets to exist and be exchanged natively within digital networks without relying solely on

traditional intermediaries (Nakamoto, 2008; Tapscott and Tapscott, 2016). This transformation — described as the Internet of Value — established digital identity for financial assets through wallet addresses, token protocols, and distributed ledger systems.

Despite these profound developments, a large segment of the global economy remains comparatively under-digitized: the physical economy of manufactured goods. Each year, trillions of dollars of products move through complex global supply chains. Yet once products leave manufacturing environments, their individual identities often dissolve into fragmented logistics records. This situation creates a structural paradox: highly sophisticated digital infrastructures have been developed to track information and financial assets with extraordinary precision, while the physical goods underpinning economic activity often exist as anonymous objects within those same systems.

This anonymity imposes significant economic costs. Drawing on Akerlof's (1970) theory of information asymmetry, markets for physical goods are characterized by buyers' inability to verify product provenance, authenticity, and condition — precisely the conditions that generate counterfeit markets, unsafe products, and inefficient recycling. Globally, counterfeit goods account for approximately 3.3% of world trade, representing USD 467 billion annually (OECD, 2023). Applying Coase's (1937) transaction cost lens, anonymous products generate high costs of search, verification, and contract enforcement across supply chains — costs that persist because no infrastructure exists to make product histories credibly observable.

This paper proposes the Internet of Products (IoP) as the emerging third stage of Internet infrastructure evolution. In this model, each physical product is assigned a persistent digital identity that allows it to accumulate lifecycle data, interact with digital platforms, and potentially participate in broader economic systems — including financial markets through tokenization of Real World Assets (RWA). The concept is grounded in digital infrastructure theory (Hanseth and Lyytinen, 2010; Tilson et al., 2010), which positions such systems as shared, open, and generative technological platforms capable of evolving beyond any single application.

The paper makes three theoretical contributions. First, it defines the Internet of Products and its Product Identity Layer as a new infrastructure layer of the digital economy, extending the evolutionary logic of DNS (for information) and blockchain addresses (for financial value) to

physical goods. Second, it proposes the 4E Model of Product Digitization — Encode, Enrich, Exchange, and Execute — with explicit boundary conditions and failure mode analysis. Third, it integrates previously fragmented research streams under a unified theoretical lens and proposes testable hypotheses to guide empirical investigation.

2. Literature Review

2.1 The Evolution of Digital Infrastructure

The development of the internet can be understood as a progressive expansion of the range of entities that can possess identity and interact within digital networked environments. Scholars have documented two primary phases of this expansion.

The Internet of Information phase established digital identity for informational objects. Domain names and URLs allowed documents and media to be organized and accessed across global networks. This infrastructure enabled what Shapiro and Varian (1999) describe as the economics of information goods — characterized by near-zero marginal cost of reproduction, strong network effects, and winner-takes-most market dynamics.

The Internet of Value phase established digital identity for financial assets. Nakamoto's (2008) Bitcoin protocol demonstrated that financial value could be transferred directly between parties without intermediaries by solving the double-spending problem through distributed consensus. Tapscott and Tapscott (2016) articulate the broader implications for programmable financial systems. This phase created new economic possibilities for decentralized exchange and smart contract-based commerce (Buterin, 2013).

Digital infrastructure theory provides a powerful lens for understanding these evolutionary phases. Hanseth and Lyytinen (2010) define information infrastructures as shared, open, heterogeneous, and evolving socio-technical systems, characterized by path dependency, network effects, and unbounded scale. Their framework identifies two critical design challenges relevant to emerging infrastructures: the bootstrap problem — new infrastructures must create value for early adopters

before achieving network scale — and the adaptability problem — designs must accommodate unbounded functional evolution beyond initial purposes.

Tilson et al. (2010) extend this perspective by highlighting the concept of generativity: the capacity of a digital infrastructure to enable unanticipated innovations from diverse actors. The Internet's generative architecture — in which core protocols remain neutral while applications proliferate without central permission — explains the explosive innovation it enabled. The question of whether product identity infrastructure can be designed with comparable generativity is central to the IoP's long-term potential.

2.2 Internet of Things and Connected Physical Objects

The Internet of Things (IoT) literature, originating with Ashton's (2009) coinage, describes ecosystems in which physical devices are connected to the internet through sensors and communication technologies. Research has documented IoT applications in manufacturing, logistics, and supply chains (Gubbi et al., 2013; Lee and Lee, 2015), including RFID-based product tracking across global supply networks (Zhou, Piramuthu and Chu, 2020).

However, IoT research primarily focuses on device connectivity and operational data collection rather than the economic identity of products themselves. Physical objects in IoT systems are treated as data-generating nodes within sensor networks — objects being monitored — rather than as economic entities with persistent identities capable of acting within market systems (Xu, He and Li, 2014). This distinction between object (tracked, passive) and entity (identified, active) represents the core conceptual gap that IoP addresses.

2.3 Digital Supply Chains and Traceability

Research on digital supply chain management has examined RFID, blockchain, and cloud-based systems as mechanisms for improving supply chain transparency (Christopher, 2016; Ivanov, Dolgui and Sokolov, 2019). Traceability systems have been studied extensively in pharmaceuticals and food sectors, where safety and authenticity are critical (OECD, 2021). Blockchain has been proposed for tamper-resistant supply chain records (Saberi et al., 2019; Treiblmaier, 2018).

While these systems enhance supply chain visibility, most solutions remain organization-centric. Product data is stored in proprietary databases controlled by individual firms. Products rarely

possess persistent digital identities that exist independently across organizational boundaries (Nguyen et al., 2018). The Walmart Food Trust blockchain, which reduced produce traceability time from seven days to 2.2 seconds (IBM, 2018), illustrates the potential — but also reveals that such systems require a powerful orchestrating actor to mandate participation, highlighting the governance challenges that infrastructure-level solutions must address.

2.4 Smart Products and Product-Service Systems

Porter and Heppelmann (2014, 2015) demonstrate that smart connected products enable new forms of value creation — including predictive maintenance, remote monitoring, and product-service systems — by enabling continuous interaction between manufacturers and products after sale. The emergence of product-service systems (PSS) — in which manufacturers shift from one-time transactions to ongoing service provision — has been extensively documented (Baines et al., 2007; Vandermerwe and Rada, 1988).

The Rolls-Royce Power by the Hour model (1962 onward), in which engine performance is sold as a service, represents the earliest large-scale PSS. Contemporary examples include Signify's Light-as-a-Service for Schiphol Airport and Michelin's tire management services. However, smart product research primarily focuses on product functionality and service innovation rather than the broader infrastructure implications of persistent product identity across multiple digital systems.

2.5 Digital Product Passports and Sustainability Infrastructure

The European Union's Ecodesign for Sustainable Products Regulation (ESPR, EU 2024/1781) mandates Digital Product Passports (DPP) for most physical goods sold in EU markets, with implementation timelines extending from battery passports in 2027 through textiles, electronics, and construction materials to 2030. DPP systems record detailed lifecycle information including materials, environmental footprint, repairability, and recyclability (European Commission, 2022; World Economic Forum, 2023).

DPP systems represent the most significant regulatory instantiation of product identity infrastructure to date. However, as currently designed, they function primarily as compliance instruments — providing specified data fields to regulators and consumers — rather than as generative economic infrastructure. They do not conceptualize products as independent digital

entities capable of interacting with financial systems, nor do they provide open identity protocols enabling third-party innovation on top of product data.

2.6 Tokenization and Real-World Assets

A growing body of research examines the tokenization of real-world assets (RWA) using blockchain technologies. Tokenization converts ownership rights over physical or financial assets into digital tokens on distributed ledgers, enabling programmable ownership transfers, fractional ownership, and integration into decentralized financial systems (Yermack, 2017; Casino, Dasaklis and Patsakis, 2019). The tokenized RWA market has grown from under USD 3 billion in 2022 to over USD 30 billion in 2025 (RWA.xyz, 2025), with major institutions including BlackRock, JPMorgan, and Franklin Templeton launching tokenized products.

A fundamental challenge for tokenization systems is the reliable linkage between digital tokens and underlying physical assets. Without trusted identity mechanisms for physical goods — mechanisms that establish and maintain the connection between physical object and digital representation across the asset's lifecycle — the credibility of tokenized asset systems remains limited. This 'oracle problem' represents a critical weakness at the intersection of IoT and blockchain that the IoP framework must directly address.

2.7 Prior Uses of the Term 'Internet of Products'

The term Internet of Products has appeared in earlier discourse. Sarma, Brock and Ashton (2000) at the MIT Auto-ID Center described a communications network for tracking physical goods in supply chains, primarily through RFID-based inventory visibility. Neumann (2013) developed the concept in The Internet of Products: An Approach to Establishing Total Transparency in Electronic Markets, examining product information accessibility in e-commerce through semantic models. Industry publications such as Qliktag Software (2018) have used the term for digital representations of consumer products accessible through QR codes and product databases.

While these prior uses are valuable contributions, they primarily conceptualize IoP as a product information or logistics tracking system. The present study extends this concept significantly by reframing product identity as a generative economic infrastructure layer — one that enables

physical goods to participate as identifiable entities across digital platforms, supply chains, and financial systems throughout their full lifecycle.

2.8 Theoretical Foundations

Three theoretical traditions provide the foundational grounding for the Internet of Products framework.

Transaction Cost Theory (Coase, 1937; Williamson, 1981). Coase's theory posits that the structure of economic organization — what activities occur within firms versus through markets — is determined by the costs of searching for information, negotiating contracts, and enforcing agreements. Williamson (1981) extends this by identifying asset specificity, uncertainty, and transaction frequency as key determinants of governance form. IoP directly addresses three categories of transaction costs that pervade physical goods markets: search costs (who made this product, from what materials, under what conditions?); verification costs (is this product genuine, compliant, in the claimed condition?); and enforcement costs (can warranty and compliance obligations be automatically executed?). By making product histories credibly observable and verifiable, IoP reduces information asymmetry and lowers transaction costs — potentially enabling market governance to replace organizational governance in contexts where high transaction costs currently force vertical integration.

Information Asymmetry Theory (Akerlof, 1970). Akerlof's 'market for lemons' demonstrates how information asymmetry between buyers and sellers — in which sellers know product quality but buyers do not — can cause market failure. In physical goods markets, buyers cannot observe provenance, manufacturing conditions, or usage history, creating conditions that support counterfeit markets, unsafe products, and under-investment in quality. IoP addresses this by providing verifiable, cryptographically secured product histories — reducing the information gap that enables 'lemons' to displace quality goods. The 4E Model's Execute stage, where smart contracts automate enforcement of product claims, represents the mechanism through which information asymmetry reduction translates into economic value.

Digital Infrastructure Theory (Hanseth and Lyytinen, 2010; Tilson et al., 2010). Information infrastructure theory characterizes shared, open, and evolving socio-technical systems with three properties central to IoP analysis. Generativity (Zittrain, 2006) refers to the capacity to produce

unanticipated innovations — a product identity infrastructure with open standards enables innovation layers that designers cannot predict, as DNS enabled the Web and the Web enabled e-commerce. The bootstrap problem — how to generate sufficient adoption to create network value before scale is achieved — is particularly acute for product identity: identity data for one product has little value; identity data for a billion products creates a transformative infrastructure. The installed base problem highlights that IoP must evolve from existing identification systems (GS1 barcodes, RFID networks) rather than replacing them. These theoretical lenses predict both the transformative potential and the adoption challenges the IoP framework will face.

2.9 Research Gap

Taken together, existing research streams reveal an important conceptual and theoretical gap. IoT research treats products as data sources rather than economic entities. Supply chain research provides logistics visibility but organization-centric data silos. Smart product literature focuses on functional innovation without addressing persistent identity infrastructure. DPP systems create compliance instruments rather than generative economic infrastructure. Tokenization research addresses financial representations without trusted identity linkage to physical goods.

More fundamentally, no existing framework addresses how individual products might function as persistent digital entities — possessing durable, generative identities that allow them to interact across digital platforms, financial infrastructures, and regulatory systems throughout their entire lifecycle. This gap is not merely descriptive but ontological: existing systems treat products as objects (passive, tracked, managed), whereas the Internet of Products proposes reconceptualizing them as entities (active, identifiable, participating). This ontological shift has significant implications for economic organization, market design, and infrastructure governance.

3. Conceptual Framework: The Internet of Products

3.1 From Anonymous Objects to Identifiable Entities: An Ontological Shift

In the traditional industrial economy, physical products exist as anonymous objects once they leave manufacturing facilities. They are identified by category codes — SKUs, barcodes — rather than

individual identities. This means that any two units of the same product model are functionally indistinguishable in digital systems, even if they have different production histories, material compositions, or operational experiences.

The Internet of Products proposes a fundamental ontological shift: from treating products as objects being tracked within systems to treating products as entities possessing independent digital identities within networked economic systems. This distinction, while subtle, has profound economic implications. An entity — unlike an object — can accumulate a history, establish relationships, and participate in transactions as a recognizable party. An entity can carry forward its lifecycle narrative, serve as a credible basis for contractual claims, and interact with financial systems as an identifiable asset.

This ontological reframing parallels transformations already achieved in other domains. DNS transformed internet addresses from network identifiers into economic entities: the domain 'amazon.com' is not merely a routing address but a valuable asset with history, relationships, and market value. Blockchain wallet addresses transformed cryptographic keys into economic entities: an Ethereum address holds assets, executes contracts, and participates in DeFi protocols as an identifiable actor. The Internet of Products proposes an analogous transformation for physical goods.

3.2 Defining the Internet of Products

The Internet of Products is defined as a digital infrastructure layer in which physical goods are assigned persistent digital identities that allow them to exist as identifiable entities within networked systems. Through these identities, products accumulate lifecycle data, interact with digital platforms, and participate in financial systems throughout their lifecycle.

This definition implies three necessary conditions: persistence (product identity continues to exist independently of any single organization's database); verifiability (the claimed identity and associated data can be cryptographically authenticated by any party); and network accessibility (the identity and associated data can be retrieved and used by authorized parties across different systems without proprietary barriers).

The three stages of internet infrastructure evolution can be expressed through this lens:

Internet of Information: persistent, verifiable, network-accessible digital identity for informational objects.

Internet of Value: persistent, verifiable, network-accessible digital identity for financial assets.

Internet of Products: persistent, verifiable, network-accessible digital identity for physical goods.

This progression represents not merely technological advancement but a conceptual expansion of the scope of the digital economy, extending its coordination mechanisms to the physical world.

3.3 The Product Identity Layer

The central theoretical construct of this paper is the Product Identity Layer — a digital infrastructure layer in which physical goods possess persistent, verifiable, and network-accessible digital identities. This layer functions as an intermediary connecting three previously separate economic domains: the Physical Economy (manufacturing, logistics, retail, and product use); the Digital Economy (data platforms, AI systems, and digital marketplaces); and the Financial Economy (tokenized asset markets, inventory financing, and programmable commerce).

The Product Identity Layer can be conceptualized as analogous to the Domain Name System for the Information Layer. DNS created an infrastructure that allowed information to be universally identified and accessed across networks — enabling the Web to develop as an open, generative platform for innovation. A Product Identity Layer could create similar infrastructure for physical goods — enabling product data, product-service systems, and product-backed financial instruments to develop as open, generative applications rather than proprietary systems.

Supporting technologies include GS1 identification standards (already providing a global namespace for product categories), Decentralized Identifiers (DIDs, W3C Recommendation 2022) providing item-level identity, QR codes and NFC tags as physical-digital interfaces, blockchain systems providing tamper-resistant data records, IoT sensors providing continuous data enrichment, and Digital Twins as computational representations of product state.

3.4 Architecture of the Internet of Products

The Internet of Products can be conceptualized as a layered architecture consisting of four interconnected strata, each addressing a distinct infrastructure challenge:

Identity Layer. The foundation of IoP is the assignment of a unique, persistent digital identity to each physical product. This identity serves as the anchor for all associated data and interactions. The critical design requirement is that this identity must be globally unique, cryptographically verifiable, and not dependent on any single organization's continued operation — requirements that DID standards address. The challenge of establishing item-level rather than category-level identity represents the primary departure from existing GS1 barcode infrastructure.

Data Layer. Once a product possesses a persistent identity, it can accumulate structured data throughout its lifecycle. This data layer stores manufacturing information, logistics events, ownership transfers, environmental metrics, maintenance records, and end-of-life data. The critical design challenge is interoperability: data generated by different organizations using different systems must be linkable to the same product identity. EU Digital Product Passport standards represent a regulatory mandate for a minimum viable version of this layer.

Trust Layer. Product identity and lifecycle data require mechanisms to ensure integrity, authenticity, and trust. Distributed ledger technologies, cryptographic signatures, and shared data governance frameworks provide tamper-resistant records. This layer must address the oracle problem directly: the Trust Layer can guarantee that data, once recorded, has not been modified — but it cannot guarantee that data was accurate when first recorded. Trusted hardware (secure enclaves, IoT devices with tamper-proof attestation), third-party auditors, and reputation systems represent practical mechanisms for improving data provenance, though none fully eliminates the oracle problem.

Application Layer. Built on the previous three layers, the Application Layer enables new digital services and economic interactions centered on individual products. Examples include automated product authentication systems, smart warranties and insurance contracts, circular economy marketplaces with verified product histories, tokenized ownership of physical goods, and AI-driven supply chain optimization using product-level data. The generativity of this layer — the extent to which innovators can develop unforeseen applications using the identity infrastructure — is a key measure of IoP's long-term economic potential.

Layer	Primary Function	Key Technology	Critical Design Challenge
Identity	Assign unique, persistent product identity	GS1 standards; W3C DIDs; NFC/RFID	Item-level uniqueness; organizational independence
Data	Accumulate structured lifecycle data	Cloud databases; DPP standards; IoT	Cross-organizational interoperability
Trust	Ensure data integrity and provenance	Blockchain; cryptographic signatures; auditors	Oracle problem; initial data accuracy
Application	Enable new economic interactions	Smart contracts; AI; tokenization platforms	Generativity; open vs. closed architecture

Table 1. Architecture of the Internet of Products with design challenges.

3.5 The 4E Model of Product Digitization

To describe the process through which physical products evolve into programmable economic entities within the Internet of Products, this study proposes the 4E Model of Product Digitization. The model describes four sequential stages, each building on the previous, through which products acquire progressively deeper digital identity.

Stage	Process	Economic Outcome	Enabling Technologies	Minimum Viable Indicator
E1 — Encode	Assign unique persistent digital identity to each physical product	Product becomes individually identifiable in digital systems	QR codes; NFC/RFID; serialized barcodes; W3C DIDs	Unique identifier linkable across >2 organizational systems
E2 — Enrich	Accumulate lifecycle data around the product identity as it moves through its lifecycle	Product gains a traceable digital history and narrative	IoT sensors; ERP/PLM integration; DPP standards; blockchain records	Data spans ≥3 lifecycle stages from ≥2 independent sources
E3 — Exchange	Enable product to participate in digital economic transactions	Product becomes tradeable or financeable digital asset	RWA tokenization; smart contracts; digital marketplaces	At least one financial or commercial transaction

Stage	Process	Economic Outcome	Enabling Technologies	Minimum Viable Indicator
	as a verifiable digital entity			references product identity
E4 — Execute	Automate economic interactions via smart contracts directly linked to specific product identities	Product becomes a node in programmable digital commerce	Smart contracts; IoT triggers; oracle networks; DeFi protocols	At least one economic action (payment, claim, distribution) executes automatically on verified product event

Table 2. The 4E Model of Product Digitization with enabling technologies and minimum viable indicators.

The sequential logic of the 4E Model reflects both technical and economic dependencies: E2 (Enrich) requires a persistent identity anchor from E1 (Encode) to link data across systems; E3 (Exchange) requires sufficient data richness from E2 to support credible valuation; E4 (Execute) requires the exchange mechanisms of E3 to provide the economic context in which automated execution creates value.

3.5.1 Boundary Conditions of the 4E Model

The 4E Model does not apply uniformly to all product categories. Its applicability and the economic value generated at each stage vary systematically with product characteristics.

Product Characteristic	Applicability	Most Relevant Stage	Example
High unit value (> ~$500)	High — identity ROI clearly positive	E1 through E4	Industrial machinery, luxury goods, medical devices
Regulated (pharma, food, EV batteries)	High — regulatory mandate drives adoption	E1 and E2 (compliance); E3 optional	Pharmaceuticals (EU FMD), food (FDA), batteries (EU Battery Regulation)
Durable / long lifecycle (>5 years)	High — lifecycle data creates	E2 through E4 valuable over time	Industrial equipment, vehicles, construction materials

Product Characteristic	Applicability	Most Relevant Stage	Example
	compounding value		
High counterfeit risk	High — authentication value is immediate	E1 and E2 sufficient for authentication	Luxury goods, pharmaceuticals, branded electronics
Low unit value, fast-moving consumer goods	Low — identity ROI positive only at aggregate/category level	E1 only (category tracking) typically viable	Packaged food, commodity goods
Perishable / single-use	Moderate — time-bound value	E2 (cold chain monitoring) highest value	Fresh food, vaccines, single-use medical devices

Table 3. Boundary conditions for the 4E Model by product characteristic.

3.5.2 Failure Modes of the 4E Model

Each stage of the 4E Model is subject to characteristic failure modes that reduce or eliminate the economic value it is designed to create. Recognizing these failure modes is essential for both system design and governance.

E1 Failure — Identity fragmentation: Multiple incompatible identity systems are deployed for the same product category (e.g., manufacturer assigns DID, retailer assigns own system ID, regulatory authority assigns compliance number), preventing cross-system aggregation. This is the primary reason why product identity data currently remains siloed across organizations. Mitigation: open standards adoption (GS1 Digital Link, W3C DID) enforced through regulation or market power of large buyers.

E2 Failure — Data provenance corruption (the oracle problem): Inaccurate or fraudulent data is entered at source and then permanently preserved by blockchain's immutability guarantee. A manufacturer falsely claims sustainable material sourcing; a logistics provider records false temperature compliance. The Trust Layer's cryptographic guarantees apply to data after recording, not to the accuracy of recording itself. This is the fundamental limitation of blockchain-based product data systems and the key reason why blockchain alone cannot solve supply chain fraud. Mitigation: trusted hardware attestation (IoT devices with secure enclaves), mandatory third-party

audits at critical lifecycle junctions, and insurance/liability structures that create economic incentives for accurate recording.

E3 Failure — Token-asset linkage breakdown: The physical asset underlying a tokenized product changes state (is damaged, stolen, or substituted) while the digital token continues to represent the original claimed value. This 'physical-digital divergence' is particularly acute in long-lived assets where physical condition can change significantly over time. Mitigation: continuous IoT monitoring integrated with token smart contracts, periodic physical verification requirements, and insurance products covering divergence risk.

E4 Failure — Oracle manipulation: Smart contract execution is triggered by oracle data that has been manipulated to produce a desired outcome. The Mango Markets exploit of 2022 — in which USD 117 million was stolen by manipulating price oracles — illustrates the severity of this risk. In product contexts, falsified IoT sensor readings could trigger fraudulent insurance payouts, unwarranted warranty claims, or improper supply chain payments. Mitigation: multi-source oracle aggregation, circuit breakers that pause execution on anomalous data, and decentralized oracle networks (e.g., Chainlink) that distribute the attack surface.

3.6 Bridging the Three Economies

The Internet of Products introduces infrastructure that bridges three previously separate economic domains. The digital economy has operated through information and data flows; the financial economy through capital markets and financial instruments; the physical economy through global supply chains and product markets. Most current IoT, supply chain, and smart product systems operate within one domain without full integration into the others.

The Product Identity Layer connects these domains through a progression of integration. When products acquire persistent digital identities (E1: Encode), product data flows into digital analytics systems and enables AI-driven optimization — connecting the physical and digital economies. When identities are enriched with verified lifecycle data (E2: Enrich), goods can serve as credible inputs to financial systems through tokenization and programmable commerce — connecting the physical and financial economies. When smart contracts automate economic interactions on product events (E4: Execute), the three economies operate as an integrated system with information, physical, and financial transactions synchronized in real time.

This integration does not occur automatically or costlessly. As both the TradeLens failure and the Walmart Food Trust success illustrate, the governance architecture — who controls the identity layer, what standards govern data sharing, and who has authority to validate data provenance — determines whether the connecting infrastructure generates broad economic value or merely replicates existing power structures in digital form.

4. Critical Analysis: Counter-Arguments and Limitations

4.1 The Oracle Problem: The Fundamental Limitation of Blockchain-Based Product Systems

The most significant theoretical limitation of the Internet of Products framework is what has been termed the oracle problem in blockchain literature: the impossibility of guaranteeing the accuracy of data at the point of entry into an immutable system. Blockchain technology provides strong guarantees about data integrity — once recorded, data cannot be altered. But it provides no guarantee about data provenance — whether the data was accurate when first recorded (Breidenbach et al., 2021).

In product contexts, the oracle problem manifests as the possibility that a manufacturer records false sustainability certifications, a logistics provider records false temperature compliance, or a repair service records false maintenance history — all of which will then be permanently and credibly preserved on-chain. The more authoritative product identity systems become, the higher the stakes for initial data accuracy, and the greater the incentives for fraud at the point of entry.

This limitation does not invalidate the IoP framework but significantly shapes its design requirements. Product identity systems that rely solely on organizational self-reporting without independent verification mechanisms will replicate existing information asymmetry problems in a more durable form. Credible IoP architectures require trusted hardware with tamper-proof attestation at critical lifecycle junctions, third-party auditors with skin-in-the-game through insurance or liability, and statistical sampling verification combined with reputational mechanisms.

4.2 Governance Failure: The TradeLens Cautionary Tale

The failure of TradeLens — Maersk and IBM's blockchain-based maritime logistics platform, shut down in November 2022 after four years and significant investment — provides the most important real-world test of supply chain identity infrastructure to date. The technical implementation was sound; the failure was economic and political.

Competing container shipping companies refused to participate because they were unwilling to share sensitive operational data with a system controlled by their largest competitor. The governance architecture of TradeLens — controlled by Maersk and IBM, with data flowing through a permissioned blockchain — created justified concerns about competitive advantage asymmetry. Firms that shared their data would provide intelligence to a rival while receiving operational information in return that the rival already possessed.

This failure suggests a critical design principle for product identity infrastructure: systems shared among horizontal competitors require governance neutrality as a precondition for participation. The DNS analogy is instructive — DNS succeeded as a global infrastructure because it was governed by a multi-stakeholder body (ICANN) with no single commercial interest, not by a commercial competitor. The contrast between TradeLens (competitor-controlled, failed) and Walmart Food Trust (buyer-orchestrated with aligned incentives, succeeded) reveals that governance architecture, not technical design, is the primary determinant of multi-actor IoP adoption.

4.3 Privacy-Transparency Tension

The Internet of Products, by making product histories verifiable and potentially public, creates surveillance infrastructure for goods — and, by extension, for the behavior of people who use those goods. Vehicle IoT data reveals location patterns; smart appliance data reveals domestic routines; wearable device data reveals health behaviors. In supply chains, detailed product data may reveal commercially sensitive manufacturing processes, supplier relationships, and cost structures.

These concerns are not merely hypothetical. The EU's Data Act (2023), entering into force in September 2025, explicitly addresses IoT data ownership and access rights, recognizing that product data generated by users belongs, in important senses, to those users rather than exclusively

to manufacturers. GDPR imposes strict requirements on personal data generated by connected products. The design of product identity systems must balance the transparency benefits of rich, shared product data against privacy rights, commercial confidentiality, and the risk that surveillance infrastructure creates new power asymmetries.

Architectural responses to this tension include tiered access systems — with public data (product category, general provenance), restricted data (detailed supply chain events, accessible to verified supply chain participants), and private data (usage patterns, accessible only with explicit consent); selective disclosure using zero-knowledge proofs enabling parties to verify specific claims without revealing underlying data; and privacy-preserving computation allowing analytics on encrypted product data without exposing raw records.

4.4 Scalability and Economic Viability for Low-Value Products

The economic case for IoP is strongest for high-value, regulated, or long-lived products where lifecycle data creates compounding value. For low-value, fast-moving consumer goods — packaged food commodities, basic apparel, common hardware — the per-unit economics of item-level identity assignment and data management may be negative at current technology costs.

This creates a stratified adoption pattern where IoP progresses fastest in sectors where regulatory mandates (EU Battery Regulation, EU ESPR) or business case clarity (pharmaceutical serialization, luxury authentication) overcomes economic barriers. Broad adoption in commodity sectors likely requires either dramatic reduction in identity assignment costs (approaching zero with universal product serialization), regulatory mandate (EU DPP progressively extending to most product categories by 2030), or emergence of platform models in which identity infrastructure costs are distributed across applications generating value.

5. Illustrative Case Analysis

While empirical validation of the full IoP framework awaits future research, three existing deployments illustrate key propositions and reveal conditions for success and failure. These cases are presented as theoretical illustrations, not systematic empirical evidence.

5.1 EU Battery Regulation and Battery Passport (2027): Mandated E1–E2

EU Regulation 2023/1542 mandates Battery Passports for all EV batteries and industrial batteries above 2 kWh sold in EU markets from February 2027. Battery Passports must contain over 100 data attributes including carbon footprint by lifecycle stage, material composition with geographic origin of raw materials, recycled content percentages, and State of Health indicators.

The Battery Passport represents mandated E1 (Encode — each battery receives a unique identifier) and E2 (Enrich — lifecycle data must be recorded and accessible). The regulatory mandate addresses the bootstrap problem by creating a minimum installed base across all EU market participants simultaneously. Pilot programs by Audi, Tesla, and KIA (Global Battery Alliance, 2023) reveal that the primary implementation challenge is cross-tier data collection — aggregating data from mining (lithium from Chile, cobalt from Congo) through cell manufacturing (Korea, China) to pack assembly (Germany) into a coherent product record.

This case illustrates how regulatory infrastructure mandates can accelerate IoP adoption past the bootstrap problem while revealing the E2 Data Layer's critical dependence on multi-tier supply chain cooperation — a governance challenge that technology alone cannot solve.

5.2 Parmigiano Reggiano Microchip Authentication (2022): E1 with Immediate E3 Value

The Parmigiano Reggiano Consortium began embedding edible RFID microchips (1mm diameter, estimated cost < USD 0.01 per unit) in cheese rinds during production. The microchip, scannable throughout the product lifecycle including by end consumers, enables immediate verification of authentic geographic origin, production facility, production date, and conformance with DOP (Protected Designation of Origin) standards.

This case illustrates E1 (Encode) creating immediate E3 (Exchange) value without requiring full E2 data richness: even minimal authenticated identity data — this is genuine Parmigiano Reggiano, from this facility, on this date — is sufficient to command price premiums and prevent counterfeit substitution in retail and distribution. The cheese counterfeit market was estimated to exceed the authentic market in some segments. The microchip cost is recaptured within a small fraction of the price premium associated with verified authenticity.

Importantly, this case also illustrates appropriate boundary conditions: item-level identity creates clear economic value for a high-value, heavily counterfeited product with a protected designation. The model would not translate directly to commodity cheeses where counterfeit risk is low and margins thin.

5.3 Homie Washing Machine-as-a-Service (Netherlands): E1–E4 Integration

Homie, a Dutch startup, deploys washing machines as a service — customers pay approximately EUR 20–30 per month rather than purchasing the machine — with IoT sensors monitoring cycle count, energy consumption, and fault indicators. Homie retains ownership and full responsibility for maintenance and replacement.

This case represents near-complete 4E Model instantiation: E1 (each machine has a persistent identity linked to the service contract); E2 (continuous operational data enrichment enables predictive maintenance and lifecycle management); E3 (the machine is an asset on Homie's balance sheet, potentially financeable against future contracted cash flows); E4 (maintenance scheduling is automatically triggered by IoT data without human intervention). The IoT connectivity transforms the economic structure of the relationship: machines average 15–20 year lifespans in the service model versus 6–8 years in conventional retail, with component reuse rates exceeding 90% (Firmhouse, 2025).

This case illustrates how complete 4E implementation enables servitization business models that would be economically infeasible without continuous product identity and data — and how the economic benefits are distributed between manufacturer (durable design, lower material costs, recurring revenue) and customer (lower upfront cost, no repair risk) in ways that align incentives toward sustainability outcomes.

6. Research Propositions and Testable Hypotheses

Based on the conceptual framework and critical analysis developed above, six research propositions are formulated. Each proposition is accompanied by a testable hypothesis with operationalized constructs to guide empirical investigation.

Proposition 1: Product Identity as Digital Infrastructure

Products with persistent digital identities will function as identifiable entities within digital economic networks, enabling participation in digital systems beyond traditional supply chain management.

H1: Supply chain actors who adopt item-level product identity (operationalized as: unique identifier linkable across ≥3 independent organizational systems) will demonstrate significantly lower inter-organizational transaction costs (measured as: time and cost of product verification, traceability, and dispute resolution) compared to actors using category-level identification only.

Proposition 2: Product Lifecycle Data and Transparency

Products with persistent digital identities will generate continuous lifecycle data that significantly increases supply chain transparency, enabling more effective risk management, compliance monitoring, and circular economy initiatives.

H2: Higher completeness of product lifecycle data records (operationalized as: percentage of lifecycle stages with verified data from independent sources) will be positively associated with: (a) reduction in counterfeit detection time; (b) reduction in product recall scope (number of products recalled relative to actual contaminated units); and (c) material recovery rate at end of life.

Proposition 3: Supply Chain Transformation

IoP adoption will increase supply chain transparency and traceability at the product level, leading to measurable reductions in counterfeiting, improved recall efficiency, and enhanced supply chain coordination.

H3: Firm-level adoption of product-level identity and lifecycle data systems (operationalized as: 4E stage reached, E1 through E4) will predict: (a) reduction in counterfeit claims by product category; (b) reduction in product recall time-to-containment; (c) improvement in on-time-in-full delivery rates. Relationship will be moderated by supply chain complexity (number of tiers and countries).

Proposition 4: Emergence of Product Data Ecosystems

Product identity proliferation will enable digital ecosystems centered on lifecycle data, in which platform-based services, analytics applications, and circular economy markets develop.

H4: Industries with higher product identity infrastructure maturity (operationalized as: percentage of products with E2-level or higher digital identity) will demonstrate higher rates of new service and application development around product data (measured as: number of third-party applications, APIs, and services referencing product identity data per industry). Relationship will be mediated by openness of identity standards (open vs. proprietary).

Proposition 5: Product-Based Financial Systems

IoP will facilitate integration of physical goods into digital financial systems through product-level identity and tokenization, enabling new financial instruments.

H5: Products with E3-level digital identity (operationalized as: product identity referenced in at least one financial transaction) will demonstrate significantly lower cost of capital for inventory financing (measured as: interest rate spread versus unsecured financing) compared to equivalent products without verified digital identity. Relationship will be moderated by asset liquidity in the tokenized market.

Proposition 6: Governance of Product Identity Infrastructure

IoP development will produce competing governance models with significant implications for market competition and data ownership.

H6: The governance architecture of product identity infrastructure (operationalized as: a four-category typology — platform-controlled, industry standards-based, blockchain-decentralized, government-mandated) will significantly predict: (a) adoption rate among competing supply chain actors (highest for standards-based and government-mandated; lowest for platform-controlled by a market participant); (b) data sharing breadth across supply chain tiers; and (c) third-party innovation development on the infrastructure.

7. Discussion: Theoretical Contributions and Implications

7.1 Theoretical Contributions

This study advances theory in three directions. First, by framing the Internet of Products as a digital infrastructure layer — with explicit grounding in Hanseth and Lyytinen's (2010) infrastructure design theory — rather than as an application system, it generates predictions about generativity, bootstrap dynamics, and governance challenges that domain-specific framings (IoT, supply chain management, smart products) do not produce. Infrastructure framings predict that early design decisions about openness and standards will have long-lasting, path-dependent consequences — a prediction absent from existing IoP-adjacent literatures.

Second, by integrating transaction cost theory (Coase, 1937) and information asymmetry theory (Akerlof, 1970) as the primary economic mechanisms through which product identity creates value, the paper provides micro-foundations absent in existing digital supply chain and IoT research. These theoretical lenses specify not just that product identity creates value but through which mechanisms — search cost reduction, verification cost reduction, enforcement cost reduction, and adverse selection mitigation — and therefore predict which product categories and market conditions will generate the highest returns from IoP adoption.

Third, the 4E Model with explicit boundary conditions and failure modes constitutes a theoretical contribution beyond prior descriptive frameworks (including Sarma et al., 2000; Neumann, 2013; and the original version of the current study). The boundary conditions table and failure mode analysis make the framework falsifiable and practically actionable — supporting both empirical research design and managerial decision-making.

7.2 Implications for Research

The research agenda emerging from this paper spans multiple disciplines. Information systems researchers can investigate the generativity mechanisms of product identity infrastructure — which design choices enable or constrain third-party innovation. Operations management researchers can empirically test H1–H3 regarding transaction cost and supply chain performance. Financial economics researchers can examine H5 regarding product identity and cost of capital. Governance scholars can test H6 regarding the competitive implications of alternative governance models for product identity.

Cross-disciplinary collaboration is particularly important for investigating the oracle problem (requiring both cryptography expertise and organizational trust theory) and the privacy-transparency tension (requiring both technical privacy engineering and sociological analysis of surveillance).

7.3 Implications for Practice

For business leaders, the 4E Model provides a staged framework for assessing current position and investment priorities. Organizations in regulated industries (pharmaceuticals, EV batteries, food safety) face imminent compliance mandates that require E1–E2 capability; these mandates create a foundation that can be extended toward E3–E4 value creation. High-value product manufacturers facing significant counterfeit problems have the clearest business case for immediate investment. Industrial equipment manufacturers can assess E2–E4 investment through the lens of service model transformation — the Rolls-Royce, Homie, and Kone case evidence suggests substantial value creation potential.

For policymakers, the governance implications of H6 suggest that public investment in open identity standards infrastructure — analogous to governments supporting internet infrastructure development — may be economically justified given the positive externalities of open product identity. The EU's ESPR/DPP, if extended with open API standards and multi-stakeholder governance, could become the 'DNS for products' that unlocks broad private innovation.

8. Research Agenda for Future Studies

8.1 Empirical Validation of the 4E Model

The most immediate research priority is empirical validation of the 4E Model's stage structure and boundary conditions. Mixed-methods designs — combining quantitative analysis of IoP adoption data with qualitative case studies of implementation journeys — would test whether stage progression is indeed sequential, identify conditions under which stages are skipped or combined, and quantify the economic value created at each stage transition. Longitudinal designs are particularly valuable given that lifecycle data accumulation value grows over time.

8.2 Oracle Problem and Trust Architecture

Empirical research on data provenance mechanisms in product identity systems is urgently needed. Which combination of trusted hardware, third-party audit, and reputational mechanisms most effectively addresses the oracle problem across different product categories and supply chain configurations? This requires collaboration between information systems, cryptography, and organizational trust researchers, and could leverage natural experiments created by EU DPP implementation.

8.3 Governance Models and Adoption Dynamics

Comparative analysis of competing governance models — drawing on the contrast between TradeLens failure and Walmart Food Trust success — can develop and test H6. Panel data on supply chain IoP adoption across industries and governance configurations would enable causal identification of governance effects on adoption rate, data sharing breadth, and innovation development.

8.4 Financial Integration and Capital Markets

The emergence of tokenized RWA markets provides a natural experiment for testing H5. Research can examine whether product-level identity data (E3-level) reduces cost of capital for inventory financing relative to category-level data, and whether the reduction is moderated by data completeness and audit quality. Event studies around DPP compliance announcements could identify market-level responses to product identity infrastructure improvements.

8.5 Sustainability and Circular Economy Outcomes

H2's proposition that product lifecycle data improves circular economy outcomes requires sector-specific empirical investigation. Studies examining material recovery rates before and after DPP implementation in battery, textile, and electronics sectors would provide direct evidence of the circular economy contribution of product identity infrastructure.

8.6 AI and Agentic Commerce

An emerging research frontier concerns the interaction between product identity infrastructure and AI agents. McKinsey (2025) projects that AI agents may conduct over USD 5 trillion in commerce

by 2030, with agents autonomously searching, comparing, and transacting based on machine-readable product data. Research is needed on how DPP-level product data quality affects AI agent decision quality, and whether product identity infrastructure creates new forms of algorithmic market power for products with superior data.

9. Conclusion

The internet has evolved through successive layers of digital identity infrastructure. It first gave identity to information, creating the foundations of the knowledge economy. It then gave identity to financial value, enabling decentralized digital finance. This paper has argued that the next stage — giving identity to physical products — represents a qualitative transformation in the scope and capability of the digital economy.

The Internet of Products is grounded in three theoretical foundations. Transaction cost theory explains why product identity creates economic value: by reducing search, verification, and enforcement costs that pervade anonymous product markets. Information asymmetry theory explains why markets for physical goods are structurally imperfect without persistent identity: products that cannot be distinguished from counterfeits or low-quality substitutes are priced accordingly, destroying value for quality producers and safe-product consumers alike. Digital infrastructure theory explains both the transformative potential and the adoption challenges of product identity systems: generativity enables unanticipated innovation, while bootstrap problems and governance architecture determine whether network effects take hold.

The 4E Model — Encode, Enrich, Exchange, Execute — provides a staged framework for product digitization with specified boundary conditions (not all products justify all stages) and failure modes (particularly the oracle problem, which blockchain immutability cannot solve). Six research propositions with testable hypotheses provide a structured agenda for empirical validation.

Critical counter-arguments — the oracle problem, governance failure risks as illustrated by TradeLens, privacy-transparency tensions, and economic viability limits for low-value products — do not invalidate the IoP framework but specify the design and governance requirements for

credible implementation. Three illustrative cases demonstrate that these requirements can be met in contexts with appropriate product characteristics, regulatory mandates, and governance architecture.

For most of industrial history, products have been anonymous objects once they leave the factory. The Internet of Products offers the possibility that this condition may change — and that the next great infrastructure layer of the digital economy may be built not from data or digital dollars, but from the persistent, verifiable identities of the things we make.

References

Akerlof, G.A. (1970). 'The Market for Lemons: Quality Uncertainty and the Market Mechanism.' Quarterly Journal of Economics, 84(3), 488–500.

Ashton, K. (2009). 'That Internet of Things Thing.' RFID Journal, 22 June.

Atzori, L., Iera, A. and Morabito, G. (2010). 'The Internet of Things: A survey.' Computer Networks, 54(15), 2787–2805.

Baines, T. et al. (2007). 'State-of-the-art in product-service systems.' Proceedings of the Institution of Mechanical Engineers Part B, 221(10), 1543–1552.

Breidenbach, L. et al. (2021). 'Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks.' Chainlink Labs White Paper.

Buterin, V. (2013). 'Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.' ethereum.org.

Casino, F., Dasaklis, T. and Patsakis, C. (2019). 'A systematic literature review of blockchain-based applications.' Telematics and Informatics, 36, 55–81.

Castells, M. (2010). The Rise of the Network Society. 2nd edn. Oxford: Wiley-Blackwell.

Christopher, M. (2016). Logistics and Supply Chain Management. 5th edn. Harlow: Pearson.

Coase, R.H. (1937). 'The Nature of the Firm.' Economica, 4(16), 386–405.

European Commission (2022). Digital Product Passport under the Circular Economy Action Plan. Brussels: European Commission.

European Commission (2023). Regulation (EU) 2023/1542 (EU Battery Regulation). Official Journal of the European Union.

European Commission (2024). Regulation (EU) 2024/1781 (ESPR — Ecodesign for Sustainable Products Regulation). Official Journal of the European Union.

Firmhouse (2025). 'What is Product-as-a-Service?' firmhouse.com.

Global Battery Alliance (2023). GBA Battery Passport Technical Framework. World Economic Forum / GBA.

Gubbi, J. et al. (2013). 'Internet of Things (IoT): A vision, architectural elements, and future directions.' Future Generation Computer Systems, 29(7), 1645–1660.

Hanseth, O. and Lyytinen, K. (2010). 'Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet.' Journal of Information Technology, 25(1), 1–19.

IBM (2018). IBM Food Trust: Walmart Food Safety Initiative. IBM.com.

Iansiti, M. and Lakhani, K.R. (2017). 'The truth about blockchain.' Harvard Business Review, 95(1), 118–127.

Ivanov, D., Dolgui, A. and Sokolov, B. (2019). 'The impact of digital technology and Industry 4.0 on supply chain resilience.' International Journal of Production Research, 57(3), 829–846.

Lee, I. and Lee, K. (2015). 'The Internet of Things: Applications, investments, and challenges.' Business Horizons, 58(4), 431–440.

McKinsey Global Institute (2025). 'Agentic Commerce: The Next Productivity Frontier.' mckinsey.com.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org.

Neumann, R. (2013). The Internet of Products: An Approach to Establishing Total Transparency in Electronic Markets. Berlin: Springer.

Nguyen, T. et al. (2018). 'Big data analytics in supply chain management.' International Journal of Logistics Management, 29(2), 489–514.

OECD (2021). Global Trade in Fakes: A Worrying Threat. Paris: OECD Publishing.

OECD (2023). 'Trade in Counterfeit and Pirated Goods.' oecd.org.

Porter, M. and Heppelmann, J. (2014). 'How smart, connected products are transforming competition.' Harvard Business Review, 92(11), 64–88.

Porter, M. and Heppelmann, J. (2015). 'How smart, connected products are transforming companies.' Harvard Business Review, 93(10), 96–114.

Qliktag Software Inc. (2018). The Internet of Products. Qliktag.

RWA.xyz (2025). Real World Assets On-Chain Market Data. rwa.xyz.

Saberi, S. et al. (2019). 'Blockchain technology and its relationships to sustainable supply chain management.' International Journal of Production Research, 57(7), 2117–2135.

Sarma, S., Brock, D. and Ashton, K. (2000). The Networked Physical World. MIT Auto-ID Center.

Shapiro, C. and Varian, H. (1999). Information Rules: A Strategic Guide to the Network Economy. Boston: Harvard Business School Press.

Tapscott, D. and Tapscott, A. (2016). Blockchain Revolution. New York: Portfolio/Penguin.

Tilson, D., Lyytinen, K. and Sørensen, C. (2010). 'Digital Infrastructures: The Missing IS Research Agenda.' Information Systems Research, 21(4), 748–759.

Treiblmaier, H. (2018). 'The impact of blockchain on the supply chain.' Supply Chain Management: An International Journal, 23(6), 545–559.

Vandermerwe, S. and Rada, J. (1988). 'Servitization of Business.' European Management Journal, 6(4), 314–324.

W3C (2022). Decentralized Identifiers (DIDs) v1.0 — W3C Recommendation. w3.org.

Williamson, O.E. (1981). 'The Economics of Organization: The Transaction Cost Approach.' American Journal of Sociology, 87(3), 548–577.

World Economic Forum (2023). Digital Product Passport: Unlocking the Circular Economy. Geneva: WEF.

Xu, L., He, W. and Li, S. (2014). 'Internet of Things in industries: A survey.' IEEE Transactions on Industrial Informatics, 10(4), 2233–2243.

Yermack, D. (2017). 'Corporate governance and blockchains.' Review of Finance, 21(1), 7–31.

Zhou, W., Piramuthu, S. and Chu, F. (2020). 'RFID-enabled traceability in supply chains.' International Journal of Production Economics, 220, 107463.

Zittrain, J. (2006). 'The Generative Internet.' Harvard Law Review, 119, 1974–2040.