

PEER REVIEWED RESEARCH

OPEN ACCESS

ISSN Online: 2516-3957

ISSN Print: 2516-3949

[https://doi.org/10.31585/jbba-9-2-\(10\)2026](https://doi.org/10.31585/jbba-9-2-(10)2026)

Evaluating Blockchain-Based Consortia for Enhancing Open Banking and Banking-as-a-Service Ecosystems

Irem Akinci

Bahçeşehir University, Istanbul, Türkiye

Correspondence: iremakinci.legal@outlook.com**Received:** 15 April 2026 **Accepted:** 6 July 2026 **Published:** 24 August 2026

Abstract

The financial sector is experiencing a profound transformation driven by innovations such as open banking and Banking-as-a-Service (BaaS), which aim to create more accessible, interoperable, and innovative financial ecosystems. Despite their potential, these models face significant challenges related to trust, data integrity, interoperability, and operational efficiency across multiple institutions. Blockchain technology offers a decentralised infrastructure that addresses these challenges by ensuring trust, transparency, traceability, and transaction integrity, whilst enabling the formation of blockchain-based consortia. This study investigates the applicability of blockchain in enhancing open banking and BaaS frameworks, focusing on the integration of APIs, smart contracts, and decentralised governance mechanisms. By analysing sectoral applications and potential use cases, the study highlights how blockchain-enabled consortia can provide a robust, scalable, and secure foundation for next-generation financial services. The findings suggest that the integration of blockchain not only facilitates innovation and collaboration but also contributes to systemic reliability and sustainable financial transformation.

Keywords: *Open banking, Banking-as-a-Service (BaaS), Blockchain, APIs, Smart contracts.*

JEL Classifications: *A40, B47, D53, 001, D02*

1. Introduction

Improving user access to financial services, automating time-consuming processes, and enabling services that can be accessed from anywhere have become fundamental objectives of digital transformation in the financial sector. This transformation is actively supported by various stakeholders, among which financial technology (FinTech) companies play a prominent role.

With the increasing involvement of FinTech companies, the provision of banking services has undergone a further shift towards more open and integrated models. This evolution has led to the emergence of the open finance paradigm, which enables the sharing of financial data with multiple service providers based on user consent, as well as to the concept of embedded finance, which refers to the integration of financial products into the user experience of non-bank platforms. Within the scope of this study, open banking, as a sub-domain of open finance, and Banking-as-a-Service (BaaS), as a component of embedded finance, are examined.

In this study, Open Banking is considered as a framework that enables authorised third-party providers to access customer

financial data and selected banking functionalities through secure interfaces. This access allows consumers to perform banking-related activities digitally without the need for physical branch visits, often via non-bank entities such as FinTech service providers.

BaaS approach represents a significant transformation in the way financial services are delivered, enabling greater flexibility and accessibility. Within this model, banks expose their infrastructure and data through APIs, allowing “bank-like services to be used outside bank-owned channels.” As a result, financial products can be seamlessly integrated into various digital platforms, contributing to a more cohesive, efficient and customer-centred user experience [1]. Open banking and BaaS ecosystems are inherently shaped by regulatory frameworks that promote data sharing whilst simultaneously imposing strict requirements on data protection and privacy. The increasing reliance on customer-permissioned data exchange across multiple actors introduces challenges related to secure data management and regulatory compliance. Moreover, traditional banking infrastructures, often characterised by siloed data architectures and legacy systems, create additional complexity in integrating and processing data

consistently across organisational units. These structural limitations may hinder effective data governance, raise concerns regarding operational resilience, and complicate the implementation of cohesive data strategies in open finance environments [2]. Similarly, Know Your Customer (KYC) processes, which constitute a significant operational burden within open banking and BaaS structures, play a critical role in the prevention of financial crime and the ensuring of regulatory compliance.

In addition, this study examines blockchain technologies and evaluates whether consensus-based processes in multi-participant structures, such as open banking and BaaS, can be supported through blockchain-based infrastructures by leveraging the decentralisation, immutability, transparency, and traceability characteristics of blockchain. The literature includes studies suggesting that certain operational processes required for open banking and BaaS can be supported through consortium-based blockchain infrastructures. Whilst a growing body of research has examined open banking and blockchain technologies, these topics are often addressed separately or from limited perspectives. This study is motivated by the need to bring together these strands of literature and to provide a more integrated evaluation of how blockchain-based approaches can address the practical challenges of open banking and BaaS ecosystems.

The following research questions guide this study:

RQ1: Which challenges in open banking and BaaS ecosystems can be effectively addressed through blockchain-based consortium architectures compared to traditional API-based systems?

RQ2: How can key challenges in open banking and BaaS (e.g., trust, data integrity, interoperability, and regulatory compliance) be systematically mapped to the core capabilities of blockchain technologies?

RQ3: How do different consortium governance structures and consensus mechanisms influence performance, security, and operational risk in blockchain-based financial ecosystems?

2. Background

This section establishes the conceptual foundations of the study by clearly defining and differentiating the key concepts that underpin open banking and BaaS ecosystems.

To establish this conceptual foundation, open finance is first introduced as the overarching framework within which open banking is positioned. Open finance is a framework that enables the sharing and access to financial data across a wide range of financial services – such as banking, savings, credit, insurance, and investments – through secure systems, with the customer's consent, in order to support the provision of innovative financial products and services [3]. Within this broader framework, open banking is defined as a collaboration model in which bank customer data is shared with third parties via APIs [4]. Open Banking extends beyond the introduction of new products by enabling existing financial services to be delivered through new channels and in collaboration with third

parties, thereby fostering a broader ecosystem structure. Within this paradigm, banks retain the flexibility to determine their level of openness and the type of value they create, depending on strategic, organisational, and cost-related considerations. They may also choose to embed their services into the business models of other actors [5].

Complementing this perspective, embedded finance can be understood as the integration of financial products and services into non-financial customer journeys or digital platforms [6]. In embedded finance applications, financial functions are no longer limited to traditional banking institutions but are carried out through interconnected systems involving multiple stakeholders. In this context, BaaS can be understood as an infrastructure model that enables this transformation by allowing financial institutions to deliver their services through modular and interoperable interfaces. These developments coincide with the emergence of distributed and automated financial systems, where transaction processes, data sharing, and compliance mechanisms are increasingly integrated into the core technological infrastructure, reducing operational challenges and enabling more seamless financial service delivery [7].

Based on these definitions, whilst open finance and embedded finance encompass a broader range of models and sub-layers, this study focuses on open banking as a data-sharing framework and BaaS as an infrastructure layer enabling embedded finance applications. This scoped approach provides a focused foundation for evaluating consortium-based blockchain models within these ecosystems.

3. Methodology

A. Literature Selection and Scope

This study is based on a review of academic literature, regulatory publications, and industry reports related to open banking, Banking-as-a-Service (BaaS), blockchain technologies, and consensus mechanisms. Relevant literature was identified through structured searches conducted across Google Scholar, SSRN, and arXiv, supplemented by institutional, regulatory, and industry publications obtained from OECD, FCA, Springer, McKinsey, and related technical sources, covering the period between 2008 and 2026. The review period begins in 2008 to capture the emergence of foundational blockchain literature following the publication of Nakamoto's Bitcoin framework, which significantly influenced subsequent developments in distributed ledger technologies and consortium-based blockchain architectures.

The search process focused on studies, regulatory reports, and technical publications related to open banking, BaaS, blockchain technologies, and APIs. The primary search strings included combinations of "Open Banking," "Blockchain," "Open Banking," "APIs," "Banking-as-a-Service (BaaS)," "Blockchain," and related keyword variations. The initial search yielded approximately 120 records. Following screening and relevance assessment, 53 records were excluded based on the predefined inclusion and exclusion criteria. The remaining

sources were reviewed in detail and informed the conceptual and comparative analysis presented in this study. Of these, 31 of the most relevant sources were directly cited and included in the reference list, whilst additional sources were used as supporting background material during the literature review process.

The screening process applied predefined inclusion and exclusion criteria. Sources were included if they provided direct conceptual, technical, empirical, or regulatory insights into open banking, BaaS, blockchain technologies, APIs, or their integration within financial services. Peer-reviewed articles, regulatory reports, and technical publications with substantial academic and technical relevance were retained. Records were excluded if they were duplicate entries, outside the scope of the study, lacked sufficient academic or technical contribution, or focused exclusively on public blockchain networks without relevance to financial-sector permissioned or consortium blockchain architectures.

B. Analytical Approach

This study adopts a structured, problem-driven analytical approach to evaluate the applicability of blockchain technologies in open banking and Banking-as-a-Service (BaaS) ecosystems. The analysis proceeds in several stages.

First, the key concepts and architectural characteristics of open banking, BaaS, and blockchain systems are examined to establish a conceptual foundation. Based on this foundation, the main challenges within open banking and BaaS ecosystems are identified and categorised.

These challenges are then used as evaluation criteria, reflecting the core problem areas that any proposed solution must address. Subsequently, the fundamental capabilities of blockchain architectures are analysed, and a systematic mapping is established between the identified challenges and relevant blockchain features.

Building on this mapping, a multi-criteria evaluation framework is developed to assess the suitability of different architectural approaches. To support a structured comparison, each criterion is assessed using a qualitative three-level scale (1–3), where 1 indicates limited suitability, 2 indicates moderate suitability, and 3 indicates strong suitability.

C. Scope and Platform Selection

Following this approach, suitable blockchain platforms are evaluated for implementing the proposed model, taking into account factors such as performance, security, transaction efficiency, and consensus mechanisms. Within the context of open banking and BaaS ecosystems, particular emphasis is placed on the transparent, auditable, and immutable recording of regulated consent management and data access processes. Accordingly, platforms such as Hyperledger Fabric and Corda are selected due to their widespread adoption in enterprise and financial use cases, and are analysed in terms of their suitability for supporting consortium-based financial networks.

D. Validity and Limitations

This study adopts a qualitative and conceptual approach based on the analysis of existing literature and architectural evaluation of blockchain-based systems. As such, the findings are not derived from empirical testing or real-world implementation, which may limit the ability to generalise the results across all operational contexts.

In addition, the study focuses on selected platforms, such as Hyperledger Fabric and Corda, as representative examples of consortium-based blockchain architectures. Other platforms and alternative implementations may exhibit different characteristics and performance outcomes.

4. Key Challenges in Open Banking and BaaS Ecosystems

A. Trust and Multi-Party Governance

Both open banking and Banking-as-a-Service (BaaS) ecosystems involve inherently multi-party processes. In open banking, customer financial data is shared with authorised third parties, whereas in BaaS, banking infrastructure and services are exposed to external providers. In this context, the ecosystem comprises multiple regulated actors, including Account Information Service Providers (AISPs), Payment Initiation Service Providers (PISPs), and Card-Based Payment Instrument Issuers (CBPIIs), as defined by the Financial Conduct Authority (FCA) [8]. Given the distinct roles and regulatory obligations of these participants, ensuring interoperability across the ecosystem emerges as a critical concern.

However, the involvement of multiple independent and regulated actors introduces significant challenges in establishing trust, coordinating responsibilities, and maintaining consistent governance structures. The absence of a unified control mechanism may lead to issues related to data ownership, accountability, and operational risk, particularly in scenarios involving sensitive financial data sharing and cross-institutional processes.

B. Data Integrity and Auditability

Data integrity and auditability are critical challenges, particularly in widespread, modern financial ecosystems driven by increasing digitalisation and multi-system operations. In such distributed and technology-driven environments, financial data is often processed across multiple platforms, increasing the risk of inconsistencies and fragmented records. This situation, especially with the separate verification and regular splitting of different data, makes it difficult to create a reliable and unified audit trail. Lacking a shared and regulated record-keeping structure, it can hinder effective tracking and complicate consistent audits [9].

C. Interoperability and API Fragmentation

The integration of third-party services through APIs enables banks to attract new customers and expand their customer

base. Such integrations also reinforce data flows within internal banking systems, enhancing the effectiveness of customer relationship management and enabling the delivery of more personalised, responsive, and customer-centric services [10].

However, APIs are not static and continuously evolve over time, which introduces additional challenges related to compatibility and integration. Changes in API structures and versions may affect not only the service providers but also third-party users, requiring continuous adaptation and increasing the complexity of interoperability across systems.

D. Privacy and Data Protection

The expansion of open banking and FinTech ecosystems introduces significant challenges related to privacy and data protection. As financial services increasingly rely on the sharing of customer-permissioned data across multiple stakeholders, the number of entities accessing sensitive financial information expands, thereby increasing the risk of data exposure and misuse. In particular, open banking frameworks inherently create a privacy challenge, as they require the transmission and processing of financial data beyond traditional bank-controlled environments [11].

E. KYC and Identity Management Complexity

Implementing KYC (Know Your Customer) in the banking sector, and consequently in Open Banking and BaaS processes, imposes significant obligations on banks in terms of data collection, verification, and continuous updating. These requirements increase the complexity of operational processes, reduce operational efficiency, and significantly raise compliance-related costs.

F. Regulatory and Compliance Challenges

Regulatory and compliance challenges represent a significant constraint in the evolution of open banking and Banking-as-a-Service (BaaS) ecosystems. The introduction of regulatory frameworks such as PSD2 has opened the financial services market to new actors, including FinTech firms, whilst simultaneously imposing stricter requirements on traditional banks. This creates an asymmetrical regulatory environment in which incumbent institutions remain subject to more comprehensive and stringent rules compared to newer entrants. Moreover, banks are required to ensure secure data sharing, transparency, and customer protection whilst adapting their infrastructures to comply with regulatory mandates. These obligations increase operational burdens and necessitate continuous adjustments to both technological and organisational structures [12].

5. Blockchain Capabilities Mapping

Building on the challenges identified in open banking and BaaS ecosystems, this section establishes a conceptual mapping between key challenges – including trust, data

integrity, interoperability, and regulatory compliance – and the corresponding architectural features of blockchain systems. This mapping provides the foundation for the evaluation framework presented in the following section.

In a blockchain network, participants are represented by computer programs, commonly referred to as nodes. Rather than relying on inherent trust in individual nodes, blockchain systems employ predefined consensus mechanisms to determine how transaction validity is established. Depending on the underlying protocol, the influence of a node within the decision-making process may be derived from factors such as computational resources, stake, or authorisation, rather than institutional trust [13].

In addition, the immutability of blockchain records is achieved through cryptographic hash linking, whereby each transaction is time-stamped and incorporates the hash of the preceding record. When new data is appended to the ledger, the resulting cumulative hash is propagated across the network, enabling participants to independently verify the integrity of the stored data. Any unauthorised modification would alter the corresponding hash value, thereby making tampering computationally impractical and readily detectable by all participants [14]. However, in regulated financial environments, personal data can be cryptographically protected and managed in a manner that avoids direct on-chain exposure. Rather than storing personally identifiable information directly on the blockchain, such architectures typically record only cryptographic hashes or commitments on-chain, whilst sensitive data remains under the control of the data owner in off-chain storage.

Beyond consensus and data integrity mechanisms, blockchain platforms also support programmable business logic through smart contracts. Smart contracts inherit the security, integrity, and immutability properties of the underlying blockchain infrastructure. As a result, contractual rules and automated business processes can be executed in a transparent and verifiable manner without requiring a central intermediary. In consortium blockchain environments, access restrictions may further limit the visibility and execution of specific smart contracts to authorised participants only [15].

Building on this conceptual mapping, the following section introduces an evaluation framework to systematically assess the suitability of different architectural approaches.

6. Evaluation Framework

A. Framework Overview

To evaluate the applicability of blockchain-based consortium models in open banking and Banking-as-a-Service (BaaS) ecosystems, this study proposes a multi-criteria evaluation framework. This framework aims to assess whether permissioned and consortium-based blockchain architectures provide measurable advantages over traditional API-based systems in addressing key sectoral challenges such as trust, data integrity, interoperability, and regulatory compliance. Furthermore, it enables a more systematic and transparent evaluation of different architectural alternatives.

B. Evaluation Criteria

Trust and multi-party governance, as key criteria derived from the challenges in open banking and BaaS ecosystems, evaluate the extent to which secure coordination among multiple participants is supported, as well as how governance structures are established among participating entities.

Data Integrity and Auditability evaluates the extent to which the architecture ensures the accuracy, consistency, and immutability of financial data across multiple systems. It considers the ability to maintain a unified and tamper-resistant record structure, support traceability of transactions, and enable reliable and transparent audit processes in multi-party environments.

Interoperability and API Fragmentation evaluates the extent to which an architecture enables seamless integration and data exchange among financial institutions, third-party providers, and supporting infrastructures. It considers the ability to support standardised communication, minimise integration complexity, and reduce operational challenges arising from fragmented systems and inconsistent implementation practices across participating entities.

Privacy and data protection, as a critical requirement in open banking and BaaS ecosystems, is considered a key evaluation criterion in this study. This criterion evaluates the extent to which an architecture ensures the secure handling of sensitive financial data in multi-party environments. It considers the ability to limit unnecessary data exposure, enforce access-control mechanisms, and support privacy-preserving approaches such as data minimisation and selective disclosure. Furthermore, this criterion considers architectural approaches that avoid storing personally identifiable information directly on-chain, instead relying on cryptographic commitments and off-chain storage mechanisms.

In BaaS environments, the integration of banking services into third-party platforms introduces additional operational complexity, requiring continuous system maintenance, updates, and coordination among multiple actors. This increases the burden of identity verification and compliance processes, particularly in multi-institutional settings [16]. Accordingly, the KYC and Identity Management Complexity criterion evaluates the extent to which an architecture reduces operational complexity by enabling reusable identity verification mechanisms, minimising redundant KYC procedures.

Regulatory and compliance challenges are considered a key evaluation criterion in this study, particularly in the context of highly regulated open banking and BaaS ecosystems. This criterion evaluates the extent to which an architecture supports compliance with regulatory requirements whilst minimising the associated operational and technological burden. It considers the ability to ensure secure data sharing, maintain transparency, and enforce customer protection mechanisms in line with regulatory frameworks such as PSD2.

To enable a comparison, a qualitative scoring system is employed based on the defined evaluation criteria. This

scoring approach is not intended to provide absolute measurements, but rather to facilitate a comparative evaluation of different alternatives.

C. Comparative Evaluation

In blockchain technology, consensus mechanisms play a central role in ensuring the consistency and reliability of data across distributed networks and differ according to the types of faults they are designed to tolerate. However, permissioned blockchain environments are not fully trustless, as governance structures, access-control configurations, and override authorities may still influence transaction validation and operational coordination.

The threat model considered in this study assumes a permissioned consortium blockchain environment in which participants are authenticated but not fully trusted. Potential adversaries include (i) colluding consortium participants seeking to influence governance or transaction validation, (ii) compromised validation or notary components providing inaccurate transaction information, (iii) Byzantine behaviour by validating or ordering nodes resulting in inconsistent transaction processing, and (iv) misuse of override authorities capable of affecting transaction finality. These threats may undermine the integrity, reliability, and governance of consortium-based financial blockchain networks. Consequently, such environments may remain exposed to risks including manipulation of transaction validation, operational failures, communication disruptions, and reduced confidence in transaction finality [17, 18].

RAFT and Byzantine Fault Tolerance (BFT) are presented as alternative consensus mechanisms. Whilst both operate at the queuing service layer to ensure transaction queuing and agreement, they differ fundamentally in terms of fault assumptions and performance characteristics. RAFT assumes a crash failure model and is optimised for performance and low latency, making it suitable for permissioned environments with trusted participants. In contrast, BFT-based mechanisms tolerate malicious or arbitrary behaviour and provide stronger fault tolerance at the cost of higher communication overhead and increased latency [19, 20].

Among these alternatives, RAFT has been widely adopted in permissioned blockchain platforms such as Hyperledger Fabric due to its performance characteristics and suitability for environments in which participants are authenticated.

RAFT is a consensus protocol implemented in Hyperledger Fabric to ensure ordering and consistency among network nodes. As a consensus algorithm designed to operate in medium-scale systems with strong consistency requirements, it is relatively straightforward to implement [21]. Unlike traditional blockchain architectures that follow an order-execute model, Hyperledger Fabric adopts an execute-order-validate paradigm, which enhances scalability, flexibility, and confidentiality in permissioned environments [22].

Proof-of-Vote (PoV) has been proposed as a voting-based consensus mechanism specifically designed for consortium

blockchain environments. As an alternative to conventional BFT-based approaches, PoV seeks to improve scalability and communication efficiency by allowing authorised consortium members to reach consensus through structured voting procedures. Similar to other voting-based consensus protocols used in permissioned environments, PoV relies on agreement among authorised participants rather than computational competition, making it conceptually suitable for consortium blockchain applications where participant identities are known and governance structures are predefined.

Although PoV represents an interesting alternative consensus proposal for consortium blockchain environments, it is not included in the comparative evaluation presented in Table I because the comparison focuses on architectural platforms and deployment approaches rather than individual consensus protocols [23, 24].

In practice, Hyperledger Fabric can be cited as a permissioned blockchain platform designed for consortium-based networks, utilising a modular and pluggable consensus mechanism. The evaluation indicates that Hyperledger Fabric has gained increasing relevance as a secure infrastructure for the protection of digital identity credentials and sensitive financial data. Within the financial sector, it has been observed to play a significant role in customer identification and verification processes required to ensure compliance with regulatory frameworks such as Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements. However, the adoption of Hyperledger Fabric is associated with certain implementation challenges, as its deployment depends on specific programming models and technical configurations, which may increase system complexity for financial institutions. Furthermore, existing studies suggest that the integration of cross-chain interoperability protocols – primarily designed around consumer-oriented criteria – has the potential to enhance the functional capabilities of Hyperledger Fabric networks by supporting identity traceability and contributing to the detection and prevention of illicit financial activities.

Although it is not fully considered a blockchain in the literature, it is worth mentioning Corda due to its operation based on distributed ledger technology and its suitability for use in the financial sector. Corda includes nodes called “notary nodes,” which are responsible for the consensus protocol. Since the notaries must be trusted to achieve consensus, the system exhibits a partially decentralised structure [25]. Whilst Corda is not a fully decentralised blockchain, it provides a permissioned distributed ledger platform that supports consortium-based governance, allowing partial decentralisation of transaction management and operational control.

On the other hand, it is important to highlight a key aspect that raises questions regarding the level of decentralisation in Corda. In Corda, concerns around decentralisation primarily stem from the role of notary nodes, which are responsible for ensuring transaction uniqueness. Within the Corda architecture, notary nodes verify whether a transaction relies on input states that have already been consumed in previous

transactions. If such reuse is detected, the transaction is deemed invalid, and all relevant parties are notified of its rejection. Whilst this mechanism effectively prevents double-spending, the assignment of transaction uniqueness validation to specific nodes represents a departure from a fully distributed trust model. Although notary nodes can be deployed in clustered configurations to enhance availability and fault tolerance, this design nonetheless supports the view that Corda embodies a partially centralised architectural approach [26].

From a different perspective, API-based architectures enable financial institutions to share data with third-party providers, thereby fostering innovation and enhancing customer-centric financial services [27]. In API-based open banking ecosystems, third-party providers receive access permissions that are explicitly defined by customer-approved parameters, including data scope, account selection, and validity period. Operational governance and auditability are typically ensured through centralised API gateways, authentication protocols, time-stamped transaction logs, and institution-specific monitoring infrastructures. In addition, customer authentication and authorisation processes are generally controlled by the account servicing payment service provider (ASPSP), ensuring that data access requests remain traceable and auditable in compliance with applicable regulatory requirements [28, 29].

Open banking APIs have been subject to formal security analysis, highlighting the importance of authentication, verification, and protocol correctness in ensuring secure financial data exchange. However, beyond technical security considerations, dispute resolution and liability allocation within API-based ecosystems are generally governed through contractual arrangements, regulatory obligations, and institution-specific compliance procedures established between ASPSPs and authorised TPPs. Whilst APIs constitute the technological foundation of open banking ecosystems and enable interoperability between financial institutions and third-party providers, it is also important to consider certain architectural and governance-related challenges associated with their adoption. In particular, the expansion of the attack surface resulting from increased interoperability and the implementation challenges arising from ambiguities in security specifications represent two notable concerns discussed in the literature. First, open banking architectures facilitate communication among multiple banks, third-party providers, and supporting infrastructures through standardised APIs, thereby creating additional points of interaction that may be targeted by malicious actors. The interoperability established between financial institutions may constitute an attractive target for cyberattacks, thereby necessitating robust security controls across the ecosystem. Second, the effective implementation of API-based financial ecosystems may be complicated by differences in the interpretation of technical security specifications and the complexity of governance processes. This may hinder the consistent application of security controls across participating entities and increase operational complexity within multi-party financial environments [30].

Building on the architectural characteristics discussed in the preceding sections, a comparative evaluation framework was developed to assess the relative suitability of Hyperledger Fabric, Corda, and API-based architectures within open banking and BaaS ecosystems. The evaluation considers the six criteria presented in Table I. Scores range from 1 to 3, where 1 indicates limited support for the corresponding criterion, 2 indicates moderate support with identifiable limitations, and 3 indicates strong support enabled through core architectural features.

Table I: Comparative Evaluation of Architectural Approaches

Criteria	Hyperledger Fabric	Corda	API-based
Trust and Governance	3	2	1
Data Integrity and Auditability	3	3	2
Interoperability and API Fragmentation	2	2	3
Privacy and Data Protection	2	3	2
KYC / Operational Efficiency	3	2	2
Regulatory Compliance	3	2	2

Trust and Governance: Hyperledger Fabric received the highest score due to its permissioned governance structure and consensus-based transaction validation mechanisms, which support coordinated trust among consortium participants. Corda provides consortium governance but relies on notary services to ensure transaction uniqueness, introducing a degree of centralisation. In contrast, API-based architectures primarily depend on contractual arrangements and institution-specific governance mechanisms rather than shared validation and consensus processes.

Data Integrity and Auditability: Hyperledger Fabric and Corda both received the highest score due to their distributed ledger architectures, which incorporate transaction validation mechanisms designed to preserve data integrity and provide verifiable records of transaction activity. In Hyperledger Fabric, transaction consistency is supported through consensus-based ordering and the execute-order-validate model, whilst Corda ensures transaction validity and uniqueness through notary-based verification mechanisms. API-based architectures received a score of 2 because auditability is typically achieved through time-stamped transaction logs, authentication controls, monitoring infrastructures, and institution-specific record-keeping processes. However, the maintenance and verification of records remain distributed across participating institutions rather than being coordinated through a common ledger infrastructure.

Interoperability and API Fragmentation: API-based architectures received the highest score because they are

specifically designed to facilitate standardised communication and data exchange between financial institutions and authorised third-party providers. Hyperledger Fabric and Corda received moderate scores, as interoperability can be supported within consortium-based environments through various integration approaches. However, interoperability may depend on platform-specific configurations and governance arrangements, which can limit seamless interaction across different systems. As a result, interoperability is generally more directly supported in API-based ecosystems.

Privacy and Data Protection: Corda received the highest score due to its selective data-sharing model, which limits transaction visibility to relevant participants and reduces unnecessary data exposure. Hyperledger Fabric and API-based architectures received moderate scores, as both support privacy through permissioned access controls, authentication mechanisms, and the protection of sensitive information. However, API-based environments generally rely on customer consent, access permissions, and institution-specific controls to manage data sharing, whereas Corda provides more granular control over transaction visibility.

KYC / Operational Efficiency: Hyperledger Fabric received the highest score due to its support for digital identity management, identity traceability, and customer verification processes associated with AML and KYC compliance requirements. Corda received a moderate score because its permissioned and consortium-based structure supports controlled participation and operational coordination within regulated financial environments. API-based architectures also received a moderate score, as they support customer authentication, authorisation, and consent management processes. However, identity verification and compliance procedures are typically managed through institution-specific arrangements and governance processes across participating entities.

Regulatory Compliance. Hyperledger Fabric received the highest score due to its ability to support compliance requirements within regulated financial environments through auditability, transparency, and controlled participation mechanisms. Corda received a moderate score because its permissioned governance structure and suitability for financial-sector applications support regulatory oversight and controlled information sharing. API-based architectures also received a moderate score, as regulatory compliance is supported through authentication and authorisation mechanisms, auditability measures, contractual arrangements, and regulatory obligations established between participating entities.

To complement the qualitative assessment presented in Table I, Table II summarises selected performance metrics reported in the literature for Hyperledger Fabric and Corda. The table provides an indicative comparison of throughput, finalisation latency, transaction finality, and network size characteristics reported in published studies.

Table II. Literature-Derived Performance Metrics
(adapted from [31])

	Throughput MTPS	Finalisation Latency (MFLS)	Finality Mechanism	Nodes
H. Fabric	1461.05	13.92 s	Deterministic	4
Corda	13.51	31.59 s	Notary-based	4

The study by Geyer et al. evaluates multiple blockchain systems under a common experimental framework and reports performance metrics including Mean Transactions Per Second (MTPS) and Mean Finalisation Latency (MFLS). Hyperledger Fabric and Corda were selected from this benchmark because both platforms are considered within the scope of the present study. The reported results are included to provide an indicative quantitative comparison based on measurements obtained under the same experimental conditions, thereby improving comparability across platforms. The comparison is intended to complement the architectural evaluation presented in Table I rather than to establish definitive performance rankings.

7. Conclusion

This study examined the extent to which consortium blockchain architectures can address key challenges in open banking and BaaS ecosystems. The analysis demonstrates that blockchain capabilities, including consensus-based validation, immutable record-keeping, and smart contract functionality, may contribute to addressing challenges related to trust, data integrity, transparency, and multi-party governance in financial environments involving multiple independent stakeholders.

At the same time, the findings do not suggest that blockchain architectures universally outperform conventional API-based approaches. The comparative evaluation indicates that Hyperledger Fabric, Corda, and API-based architectures each provide distinct advantages and limitations depending on operational requirements, governance structures, privacy expectations, and regulatory constraints. Consequently, the selection of an appropriate architecture remains context-dependent rather than universally prescriptive.

These findings further suggest that consortium blockchain platforms should be viewed not solely as replacements for existing open banking infrastructures, but as complementary technologies capable of strengthening trust, transparency, and coordination across financial ecosystems. In this context, hybrid approaches that combine blockchain-based infrastructures with API-driven systems may provide a more balanced and practical solution for open banking and BaaS ecosystems.

As future work, further research may focus on privacy-preserving mechanisms, regulatory compliance frameworks, and the scalability of hybrid architectures in multi-stakeholder financial environments.

Competing Interests:

None declared.

Ethical Approval:

Not applicable.

Author's Contribution:

LA solely conceived and designed the study, conducted the literature review, developed the methodology, performed the comparative analysis, prepared all tables and figures, wrote and revised the manuscript, addressed the reviewers' comments, and approved the final version for publication.

Funding:

No external funding was received for this research.

Acknowledgements:

The author would like to thank the reviewers for their valuable comments and constructive suggestions, which helped improve the quality of this manuscript.

References:

- [1] N. Remolina, "Open banking: Regulatory challenges for a new form of financial intermediation in a data-driven world", SSRN, 2019. [Online]. Available: <https://ssrn.com/abstract=3475019>.
- [2] L. Grassi, N. Figini, and L. Fedeli, "How does a data strategy enable customer value? The case of FinTechs and traditional banks under the open finance framework", *Financial Innovation*, vol. 8, no. 75, 2022, doi: 10.1186/s40854-022-00378-x.
- [3] OECD, **Open Finance Policy Considerations**. Paris: OECD Publishing, 2023. [Online]. Available: <https://doi.org/10.1787/19ef3608-en>.
- [4] L. Brodsky and L. Oakes, "Data sharing and open banking", McKinsey & Company, New York, NY, USA, Sep. 2017.
- [5] A. Coletti, M. De Bonis, and A. Pieri, "Banks and Fintechs: How to develop a digital open banking approach for the bank's future", *International Business Research*, vol. 11, no. 9, pp. 23–36, 2018.
- [6] A. Dresner, A. Murati, B. Pike, and J. Zell, "Embedded finance: Who will lead the next payments revolution", McKinsey & Company, 2022.
- [7] R. Auer, "Embedded supervision: How to build regulation into blockchain finance", Federal Reserve Bank of Dallas, Globalization Institute Working Paper, no. 371, Oct. 2019, doi: 10.24149/gwp371.
- [8] Financial Conduct Authority, *Call for Input: Open Finance*. London: FCA, 2019. [Online]. Available: <https://www.fca.org.uk/publications/calls-input/call-input-open-finance>. Accessed: Dec. 2025.
- [9] P. Gomber, R. J. Kauffman, C. Parker, and B. W. Weber, "On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services", *Journal of Management Information Systems*, vol. 35, no. 1, pp. 220–265, 2018.
- [10] X. Lin, S. S. Zhang, and M. Zachariadis, "Open data and API adoption of U.S. banks", *Journal of Financial Intermediation*, vol. 63, Art. no. 101162, Jul. 2025.
- [11] A. Wolska, "Open banking and the catalysts for digital transformation in the financial ecosystem", SSRN Electronic

- Journal, Dec. 2024. [Online]. Available: <https://doi.org/10.2139/ssrn.5075577>.
- [12] V. Stefanelli and F. Manta, "Digital financial services and open banking innovation: Are banks becoming 'invisible'?", *Global Business Review*, 2023. [Online]. Available: <https://doi.org/10.1177/09721509231151491>.
 - [13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008. [Online]. Available: <https://Bitcoin.org/Bitcoin.pdf>.
 - [14] M. D. Pierro, "What is the blockchain?", *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92–95, 2017.
 - [15] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges", *International Journal on Advances in Telecommunications*, vol. 11, no. 1 & 2, pp. 51–64, 2018.
 - [16] P. Bansal, "BaaS: Banking as a service brings industry disruption", *International Journal of Science and Research Archive*, vol. 13, no. 1, pp. 1258–1263, Sep. 2024, doi: 10.30574/ijrsra.2024.13.1.1708.
 - [17] M. Liu, K. Wu, and J. J. Xu, "How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain", *Current Issues in Auditing*, vol. 13, no. 2, pp. A19–A29, 2019.
 - [18] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery", *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, Nov. 2002.
 - [19] "The Raft Consensus Algorithm", Raft, 2025. [Online]. Available: <https://raft.github.io/>. Accessed: Dec. 2025.
 - [20] Z. Shen, Q. Qu, and X.-B. Chen, "Blockchain consensus mechanisms: A comprehensive review and performance analysis framework", *Electronics*, vol. 14, no. 17, art. no. 3567, 2025, doi: 10.3390/electronics14173567.
 - [21] H. Trabelsi and K. Zhang, "Early detection for multiversion concurrency control conflicts in hyperledger fabric", *arXiv preprint*, Jan. 2023, doi: 10.48550/arXiv.2301.06181.
 - [22] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th ACM EuroSys Conf., Porto, Portugal*, Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.
 - [23] X. Li, F. Wu, S. Gao, and K. Chen, "PoV: An efficient voting-based consensus algorithm for consortium blockchains", *Frontiers in Blockchain*, vol. 3, pp. 1–16, Mar. 2020, doi: 10.3389/fbloc.2020.00011.
 - [24] S. Luzipo and A. Gerber, "A systematic literature review of blockchain consensus protocols", in *Proc. Int. Conf. e-Business, e-Services and e-Society (I3E)*, Cham, Switzerland: Springer, 2021, pp. 580–595.
 - [25] M. Valenta and P. Sandner, "Comparison of ethereum, hyperledger fabric and corda", Frankfurt School Blockchain Center (FSBC) Working Paper, 2017.
 - [26] G. Rulev and V. Krikunov, "Development of DLT-based central bank digital currency prototype on corda network", *Journal of Advances in Information Technology*, vol. 16, no. 2, pp. 198–203, Feb. 2025, doi: 10.12720/jait.16.2.198-203.
 - [27] A. Mohammed, "Open banking and APIs: Research on how open banking frameworks and APIs are reshaping the financial ecosystem", *International Journal of Advances in Engineering and Management*, vol. 7, no. 4, pp. 770–784, Sep. 2024, doi: 10.35629/5252-0704770784.
 - [28] D. Gozman, J. Hedman, and K. S. Olsen, "Open banking: Emergent roles, risks & opportunities", in *Proc. 26th Eur. Conf. Inf. Syst. (ECIS)*, Portsmouth, U.K., 2018, Paper 183.
 - [29] Z. Nanaeva, A. F. Aysan, and N. S. Shirazi, "Open banking from EU's payment services directive to practice: The cases of Solarisbank and Insha", MPRA Paper, no. 110763, Oct. 2021.
 - [30] P. Modesti, L. Freitas, Q. Shotomiwa, and A. Almhrej, "Security analysis of the open banking account and transaction API protocol", *Cyber Security and Applications*, vol. 3, Art. no. 100097, 2025.
 - [31] F. C. Geyer, H.-A. Jacobsen, R. Mayer, and P. Mandl, "An end-to-end performance comparison of seven permissioned blockchain systems", in **Proc. 24th Int. Middleware Conf. (Middleware '23)**, Bologna, Italy, Dec. 2023, pp. 71–84, doi: 10.1145/3590140.3629106.