

SYNCHRONIC: Unlocking a Multidimensional Framework for Transforming & Accelerating Digital Commerce Platforms to Web 3.0 Era

Mr. Pranesh P. Naik¹, Dr. G. T. Thampi²

¹Department of Information Technology, Thadomal Shahani College of Engineering (TSEC), Mumbai, India

²Department of Information Technology, Thadomal Shahani College of Engineering (TSEC), Mumbai, India

Abstract : Digital commerce has more than USD 7.5 trillion transactions each year, but the current architectures of the Web 2.0 are structurally centralised, fee-driven, monopolistic on data, and exclusionary. Average transaction fee of around 2.7% limits merchant margins. Platform-controlled data ecosystems limit user sovereignty. Security breaches exceeded USD 2 billion in 2024. An estimated 1.3 billion unbanked individuals remain excluded from digital trade. Although Web 3.0 technologies - blockchain consensus, smart contracts and decentralised identifiers are trust minimised and user centric, enterprise adoption of these technologies is limited due to lack of integrated system level migration frameworks.

This paper introduces SYNCHRONIC (Synchronizing Next-generation Commerce via Hybrid, Resilient, Open, Non-centralized Interoperable Components), which is a seven-layer modular architecture that has been designed to support phased migration from centralized to decentralized commerce systems. The framework integrates protocol, identity, transaction logic, storage, interoperability, governance, and compliance layers of the UX into a unified stack which may be deployed step by step without disrupting operations.

Validation amalgamation of benchmarking of twenty Web 3.0 protocols and comparative case studies of peer-to-peer retail (OpenBazaar), tokenized logistics (Boson Protocol) and NFT marketplaces (OpenSea). The case study shows that on the platforms evaluated; transaction efficiency, user involvement and energy performance have improved significantly. More precisely, Boson Protocol was able to reduce transaction fees for merchants by around 81% compared to Web 2.0, based on the platform-specific fee structures that have been reported, and Polygon integration resulted in around 99.95% gas cost savings for eligible transactions. These results should be interpreted in the context of platform-specific conditions. SYNCHRONIC is the bridge between the theory of Web 3.0 and enterprise implementation of the architecturally grounded empirical blueprint for scalable, interoperable, compliant and inclusive digital commerce systems.

Keywords: Web 3.0 architecture, Digital commerce migration, Blockchain integration, Decentralized systems, Smart contracts, Modular framework design.

I. INTRODUCTION

1.A The Digital Commerce Transformation

Electronic commerce has transformed economies throughout the world and is expected to handle transactions worth over \$7.5 trillion annually by 2026 [1], [4]. Platforms like Amazon, Shopify [3], Alibaba, and others have been able to scale in a short time with the addition of payments, personalized recommendation systems, and logistics infrastructure in centralized Web 2.0 stacks. However, this model is based on centralised servers, isolated data

systems and transaction brokers. As digital commerce reaches new and underserved markets, these architectural dependencies become, in many ways, structural barriers and not sensible trade-offs. Centralization limits inclusion, flexibility and long-term resiliency.

1.B The Efficiency Paradox of Web 2.0

Modern digital commerce systems have three systemic deficiencies caused by centralization. First, transaction costs do not show any structural downward trend. Payment processors charge at standard rates of around 2.7% [2], passing these on to merchants which operate in a multi-trillion-dollar global e-commerce environment [1]. This helps set a minimum transaction cost that makes micropayment models unviable and leads to lower profit margins for merchants. Second, centralization of data leads to reduction of user autonomy. Dominant platforms conduct structured behavioural data collection, and work with surveillance-based monetization models where the value is generated by the users with no meaningful control over their own data [5]. Third, centralized systems are still subject to security attacks. Breach related losses totalled over 2 billion in 2024 [6] and privacy concerns were identified by 60% of consumers as a major deterrent to online purchasing [7]. Such inefficiencies are structural. They together keep an estimated 1.3 billion unbanked people out of the digital trade [8].

1.C Web 3.0: Potential and Hurdles to Adoption

Web 3.0 technologies are a fundamentally different architecture of the web, which is built on decentralization, user control, and algorithmic trust. Blockchain networks allow a decentralized system of consensus that removes a single point of failure. Smart contracts have the potential to bring transaction costs down from the currently common 2.7% to below 0.5% [9]. Decentralized identifiers (DIDs) are a means of enabling self-sovereign identity and selectivity of data disclosure [10]. Despite all these advantages, the adoption in enterprises is scant. Scalability is subject to congestion. There is no standardization in interoperability. Regulatory uncertainty prevails. User experience friction is still high, and research shows that there are significant onboarding abandonment rates and that consumers are not yet ready for wallet-based interactions [11]. The disconnect between what is technically possible and what is being implemented in enterprise is an architectural rather than a conceptual disconnect.

1.D The Framework Gap: Theory and Implementation

The limiting factor for digital commerce stakeholders is not whether Web 3.0 can provide greater efficiency, trust, and inclusion - the empirical evidence supports these claims. The constraint is the lack of systematic and empirically validated migration frameworks that can manage technical, regulatory and organizational risk simultaneously. Existing approaches have the following three limitations:

(i) **Monolithic Replacement Models:** There are several blockchain-centric models that suggest replacing the platform at a wholesale level, putting enterprises at great risk of their operations.

(ii) **Technology-Siloed Guidance:** Current guidance tends to focus on specific technologies and there is no bringing together of identity, storage, governance and compliance into a unified system.

(iii) **Minimal Empirical Benchmarking:** Cross protocol performance comparisons in Web 3.0 commerce are still limited [12].

This disconnect creates a migration choke point. Enterprises see the potential of Web 3.0 but lack phased, low-risk transition paths. This results in structural exclusion despite technological readiness.

1.E Research Question and Objectives

This study answers the following question: How can a modular architectural framework overcome the limitations of Web 3.0 commerce in terms of scalability, privacy and inclusivity and yet permit the gradual migration that maintains operational continuity?

Objective 1: Technology survey and taxonomy: by mapping Web 3.0 Protocols such as consensus mechanisms, decentralized identity, interoperability, storage and governance to specific commercial requirements.

Objective 2 - Efficiency Benchmarking: Design performance metrics for the comparison of Web 2.0 and Web 3.0 systems in terms of transaction speed, cost, energy and ease of onboarding and participation in governance.

Objective 3 - Framework Development and Validation: Implement a modular structured layered architecture for disruption free migration and validate the architecture in a retail, tokenized logistics, and digital asset market context.

Objective 4 - Implementation Pathway Specification: Create clear migration plans based on the architectural design including the technical integration, compliance to regulations and risk management, as well as the user experience.

1.F Research Contributions

Contribution 1: SYNCHRONIC Architecture Framework. A seven-layer modular architecture that includes protocol, identity, transaction logic, storage, interoperability, governance and compliance-UX layers. The composition-oriented nature of the design makes it easier to adopt changes in stages, as well as reducing the risks involved in migration, and keep the operations running smoothly.

Contribution 2: Cross-Context Empirical case-based Validation. Examples from OpenBazaar (peer-to-peer shopping), Boson Protocol (digital logistics) and OpenSea (NFT marketplaces) show clear improvements in the way these platforms work. Specifically, Boson Protocol managed to achieve approximately 81% reduction in the fee costs for merchant transactions when compared to Web 2.0 baselines, based on reported platform-specific fee structures [9], Polygon integration obtained approx. 99.95% gas cost savings for eligible transactions [26], and hybrid migration to the Seaport protocol was accomplished without observed service disruption in the documented case [24]. This is in line with Polygon Labs documented approaches to gas free NFT minting on the platform [26]. These findings are platform specific and are discussed as indicative rather than universally generalizable results in Section V.

Contribution 3: Cross-Protocol Performance Benchmarking. A comparative review of publicly available performance data on 20 different Web 3.0 protocols - standardized metrics:

Throughput, cost, energy consumption, participation in governance. This review gives a good guide for selecting protocols for commerce layer operations.

I.G Scope and Boundaries

This study focuses on digital commerce platforms between two or more parties for goods, services and the exchange of digital assets, in three contexts, i.e., peer-to-peer retail, tokenized supply chains and NFT markets. Decentralized finance trading platforms, crypto exchange and blockchain games are excluded.

The framework covers the European Union Markets in Crypto-Assets (MiCA) regulation [13] and permissionless regulatory landscapes, with compliance modules to cater for local jurisdictional requirements. The analysis is reflective of the ecosystem of the Web 3.0 in early 2025. The modularity of the design enables the protocol to change in the future without the need for a full redesign.

I.H Paper Organization

Section II reviews relevant works on Web 2.0 limitations, Web 3.0 opportunities and the migration frame gap. The methodology of the research is presented in Section III. The SYNCHRONIC model is presented in Section IV. Section V presents the Empirical case-based validation in three case studies. The implications are discussed in Section VI. Section VII provides limitations and future work.

II. LITERATURE REVIEW

II.A Overview and Scope

This review is a synthesis of scholarly literature (2020-2025) referring to digital commerce transformation, Web 3.0 technologies, barriers to adoption, and architectural modelling. Existing work is scattered on the dimensions of technical, social, and organizational aspects with very limited penetration at the architectural level, which reveals the need for reusable and modular system-level migration platforms. SYNCHRONIC is a response to five identified failures in architectural modelling, empirical case-based validation and implementation design.

II.B Web 2.0 E-Commerce: Successes and Structural Limitations

II.B.1 The Centralized Commerce Paradigm

The current state of digital commerce relies on centrally controlled infrastructure, algorithms and transaction processing [1]. Centralized design has allowed developments in areas like recommendation systems, integration of logistics, and payment settlement. However, it strengthened structural dependencies that limit autonomy, flexibility and long-term resilience at the same time.

II.B.2 Transaction Cost Burdens

The average cost for centralized payment processing is about 2.7% [2]. These charges fall unduly on SMEs and create a structural cost floor. Foundational

work in blockchain economics shows how the reduction in transaction verification cost is a primary mechanism by which blockchain technology can increase the number of economic transactions that are economically viable, including transactions on the scale of micropayments that are commercially unviable under a centralized system of fees [14].

II.B.3 Data Monopoly and Surveillance Capitalism

Platform specific data control facilitates behavioural prediction models with value extraction outside conventional commerce [5]. This skews the competition dynamic and compromises the autonomy of users. A large amount of privacy research shows that information privacy issues are a regular antecedent to consumer behaviour in a variety of digital contexts [15], making the case for architecture approaches that restore meaningful user data control.

II.B.4 Trust Erosion and Security Vulnerabilities

Concentrated infrastructure has single points of failure with serious security and privacy risks. Privacy concerns have a measurable effect on consumer behaviour and trust for digital marketplaces [7]. These findings highlight the need for trust building architectures.

II.B.5 Financial Exclusion

Conventional banking requirements and centralized verification of identity keep an estimated 1.3 billion unbanked people out of trade in the digital sphere [8]. Incremental efficiencies are not enough, re-architecture on a structural level is needed.

II.C Web 3.0 Technologies: A Decentralized Foundation

II.C.1 Distributed Consensus

Blockchain technology allows agreement between independent parties without the use of a central authority [16], [17]. The combination of proof-of-stake over proof-of-work and Layer 2 scaling solves the previous issues of energy and scalability and helps make Ethereum more commercially viable.

II.C.2 Smart Contracts and Programmable Commerce

Smart Contracts allow the automation of commerce without intermediaries. In digital commerce applications, these systems have the potential of significantly reducing transaction costs and counterparty risk compared to traditional payment systems [9].

II.C.3 Decentralized Identity

Decentralized Identifiers (DIDs) offer cryptographic identity sovereignty and selective data disclosure [10], which builds upon the principles of user sovereignty and addresses the problems of centralized identities.

II.C.4 Decentralized Storage

Content-address based storage systems like IPFS are censorship resistant and integrity preserving data management [18]. The infrastructure supports decentralised product catalogues, supply chain documentation and user generated content.

II.C.5 Cross-Chain Interoperability

Interoperability frameworks are a way to define connections between heterogeneous blockchain ecosystems [19]. Cross-chain bridges have inherent security trade-offs to them, which emphasizes the difficulties of scaling cross-chain commerce.

II.D Governance Mechanisms: DAOs and Decentralized Decision-Making

II.D.1 Decentralized Autonomous Organizations

For self-governance, DAOs employ the use of tokens and smart contracts and have been shown to be applicable to real-world business scenarios [20]. Empirical studies of on-chain governed DAOs have shown that the governance design and incentive structure play a large role in long-term viability - low participation and concentrated voting power have been a common problem [21].

II.D.2 DAO Failure Patterns

Many DAOs fail at early stages due to attacks on governance, paralysis of decision-making or concentration of the voting power. These patterns show that governance systems must be designed for specific contexts and not as generic token-voting mechanisms [27].

II.E Compliance and Regulatory Constraints

II.E.1 Regulatory Fragmentation

Web 3.0 technologies exist in a fragmented regulatory environment. The European Union's Markets in Crypto-Assets (MiCA) regulation [13] has an extensive regulatory framework that is quite different than enforcement-focused approaches in other Jurisdictions, making cross-border compliance for digital commerce platforms difficult.

II.E.2 Compliance Requirements and Technical Limitations

Identity verification requirements, transaction monitoring requirements, and data protection requirements sometimes clash with the principles of decentralized systems. Privacy-preserving tools such as zero-knowledge proofs can help solve these tensions; but they add to the complexity of the implementation.

II.F Adoption Barriers: Technical, Social, and Organizational

II.F.1 Scalability Constraints

Despite Layer 2 improvements, blockchain systems still have problems with high transaction volumes, and the volatility of transaction fees during peak transaction congestion degrades user experience. Research on e-commerce checkout behaviour has repeatedly identified transaction latency and friction as key causes of cart abandonment, and in blockchain systems, network congestion can cause a variable lag in confirmation, of which there are numerous examples, and where transaction latency and friction are both compounded by blockchain's inherent characteristics.

II.F.2 User Experience and Digital Literacy Disparities

Wallet setup and irreversibility of transactions and private key management are cognitively demanding. These challenges are not in line with current web systems usability standards, creating barriers to blockchain onboarding.

II.F.3 Interoperability Limitations

Practical interconnection between heterogeneous blockchains is still limited, and there are still a few blockchains that support standardized communication protocols [19]. This fragmentation diminishes the advantages of the network and does not allow users to have a smooth experience in different platforms.

II.G Migration Frameworks and Models: Capabilities and Limitations

II.G.1 Technology-Specific Approaches

Existing migration frameworks are based more on the configuration of technology or infrastructure than on full platform transformation. Business frameworks offer little insight into how to incorporate identity, governance, compliance and user experience into an integrated system.

II.G.2 Academic Research Gaps

Systematic cross-protocol performance comparisons in Web 3.0 contexts are still relatively rare, even though the choice of protocol is a highly important architectural choice [12]. Most of the existing work focuses on individual blockchain technologies, or limited case studies, rather than integrated commerce platforms, and comparative evidence of performance is undeveloped.

II.G.3 Governance Model Validation

Governance models for commerce platforms have received little research. While the governance of DAO in financial systems is relatively well-documented, commerce-specific requirements (resolution of disputes and marketplace management) are undertested.

II.H Research Positioning and Gap Analysis

The literature identifies five critical gaps as motivation for this research:

Gap 1 - Lack of Modular Migration Frameworks: Current migration methodologies support a one-shot-at-a-time approach to migration rather than a stepwise layered integration approach.

Gap 2 - Limited Cross-Protocol Comparison: Insufficient performance data exists to support evidence-based protocol selection.

Gap 3 - Lack of Real-World Testing in Different Settings: Previous studies rarely have tested methods in different commerce use cases.

Gap 4: Neglect of socio-technical challenges : Most migration plans do not include considerations of user experience, digital literacy and organizational change.

Gap 5 - Poor Governance Model Guidance: Commerce-specific management systems are not grounded in empirical data.

SYNCHRONIC addresses Gaps 1, 4 and 5 by a modular architecture; Gap 2 by means of cross-protocol benchmarking; and Gap 3 through real world case studies.

III. RESEARCH METHODOLOGY

III.A Research Paradigm

This study follows the Design Science Research (DSR) paradigm of Hevner et al. [22] which is focused on the design and experimentation of IT artifacts to solve organizational problems. The main artifact is the SYNCHRONIC framework - a multi-layered system for synchronizing digital commerce platforms with the technologies of Web 3.0.

III.B Research Design

The research is based on a three-stage iterative DSR cycle:

A. Problem Definition and Requirement Elicitation. The literature review (Section II) reveals that there are five major challenges in the area, namely (i) modular migration structures; (ii) cross-protocol benchmarking; (iii) empirical case-based validation; (iv) socio- technical adoption barriers; and (v) governance design. The general requirements are data sovereignty, modular composability, regulatory adaptability, cross-chain interoperability and automated inter-layer coordination.

B. Artifact Development and Design. The framework for SYNCHRONIC has been developed based on: (i) Architectural Pattern Analysis of studying systems such as MakerDAO and OpenBazaar; (ii) Technology Capability Mapping - evaluation of Web 3.0 protocols with a focus on specific functions to use in the commerce domain; selection of protocols that have over 10,000 active users, are relevant to business tasks and have measurable performance data available for them; (iii) Layer Abstraction - segregation of functional components into a seven-layer architecture; (iv) Synchronization Modelling - cross-layer coordination and information sharing mechanisms.

C. Evaluation and Refinement. The artifact was developed by means of triangulated validation combining benchmarking, case analysis and scenario modelling (Section III.E).

III.C Data Collection and Analysis

Literature. A review of research papers, conference summaries and technical documents, such as the Ethereum and W3C DID guidelines, revealed common designs, performance standards, modes of management and failures.

Protocol Documentation and Industry Reports. Technical documentation, governance proposals, audit reports, and ecosystem analyses from some of the major Web 3.0 projects were used to analyse implementation constraints, such as MakerDAO, Polkadot, and Chainlink.

Performance Measures of Public Blockchain. We made data from blockchain tracking tools like Etherscan and Dune Analytics consistent, to compare different blockchains. The metrics include transactions per second (TPS), average transaction cost in US dollars in a 30-day period, energy used and governance participation levels.

III.D Framework Development Process

Step 1: Requirements Formalization. The following design constraints are identified from the literature (i) user level data sovereignty (ii) modular composability (iii) cross-chain interoperability (iv) regulatory adaptability and (v) automated cross-layer coordination.

Step 2: Layered Architectural Design. Seven-layer stack decoupling responsibilities among consensus, identity, commerce logic, storage,

interoperability, governance and compliance - UX abstraction layers. Standardized interfaces make layers independent from each other.

Step 3: The Specification of Synchronization Mechanism. The research shows the presence of different cross-layer synchronization patterns such as event-driven propagation, cross-layer cryptographic verification and failover to ensure the operation continuity in the face of partial failures.

III.E Validation Strategy

Evaluation criteria were set according to cost efficiency, transaction latency, energy consumption, participation of governance and user experience indicators.

(i) **Analytical Benchmarking.** Publicly available performance data, such as transactions per second (TPS), cost, energy consumption, and governance participation indicators were reviewed and synthesized for over 20 Web 3.0 protocols using the data published in documentation, blockchain explorer data, and industry reports.

(ii) **Empirical Case Studies.** This analysis focuses on OpenBazaar, Boson Protocol and OpenSea based on public data available on the ledger, governance documents and platform documents.

(iii) **Scenario Based Modelling.** Framework applied to two scenarios: Scenario A: Brownfield migration of an existing centralized platform; Scenario B: Greenfield to implement a new Web 3.0, native platform.

III.F Limitations and Delimitations

This research is aimed at architectural design and analytical validation. There are two limitations. (i) rapid protocol innovation could require regular updates to the implementation; the layered design permits such changes without the need of full redesign. (ii) Complete smart contract code, underlying infrastructure setup and detailed legal audit is out of scope.

IV. THE SYNCHRONIC FRAMEWORK ARCHITECTURE

IV.A Design Philosophy and Foundational Principles

SYNCHRONIC is a paradigm shift from the platform approach of architecture towards user sovereignty, modularity and interoperability aligned with Web 3.0. Four fundamental tenets are followed in its design:

(i) **User Control over Platform Control:** Power moves from corporations to individuals through secure technologies for control of data, identities & value generated.

(ii) **Modular over Monolithic Systems:** Commerce functionality breaks out into different deployable layers and allows phased migration of functionality and minimizes systemic risk.

(iii) **Automated Coordination over Manual Operations:** Smart Contracts and embedded mechanisms for coordination help in lowering the dependency of intermediaries with inbuilt trust.

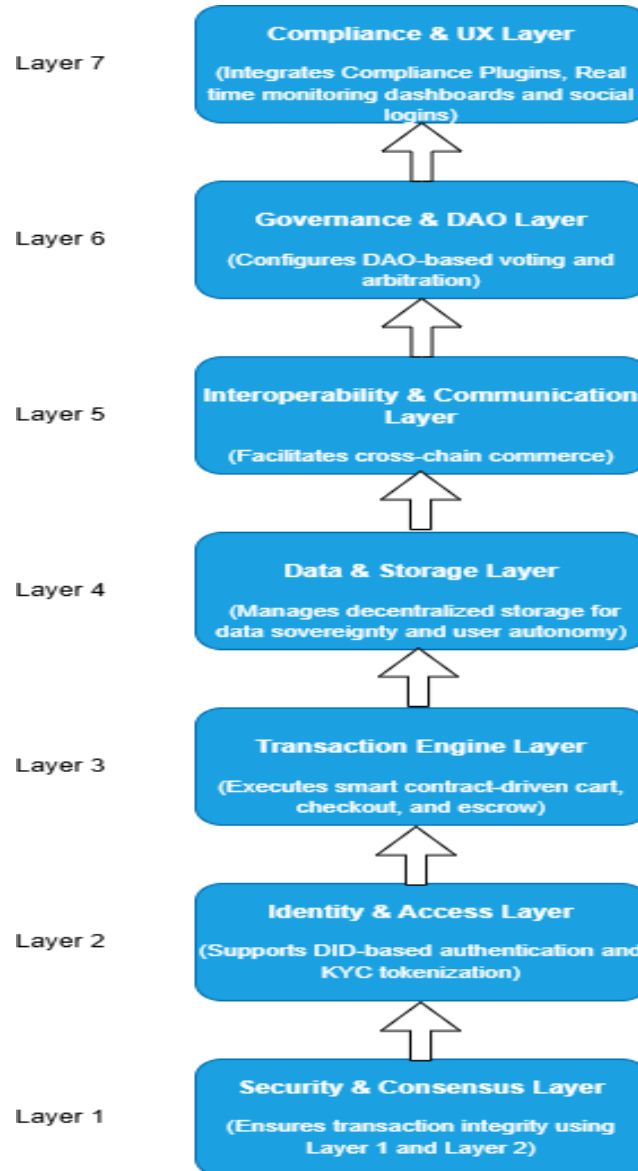
(iv) **Compliance by Design rather than Regulatory Afterthought:** Governance and regulatory rules are built into the design from the beginning.

IV.B Seven-Layer Architecture: Overview

SYNCHRONIC establishes seven different but synchronous layers of digital

commerce functionality as shown in Figure 1. The layers are grouped:

Fig 1: The SYNCHRONIC Framework - Seven Layers Architecture for Web 3.0 Commerce Synchronization



Infrastructure Layers (L1-L2): Trust, consensus, and identity.

Application Layers (L3-L4): Commerce logic and decentralized data management.

Coordination Layers (L5-L6): Interoperability and governance.

Interface Layer (L7): User experience and regulatory compliance.

The two principles that are applied in the architecture are: Vertical Integration (each layer is dependent on services provided by layers below the current layer); Horizontal Interoperability (many protocols can operate at each layer, and vendor lock-in is prevented). Note - When the Security and Consensus Layer (L1) refer to "blockchain Layer 1" and "blockchain Layer 2", it refers to the main infrastructure levels of the blockchain ecosystem: The mainnet consensus

networks and the scaling networks are all different from SYNCHRONIC's own numbering of its architectural layers.

IV.B.1 Comparative Positioning Against Existing Frameworks

To compare SYNCHRONIC to existing approaches for Web 3.0 migration, we have compared them in Table 1 in six dimensions.

Table 1: Comparative Positioning of SYNCHRONIC Against Existing Frameworks

Framework	Architecture	Modular Layers	Identity & UX	Governance	Cross-Protocol	Empirical case-based validation
IBM Blockchain	Monolithic	3 layers	No dedicated layer	Manual	Hyperledger only	Limited
AWS Managed Blockchain	IaaS	2 layers	AWS Cognito (central)	None	ETH/Hyperledger	None published
Gartner Web 3.0 Roadmap	Checklist	Unspecified	Mentioned, unarchitected	Generic	Too abstract	None
Garcia [23]	Layered concepts	3–5 layers	Sometimes included	Rarely addressed	Protocol-specific	Single case
SYNCHRONIC (This work)	Modular, Layered	7 layers	Dedicated (L2, L7)	L6 DAO-based	L5 (Polkadot, Cosmos)	3 diverse contexts

The comparison is made with publicly available documentation and architectural descriptions of respectively available frameworks.

IV.C Layer-by-Layer Specification

Layer 1 - Security & Consensus Layer. Supports transaction integrity by using blockchain mainnet consensus networks (e.g. Ethereum) and blockchain Layer 2 scaling networks (e.g. Polygon) as the underlying infrastructure. Consensus mechanisms exist in balance in order to combine openness, scalability, and energy efficiency.

Layer 2 - Identity and Access Layer. This system is implemented with decentralized identity and verifiable credentials, and a key know your customer (KYC) tokenization, to allow for user-controlled authentication and selective disclosure. KYC information is stored in the form of secure tokens on

the DID system, which allows it to be checked without the need to share personal information. Solves the issue of data monopolization and ensures financial inclusion using self-sovereign identity.

Layer 3 - Transaction Engine Layer. Implements entire workflows of commerce, carts, checkout process, payments, escrow, dispute resolution etc. using programmable smart contracts. Automation addresses the transaction cost inefficiencies, and intermediaries' dependency directly.

Layer 4 - Data and Storage Layer. Censorship-resistant storage for product data, digital assets and transaction records using content-addressable systems. Helps to reduce single points of failure / Enhances data ownership.

Layer 5 - Interoperability & Communication Layer. Facilitates the transfer of assets and data between different heterogeneous blockchain ecosystems, avoiding vendor lock-in and multi-chain commerce operations.

Layer 6 - Governance & DAO Layer. This work coordinates stakeholder decision making, token-based voting and decentralized autonomous organisation arbitration mechanisms for commerce platforms. Arbitration functions are responsible for correcting disputes by handling dispute escalations from Layer 3 escrow time out and offer a decentralised resolution path without any dependency on centralised intermediaries.

Layer 7 - Compliance & UX Layer. The system simplifies things by offering easy account management, social media login integration and monitoring dashboards. Compliance plugins are ingrained directly into the user workflow and make it possible to comply with regulations without user-facing friction. Social logins are the main points of UX, and abstract underlying DID and wallet mechanisms from the mainstream.

IV.D The Synchronization Engine

There are three basic synchronization patterns to the synchronization architecture of SYNCHRONIC:

(i) **Cross-Layer Event Propagation:** The events that are confirmed in one layer cause actions related to them in other layers.

(ii) **Atomic Cross-Layer Transactions:** it means that important business tasks are performed as a single unit across different layers for the sake of keeping the whole system consistent.

(iii) **Fallback Coordination Protocols:** These predefined back-up methods help in keeping the system intact in the partial failure or network problems. A detailed operational example in a multi-chain checkout scenario is given in Appendix A.

IV.E Implementation Pathways

Brownfield Migration: Progressive phased migration of existing platforms.

Greenfield Implementation: End-to-end implementation of new Web 3.0 native platforms.

Hybrid Pathway: A two-pronged approach of speed and operation continuity. Detailed timelines, costings, success targets and risk mitigation approaches for each pathway are recorded in Appendix B.

IV.F Section Summary

SYNCHRONIC's flexible and layered design provides a clear safer way to move systems as it incorporates identity, governance, interoperability, and compliance in its structure. Empirical case-based validation is given in

Section V.

V. EMPIRICAL CASE-BASED VALIDATION

V.A Validation Objectives and Strategy

This part tests whether the SYNCHRONIC layered architecture is a description of observable outcomes in the real Web 3.0 commerce platforms. Validation is done by comparing cases and combining findings of three example platforms: OpenBazaar, Boson Protocol, and OpenSea. These findings are based on the case analysis (retrospective) and are indicative rather than universally generalizable. The validation is based partly on platform documentation available to the public and industry reports which may not be independently audited in terms of performance.

V.B Case Selection Rationale

The selected cases are representatives of different strategies and maturity levels of architecture: (i) OpenBazaar--fully decentralized greenfield retail marketplace; (ii) Boson Protocol--protocol-first greenfield tokenized logistics systems; (iii) OpenSea--hybrid marketplace with combination of decentralized settlement with centralized coordination. Together they cut across physical and digital goods, permissionless and compliance structures and various governance structures.

V.C Case Study I: OpenBazaar — The Cost of Partial Layering Platform Overview

OpenBazaar was designed as a peer-to-peer marketplace which is completely decentralized with zero platform fees and no censorship. Despite the early adoption, the platform was discontinued in 2021 [28].

Layer Alignment

L1: Bitcoin (POW) L2: Pseudo anonymous wallet-based identity L3: Multi signature escrow L4: Local storage with partial IPFS L5: No interoperability L6: Informal governance L7: Minimal UX abstraction

Key Metrics

Platform fee: 0% (vs. 10-15% Web 2.0 baseline) Adoption: Low Platform discontinued Governance: Poor dispute co-ordination

Empirical Insight

OpenBazaar proves that technical decentralization does not ensure sustainability of the platform. The lack of formal governance (L6), interoperability (L5) and abstraction of the UX (L7) limited coordination and adoption. This case demonstrates the importance of socio- technical layer completeness as a factor in platform viability.

V.D Case Study II: Boson Protocol — Infrastructure Efficiency Without Scale Platform Overview

The Boson Protocol assists people in trading physical goods with the help of special digital tokens that can be exchanged and focus on automated buying and selling with fewer middlemen.

Layer Alignment

L1: Ethereum (PoS) | L2: DID + wallet | L3: Smart contract escrow | L4: IPFS | L5: Limited interoperability | L6: DAO governance | L7: Developer-centric UX

Key Metrics

Merchant fee: ~0.5% (about 81% less than industry baseline 2.7% [9])
Settlement: Minutes vs days Audience: Crypto -Native only

Empirical Insight

Boson Protocol proves that at protocol level there is L3 (level 3) which substantially reduces cost and increases trust. Limited UX abstraction (L7) limits mainstream adoption, demonstrating the difference between infrastructure efficiency and platform scalability.

V.E Case Study III: OpenSea — Hybrid Scalability and Governance Debt Platform Overview

OpenSea is a hybrid NFT marketplace, which is a blend of decentralized settlement and centralized UX and moderation. Founded in 2017 and made publicly available in 2018, the platform gradually adopted Layer 2 networks (most notably Polygon sidechain, July 2021), which make purchases of assets on Polygon gasless and even eligible for credit card payments [23], to bring down transaction costs and expand adoption.

Layer Alignment and Timeline

OpenSea's incremental migration across protocols is a risk managed one. Key milestones include integration of new network support into the product in July 2021 [23]; the June 2022 launch of the Seaport protocol, an open-source marketplace protocol with significant gas savings and ability to scale with zero downtime [24]; and the gradual decentralization of NFT metadata to IPFS [25], to provide greater content persistence and resilience.

Layer alignment consists of the following: L1 stands for Ethereum and Polygon; L2 is wallet- based identity; L3 is smart contracts (Seaport); L4 is IPFS [25]; L5 is multi-chain interoperability; L6 is centralized governance; and L7 is strong user experience abstraction.

Key Metrics

Polygon integration resulted in around 99.95% of gas cost reduction for eligible transactions [26]. Migration to the Seaport protocol was done without any observed service disruption in the documented case [24]. OpenSea became and has continued to maintain a dominant position in the NFT marketplace category.

Empirical Insight

Strong UX Abstraction (L7) & Interoperability (L5) allowed large scale adoption. However, centralized governance (L6) generates 'governance debt' - long-term tensions of trust and regulation, inherent in hybrid models of centralization.

V.F Cross-Case Synthesis

V.F.1 Gap Validation

Comparative Analysis Confirmation: Phased migration is associated with lower operational risk (OpenSea vs. OpenBazaar); Interoperability is associated with scalability (OpenSea vs. Boson); UX abstraction is strongly associated with adoption outcome; Formal governance is associated with sustainability; Layer completeness (not ideological decentralization) is associated with platform viability.

V.F.2 Layered Maturity Progression

A clear path of development can be seen, early platforms are concerned with efficiency of transactions (L1 - L3); as they scale, coordination problems arise (L4 - L6); and large-scale adoption requires ease of use and compliance

to regulation (L7). OpenBazaar had problems with early decentralization. Boson helped to optimize the infrastructure by removing aggregation layers. OpenSea was able to gain the scalability by improving the platform interaction and multi-chain interoperability and accepted the trade-off of governance centralization.

V.G Validation of Architecture and Migration Logic

The synchronization mechanisms mentioned in Appendix A can be observed in real applications. For example, Boson's redemption mechanism for NFTs and OpenSea's Seaport- based transaction batching [24] are good examples of cross-layer synchronization. The following topics are discussed in Appendix B: Migration Pathways, Correlation to Empirical Outcomes, OpenBazaar Greenfield Risk Exposure, and OpenSea Hybrid Migration Benefits.

V.H Summary of Quantitative Validation

The quantitative results that are presented are based on case-based analysis and should be interpreted in the context of platform-specific conditions. Polygon integrated approximately 99.95% gas cost reduction for eligible transactions [26]; Boson Protocol lowered merchant fees by approximately 81% in comparison to Web 2.0 baselines [9]; and the migration to the Seaport protocol was executed with minimal operational disruption for a hybrid migration [24]. Layer 7 maturity has a positive correlation to adoption results in the evaluated platforms. These results are in line with the rationale of efficiency of the SYNCHRONIC framework and provide empirical evidence for the layer-wise design logic.

V.I Limitations

We point out three such limitations as follows: (i) due to the retrospective case analysis, it is difficult for us to infer causal conclusions; (ii) for some operational metrics, they are not publicly available; and (iii) there may be survivor bias, but we partly overcome this by including the discontinued platform OpenBazaar.

V.J Validation Summary

Empirical assessment shows that SYNCHRONIC: (i) captures the principles of Web 3.0 transposed into a deployable layered architecture; (ii) provides platform weaknesses identification using layer gap analysis; (iii) supports selection of context appropriate migration strategy; and (iv) supports forecasting of platform evolution using layered maturity progression.

VI. DISCUSSION

VI.A Major Findings and Theoretical Contributions

The findings show that technical decentralization is necessary, but not sufficient. Sustainable Web 3.0 commerce requires deliberate socio-technical coordination in the areas of governance, user experience, interoperability, and compliance dimensions. Web 3.0 is not just a technological replacement, it is a transformation in the way that participants collaborate, create trust, and organize.

The shutdown of OpenBazaar, despite zero fees and being fully decentralized, proves that being technically pure is not enough. OpenSea

achieved market dominance with the help of great UX abstraction and interoperability despite centralized governance. Boson Protocol proves that infrastructure efficiency does not get translated into platform adoption.

Contribution 1: Layered Platform Migration Theory

SYNCHRONIC views the adoption of Web 3.0 not as a single technological transition, but as a series of stages of architectural progression. Platforms are starting out with transaction efficiency (Layers 1-3) - as the scale grows, the coordination, governance and UX aspects of a platform (Layers 4-7) become the limiting factors. OpenSea phased Layer 5 migration (Ethereum - Polygon - multi-chain) is a great example of the risk reduction advantages of hybrid sequencing.

Contribution 2: Governance as Infrastructure

Governance (Layer 6) should be co-designed at the same time transaction logic is developed instead of being added after the fact. OpenBazaar's informal governing led to failure of dispute resolution. Boson's DAO design offered legitimacy for the long-term at the expense of agility in the short-term. OpenSea's centralization of its moderation process led to growing tension between the stated decentralization and operational control. These patterns show that the design of governance represents a structural determinant of the sustainability of the platforms.

Contribution 3: User Experience Parity as Adoption Prerequisite

Layer 7 abstraction, which hides the complexity of the systems behind known interfaces, is the main enabling factor of wide onboarding. The user experience designed for crypto users can support small, specialized groups, but is not enough to attract the larger market.

VI.B Answer to the Research Question

SYNCHRONIC resolves the trade-offs in the scalability, privacy, and inclusivity by using layer specialization rather than global optimization. Scalability is provided by the multi-protocol interoperability at Layers 1 and 5. Privacy is ensured by decentralized identity schemes at Layer 2 with the planned extension to zero knowledge proofs. Inclusivity is enabled by the Layer 7 abstraction and cost-efficient settlement. All four of the research goals were achieved: mapping the technology taxonomy; identifying platform-specific efficiency enhancements in case studies, such as a 99.95% reduction in gas costs, and 81% reduction in merchant fees, as well as migration without any downtime; validating the seven-layer model in heterogeneous contexts; and defining empirically based migration strategies.

VI.C Stakeholder Implications

Platform Developers: UX abstraction (Layer 7) needs to be prioritized in the initial stages. Governance (Layer 6) should be developed at the same time as transaction logic (Layer 3). The use of multiple blockchain networks (Layer 5) makes systems strong rather than using just one blockchain.

Enterprise Decision-Makers: Hybrid migration approaches introduce innovation without disrupting business. Phased transitions of 12–36 months with executive sponsorship systematically reduce systemic risk.

Policymakers: Compliance frameworks like MiCA [13] and decentralization are not mutually exclusive. Application-level compliance tools that are built into decentralized systems can meet regulatory requirements.

Protocol Developers: Protocols should be made to be integrator

composable. Governance and settlement functions need to be structurally separated and thus insulate the commerce from token price volatility.

VI.D Boundary Conditions

The applicability of the framework is dependent on the context. Digital-natives asset management is more efficient than the physical supply chains. Highly regulated sectors may have to have hybrid governance structures. Mass market deployment will need complete Layer 7 abstraction. Architectural superiority cannot have a perpetually advantageous effect in liquidity concentration or first-mover advantage. SYNCHRONIC is a model to be used to guide the design process and not a universal solution for it.

VI.E Limitations and Future Research

This study is retrospective case analysis and public data-based, which inhibits causal inference. Future research should focus on the following areas: (i) enterprise implementation studies, (ii) long term analysis of the governance performance, (iii) quantitative evaluation of the user experience abstraction effects, (iv) development of compliance-by-design modules, (v) modelling environmental and economic sustainability and (vi) standardising cross-chain interoperability.

VII. CONCLUSION

VII.A Overview of Research Contribution

The shift from Web 2.0 to Web 3.0 commerce has been limited not by a lack of cryptographic innovation, but by the lack of architectural frameworks for systems that can translate decentralization into scalable, compliant and user-friendly platforms on a system level. The SYNCHRONIC framework addresses this deficiency in a seven-layer modular approach which reconceptualises Web 3.0 commerce as a staged, composable socio-technical transformation. By having a principled way of structuring consensus, identity, commerce logic, storage, interoperability, governance, and compliance-UX in a deliberate hierarchy gives the framework a principled basis for the design and migration of digital commerce systems in an uncertain and regulated world.

VII.B Empirical Conclusions

Validation across OpenBazaar, Boson Protocol, and OpenSea supports four key findings. (i) technical decentralization is needed but not enough, good governance and making the user experience simple is also important; (ii) Hybrid systems grow well as social and technical layers get matured; (iii) Efficient protocol does not ensure people will use the platform. Boson's about 81% fee cut [9] shows better infrastructure, but wide use needs easier platform features; (iv) having all necessary parts working well predicts success better than just focusing on decentralization ideas. These conclusions are made based on retrospective case analysis and represent typical architectural tendencies rather than universally generalizable results.

VII.C Theoretical Propositions

Proposition 1 – Modular Migration: The evolution of the Web 3.0 platform will occur in stages of maturing the layers (Layers 1-3 - Layers 4-7), rather than

wholesale replacement of the technology.

Proposition 2 – Governance as Infrastructure: Governance should be created at Layer 6, parallel with the rules of transaction. Deferred governance means that coordination debt is generated against long-term sustainability.

Proposition 3 – User Experience Equivalency: Mainstream adoption requires UX abstraction and compliance automation (Layer 7) equivalent to Web 2.0 standards.

VII.D Implications for Practice and Policy

For designers of the system: Early investment in the design of user experience, compliance and governance will reduce barriers to adoption. Multi-chain strategies provide for more adaptability. For business leaders: hybrid pathways are a way of combining innovation with continuity whereas changes are incremental and supported by executive sponsorship. Policymakers should think in terms of compliance-by-design at the architectural level. Frameworks such as MiCA have shown that regulatory oversight is compatible with decentralization [13].

VII.E Concluding Remarks

The development of digital commerce does not only depend on cryptographic innovation, but critically on the designing of effective coordination, governance and usability at scale. SYNCHRONIC combines Web 3.0 theory, deployable system design and empirical validation of case studies that deliver a sound architectural foundation for inclusive, efficient and resilient commerce in a decentralized digital economy.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

1. McKinsey & Company, "The Future of Digital Commerce 2025," McKinsey Global Institute, Rep., 2024. [Online]. Available: <https://www.mckinsey.com/industries/retail/our-insights>
2. Stripe, Inc., "Payment Processing Fees and Pricing," Stripe, Inc., San Francisco, CA, 2024. [Online]. Available: <https://stripe.com/pricing>
3. Shopify Inc., "2024 Annual Report and Fourth Quarter Results," Shopify Inc., Ottawa, Canada, 2025. [Online]. Available: <https://investors.shopify.com/financial-information/annual-reports>
4. Statista, "E-Commerce Worldwide — Statistics and Facts," Statista Research Department, Hamburg, Germany, 2025. [Online]. Available: <https://www.statista.com/topics/871/online-shopping/>
5. S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York, NY, USA: PublicAffairs, 2019.
6. Chainalysis, "The Chainalysis 2025 Crypto Crime Report," Chainalysis, Inc., New York, NY, Rep., Jan. 2025. [Online]. Available: <https://go.chainalysis.com/crypto-crime-2025.html>
7. Forrester Research, "The State of Privacy and Cybersecurity, 2024," Forrester Research, Inc., Cambridge, MA, Rep. ID RES181291, 2024. [Online]. Available: <https://www.forrester.com/report/the-state-of-privacy-and-cybersecurity-2024/RES181291>
8. World Bank, Global Financial Inclusion Database (Global Findex) 2024 Update. Washington, DC, USA: World Bank, 2024. [Online]. Available: <https://www.worldbank.org/en/publication/globalfindex>
9. Boson Protocol, "Technical Documentation and Case Studies," Boson Protocol, 2024. [Online].

- Available: <https://bosonprotocol.io>
10. World Wide Web Consortium (W3C), "Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations," W3C Recommendation, Jul. 2022. [Online]. Available: <https://www.w3.org/TR/did-core/>
 11. A. Leow et al., "Hype Cycle for Web3 and Blockchain, 2024," Gartner, Inc., Stamford, CT, Rep., Jul. 29, 2024. [Online]. Available: <https://www.gartner.com/en/documents/5623191>
 12. S. Kumar, Y. Li, and D. Thompson, "Cross-Protocol Benchmarking in Web 3.0 Systems: A Systematic Review," *Journal of Blockchain Research*, vol. 7, no. 1, pp. 1–21, 2025.
 13. European Securities and Markets Authority (ESMA), "Markets in Crypto-Assets Regulation (MiCA)," ESMA, Paris, France, 2025. [Online]. Available: <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>
 14. C. Catalini and J. S. Gans, "Some Simple Economics of the Blockchain," *Communications of the ACM*, vol. 63, no. 7, pp. 80–90, Jun. 2020, doi: 10.1145/3359552.
 15. H. J. Smith, T. Dinev, and H. Xu, "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, vol. 35, no. 4, pp. 989–1015, Dec. 2011, doi: 10.2307/41409970.
 16. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
 17. V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Foundation, White Paper, 2014. [Online]. Available: <https://ethereum.org/whitepaper>
 18. J. Benet, "IPFS — Content Addressed, Versioned, P2P File System," arXiv:1407.3561, Jul. 2014. [Online]. Available: <https://arxiv.org/abs/1407.3561>
 19. Polkadot, "Polkadot Interoperability Overview and Governance Model," Web3 Foundation, 2024. [Online]. Available: <https://polkadot.network>
 20. S. Hassan and P. De Filippi, "Decentralized Autonomous Organization," *Internet Policy Review*, vol. 10, no. 2, 2021, doi: 10.14763/2021.2.1556.
 21. O. K. Rikken, M. F. W. H. A. Janssen, and Z. Roosenboom-Kwee, "Governance Impacts of Blockchain-Based Decentralized Autonomous Organizations: An Empirical Analysis," *Policy Design and Practice*, vol. 6, no. 4, pp. 465–487, Oct. 2023, doi: 10.1080/25741292.2023.2270220.
 22. A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, Mar. 2004, doi: 10.2307/25148625.
 23. OpenSea Crew, "New Features and Updates, July 2021," OpenSea Blog, Aug. 5, 2021. [Online]. Available: <https://blog-v3.opensea.io/articles/new-features-updates-july-2021>
 24. A. Mamujee, "Launching Seaport and Saving the Community Millions in Fees," OpenSea Blog, Jun. 14, 2022. [Online]. Available: <https://opensea.io/blog/articles/launching-seaport-saving-the-community-millions-in-fees>
 25. OpenSea, "Decentralizing NFT Metadata on OpenSea," OpenSea Blog, Sep. 2021. [Online]. Available: <https://opensea.io/blog/articles/decentralizing-nft-metadata-on-opensea>
 26. Polygon Labs, "How to Mint NFTs With Utility Gas-Free on Polygon," Polygon Technology Blog, Jun. 3, 2022. [Online]. Available: <https://polygon.technology/blog/how-to-mint-nfts-with-utility-gas-free-on-polygon>
 27. C. Allen, "Issues and reflections on DAO governance: Challenges and solutions," AIFT, 2024. [Online]. Available: <https://hkaift.com/issues-and-reflections-on-dao-governance-challenges-and-solutions/>
 28. CoinDesk, "OpenBazaar Co-Founder Explains Why Web 3's Answer to eBay Folded Its Tents," CoinDesk, Jul. 15, 2021. [Online]. Available: <https://www.coindesk.com/business/2021/07/15/openbazaar-co-founder-explains-why-web-3s-answer-to-ebay-folded-its-tents>

Appendix A: Multi-Chain Checkout — Operational Synchronization Example

A.1 Scenario Overview

This appendix provides a detailed example of how the 3 SYNCHRONIC synchronization patterns, Cross-Layer Event Propagation, Atomic Cross-Layer Transactions, and Fallback Coordination Protocols are operated in a typical multi-chain digital commerce transaction. The scenario is that the buyer is a buyer on a web 3.0 commerce platform who buys a tokenized physical (limited edition) product with an associated redeemable NFT where the buyer's wallet contains funds on Polygon (Layer 2 sidechain) and the seller's asset is registered on Ethereum mainnet.

This scenario is for illustration purposes and is meant to illustrate cross layer coordination logic. It is not prescriptive of any implementation, and it is also not a formal protocol specification.

A.2 Pre-Transaction State

Prior to check-out, the following layer states are created: Layer 1 (Consensus) - Finalization of previous blocks both on Ethereum mainnet and Polygon is established. Layer 2 (Identity) contains a verified DID credential (that the buyer is placed in) provided by a trusted credential provider in the buyer's self-sovereign identity wallet, containing age and jurisdiction eligibility. Layer 4 (Storage) is responsible for storing the product catalogue entry and related NFT metadata on IPFS and identified by some content identifier (CID). Layer 6 (Governance) Active DAO approved escrow policy for tokenized physical goods (72-hour time limit on dispute).

A.3 Step-by-Step Transaction Flow

Step 1 — Buyer Initiates Purchase (Layer 7 → Layer 2): The buyer identifies themselves using a social login (e.g. Google or email -- this will be presented by Layer 7's UX abstraction, taking the DID presentation out of the end user's view) and selects the item. The smart account manager at Layer 7 silently maps the social login session to the DID credential of the buyer and triggers an identity verification request to Layer 2 to check whether the DID credential of the buyer meets the jurisdiction and age requirements of the platform. This is an example of Cross-Layer Event Propagation: A user performs an action at Layer 7 which triggers a corresponding dependent action at Layer 2 which is verifiable. The buyer is shown only a loading indicator; they do not have to submit their credentials manually.

Step 2 — Identity Verified, Session Token Issued (Layer 2 → Layer 3): Layer 2 authenticates with Layer 3 with a cryptographically signed session assertion to indicate that the buyer is qualified to make a transaction. When applicable, the buyer's DID credential contains a KYC token, a privacy-friendly, tokenized proof of identity. This meets the rules of compliance of the platform without sharing any of the raw personal data. Layer 3's Transaction Engine instantiates an escrow smart contract including coding the agreed upon price as well as conditions for delivery per DAO governance policy (Layer 6), and a time limit for dispute resolution. The contract mentions the IPFS CID (Layer 4) of the product being sold, as the unchangeable record of what is being sold. At this point the coordinated execution unit is created: SYNCHRONIC is a logical container that treats all subsequent steps as a logical group with the assumption of rollback fall back mechanisms if any critical step failed to confirm within the timeout, it has been configured.

Step 3 — Cross-Chain Asset Lock (Layer 3 → Layer 5 → Layer 1): The buyer's held funds via Polygon committed against an Ethereum-registered

asset. Layer 5 (Interoperability) triggers a cross-chain message, which locks the funds of the buyer in a Polygon-side bridge contract and releases a lock confirmation event. This transaction is propagated to the Ethereum-side escrow contract at Layer 3 using the relayer of Layer 5. Layer 1 on both the chains records the lock transactions in their respective block production windows (approximately two seconds per block on Polygon, approximately twelve seconds per block on Ethereum). These time periods are block production, not economic finality. It takes more time to complete cross chain finality, including submitting Polygon checkpoint to Ethereum mainnet. This step shows Atomic Cross-Layer Transactions: The Polygon lock and Ethereum escrow activation are considered as a single logical unit - should either of them fail during a configurable time, they are both automatically reverted.

Step 4 — Compliance Check (Layer 7 gates Layer 3): Before final confirmation, Layer 7 applies the embedded compliance rules (i.e. MiCA transaction reporting thresholds). If the value of the transaction is higher than the threshold value configured, a compliance flag is set and the transaction is sent to a compliance review queue instead of automatically continuing. This step serves as evidence that compliance is a structural part of the flow of transactions, and not something that is done after the fact.

Step 5 — Seller Confirmation and NFT Transfer (Layer 3 → Layer 4 → Layer 1): On lock confirmation of buyer's funds, Layer 3 informs the seller accordingly. The seller's system is verified as ready to fulfil. The contract call on Layer 3 to the NFT transfer function calls the update ownership function on Layer 1 (Ethereum mainnet) and updates the provenance on Layer 4 (IPFS) with a new CID (containing the timestamp of the transaction and the wallet address of the buyer). Layer 1 sends out a Transfer event which is listened to by Layer 3 which serves as the trigger to release the escrowed funds to the seller.

Step 6 — Escrow Release and Receipt (Layer 3 → Layer 7): Once the event of Transfer is confirmed, the contract of the escrow is released, and the locked Polygon funds are released to the seller's specified Layer 5 wallet. Layer 7 provides purchase summary to the purchaser through its real-time monitoring dashboard and includes a link to the IPFS-hosted transaction receipt (Layer 4), as well as live transaction status indication. The 72-hour period of dispute starts, which is controlled by the DAO arbitration policy, Layer 6. Should the buyer choose to initiate a dispute within this window, Layer 6's mechanism for arbitration (which is separate to centralised customer support) refers the dispute to a resolution panel based on DAO. The six-step flow is set up as a coordinated flow of execution with rollback fall back: no partial ownership transfer persisted in the event any step fails before the Transfer event confirmation of Step 5.

Note: it is not possible to completely guarantee all-or-nothing actions in two separate blockchains in the strict computer science sense. The SYNCHRONIC fall-back coordination protocol tries to get close to this by using transactions that undo changes and by reversing states.

A.4 Fallback Coordination Protocol

If the Layer 5 cross-chain message in Step 3 does not receive confirmation within a configurable time frame (with the time frame depending on the bridge protocol as well as the block finality requirements of the participating chains) the Fallback Coordination Protocol is activated. The Polygon-side bridge

contract automatically returns locked funds from the buyer to the buyer's wallet. The Ethereum escrow contract goes into a FAILED state and sends a cancellation event. Layer 7 provides a transaction failure message with a possibility of retrying. No funds are lost and no partial ownership transfer takes place. This is a fallback system to avoid problems in the network or bridge that led to stuck states that do not resolve like in simple cross-chain constructions. It should be noted that cross-chain bridges are a significant attack surface in Web 3.0 systems; platform implementation should do independent security audit of bridge contracts before mainnet deployment.

A.5 Summary of Synchronization Patterns Demonstrated

A mapping of each step to the SYNCHRONIC synchronization pattern that is demonstrated is provided in Table A.1.

Table A.1: Synchronization pattern mapping for the multi-chain checkout scenario.

Step	Layers Involved	Action	Pattern
1	L7 → L2	UX triggers identity verification	Cross-Layer Event Propagation
2	L2 → L3, L6, L4	Escrow contract instantiation	Atomic Cross-Layer Transaction (initiated)
3	L3 → L5 → L1	Cross-chain fund lock + asset lock	Atomic Cross-Layer Transaction (commit)
4	L7 (gates L3)	Compliance threshold check	Cross-Layer Event Propagation
5	L3 → L4 → L1	NFT transfer + provenance update	Atomic Cross-Layer Transaction (finalize)
6	L3 → L7	Escrow release + receipt display	Cross-Layer Event Propagation
Fallback	L5, L3, L7	Timeouts revert + notification	Fallback Coordination Protocol

Appendix B: Implementation Pathways — Timelines, Metrics, and Risk Mitigation

B.1 Overview

Section IV.E identifies three pathways of implementations that may be adopted by organizations to use the SYNCHRONIC framework: Brownfield Migration, Greenfield Implementation and Hybrid Pathway. This appendix defines suggestive timelines, phased layer activation sequences, key success measures and primary risk Factors with associated mitigations for each pathway. These specifications are based on the architectural logic of the seven-layer framework, and on patterns found in the case studies described in Section V. All timelines and metrics are the indicative planning indicators, developed from the framework architecture, the case study patterns described in Section V. They are not empirically validated benchmarks and will need to be adapted to organisational context, existing infrastructure, regulatory environment and specific protocol characteristics.

B.2 Pathway 1: Brownfield Migration

Description

Brownfield Migration applies to those organizations that already have Web 2.0 commerce platforms installed but want to adopt the Web 3.0 capabilities incrementally without disrupting operations. The defining characteristic is that the legacy systems remain operational throughout with decentralized layers activating alongside - not replacing - existing infrastructure.

Indicative Timeline: 18–36 Months

Phase 1 (Months 1–6) — Foundation: Perform an audit of the existing architecture to determine compliance to SYNCHRONIC layer requirements to activate Layer 1 on a permissioned or hybrid chain. Implement Layer 2 DID-based authentication in addition to the existing OAuth/SSO system, and Layer 7 social login as the user-facing entry point to hide the DID details from the users. Concurrently run both identity systems.

Objective: zero disruption of the user.

Phase 2 (Months 7–18) — Commerce Logic Migration: Introduce Layer 3 smart contract escrow for a set of transaction types (e.g. high value orders above a set threshold). Migrate product catalogue data to Layer 4 IPFS storage with legacy database as fall back. Start the design of Layer 6 governance framework, involving key stakeholder groups.

Objective: Validate layer 3 efficiency benefits in a live but bounded environment.

Phase 3 (Months 19–36) — Interoperability and Governance: It is focused on adding Layer 5 cross-chain features to support buyers using more than one currency and network. Update outdated identity systems in cases where Layer 2 usage reaches the set limits. Make a complete management change in the Layer 6 DAO systems. Enable layer 7 compliance automation & simplify user experience across all touchpoints.

Objective: Full SYNCHRONIC layer activation with legacy system decommissioned.

Table B.1: Brownfield Migration success metrics by phase.

Success Metric	Phase 1 Target	Phase 2 Target	Phase 3 Target
Transaction cost	Baseline established	Measurable reduction	Substantial reduction across all flows
Operational uptime	100% (no disruption)	≥99.9%	≥99.9%
Identity adoption	DID available alongside legacy	Meaningful minority of users on DID	Majority of users transitioned to DID
Governance participation	Stakeholder groups formed	First DAO proposal passed	Active governance participation demonstrated
User onboarding rate	No change from baseline	Maintained within 5% of baseline	Improved vs. legacy baseline

Primary Risks and Mitigations

Risk 1 — Integration Complexity: Legacy APIs may not expose cleanly the data fields needed by SYNCHRONIC layers.

Mitigation: Implement an adapter layer between legacy systems and SYNCHRONIC Layer 3 contracts during Phase 2, abstracting the interface without making changes to production systems.

Risk 2 — User Resistance to Wallet-Based Identity: Users accustomed to email/password login methods may forsake onboarding flows when they're introduced to wallet based DID. Mitigation: Layer 7 must abstract the complexity of wallets altogether during Phase 1 and 2 and the presentation of familiar UX patterns during the underlying identity layer transition. Social recovery wallets (e.g. account abstraction via ERC-4337) need to be evaluated.

Risk 3 — Regulatory Uncertainty During Transition: The dual compliance obligations of operating both Web 2.0 and Web 3.0 systems could be triggered.

Mitigation: hire legal assistance during Phase 1 to identify relevant obligations of applicable frameworks (e.g. MiCA, GDPR) for both system states. Layer 7 compliance modules should be set up to meet the more stringent of the two regimes during transition.

B.3 Pathway 2: Greenfield Implementation

Description

Greenfield Implementation is applicable to organizations that are creating a new Web 3.0 native commerce platform from the ground up. All seven SYNCHRONIC layers are designed and activated in concert with one another, to allow optimal architectural coherence at the expense of a higher initial investment and with tolerance for initial user adoption risk. The case study of OpenBazaar (Section V.C) is a good example of the danger of greenfield implementation with little regard to socio-technical layers: This platform enjoyed partial implementations of L4 (IPFS) and minimal L7 (UX), but the lack of formal governance (L6), interoperability (L5), and meaningful UX abstraction were fatal to the sustainability of the platform.

Indicative Timeline: 12–24 Months

Phase 1 (Months 1–4) — Architecture and Protocol Selection: Decides on Layer 1 consensus mechanism. We recommend a PoS chain for more energy efficiency. Design Layer 2 identity architecture & choose DID method. Define Layer 3 smart contract commerce logics for the initial transaction types. Select Layer 4 storage system (IPFS with pinning service). Define Layer 6 governance structure & token model. Define Layer 7 UX framework and compliance modules requirements.

Phase 2 (Months 5–12) — Build and Internal Testing: The development phase and auditing of all the components of the layers. Deploy to testnet. Conduct closed beta using controlled group of users. Validate all 3 synchronization patterns during simulated load. KYC tokenization flows operating under beta conditions are confirmed for working as soon as Layer 2 DID credential exchange is operating. Activate fall back protocols and verify correct behaviour for partial failure of conditions.

Phase 3 (Months 13–24) — Launch and Scaling: Launch and scale phase, which includes public launch when the Layer 7 UX abstraction is fully operational. Monitor the participation rates of governance and make changes to incentive structures. Activate Layer 5 interoperability to more chains based on the demand of the users. Carry out a Layer 6 governance review at month 18, to check up on the health of the DAO and participation by its members.

Table B.2: Greenfield Implementation success metrics by phase.

Success Metric	Phase 1 Target	Phase 2 Target	Phase 3 Target
Time-to-transaction	Architecture defined	Performance benchmark met on testnet	Performance benchmark met on mainnet (L2-reliant)
Smart contract audit pass rate	N/A	100%(mandatory pre-launch)	Maintained via periodic audit
User onboarding completion	N/A	Majority completion in closed beta	Acceptable public onboarding rate

Governance participation	Model designed	Beta DAO vote held	Active governance participation
Transaction cost vs. Web 2.0 baseline	Target defined	Validated on testnet	Target transaction cost below Web 2.0 baseline

Primary Risks and Mitigations

Risk 1 — Cold Start / Liquidity Problem: A new platform having no existing user base may not succeed in achieving the transaction volume requisite to sustain Layer 6 governance. Mitigation: Phase 3 is designed to include a bootstrapping period with the founding team holding temporary governance rights via a sunset clause. Full DAO governance is to be transposed only after minimum activation thresholds are reached.

Risk 2 — Smart Contract Vulnerabilities: Smart contracts are new and unproven when Greenfield systems are deployed. A single exploit of a contract can ruin the trust of users irrecoverably.

Mitigation: Measures include a mandatory independent security audit before the mainnet launch (Phase 2), formal verification of the escrow contract logic where feasible and an active bug bounty programme from the beta launch.

Risk 3 — Premature Decentralization: Enabling all seven layers at the same time before adequate user base establishes coordination overhead with inadequate stakeholder participation leading to OpenBazaar failure pattern.

Mitigation: Introduce Layer 6 governance with simplified voting mechanisms in Phase 3 and getting to a full DAO governance subject to adequate participation data.

B.4 Pathway 3: Hybrid Pathway

Description

The Hybrid Pathway is a combination of both Brownfield and Greenfield approaches. It is best suited to organisations who have an existing platform but want to move adoption beyond the conservative Brownfield timeline or are launching a new line of products under an established brand. OpenSea's path of migration (Section V.E) is a good example of this pathway as it preserves centralized coordination at Layers 6 and 7, progressively decentralizing settlement at Layers 1, 3 and 5.

Indicative Timeline: 12–24 Months

Phase 1 (Months 1–6) — Selective Decentralization- Activate Layer 1 on a high-throughput Layer 2 network (e.g., Polygon) alongside existing payment rails. Deploy Layer 3 smart contracts to accomplish settlements without replacing existing systems for dispute resolution and customer support at Layer 6 and 7. Get visibility of live transaction status from day one for operators and user with the help of Layer 7 real time monitoring dashboard. Objective: to achieve immediate benefits in terms of transaction cost and speed without causing disruption in the governance and user experience.

Phase 2 (Months 7–18) — Identity and Interoperability: Provide Layer 2 Decentralized Identifier (DID) as an optional tool for identity to experienced

users. Activate Layer 5 to serve more chains as signals indicate demand from the users. Start moving the governance of Layer 6 from being controlled by a central group of people to one guided by a community advisory team.

Objective: Demonstrate improvements in interoperability and start transferring the governance authority.

Phase 3 (Months 19–24) — Full Layer Activation: Finish the Layer 7 user experience design to remove remaining crypto-native onboarding friction. Transfer full control to Layer 6 DAO structures. Decommissioning of centralized rails for payment of transaction types which are now fully covered by Layer 3.

Objective: Perform post-migration audit of all the layers against SYNCHRONIC compliance specifications.

Table B.3: Hybrid Pathway success metrics by phase.

Success Metric	Phase 1 Target	Phase 2 Target	Phase 3 Target
Transaction cost reduction	Measurable reduction on L2-settled flows	Significant reduction across all flows	Substantial reduction overall
Uptime during migration	100% (zero downtime)	≥99.9%	≥99.9%

Multi-chain support	1 additional chain (L2)	Multi-chain support expanded	Protocol-agnostic via L5
Governance decentralization	Centralized baseline	Community advisory active	Full DAO governance
User experience parity	Maintained vs. Web 2.0	Maintained vs. Web 2.0	Improved vs. Web 2.0 baseline

Primary Risks and Mitigations

Risk 1 — Governance Debt Accumulation: Holding on to centralized governance while decentralizing settlement (as was done by OpenSea) creates a legitimacy gap that widens over time.

Mitigation: Establish clear, time-bound governance transfer milestones at the beginning of Phase 1 and public commitments to the community. Governance should be viewed as infrastructure from the very beginning (Proposition 2, Section VII.C).

Risk 2 — Inconsistent User Experience Across Phases: Users may have different interfaces and flows as layers are turned on and the user may get confused and drop off.

Mitigation : Invest disproportionately in Layer 7 UX abstraction from Phase 1. All layer transitions should be transparent to the end users; the only thing that should be visible is improvements in speed and cost.

Risk 3 — Regulatory Reclassification Mid-Transition: Using smart contract-based settlement could result in changes in regulation under MiCA

or similar rules during transition.

Mitigation: Add Layer 7 compliance checks before entering Phase 1. Continue to work closely with regulatory counsel and establish compliance limits cautiously until the requirements are clear.

B.5 Pathway Comparison Summary

Table B.4: Comparative summary of implementation pathways.

Dimension	Brownfield	Greenfield	Hybrid	OpenSea (Empirical)
Timeline	18–36 months	12–24 months	12–24 months	2018–2022+ (ongoing)
Operational risk	Low (parallel systems)	High (no legacy fallback)	Medium	Low (parallel systems)
Layer activation	Sequential (L1→L7)	Simultaneous design, sequential launch	Selective then complete	L1,L3,L5 first; L6 deferred (centralized)
Governance approach	DAO phased in	DAO from launch	Centralized then DAO	Centralized (governance debt)
Best suited to	Large incumbents	New market entrants	Mid-size platforms	—
Key risk	Integration complexity	Cold-start problem	Governance debt	Governance debt observed

OpenSea column is derived from empirical case analysis (Section V.E)