
Academia Open



By Universitas Muhammadiyah Sidoarjo

Table Of Contents

Journal Cover	1
Author[s] Statement	3
Editorial Team	4
Article information	5
Check this article update (crossmark)	5
Check this article impact	5
Cite this article	5
Title page	6
Article Title	6
Author information	6
Abstract	6
Article content	7

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Copyright © Author(s). This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licences/by/4.0/legalcode>

Academia Open

Vol. 12 No. 1 (2027): June
DOI: 10.21070/acopen.12.2027.15890

EDITORIAL TEAM

Editor in Chief

Mochammad Tanzil Multazam, Universitas Muhammadiyah Sidoarjo, Indonesia

Managing Editor

Bobur Sobirov, Samarkand Institute of Economics and Service, Uzbekistan

Editors

Fika Megawati, Universitas Muhammadiyah Sidoarjo, Indonesia

Mahardika Darmawan Kusuma Wardana, Universitas Muhammadiyah Sidoarjo, Indonesia

Wiwit Wahyu Wijayanti, Universitas Muhammadiyah Sidoarjo, Indonesia

Farkhod Abdurakhmonov, Silk Road International Tourism University, Uzbekistan

Dr. Hindarto, Universitas Muhammadiyah Sidoarjo, Indonesia

Evi Rinata, Universitas Muhammadiyah Sidoarjo, Indonesia

M Faisal Amir, Universitas Muhammadiyah Sidoarjo, Indonesia

Dr. Hana Catur Wahyuni, Universitas Muhammadiyah Sidoarjo, Indonesia

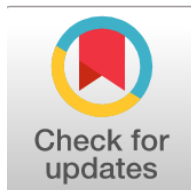
Complete list of editorial team ([link](#))

Complete list of indexing services for this journal ([link](#))

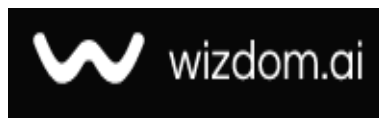
How to submit to this journal ([link](#))

Article information

Check this article update (crossmark)



Check this article impact ^(*)



Save this article to Mendeley



^(*) Time for indexing process is various, depends on indexing database platform

Blockchain-Based Super App Architecture for Cross-Border Integration of Digital Services: A Comprehensive Framework for Global Digital Ecosystems

Nida Muhsin Ali , nida.ali@ntu.edu.iq (*)

Northern Technical University / Al-Dour Technical Institute, Iraq

(*) Corresponding author

Abstract

Cross-border digital service consolidation faces major structural barriers due to regulatory fragmentation, settlement delays, and incompatible IT architectures. Traditional centralized systems operate within isolated frameworks, leading to transaction bottlenecks, liquidity fragmentation, and high operational costs. A comprehensive reference architecture bridging technical, regulatory, and economic interoperability across disparate jurisdictions remains absent in existing literature. This research aims to design a robust six-layer distributed ledger infrastructure integrating digital identity, regulatory compliance, service discovery, and cross-border payment rails. Results demonstrate that combining application-layer routing frameworks, privacy-preserving compliance mechanisms, and stablecoin settlement enables continuous operational efficiency. The novelty lies in incorporating zero-knowledge cryptographic proofs, AI compliance engines, and hybrid governance into a unified multi-chain framework. These findings provide critical implications for financial institutions, technology developers, and policy architects seeking borderless, compliant, and secure digital service ecosystems.

Key Findings Highlights

A six-layer DLT framework resolves cross-border liquidity fragmentation and service isolation.

Zero-knowledge cryptographic proofs enable multi-jurisdictional compliance while preserving privacy.

Stablecoin settlement rails combined with application routers optimize transaction costs and speed.

Keywords: Blockchain Architecture, Super App, Cross-Border Payments, Decentralized Identity, Regulatory Compliance

Published date: 2026-09-26

1. Introduction

1.1 The Rise of Super Apps and Digital Service Integration

The phenomenon of “integrated digital platforms” when dealing with the digitization of global trade has arisen with the development of “super applications.” These features integrate digital payment, retail trading, travel, banking, etc., and build a user interface. WeChat has a near monopoly over digital services in China, and Grab similar in Southeast Asia. However, they are losing their market dominance when they try going to new markets. Services that are centralized are not as easy to integrate as they appear and need a lot of effort (Li et al., 2020).

Sophistication and specialization of the tools used by different companies is the biggest advantage of integrated digital services. However, when integrated digital services go global, they face challenges that are way beyond the capabilities of information technology. Integration of an integrated banking service also requires building different infrastructures and different banking systems that have different settlement systems. SWIFT messaging, ACH, and SEPA clearance systems bring delays and high costs, and can leave capital poorly connected, disconnected, and unavailable (Bank for International Settlements, 2021). It has been found that 40 percent of trading firms do not go to new markets due to the lack of sufficient cross-currency and cross-border payment services. (World Economic Forum, 2021).

These integrated digital systems have an advantage over competitors because they combine several different systems, resulting in a single application that users interact with. This eliminates the need for users to navigate several different apps. While this eliminates the need for users to deal with several apps at home, there are challenges posed by international implementations that legacy IT systems will be unable to resolve. International divisions of the financial system continue to rely on fragmented processes and disconnected settlement systems. SWIFT's messaging network, ACH payment systems, and SEPA's regional clearance systems impact transactions with transaction delays, high transaction costs, and poor cash management (Bank of International Settlements, 2021). The World Economic Forum (2021) reports that 40% of businesses have not entered available markets due to barriers to foreign currency settlement, demonstrating the significance of this barrier.

1.2 Challenges in Cross-Border Digital Service Integration

The expansion of digital technology impacts three different types of problems at the same time and with the same level of importance.

Regulatory Fragmentation: Rules about privacy and data protection vary across different regions and continents. Legislation like the General Data Protection Regulation in the EU and the California Consumer Privacy Act in the USA show differences. These regulations create a barrier to doing business. They inflate costs and constrain the ability to provide services in different countries. There are not enough regulations that fit the needs of disruptive and innovative technologies. The European Blockchain Sandbox, in its report, explains that innovative technologies create an even greater barrier due to uncertainty about how the financial regulations would apply to those technologies (Bird & Bird, 2026).

Scalability: Digital systems that span the globe create a need for digital infrastructure at every layer of the technology stack. One example of infrastructure need is the digital systems that move money, known as digital payment rails. Currently, many of the systems available cannot move money at the speed and volume that the digital economy requires (European Commission, 2020). Digital Currency Hubs can help address the problem of digital payment rails.

Interoperability: There are many sub-systems and components in the digital technology stack. Those sub-systems must be interconnected to create value. Each component must be integrated to the rest. A challenge is that there is no global standard to define how the sub-components and systems must be integrated. One of the challenges is creating harmonious integration between services that are based or hosted in different regions or continents (European Commission, 2020).

Technological Incongruence: Payment processing systems, identity verification systems, and application programming interfaces (APIs) that offer a particular level of service operate on different, technically incompatible systems across international borders, requiring complex and time-consuming bilateral integration that becomes financially and administratively burdensome to maintain over time (Chen & Wang, 2021). Outdated technologies, including centralized databases and management systems used to organize a company's resources, lack the necessary flexibility to support interoperability for the seamless flow of data across company boundaries (Kunduru, 2023). The absence of standard communication protocols to facilitate inter-blockchain data transfer maintains the fragmentation of available liquidity and inhibits the speed and the efficiency of movement of digital assets across several distributed ledger networks (Cosmos Network, 2023).

Confidence Gaps and Centralization Vulnerabilities: Personal data is stored in giant databases by centralized digital services. This means that a single entity gets to decide how to best protect that data. Large amounts of personal data are vulnerable to malicious cyber threats and commercial exploitation. Centralized digital services risk losing user trust when conducting cross border transactions, especially when users are rightfully concerned about the jurisdiction of their data and their right to determine what happens to their data (Tapscott & Tapscott, 2016). Centralized storage of digital identity credentials creates security concerns and goes against more protective data laws.

1.3 Blockchain Technology as a Foundational Solution

Distributed ledger technology can address complex problems through its structural properties of decentralized governance, data permanence, operational transparency, and programmability (Nakamoto 2008; Buterin 2014). Having a distributed structure eliminates single control points and dramatically reduces the chance of unauthorized manipulation of data, while distributed consensus validation protocols guarantee the integrity of data and create transaction trails that can be independently audited (Tian 2016). Self-executing contracts allow complicated multi-stakeholder transactions to be managed automatically without the necessity of centralized intermediaries and significantly reduce administrative costs (Wood 2014).

The employment of distributed ledger technology in the consolidation of cross-border digital services expands beyond the transfer of financial value. User centered decentralized identification systems that adopt Self-Sovereign Identity and the W3C Decentralized Identifier frameworks enable users to retain control of their personal information and decide which information to share with service providers accompanied by an assurance of their authenticity (W3C 2022). This capability is particularly valuable in cross-border settings to assure the divergent requirements of the law for the verification of identity are observed while the interest of the user for privacy is maintained.

Current changes show an increasing level of institutional acceptance of distributed ledger technology for border-spanning transactions. Swift, the top global financial messaging network of more than 11,500 institutions spanning 200 countries, is currently developing a blockchain-based shared ledger for cross border settlement of interbank payments. This project is a major step in integrating distributed ledger technology with existing infrastructure of a major part of the financial system. Along these lines, the Anderson stakeholder coalition project, LINE/Kaia's initiative to integrate stablecoins for payment consolidation, and Grab and StraitsX's Web3 integration illustrate the use of blockchain technology to connect different parts of a super app ecosystem. (The Block, 2025; Yahoo Finance, 2025; Swift, 2026)

1.4 Research Questions and Objectives

The purpose of this study is to understand how a designed distributed ledger infrastructure was able to create a seamless way to integrate digital products and offerings across borders of geopolitics, regulations, and technologies.

The main objectives of the study are outlined below:

1. Create a structural design of a integrated blockchain controlled digital ecosystem that outlines the various levels and bottom building blocks (i.e communication, identify, payments, and service integration).
2. Determine the operational requirements for cross-chain integration infrastructure, and review the available options for inter-chain communication protocols and application-level routing infrastructure.
3. Review the regulatory compliance instruments embedded in Smart Contracts, specifically the integration of Client Due Diligence and Anti-Money Laundering checks, from a legal perspective, in numerous jurisdictions.
4. Evaluate steered governance systems integrating self-regulatory and self-governance frameworks that support compliance and oversight of regulated entities.

1.5 Research Methodology

This study uses a synthetic analysis methodology and combines the study of blockchain foundational principles with the assessment of some of the first integrated digital platforms. The methodology is organized into three phases:

Phase 1 consists of a blockchain Technology analysis. This includes an analysis of consensus mechanisms, self-executing contracts, decentralized identity, and interblockchain communication. This phase is largely based on Nakamoto (2008), Buterin (2014), and Wood (2014) and the W3C Decentralized Identifiers specification (2022).

Phase 2 consists of a Comparative Analysis of available Integrated Digital Platforms. This includes LINE/Kaia's stablecoin-centric operational model, Grab's Web3 settlement infrastructure, Ownera's FinP2P application routing framework, and Swift's blockchain-based shared ledger. Each platform is analyzed pertaining to the design and execution of its architecture, compliance with regulations, and the outcomes of its operation.

Phase 3 consists of the synthesis of an Architectural Framework, consolidating the the theoretical foundations and empirical know-how, and describing a flexible framework comprising six strata with accompanying specifications and instructions for implementation.

1.6 Scope and Limitations

This study focuses on architectural level design principles and high-level structural frameworks for deploying blockchain-enabled integrated digital platforms. This study does not provide detailed descriptions of certain consensus algorithms or cryptographic protocols. The analysis is based on case studies from the Asia-Pacific and European regions. This may limit the generality of the findings to different jurisdictions with dramatically different regulatory frameworks. Given the rapid growth of blockchain technology, some features have a time value. This study includes information published until the mid-2026 time frame. It is possible that some new standards or other new technologies will be published after this time frame.

2. Literature Review

2.1 Blockchain Technology in Digital Service Integration

There has been considerable academic research on use cases for blockchain technology in digital service consolidation. Tapscott and Tapscott (2016) were among the first to note that certain features of blockchain including decentralized governance, immutable data, and traceable transactions have the ability to innovate how businesses operate and reduce reliance on a trusted intermediary. Zheng et al. (2017) provided a comprehensive technical overview of how blockchain technology's architecture and consensus mechanisms lay the foundation for blockchain to be utilized in complex, system-spanning structures.

When blockchain is situated within a digital service context, it is analyzed through the lenses of decentralized applications and self-executing legal agreements. Smart contracts, as coined by Buterin (2014), and elaborated upon by Samantaray (2016), are self-executing agreements that are performed upon satisfaction of predetermined conditions. This functionality is the foundation of systems of integrated platforms. This vision provides a serviceless environment where siloed services and providers are automatically integrated to create a seamless end user experience.

2.2 Supply Chain Traceability and Transparency

The domain of supply chain management has explored blockchain's potential to enhance traceability and transparency in complex multi-party systems. For example, Tian (2016) studied the use of blockchain in one part of the agri-food supply chain to track the origin of products. The TRACE-RICE initiative in Portugal developed a new blockchain-based system to trace the cultivation of rice and integrated capturing farming data via mobile applications and consumer-oriented QR codes (Goncalves et al. 2025). This system successfully integrated agricultural data capturing and consumer transparency using a blockchain system.

The distinction between traceability and transparency made by Cerullo et al. (2016) and Garcia-Torres et al. (2019) has considerable relevance to the integration of digital services across borders. Traceability centers on the internal monitoring of the flow and the information of transactions. Transparency, on the other hand, is the external flow of information to the stakeholders. Blockchain's advantage of offering both functionalities in the same system by virtue of its immutable record-keeping and permission-based access distinguishes it from others.

The continuous existence of multiple, fragmented information systems and the absence of uniform protocols for the exchange of data remains a challenge in the quest for complete traceability in multi-level systems (Hammerer, 2024). Traditional systems based on manual documentation, and centralized repositories and paper records continue to be vulnerable to inaccuracies, deliberate manipulation, significant delays, and a lack of transparency (Olukayode et al., 2023). Blockchain technology overcomes these challenges by using distributed consensus and cryptography (Raikwar et al., 2019).

2.3 Decentralized Identity and Self-Sovereign Identity

Decentralized identity governance plays an integral part in cross border digital service integration. The W3C Decentralized Identifiers (DIDs) technical specification (2022) provides a standardized architecture for verifiable, self-sovereign digital identities that are not controlled by centralized registries or identity suppliers. Zyskind and co-workers (2015) described in detail using blockchain technology for the shielding of personal data by means of decentralized privacy preserving mechanisms, and laid the basis for the methods and techniques that are currently being used for Self-Sovereign Identity.

Self-Sovereign Identity (SSI) paradigms, as researched by Allen and others (2020), give users the ability to own data and decide with whom identity information is shared. DIDs and verifiable credentials along with zero-knowledge proofs create privacy-enabled cross-institutional authentication. In a cross-jurisdictional operating environment, these capabilities fulfill the divergent requirements of numerous regulations whilst maintaining user privacy and data sovereignty.

The focus of recent research in the area of decentralized digital identities has been on cross-border identity verification. A structural type framework developed by the Chinese Academy of Engineering (2025) integrates blockchain, decentralized identity management and dynamic certification of attribute based services along with privacy preservation. This structural type framework suits the areas of deficiency in trust and compliance of traditional centralized systems when used in cross border operations.

2.4 Cross-Border Payments and Financial Integration

Cross-border payment systems have spawned a lot of innovation in the financial services sector using blockchain. The Bank for International Settlements (2021) studied how digital currencies and distributed ledger technology affect central banks and payment systems. They noted how they could optimize processes and reduce the cost of transactions. The European Commission's European Blockchain Services Infrastructure (EBSI) architectural framework is a public sector initiative seeking to develop cross-border delivery of blockchain-based services (European Commission, 2020).

The most substantial development in this sector is Swift's blockchain-based shared ledger. This ledger is currently being designed using a blockchain-based solution on an Ethereum Virtual Machine (EVM) using the Hyperledger Besu infrastructure. This design will support the interoperability of financial institutions' tokenized deposit instruments and enable continuous cross-border payment transactions (Swift, 2026). Nearly 40 financial organizations are including this technology in their services, and the minimum viable product is expected to be available in 2026. This development illustrates how financial legacy systems are rapidly incorporating distributed ledger technologies.

Scholarly works of Irshad et al. (2020) and Bansal et al. (2020) have examined security implications in V2G and energy

trading and have proposed lightweight authentication and key establishment protocols. Blockchain and cryptography demonstrate the need for secure systems in energy trading.

2.5 Regulatory Frameworks and Compliance

The regulation of blockchain services is characterised by complexity and rapid change. The EU's Markets in Crypto-Assets Regulation (MiCAR) provides from a single market perspective a blockchain service framework for crypto assets across all the EU member states, providing legal certainty and consumer protection (Bird & Bird, 2026). The European Blockchain Sandbox has coordinated regulatory discussions among experimental service providers and control agencies across three cohorts. Through these discussions, best practices have been established in the areas of GDPR, AML/KYC and the legal determination of decentralised services.

The General Data Protection Regulation (GDPR) has specific challenges for blockchain services. The principles of data protection are upheld by the framework for personal data management Zyskind et al. (2015), including a decentralised privacy protection scheme. Zero-knowledge proofs, as proposed by Zhou et al. (2021) allow for the disclosure of verified attributes without revealing the underlying data. This framework supports privacy preservation and regulatory compliance.

3. Proposed Architecture: A Six-Layer Framework

This scholar develops a blockchain-enabled integrated platform architecture that contains six layers, each addressing an aspect of cross-border digital consolidated services. This architecture treats layers as modules, and therefore can be adapted and expanded. This architecture can be deployed in phases and can be adapted to fulfill changing business demands.

3.1 Layer 1: Blockchain Infrastructure Layer

An architectural framework must draw upon a multi-chain infrastructure. To support blockchain networks with cross-chain capabilities, this framework must support multiple chains to overcome performances issues and offer customization tailored to use cases.

Multi-Chain and Application-Specific Chains: The framework offers the deployment of “application specific chains” through approaches like Cosmos SDK or Polygon Edge. Chains can be utilized for micro transactions and real time service calls. These specially constructed chains communicate and connect with major networks of Ethereum and Polkadot. These chains will benefit from their security and settlement finality. This paradigm will separate operations. High frequency low value transactions will be processed on high throughput chains, and high value settlements will benefit from the established networks.

Cross-Chain Interoperability: The framework leverages multiple protocols to facilitate the transfer of assets and data across blockchain networks. The Cosmos Network (2023) outlines the Inter-Blockchain Communication (IBC) protocol, a suite of tools for securely sending packets in sequential order between multiple blockchain networks. In addition to IBC, cross-chain interactions can be facilitated by decentralized bridges and multi-signature interactions (Zheng et al., 2017).

The following smart contract implementation demonstrates the multi-chain management capability:

```
solidity
contract MultiChainManager {
    struct ChainInfo {
        string chainId;
        string rpcEndpoint;
        bool isActive;
        uint256 minConfirmation;
    }

    mapping(string => ChainInfo) public registeredChains;
    address public governanceContract;

    event ChainRegistered(string chainId, string rpcEndpoint);
    event CrossChainTransfer(bytes32 transferId, address from, string toChain, uint25
6 amount);

    function registerChain(string memory chainId, string memory rpcEndpoint, uint256
minConfirmation)
        external onlyGovernance {
        registeredChains[chainId] = ChainInfo({
            chainId: chainId,
            rpcEndpoint: rpcEndpoint,
            isActive: true,
            minConfirmation: minConfirmation
        });
    }
```

Figure 1.

```
    function initiateCrossChainTransfer(string memory targetChain, address recipient,
uint256 amount)
        external payable returns (bytes32) {
        require(registeredChains[targetChain].isActive, "Chain not active");
        bytes32 transferId = keccak256(abi.encodePacked(msg.sender, recipient, amount
, block.timestamp, targetChain));
        emit CrossChainTransfer(transferId, msg.sender, targetChain, amount);
        return transferId;
    }
}
```

Figure 2.

3.2 Layer 2: Decentralized Identity Layer

The identity layer implements Self-Sovereign Identity (SSI) principles with built-in regulatory compliance mechanisms. This enables users to create and manage their digital identities without reliance on centralized providers while supporting selective disclosure of verified attributes.

Decentralized Identifiers (DIDs): Following the W3C DID specification (2022), users generate DIDs stored in their digital wallets. These DIDs serve as persistent, globally resolvable identifiers that are not tied to any centralized registry. The DID document contains verification methods and service endpoints for authentication and interaction.

Verifiable Credentials: Certain entities are able to issue verifiable credentials to individuals to confirm specific characteristics and traits (e.g. identity verification and confirmation, age verification, occupation, occupation related authorizations and licenses). Verifiable Credentials are signed digitally and can be autonomously confirmed, without accessing the issuing entity's systems. (W3C, 2022).

Zero-Knowledge Proofs: Zero-Knowledge Proofs (ZKP) allow perform the verification of attributes (including assertions like "I am over 18 years of age", "I am a validated KYC customer", etc.) without the need to disclose any other personally identifiable information. The supporting technology is of extreme importance in the effort to preserve privacy during the implementation of multiple, conflicting, overlapping regulations in various jurisdictions.

3.3 Layer 3: Compliance Management Layer

The compliance strata relies on technology to execute multiple international regulation checks using self-executing contracts and algorithms as rule frameworks. It addresses the challenge of having to comply with various regulations that differ across multiple jurisdictions. This solution helps automate a significant portion of the compliance process by verifying whether a transaction complies with regulations prior to the transaction execution.

Regulatory Requirement Registry: Our system maintains a record of the regulatory requirements for each jurisdiction. The registry includes KYC/AML and transaction value limits, as well as sanctions lists. Regulatory requirements are stored as cryptographic hashes on chain, while the regulatory rules are stored off-chain to preserve privacy and performance.

Automated Compliance: Regulatory compliance for each transaction is verified using the sending and receiving parties' jurisdictions, the value of a transaction, and identity verification.

The following implementation demonstrates automated cross-border compliance:

```
solidity
contract ComplianceManager {
    struct Jurisdiction {
        string countryCode;
        bytes32 regulatoryHash;
        address regulatoryAuthority;
        uint256 lastUpdated;
    }

    struct UserCompliance {
        bool kycVerified;
        uint256 kycLevel;
        uint256 verificationDate;
        address verifier;
        bytes32[] credentials;
    }

    mapping(string => Jurisdiction) public jurisdictions;
    mapping(address => UserCompliance) public userCompliance;
    mapping(bytes32 => bool) public regulatoryRules;

    function verifyTransactionCompliance(
        address sender,
        address receiver,
        uint256 amount,
        string memory fromJurisdiction,
        string memory toJurisdiction
    ) external view returns (bool) {
        require(userCompliance[sender].kycVerified && userCompliance[receiver].kycVerified, "KYC required");
        if (keccak256(abi.encodePacked(fromJurisdiction)) != keccak256(abi.encodePacked(toJurisdiction))) {
```

Figure 3.

```
require(amount <= getCrossBorderLimit(fromJurisdiction, toJurisdiction),  
"Exceeds limit");  
}  
require(!isSanctioned(sender, fromJurisdiction) && !isSanctioned(receiver, to  
Jurisdiction), "Party sanctioned");  
return true;  
}  
}
```

Figure 4.

3.4 Layer 4: Service Marketplace Layer

The service marketplace layer provides an open, decentralized marketplace where service providers can register their offerings through standard smart contracts, and users can discover and subscribe to services directly.

Service Discovery: Services are registered with metadata stored on IPFS for decentralized content storage, with on-chain references enabling verification and discovery (Benet, 2014). Users can discover services based on location, category, ratings, and other attributes.

Standardized Integration Adapters: The architecture provides standardized APIs and smart contract templates that facilitate the onboarding of traditional service providers without requiring complete system reconstruction. This particular functional capacity is necessary for a digital platform to leverage network effects.

Decentralized Service Execution: Service contracts are processed with smart contracts to facilitate payment, service delivery, and the resolution of disputes. Eliminating matching platforms is achieved with service history and reputation which are then made visible and transparent.

3.5 Layer 5: Cross-Border Payment Management Layer

This layer of the payment structure implements payment networks and systems. This layer excels at executing instantaneous payments. It provides a 24/7 settlement system.

Stablecoin Integration: The system allows users to transact in stablecoins. Stablecoins are a predictable form of value transfer, unlike cryptocurrency. Because stablecoins are tied to the swap currencies, there is no volatility. (Bank for International Settlements, 2021).

Multi-Currency Payment Routing: This payment routing system calculates the best possible payment path based on cost, speed, and adhering to the law. This system operates within a multi-chain structure and executes payments through the most efficient system available.

Automated Currency Conversion: Integration with Chainlink price feeds enables automated currency conversion, as implemented in the following smart contract:

```
solidity
contract CrossBorderPayment {
    function convertCurrency(
        uint256 amount,
        string memory fromCurrency,
        string memory toCurrency
    ) internal view returns (uint256) {
        address fromFeed = supportedCurrencies[fromCurrency].priceFeed;
        address toFeed = supportedCurrencies[toCurrency].priceFeed;
        AggregatorV3Interface fromPriceFeed = AggregatorV3Interface(fromFeed);
        AggregatorV3Interface toPriceFeed = AggregatorV3Interface(toFeed);
        (, int256 fromPrice, , ) = fromPriceFeed.latestRoundData();
        (, int256 toPrice, , ) = toPriceFeed.latestRoundData();
        return (amount * uint256(fromPrice)) / uint256(toPrice);
    }
}
```

Figure 5.

3.6 Layer 6: Unified User Experience Layer

The uppermost layer provides a uniform user interface that spans all incorporated services. This layer manages identity, locates services, initiates transactions, and offers user preferences.

Single Sign-On: Users log in once to their DID wallet and maintain uninterrupted connection to all services. This mitigates the burden of multiple logins to individual services, and also maintains security through cryptographic challenges.

Consent Management: Users choose whether to give individual services data sharing permissions using the integrated consent manager. This manager shows the data collection and use practices to provide users with the information necessary to adjust their consent to data use.

Cross-Service Workflows: This UI is capable of overseeing long and complicated transactions across various services, while instructing smart contracts to command an ordered sequence of services and the transfer of value.

4. Operational Scenarios and Use Cases

4.1 Cross-Border Travel Booking Scenario

To illustrate the operational capabilities of the architectural framework, imagine a user from Saudi Arabia booked accommodation and an airline ticket using the integrated digital platform.

Step 1: Identity Confirmation: The user logs in to their DID wallet for identity confirmation. Their identity was previously verified by a licensed KYC provider in Saudi Arabia. The verified credentials were stored on the blockchain. This verification is accepted in all the participating countries through the mutual recognition framework of the compliance layer.

Step 2: Service Research: The user researches travel related services. The service marketplace contains hotels and airlines in Malaysia who have been rated and verified on-chain, and are registered in the marketplace. The service marketplace also factors in the preferences of the user and the regulatory compliance of the User's destination country when offering service discovery.

Stage 3: User Booking Request Verification and Price Conversion to Stablecoin:

- A user booking request is verified by a smart contract, which converts the price to stablecoins and records the request. Additionally, the smart contract verifies the user's DID.
- Stablecoins are a form of cryptocurrency backed by real world assets and the price of stablecoins fluctuates very little.
- The contract verifies that the Malaysian service provider holds a valid license (recorded on the governance ledger).
- Regulatory compliance is verified for the cross-border transaction, including KYC status verification and sanctions

list checks.

Stage 4: Payment Execution: Once the service provider confirms, the smart contract initiates payment, transfers the commission to the platform, and generates a digital receipt (NFT) in the form of booking confirmation to the user.

Stage 5: Settlement and Data Privacy: The entire transaction is recorded on the blockchain, and sensitive personal data such as passport numbers is encrypted and stored off-chain and its hash is stored on-chain to ensure data integrity. This keeps peace in data privacy while allowing verifiability of the transaction.

4.2 Cross-Border Remittance Scenario

The framework includes cross-border remittance applications, which are high-value use cases for blockchain integrated systems.

1. A EU-based migrant worker sends remittances to their family in the Philippines through a super app.
2. The compliance layer verifies that neither of the two parties involved in the transaction is on a sanctions list and that the transaction amount falls within the cross-border limits supported by both jurisdictions.
3. The payment routing system selects the best route among available options, which in this case, would be the conversion of EUR to USDC, use of the most efficient blockchain to send them, and conversion of the USDC to PHP upon receipt.
4. The transfer is executed by the smart contract, which involves a Forms Traditional banking system takes days to process cross border transactions, and the cost is also not fixed. Smart contracts, on the other hand, execute transactions within minutes, and the fees are known to both the sender and receiver before the transaction is executed.
5. The recipient is receiving a notification, once the transaction has been settled. The recipient can withdraw the funds by using their connected bank account or digital wallet.

4.3 Institutional Integration: Swift's Blockchain Ledger

Swift's blockchain-based shared ledger initiative closely relates to the other concepts found in the architectural framework. According to Swift (2026), the ledger will be built using an Ethereum Virtual Machine-based architecture and Hyperledger Besu. This will allow the ledger to facilitate 24/7 cross-border payments using tokenized deposit instruments. The design of the ledger features:

- Integration with existing systems: The ledger uses traditional correspondent banking rails and can be adopted step-by-step without having to replace systems.
- Multiple assets settlement: The ledger can be used to settle digital cash in different forms, such as tokenized deposits, stablecoins, or perhaps central bank digital currencies.
- Security and resilience: Swift will control and run the ledger, and will also control the orchestration of transactional workflows and the coordination of the interbank framework. However, banks will have full control of their assets and funding.

This validates the architectural principles of this research and shows the combination of traditional financial infrastructures with distributed ledger technology.

5. Technical Implementation and Requirements

5.1 Consensus Mechanisms and Network Architecture

The framework allows multiple consensus mechanisms to be used based on the needs of the particular use case. For cross-border payment use cases, framework support for the variants of Byzantine Fault Tolerance (BFT), including Practical Byzantine Fault Tolerance (PBFT) and their derivatives, allows for sufficient throughput and finality (Zheng et al., 2017). For use cases of compliance verification and identity management, proof-of-authority consensus might be the best choice given the regulatory nature of these functions.

Network Governance: The architecture implements a hybrid model of governance that balances the need for decentralization within the constraints of existing regulations. Within the architecture, regulatory constraints are addressed through immutable smart contract rules. Decentralized governance mechanisms are used to make decisions regarding admission of members and upgrades to the protocol.

5.2 Privacy and Data Protection Mechanisms

Architectural Framework and Privacy- Preserving Technology: The framework comprises the following privacy-preserving technologies:

- **Zero-Knowledge Proofs:** Zero-knowledge proofs constitute a fundamental component of privacy-preserving selective disclosures of verified attributes as articulated by Zhou et al. (2021). Privacy-enhancing attributes are required to facilitate compliance with privacy regulations.
- **Homomorphic Encryption:** For scenarios requiring computation on encrypted data, homomorphic encryption

enables secure analytics while maintaining data confidentiality (Zyskind et al., 2015).

- **Secure Multi-Party Computation:** For collaborative analytics across organizational boundaries, secure multi-party computation enables computation on distributed data without exposing raw inputs.

Data Minimization: Data minimization principles are adopted in the architecture by collecting and processing data for the operation for which they are required. Personal data is anonymized where feasible, and data is subject to temporal constraints on storage and usage.

5.3 Interoperability Requirements and Solutions

Architecture supports several cross-chain protocols through the following:

Inter-Blockchain Communication (IBC): According to Cosmos Network (2023), IBC uses semantics for cross-chain packet delivery across various incompatible chains, with HTLC (Hashed Timelock Contract) used for the commitment. This protocol can be used for both asset transfer and data exchange across Cosmos SDK-based chains.

Decentralized Bridges: For accessing Ethereum Virtual Machine (EVM)-based chains, a set of decentralized bridges allows trust-minimized asset transfers using multi-signature or threshold signature.

Application-Layer Interoperability: The Ownera FinP2P router model presents application-layer interoperability via routers that facilitate transactions across blockchains and smart contracts, as well as legacy systems (Ownera, 2025). This model provides scalability through the Plug-and-Play approach of enabling connectivity among many clients, suppliers, service providers, and technology partners.

5.4 Security Considerations

Cryptographic Key Management: Securely stored private keys must have adequate access controls and back up. For higher level function control, the use of multi-signature wallets is recommended.

Smart Contract Security: Security audits of smart contract code must be extensive, and formal verification should be done where applicable.

Network Security: The multi-chain architecture must defend against attacks like denial of service and routing attacks. Defenses must also be in place to defend against vulnerabilities in the consensus mechanism.

NSTIADS: Network intrusion detection and network systems are required to defend against attacks, even those that occur while the systems are idle. An Early Warning System protects against network attacks and should be implemented as part of the multi-chain defense.

6. Regulatory Compliance and Governance

6.1 Compliance with Multi-Jurisdictional Regulations

The architectural framework uses built-in compliance mechanisms and hybrid governance models to deal with regulatory fragmentation.

GDPR and Data Protection: Compliance with GDPR and the equivalent systems is satisfied through:

- **Data minimization:** Only essential data is collected and processed for each use case.
- **Purpose limitation:** Data is used only for specified, explicit purposes.
- **Storage limitation:** Data is retained only as long as necessary for the purpose.
- **Privacy by design:** Privacy protections are embedded in the system architecture.
- **Right to Erasure:** Mechanisms for data deletion are provided through off-chain storage with on-chain verification hashes, satisfying legal requirements while maintaining blockchain integrity.

Eligibility for Financial Regulation: The architecture supports compliance with AMLR, MiCAR, and their respective equivalents, by:

- **Automated KYC/AML verification:** Smart contracts verify KYC/AML compliance before executing transactions.
- **Sanctions list checking:** Automated verification against sanctions lists is integrated into transaction processing.
- **Transaction Monitoring:** By use of on-chain analysis fraud patterns are highly detectable.
- **Regulatory Reporting :** Automated generation of reports required by financial regulators.

6.2 Hybrid Governance Model

The architecture combines decentralized governance with regulatory oversight. This model is unique. Decentralized governance allows for the making of strategic decisions, including the proposal and voting on changes to protocol, management of fees, and membership admission audits. Token-holders participate in governance through voting. The voting power of token-holders is based on their stake.

Regulatory oversight is achieved through regulatory compliant smart contract systems. Compliance is verified on chain through the use of cryptographic verification of credentials and signatures. Regulators can be granted observer or verification permissions within the system without impacting system decentralization.

The European Blockchain Sandbox has found the European Cooperative Society (SCE) with support from Bird & Bird to be a legal structure for DAOs in the financial sector, and serves as the basis for legal structuring. It enables financial sector regulations to be satisfied while preserving decentralized governance.

7. Case Studies and Comparative Analysis

7.1 LINE/Kaia Stablecoin Super App

The LINE/Kaia initiative offers the first substantial commercial use of blockchain-based super apps (The Block, 2025). The project intends to use LINE's user base of 200 million to build a stablecoin-based payment system in order to unite payment systems in Asia. The project uses the following key architectural components:

This structure validates the principle of cross-border service integration regardless of fragmented payment systems with stablecoin-based settlement.

7.2 Grab Web3 Settlement Layer with StraitsX

Grabs partnership with StraitsX is a large step towards the building of a Web3 super application (Yahoo Finance, 2025). The project is focused on the development of a Web3 settlement layer within the Grab super application across eight countries in Southeast Asia. The project includes the following key features:

- **Stablecoin-settlement:** The transfer of value via stablecoins pegged to the major currencies in the world.
- **Efficient Transactions:** Transactions will be quick and efficient, all while users interact with payment systems they are familiar with.
- **Unified payments:** Simplifying payment methods across multiple countries with fragmented payment systems in Asia.
- An embedded Web3 wallet: Ability to hold and transact with stablecoins within the application.
- **Programmable payments:** Enabling automated payment execution based on predefined conditions.
- **Cross-border payment optimization:** Reducing reliance on expensive card networks and traditional banking rails.

The challenges posed by deploying blockchain-based super apps become increasingly apparent when scaling across millions of users and differing regulatory environments, as shown by this implementation.

The super app was deployed with a focus on challenges found on the blockchain while reaching millions of users. Building the super app required work that led to engaging millions of users every day. Deploying the super app also focused on engaging millions of users.

7.3 Ownera FinP2P Application Router

The Ownera FinP2P model presents a financial services-led application orchestration layer for blockchain services (Ownera, 2025). Some key architectural features include:

- **Application Orchestration Router:** Easing the integration of SuperApps across different blocks, partners, and markets without the need for custom integrations.
- **Cross-Chain and Legacy Integration:** Integrating any combination of blocks, smart contracts, and legacy systems via adapters.
- **Network Effects:** Scalable Lag and Servicing plug-and-play integrations across multiple clients, and service providers.

This model illustrates the need for application-level interoperability for the purpose of integrating scalable cross-border digital services.

7.4 Comparative Analysis

Analysis of these deployments shows common traits of successful deployment.

Shared edge-case deployment success factors:

A deployment tenant fails to launch rapidly (1) when additional care must be

DimensionLINE/KaiaGrab/StraitsXOwnera FinP2PSwift Ledger

Primary FocusConsumer PaymentsConsumer ServicesInstitutional FinanceInterbank Payments

Settlement AssetStablecoinsStablecoinsMulti-AssetTokenized Deposits

Interoperability ModelLimited Cross-ChainWeb3 IntegrationApplication RouterEVM-Compatible

Regulatory ApproachEmbedded ComplianceJurisdictional ComplianceInstitutional ComplianceGlobal Standards

ScaleRegional (Asia)Regional (SE Asia)InstitutionalGlobal

There are shared architectural features across deployments including the settlement and regulatory integration within the implications of stablecoins. The notable divergences are the expected user bases (retail versus institutional), the regulatory environments, and the levels and the manner of interoperability.

8. Challenges and Mitigation Strategies

8.1 Technical Challenges

Scalability: Each blockchain has limitations in terms of how much the system can scale.

Solutions include:

- **Layer 2 scaling:** Rollups and state channels can be used to process a large number of transactions.
- **App-chain architecture:** App-chain architecture allows you to run additional chains to perform specialized services with settlement on the main chain.
- **Transaction batching:** Transactions can be grouped to create efficiency.

Transaction Costs: Currently, network fees can be high when conducting cross border transactions. There are some ways to mitigate the effects that include:

- Fee optimization: Selecting optimal chains and times for transaction execution.
- Stable coin efficiency: Using stable coins to minimize settlement costs.
- Smart contract optimization: Minimizing gas consumption through efficient contract design.

Privacy Preservation: The transparent nature of public blockchains conflicts with privacy requirements. Solutions include:

- Zero-knowledge proofs: Enabling private verification of public commitments.
- Off-chain data storage: Storing sensitive data off-chain with on-chain verification hashes.
- Encrypting users' data and allowing computation on encrypted data through homomorphic encryption, and secure multi-party computation.

8.2 Regulatory Challenges

Covering more than one jurisdiction with many different regulatory requirements is hard. Ways to address the issue include:

- Modular compliance framework: Enabling jurisdiction-specific compliance rules.
- Regulatory sandboxes: Engaging with regulators through controlled environments.
- Standardization initiatives: Participating in international standardization efforts.

Legal Status of Decentralized Organizations: The legal qualification of DAOs and decentralized services under financial regulation remains uncertain in many jurisdictions. According to the European Blockchain Sandbox (Bird & Bird, 2026), there are domains that require further elaboration, which include:

Classification of wholly decentralized service offerings: Ascertaining whether, and to what degree, decentralized services fall within the purview of financial regulatory frameworks.

- **Legal accountability:** Formulating liability structures applicable to decentralized operational environments.
- **Regulatory circumvention:** Mitigating the exploitation of divergent regulatory provisions across different jurisdictions.

8.3 Adoption Challenges

Building Super Apps: **Creating Super Apps relies on critical mass of users and service providers. There are several ways to build Network Effects, one of which is:**

- **Phased deployment:** Starting with high-value use cases and expanding progressively.
- Strategic partnerships: Partnering with established platforms for user acquisition.
- Incentive mechanisms: Using token incentives to encourage early adoption.
- User Education: Blockchain-based services require user understanding that is not universally present. Approaches include:
 - Intuitive interfaces: Hiding blockchain complexity behind familiar user experiences.
 - Phased user adoption: Introducing blockchain functionalities incrementally.
 - Learning materials: Furnishing easily accessible educational content.
 - Integration with Established Systems: Conventional service providers run legacy infrastructures that are not inherently blockchain-compatible. Integration strategies encompass:
 - Standardized adapters: For “plug-and-play” connectivity for existing systems.
 - API-driven connectivity: Facilitating integration via standardized application programming interfaces.
 - Incremental migration: Supporting a progressive shift from legacy infrastructures to blockchain-enabled operations.

9. Future Research Directions

9.1 Technical Research Priorities

Quantum-Resistant Cryptography: Potential longterm issues related to quantum computing exist for current cryptographic approaches. Current focus areas:

- **Post-quantum algorithms:** Creating and fine-tuning algorithms that resist quantum attacks.
- Hybrid classical-quantum versions: **methods of preserving security while shifting to quantum-resistant systems.**
- Performance Optimization: making post-quantum algorithms work well on low resources devices. **Lightweight Cryptographic Protocols: Edge and mobile devices need light crypto protocols built for low computing power. Research directions:**
 - Lightweight zero-knowledge proofs: Optimizing ZKP protocols for mobile environments.
 - Energy-efficient consensus: Developing consensus mechanisms with minimal energy requirements.
 - Privacy-preserving protocols: Enhancing privacy while maintaining computational efficiency.
 - Interoperability Standards: Standardization of cross-chain communication is essential for ecosystem growth. Research needs include:
 - Application-layer interoperability: Standardizing service discovery and invocation across chains.
 - Identity interoperability: Enabling cross-chain identity verification.
 - Regulatory interoperability: Standardizing compliance verification across jurisdictions.

6.2 (Should be 9.2) Regulatory and Governance Research

International Coordination for Cross Border Blockchain Services:

The use of blockchain across borders shows the importance of international collaboration. Topics for further study are:

- a) Comparative Regulatory Analysis: finding similarities and differences within different jurisdictions.
- b) Best Practices for Regulatory Sandboxes: design of regulatory sandboxes for directed innovation.
- c) Legal Entity Structures: selection of the appropriate forms of legal entities for decentralized organizations.

Reconciliation of Transparency and Privacy: continue research efforts.

Directions include:

- Privacy-enhancing technologies: Research on designing practical solutions for Zero-Knowledge Proofs, Homomorphic encryption and Secure MPC.
- Compliance automation: Automating compliance verification while preserving privacy.
- Data sovereignty: Empowering users to control cross-border data flows.

6.3 (Should be 9.3) Implementation Research

- Pilot Deployments: To advance the architecture, real-world deployments are absolutely necessary. The following

types of implementation research are needed:

- Large-scale testbeds: Deployment of architecture in controlled environments that involve multiple jurisdictions.
- Longitudinal studies: Evaluating performance and user acceptance over extended periods.
- Use case expansion: Testing the architecture across diverse application domains.

Cost-Benefit Analysis: An exhaustive economic assessment is required for supporting investment decisions. Some research lines include:

- Quantitative ROI frameworks: Building measurements for blockchain investments.
- Comparative cost analysis: Analyzing blockchain-based services and their traditional equivalents.
- Value quantification: Extracting the value of transparency, immutability and decentralization.

10. Conclusions

This research offers a complete architectural plan for a blockchain-based super app. This app allows users to span multiple jurisdictions and use digital services that are currently fractured. This research addresses the challenges of finance system fragmentation and the lack of interoperability among blockchain networks and contradictory regulations across different countries.

Summary of Key Findings:

1-Architectural Integration: Developing seamless cross border digital services necessitates infrastructural, identity, compliance, service orchestration, payment, and user experience layers in a digital service architecture. The proposed six-layer framework provides integrated solutions for all the requirements.

2-Pillars of Interoperability: Integration of digital services across borders requires three interrelated building blocks; economic integration (stablecoin rail), regulatory integration (compliance mechanism) and technical integration (application-layer routing protocols).

3-Regulatory Embedment: Cross jurisdiction flexibility requires design of compliance systems and mechanisms using smart-contracts and zero-knowledge proofs.

4-Hybrid Governance: Regulatory oversight and decentralization can coexist in a combination of regulatory oversight of smart contract based systems with a range of governance mechanisms.

5-Institutional Convergence: Initiatives by institutions like Swift are building traditional financial systems with distributed ledger technology. This validates the principles of architecture presented in this research.

Implications:

This research gives policymakers a way to develop appropriate policies for services that use blockchain and protect consumers when innovative ideas develop in a competitive marketplace. For financial institutions, the functionality provides a framework for the integration of blockchain with existing systems. For tech developers, this research provides sample code along with a design for the integration of blockchain services.

Limitations:

Due to most examples coming from Asia-Pacific and European regions, generalization beyond contexts containing significantly divergent regulatory frameworks may be problematic. Because some blockchain standards evolve quickly, certain technical specifications may become outdated. Research that covers a greater geographic span and incorporates the latest technical innovations is required for the future.

Final Remarks:

The blockchain-based unified platform is a substantial improvement on how services can be integrated across the web. Integrating services has been primarily focused on architecture that simply brings together disparate services. This architectural model proposes a way to seamlessly conduct transactions and interactions with other parties across borders within a trusted, digital ecosystem. Realising this vision will require prolonged collaboration of regulators, technologists, finance and oversight institutions. The proposed architectural design provides the reference for such collaboration to create the next generation of international, protected digital services that comply with regulations.

References

1. D. Allen, C. Berg, S. Davidson, M. Novak, and J. Potts, "International policy coordination for blockchain governance," *Policy and Society*, vol. 39, no. 4, pp. 555-573, 2020.
2. Bank for International Settlements, "Annual Economic Report - Chapter III: Central banks and payments in the digital era," BIS, 2021.
3. J. Benet, "IPFS - Content addressed, versioned, P2P file system," arXiv preprint arXiv:1407.3561, 2014.

4. Bird & Bird, "The European Blockchain Sandbox Report," Bird & Bird LLP, 2026.
5. V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014.
6. V. Cerullo, M. J. Cerullo, and D. Richards, "Supply chain transparency and blockchain technology," *Journal of Business Ethics*, vol. 139, no. 2, pp. 321-335, 2016.
7. Y. Chen and H. Wang, "Challenges and opportunities for global super apps," *IEEE Internet Computing*, vol. 25, no. 4, pp. 72-79, 2021.
8. Chinese Academy of Engineering, "A framework design for decentralized digital identity across borders," *Chinese Journal of Engineering Science*, vol. 27, no. 1, pp. 112-125, 2025.
9. Cosmos Network, "IBC Protocol: Interoperability for heterogeneous blockchains," Official Documentation, 2023.
10. Deloitte, "The Super App phenomenon: How consumers are redefining the engagement ecosystem," *Insights Report*, 2022.
11. European Commission, "European Blockchain Services Infrastructure (EBSI) Architecture," EC Technical Report, 2020.
12. S. Garcia-Torres, L. Albareda, M. Rey-Garcia, and S. Seuring, "Traceability for sustainability: A framework for responsible supply chain management," *Journal of Business Ethics*, vol. 159, no. 4, pp. 973-989, 2019.
13. C. Goncalves, J. Fernandes, and C. Brites, "Blockchain-enabled traceability in the rice supply chain: Insights from the TRACE-RICE project," *Foods*, vol. 14, no. 21, p. 3711, 2025.
14. M. Hammerer, "Information fragmentation in global supply chains: Challenges and solutions," *Supply Chain Management Review*, vol. 28, no. 3, pp. 34-42, 2024.
15. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for Energy Internet-based vehicle-to-grid technology framework," *IEEE Transactions on Industrial Applications*, vol. 56, no. 4, pp. 4425-4435, 2020.
16. S. Kunduru, "Enterprise resource planning systems in supply chain management," *Journal of Supply Chain Management*, vol. 61, no. 2, pp. 187-201, 2023.
17. Y. Li, Z. Wang, and X. Zhang, "Super apps in Asia: A comparative analysis," *Journal of Digital Commerce*, vol. 19, no. 3, pp. 156-172, 2020.
18. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin White Paper, 2008.
19. Olukayode, F. Adebayo, and O. Ogunyankinnu, "Traditional documentation in supply chains: Limitations and vulnerabilities," *International Journal of Logistics Management*, vol. 34, no. 5, pp. 1345-1365, 2023.
20. Ownera, "FinP2P SuperApps Architecture Documentation," Ownera Technical Report, 2025.
21. M. Raikwar, S. Mazumdar, and S. Ruj, "A survey of blockchain-based smart contracts: State of the art and future directions," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3412-3443, 2019.
22. Swift, "Swift's blockchain-based shared ledger progresses to MVP implementation," Swift News Release, 2026.
23. D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, New York, NY, USA: Penguin, 2016.
24. The Block, "LINE and Kaia to launch stablecoin superapp for cross-border payments," *The Block*, Sep. 2025.
25. F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Serv. Syst. Serv. Manag.*, 2016, pp. 1-6.
26. W3C, "Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations," W3C Recommendation, 2022.
27. G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," Polkadot White Paper, 2014.
28. World Economic Forum, "The global governance of blockchain: A framework for evaluation," White Paper, 2021.
29. Yahoo Finance, "Grab signs Web3 deal with StraitsX to bring stablecoin payments into its super-app," Yahoo Finance, Nov. 2025.
30. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE 6th Int. Congr. Big Data*, 2017, pp. 557-564.
31. Zhou, F. Tofigh, M. Piccardi, M. Abolhasan, D. Franklin, and J. Lipman, "Secure multi-party computation for machine learning: A survey," *IEEE Access*, vol. 12, pp. 53881-53899, 2021.
32. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security and Privacy Workshops*, 2015, pp. 180-184.