Engineering and Technology Quarterly Reviews

Assiroj, P., Hertantyo, B. B., Hartati, B., & Alam, S. (2025), PoA-PBFT Blockchain Architecture Design for Authentication and Identity Protection in Electronic Passports. In: *Engineering and Technology Quarterly Reviews*, Vol.8, No.2, 46-57.

ISSN 2622-9374

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research *Engineering and Technology Quarterly Reviews* is a peer-reviewed International Journal. The journal covers scholarly articles in the fields of Engineering and Technology, including (but not limited to) Civil Engineering, Informatics Engineering, Environmental Engineering, Mechanical Engineering, Industrial Engineering, Marine Engineering, Electrical Engineering, Architectural Engineering, Geological Engineering, Mining Engineering, Bioelectronics, Robotics and Automation, Software Engineering, and Technology. As the journal is Open Access, it ensures high visibility and the increase of citations for all research articles published. The *Engineering and Technology Quarterly Reviews* aims to facilitate scholarly work on recent theoretical and practical aspects of Education.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Engineering and Technology Quarterly Reviews
Vol.8, No.2, 2025: 46-57
ISSN 2622-9374

PoA-PBFT Blockchain Architecture Design for Authentication and Identity Protection in Electronic Passports

Priati Assiroj[1], Baluh B. Hertantyo[1], Besse Hartati[1], Sirojul Alam[2]

[1] Immigration Technology Management, Politeknik Pengayoman Indonesia, Tangerang, Indonesia
[2] Certificate Authority Department, PERURI Indonesia, Jakkarta, Indonesia

Correspondence: Priati Assiroj, Immigration Technology Management, Politeknik Pengayoman Indonesia, Tangerang, Indonesia. Tel: -. E-mail: priati.assiroj@poltekim.ac.id

Abstract
Centralized e-passport infrastructures remain vulnerable to forgery, data manipulation, and single points of failure, undermining both national and international identity management systems' integrity and transparency. These limitations restrict real-time cross-agency verification and create dependencies on centralized authorities. This study introduces a permissioned blockchain model designed to enable decentralized trust, institutional accountability, and fault-tolerant verification to overcome these challenges. The proposed framework integrates certified government entities, such as the Ministry of Immigration and Corrections and the Directorate General of Immigration, within a secure validation network governed by a National Certificate Authority (CA). This paper proposes a hybrid blockchain architecture that combines PoA for institutional legitimacy with PBFT for deterministic consensus and data immutability. All passport-related transactions, including issuance, renewal, and revocation are validated through smart contracts and recorded in a distributed ledger, ensuring secure, transparent, and interoperable data exchange compliant with ICAO standards. The model demonstrates that blockchain can be feasibly applied to national e-passport infrastructures, thereby establishing a digital identity ecosystem that is tamper-resistant and auditable. Future work includes implementing a prototype using Hyperledger Fabric to evaluate latency, throughput, and consensus efficiency.

Keywords: Blockchain, E-Passport, Proof-Of-Authority, Practical Byzantine Fault Tolerance

1. Introduction

The rapid digitalization of personal identification and cross-border travel management has introduced new challenges in maintaining the authenticity, privacy, and security of sensitive identity data. The electronic passport (e-passport), which embeds a microprocessor chip storing biometric and demographic information, has become a cornerstone of modern border control. However, despite its adoption by more than 150 countries, current e-

passport infrastructures remain dependent on centralized verification authorities, introducing single points of failure, privacy vulnerabilities, and limited transparency across international borders. Such structural weaknesses expose the system to forgery, data manipulation, and insider abuse, ultimately threatening national security and citizen trust (Jahan et al., 2023) (Diego & Gutierrez-aguero, 2025) (KOCAOĞULLAR et al., 2025). Traditional certificate-based identity management systems ensure authenticity during issuance but rely on hierarchical trust structures and periodic synchronization through the International Civil Aviation Organization (ICAO) Public Key Directory (PKD) (KOCAOĞULLAR et al., 2025). This centralized model impedes real-time interagency verification and increases operational latency. In cases where digital certificates are revoked or compromised, downstream verifiers may not immediately detect the change, allowing potentially fraudulent documents to remain active. Recent research highlights the scalability limitations of centralized verification systems and recommends hybrid trust frameworks that integrate distributed validation mechanisms for greater resilience (Butera et al., 2023) (Kuperberg, 2020).

Blockchain technology has emerged as a promising solution for identity protection and authentication by decentralizing trust and enhancing transparency. As a distributed ledger collectively maintained by authorized nodes, the blockchain guarantees immutability, integrity, and traceability for every recorded transaction (Vinoth Kumar et al., 2024) (Ricci et al., 2021) (Papatheodorou et al., 2025). In identity management contexts, it enables multiple government and border-control entities to securely share verified data without relinquishing sovereignty or administrative control. Furthermore, blockchain's transparent auditability supports compliance with accountability and privacy regulations while preventing unauthorized data manipulation. However, the selection of consensus mechanisms determines the efficiency and reliability of blockchain-based identity systems. Public blockchains, such as Bitcoin and Ethereum, which employ Proof of Work (PoW) or Proof of Stake (PoS), are energy-intensive and rely on anonymous validators—properties unsuitable for regulated identity frameworks. Consequently, research has shifted toward permissioned consensus protocols such as Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT), which enable deterministic, low-latency consensus among known institutional nodes (Kuperberg, 2020) (Ricci et al., 2021) (KOCAOĞULLAR et al., 2025).

Figure 1 illustrates the proposed blockchain-based e-passport system's conceptual model. Each authorized institution—represented by a validator node from the Ministry of Immigration and Corrections or the Directorate General of Immigration—interacts through smart contracts to record and verify passport-related transactions on a shared distributed ledger. This permissioned and auditable structure establishes a foundation for secure, transparent, and interoperable digital identity management at both national and international levels.

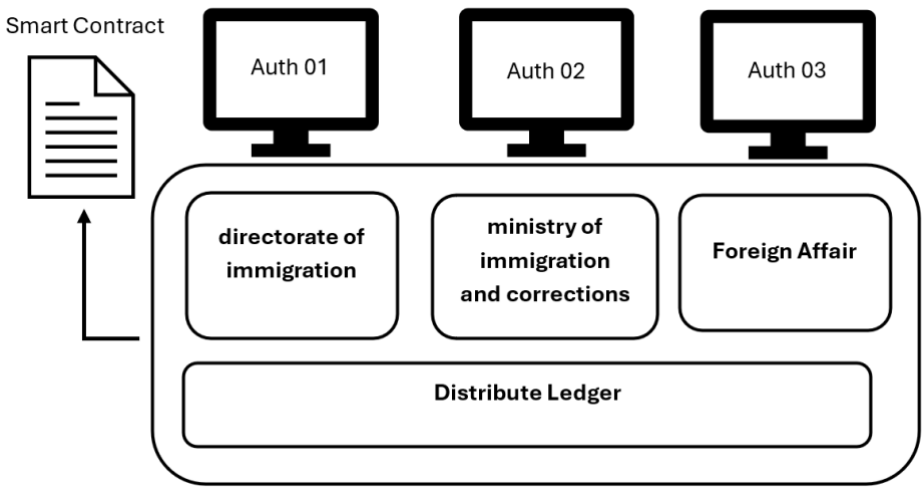

Figure 1: Conceptual model of proposed blockchain based e-passport system

Proof-of-Authority (PoA) relies on validator reputation and certified digital identities, making it suitable for governmental or inter-agency entities' consortium blockchains (Kuperberg, 2020) (Ricci et al., 2021). However,

pure PoA assume that all validators are permanently honest and online, thereby providing limited fault tolerance. In contrast, Practical Byzantine Fault Tolerance (PBFT) employs a multi-phase message exchange process—pre-prepare, prepare, and commit—to maintain ledger consistency even when up to one-third of nodes are faulty or malicious (Medina et al., 2021). Integrating both mechanisms into a single hybrid PoA-PBFT framework provides an optimal balance between performance, determinism, and resilience (Jahan et al., 2023) (Papatheodorou et al., 2025). Several recent studies have reinforced the potential of blockchain in e-governance and identity verification. Hasan et al. (Hasan et al., 2020) introduced a blockchain-based digital medical-passport framework to authenticate COVID-19 immunity credentials, enabling secure validation across institutional boundaries. Ricci et al. (Ricci et al., 2021) presented a systematic review of blockchain-enabled contact tracing and vaccine-distribution systems, emphasizing scalability and data integrity. Butera et al. (Butera et al., 2023) explored NFT-based origin verification for second-hand assets, demonstrating how ownership can be tracked using immutable digital proofs. Kuperberg (Kuperberg, 2020) provided a comprehensive survey of blockchain-driven identity management models, outlining organizational and technological challenges in enterprise and governmental contexts. Collectively, these works demonstrate the capacity of blockchain to prevent tampering, enhance transparency, and automate trust verification.

Nevertheless, the application of blockchain to e-passport authentication remains underexplored (KOCAOĞULLAR et al., 2025). Existing systems primarily address medical financial or supply-chain credentials rather than government-issued travel documents. Integrating blockchain with International Civil Aviation Organization (ICAO)-compliant infrastructures—while preserving interoperability, scalability, and legal validity—requires further architectural investigation. The absence of a standardized multi-authority framework for e-passport validation motivates the design of a secure, transparent, and auditable blockchain-based model (Terkes et al., 2024).

Therefore, this study proposes a hybrid PoA–PBFT blockchain architecture for e-passport authentication and identity protection in Indonesia. The framework leverages PoA's efficiency and PBFT's fault tolerance to form a permissioned, multi-agency network involving the Ministry of Immigration and Corrections and the Directorate General of Immigration as validator nodes. Each node receives a cryptographic certificate issued by a national certificate authority (CA), enabling secure block creation and consensus participation. Every passport issuance, renewal, or revocation is immutably recorded, and real-time verification occurs at border gates or embassies through smart contracts (Papatheodorou et al., 2025). The proposed model mitigates forgery, eliminates single points of failure, and enhances transparency in alignment with ICAO standards by decentralizing validation among certified institutions. The contributions of this study are threefold. First, a hybrid PoA–PBFT consensus framework optimized for sovereign identity systems is introduced, ensuring deterministic finality and institutional accountability. Second, it presents an architectural blueprint for integrating blockchain into existing electronic-passport infrastructures, enabling decentralized validation among trusted government authorities. Third, it evaluates expected security, efficiency, and interoperability gains, emphasizing compliance with international identity management standards (Papatheodorou et al., 2025) (KOCAOĞULLAR et al., 2025). Overall, this research establishes a foundational model for implementing and testing permissioned blockchain networks in national digital-identity ecosystems—advancing toward a transparent, tamper-resistant, and interoperable e-governance paradigm.

2. Method

The efficiency, scalability, and trustworthiness of any blockchain-based identity system primarily depend on its consensus mechanism—the protocol that enables distributed nodes to agree on the validity of transactions and blocks. The ideal consensus framework for an e-passport authentication system must ensure deterministic finality, low latency, verifiable authority, and resilience against partial node failures. To achieve this, the proposed framework adopts a hybrid PoA and PBFT mechanism, combining institutional legitimacy with Byzantine fault resilience (Jahan et al., 2023) (Kuperberg, 2020) (Papatheodorou et al., 2025).

2.1 Proof-of-Authority (PoA) Overview

Proof-of-Authority (PoA) is a permissioned consensus protocol in which, rather than anonymous participants, validators are pre-approved, identifiable, and institutionally accountable entities. Each validator node represents a recognized government organization operating under a legally verifiable identity, such as the Ministry of Immigration and Corrections or the Directorate General of Immigration. Unlike open blockchain models, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS), PoA does not depend on computational competition or financial stake. Instead, it relies on the credibility and authenticity of the validator identities, each of which is verified through cryptographic certification issued by a trusted national certificate authority (CA). This approach establishes a trust-anchored yet decentralized governance model in which the number of validators is limited but transparent and auditable. PoA offers the following intrinsic advantages that make it suitable for sovereign identity systems and inter-agency data-sharing frameworks:

2.1.1 High throughput and low latency.

Block production is deterministic and sequentially assigned among authorized validators, eliminating the probabilistic delays typical in mining-based systems.

2.1.2 Energy efficiency and sustainability.

Consensus is achieved through digital signature verification instead of computationally intensive puzzles, making it viable for government-scale deployments.

2.1.3 Institutional accountability.

Every block proposal and validation is cryptographically signed and traceable to a specific government authority, ensuring legal responsibility for all ledger operations.

In the context of the proposed blockchain-based e-passport architecture, the PoA layer functions as the primary access-control layer that governs validator participation. Only government institutions with valid CA-issued certificates are permitted to propose or validate transactions such as passport issuance, renewal, or revocation. The CA acts as the root of trust, validating institutional credentials, issuing digital keys, and managing validator lifecycle policies. This structure ensures legal auditability and operational transparency while maintaining each participating agency's sovereignty. It guarantees that all blockchain activities are technically verifiable and administratively attributable, aligning with national governance mandates and ICAO standards for cross-border identity validation (KOCAOĞULLAR et al., 2025). Consequently, PoA establishes a secure and controlled foundation on which the PBFT consensus mechanism can operate efficiently, ensuring that only trusted entities participate in subsequent block validation and message-exchange processes.

2.2 Practical Byzantine Fault Tolerance Overview

Practical Byzantine Fault Tolerance (PBFT) is a deterministic consensus algorithm designed to ensure consistency and reliability within distributed systems, even when certain nodes behave arbitrarily or maliciously—known as Byzantine faults. Such faults may result from hardware failures, software errors, or external adversarial compromise. Initially proposed by Castro and Liskov, PBFT has become one of the most widely implemented consensus mechanisms in permissioned blockchain environments, particularly in enterprise and government networks where validator identities are authenticated and authorized (Kuperberg, 2020) (Medina et al., 2021). Unlike probabilistic consensus models, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS), PBFT guarantees final and irreversible agreement through multiphase message exchange among known validators. This deterministic approach ensures that all honest nodes reach agreement on the same transaction order, provided that no more than f nodes are faulty within a network of $3f + 1$ total nodes. This reliability makes PBFT particularly suitable for national e-passport infrastructures, where integrity, non-repudiation, and auditability are essential (Ricci et al., 2021) (Terkes et al., 2024).

In the proposed hybrid PoA–PBFT architecture, each validator node—representing a certified government authority, such as the Ministry of Immigration and Corrections or the Directorate General of Immigration—engages in structured communication rounds to validate every passport-related transaction. PBFT operates through five sequential phases:

2.2.1 Request Phase.

The PBFT process begins when a client node—such as a border control system or embassy terminal—submits a digitally signed transaction request to the primary node, ensuring authenticity and integrity. In the Pre-Prepare phase, the primary verifies the signature, checks for duplicates, and assigns a valid unique sequence number before forwarding the proposal to replica nodes. This stage ensures non-repudiation, as each transaction is traceable to an authenticated source, forming the trust foundation that only legitimate, verifiable passport operations enter the blockchain network.

2.2.2 Pre-Prepare Phase.

In the pre-prepare phase, a designated primary node—also referred to as the leader—initiates the consensus process by proposing a new block that contains one or more verified transactions. In this research context, each transaction may correspond to an e-passport event, such as issuance, renewal, or revocation. The primary node aggregates these transactions into a candidate block, attaches its digital signature and a sequence number, and broadcasts a pre-prepare message to all replica nodes. This message acts as the official proposal for the current round of consensus. This phase ensures that all validators are aware of an identical block proposal and are synchronized in the same view of the system state before validation begins. At this stage, no voting or decision occurs; it is purely a dissemination step that sets the baseline for subsequent agreement.

2.2.3 Prepare Phase.

Each replica node independently verifies the block's validity by checking its cryptographic hash, each transaction's integrity, and the leader's signature authenticity upon receiving the pre-prepare message. If the verification is successful, the node broadcasts a message to all other replicas, signalling its preliminary approval of the proposal. Then, every validator collects prepare messages from its peers. The process continues until the node receives confirmations from at least $2f + 1$ distinct nodes, where "f" denotes the system's maximum number of faulty or malicious nodes. This threshold guarantees that a sufficient majority of honest validators have inspected and agreed on the same block proposal. The outcome of this phase is the formation of a qualified majority agreement—a consensus that the proposed block is valid and ready to be committed if further votes corroborate it.

2.2.4 Commit Phase.

The commit phase finalizes the consensus decision. After obtaining a quorum of prepared messages, each node broadcasts a commit message to the network, confirming its intent to append the validated block to the ledger. Once a node collects $2f + 1$ matching commit messages, it determines that a supermajority consensus has been achieved, and the block is irreversibly confirmed. The node then appends the block to its copy of the local distributed ledger, ensuring that all honest participants maintain an identical and synchronized state. This stage marks the transition from provisional agreement to deterministic finality—a state in which the block cannot be altered or replaced without the majority's cooperation. In the context of an e-passport system, each passport issuance or verification record becomes immutable, auditable, and cryptographically verifiable across all nodes of government authority.

2.2.5 Reply Phase.

Once a validator node receives at least 2f + 1 matching prepare messages, it moves into the commit phase, broadcasting to peers signed confirmations that the block is valid. When 2f + 1 commit messages are collected, the block is permanently appended to every ledger, ensuring a consistent, immutable e-passport record. Finally, during the reply phase, validators notify the client (e.g., border or embassy system) that the transaction is finalized across the network, confirming deterministic consensus and eliminating the risk of forks or conflicting records. Figure 2 shows the PBFT consensus flow in the proposed architecture. Each authorized node exchanges digitally signed messages through three communication rounds, and the system commits the transaction to the distributed ledger only when at least two-thirds of nodes confirm the block's validity. The deterministic finality achieved through PBFT eliminates the possibility of forks or conflicting passport records, thereby guaranteeing that all nodes maintain a consistent, tamper-proof copy of the e-passport ledger.

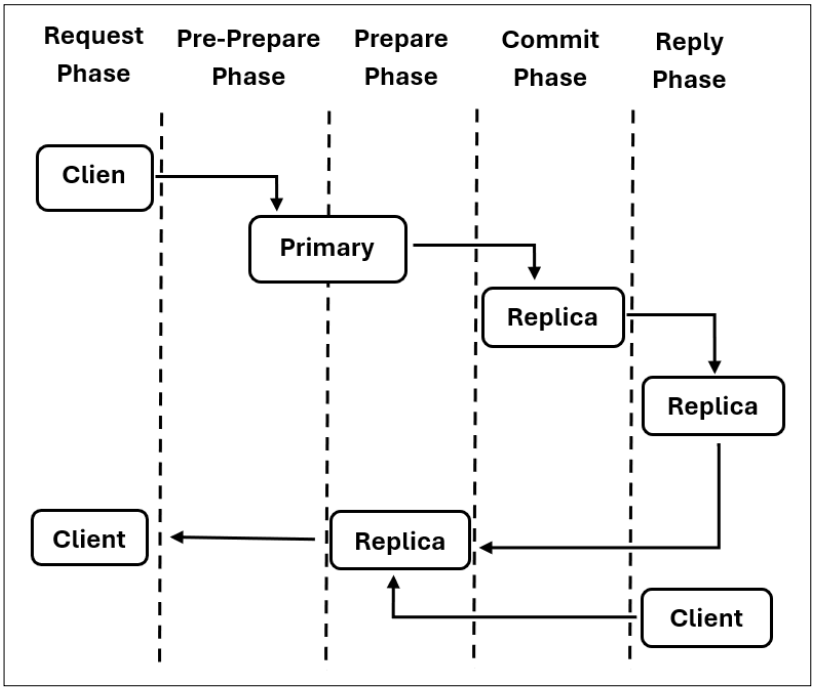

Figure 2: PBFT consensus flow on the proposed architecture

The process begins when a client node (such as a border control terminal or embassy system) sends a digitally signed request to the primary node, initiating the Request Phase. The primary node validates the request and broadcasts a proposal to the replica nodes during the Pre-Prepare Phase. Each replica then verifies the proposal and exchanges Prepare messages with its peers to confirm the transaction's validity. Once at least 2f + 1 nodes agree, the system enters the commit phase, in which all replicas append the verified block to their local ledgers. Finally, in the Reply Phase, replicas send confirmation messages back to the client, ensuring that all nodes maintain a synchronized and immutable record of the passport transaction across the distributed network.

2.3 Related Works

Several recent studies have investigated the use of blockchain technology for secure identity management and authentication within digital ecosystems. Kuperberg (Kuperberg, 2020) provided a comprehensive survey of blockchain-based identity management frameworks, emphasizing the transition from centralized identity and access management (IAM) models toward decentralized and self-sovereign identity (SSI) architectures. The study highlighted major challenges related to compliance, privacy protection, and the integration of blockchain with certificate-based authentication infrastructures and enterprise trust systems. The findings suggest that blockchain can enhance institutional trust, transparency, and accountability while minimizing the dependency on single centralized authorities.

Jahan et al. (Jahan et al., 2023) proposed a private permissioned blockchain for digital passport management combined with the InterPlanetary File System (IPFS) to achieve secure storage and traceable document verification

in the context of e-government and e-passport applications. Similarly, Hasan et al. (Hasan et al., 2020) introduced a blockchain-based digital medical passport model for verifying COVID-19 immunity certificates, demonstrating cross-institutional authentication without relying on a single national database. Al-Bassam's research further extended this concept by using smart contracts to replace conventional digital certificate authority frameworks, ensuring verifiable and tamper-resistant credential validation for government systems. Collectively, these approaches show that permissioned blockchain networks provide immutability, auditability, and verifiable identity exchange across administrative domains.

Hybrid consensus models have been developed to improve the scalability and fault tolerance of controlled blockchain environments. Butera (Butera et al., 2023) proposed an enhanced proof-of-authority (EA-PoA) model for optimizing the lifetime of wireless sensor networks through energy-aware leader selection and hierarchical clustering. Similarly, Stokkink and Pouwelse combined zero-knowledge proofs with PBFT-based validation to support identity claims in distributed ecosystems that are verifiable and privacy-preserving. These studies confirm that integrating deterministic protocols, such as PBFT, with authority-based validator selection enhances throughput, reliability, and security—key features required in regulated national identity infrastructures.

Recent decentralized identity frameworks, such as Sovrin, uPort, and Hyperledger Indy, emphasize user autonomy and cryptographic verifiability (Papatheodorou et al., 2025). However, their general SSI-based architecture renders them unsuitable for highly regulated government systems that require hierarchical control, legal accountability, and compliance with International Civil Aviation Organization (ICAO) Doc 9303 standards. To bridge this gap, de Diego and Gutiérrez-Aguero (Diego & Gutierrez-aguero, 2025) and Alaraj and Bani-Salameh (Papatheodorou et al., 2025) proposed hybrid blockchain architectures that integrate government-controlled validator networks with public verification layers to ensure interoperability and audit transparency. Based on the reviewed literature, the application of blockchain in e-Passport ecosystems remains an emerging research field. While most studies focus on digital identity or credential verification, few address multi-authority consensus, cross-border validation, or interoperability with traditional Machine Readable Travel Document (MRTD) systems. Therefore, this study proposes a hybrid PoA–PBFT blockchain model designed for national e-Passport infrastructures, combining deterministic PoA with PBFT to achieve operational efficiency, resilience, and full compliance with international security and governance standards (Jahan et al., 2023) (Butera et al., 2023) (KOCAOĞULLAR et al., 2025).

3. Results

The proposed system introduces a hybrid blockchain architecture that integrates the PoA and PBFT consensus mechanisms to ensure secure, verifiable, and tamper-resistant e-passport data management. This framework is designed to support multi-agency collaboration across the Ministry of Immigration and Corrections, the Directorate General of Immigration, and the National Certificate Authority of Indonesia. Its core objective is to overcome the limitations of centralized public key infrastructures by enabling distributed validation, auditable record-keeping, and fault-tolerant consensus among authorized government nodes. Figure 3 conceptually depicts the hybrid consensus process that integrates PoA's deterministic validator selection with PBFT's multi-phase message exchange for block confirmation.

3.1 System Overview

The proposed blockchain-based e-passport architecture establishes a permissioned, multi-authority network to enhance national identity management processes' integrity, traceability, and transparency. At its core, the system replaces the traditional centralized public key infrastructure with a distributed ledger governed by a hybrid PoA–PBFT consensus mechanism. This hybrid model ensures that only verified institutions can participate in block validation while maintaining deterministic finality and FTT across all nodes. Figure 3 shows that the architecture is composed of the following four key components:

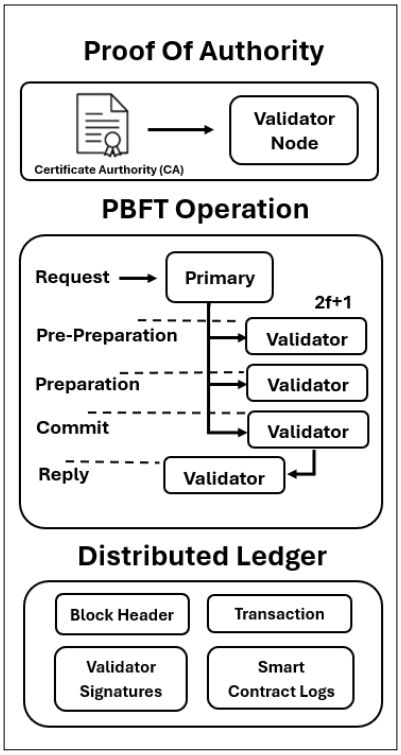

Figure 3: Hybrid PoA-PBFT consensus mechanism

3.1.1 Certificate Authority. CA is responsible for issuing cryptographic credentials to participating institutions;
3.1.2 Validator Nodes. It represents the Ministry of Immigration and Corrections and Directorate General of Immigration;
3.1.3 The PBFT Consensus Layer. It coordinates message exchanges (pre-prepare, prepare, commit, and reply phases) among validator nodes to reach agreement on each transaction; and
3.1.4 The Distributed Ledger. This is where validated e-passport events—such as issuance, renewal, or revocation—are permanently stored in a tamper-proof blockchain.

The Hybrid PoA–PBFT Consensus Mechanism for the E-Passport Blockchain Architecture illustrates the interaction between institutional authorization and distributed consensus to maintain integrity across national identity systems. In this framework, each e-passport transaction begins at the PoA layer, where a national certificate authority authenticates the validator nodes before participating in consensus. Then, the validated nodes engage in the PBFT process, exchanging signed messages across the Request, Pre-Prepare, Prepare, Commit, and Reply phases to reach a deterministic agreement.

Once the block is confirmed by a supermajority of $2f + 1$ validators, the transaction is appended to the distributed ledger, which stores block headers, validator signatures, transaction data, and smart-contract logs. This ensures that every passport issuance, renewal, or revocation is cryptographically verified, immutably recorded, and auditable across all authorized government institutions, thereby reinforcing trust and resilience within the national e-passport ecosystem.

3.2 Architecture Model

The proposed e-passport blockchain framework adopts a hybrid layered architecture that integrates the PoA and PBFT consensus mechanisms to ensure institutional legitimacy, operational resilience, and deterministic transaction finality. As shown in Fig. 3, the system operates within a permissioned environment comprising certified validator nodes representing governmental entities, each authenticated through cryptographic certificates issued by a National Certificate Authority (CA). This configuration guarantees that only trusted and legally

recognized institutions—such as the Ministry of Immigration and Corrections, the Directorate General of Immigration, and the Ministry of Foreign Affairs—participate in the validation and consensus processes. The architecture is logically structured into four functional layers, each contributing distinct responsibilities to the network's overall security and performance: the application, consensus, network, and ledger layers.

At the Application Layer, user-facing entities—such as passport issuance systems, border inspection terminals, and embassy verification nodes—initiate authenticated transactions. Each transaction request (e.g., issuance, renewal, or revocation) is digitally signed using the institution's private key to ensure data origin authenticity and integrity before blockchain submission.

The Consensus Layer governs validation operations and enforces agreement across the participating nodes. The PoA sublayer establishes validator eligibility based on institutional certification, preventing unauthorized access, and ensuring administrative accountability. Upon authentication, the PBFT sublayer manages the multiphase consensus procedure. The primary node aggregates verified transactions into candidate blocks and disseminates pre-prepare messages to all replicas. Each replica independently verifies block integrity and authenticity before exchanging prepare and commit messages. Consensus is achieved when at least $2f + 1$ validators confirm identical block states, providing deterministic finality and fault tolerance against Byzantine failures. This hybridization eliminates probabilistic delays and reduces computational overhead compared to Proof-of-Work (PoW) systems, achieving a low-latency, high-throughput consensus suitable for real-time identity verification.

The network layer enables secure communication among the validator nodes through encrypted and authenticated channels. A partially meshed topology is employed to balance fault resilience and transmission efficiency, ensuring rapid consensus message propagation even under partial node failures. All inter-node communications are digitally signed and timestamped, thereby preventing tampering, message reordering, or replay attacks.

The Ledger Layer provides immutable storage and cryptographic auditability. Each block contains a structured combination of a block header, validated transaction data, validator signatures, and smart contract execution logs. The block header links to its predecessor through a secure hash reference, ensuring temporal consistency and tamper resistance. Embedded smart contracts automate rule enforcement for passport issuance, renewal, and revocation while fine-grained access control between institutions is implemented. Sensitive biometric or personal data are encrypted or hashed to preserve privacy compliance while retaining full audit traceability.

Collectively, this architecture establishes a hierarchical yet decentralized governance model, where PoA defines validator identity and authority, and PBFT enforces deterministic consensus among validated participants. The resulting infrastructure delivers institutional accountability, Byzantine fault tolerance, and transparency of data provenance. The design aligns with the International Civil Aviation Organization (ICAO) Public Key Directory standards while extending its capabilities toward real-time, cross-agency synchronization, and multi-jurisdictional interoperability.

Consequently, the hybrid PoA–PBFT architecture provides a robust technical foundation for next-generation sovereign identity systems. It supports high integrity in e-passport authentication, reduces dependency on centralized validation intermediaries, and enables scalable integration with future e-government services, such as e-visa issuance, border security analytics, and decentralized travel record management.

3.3 Operation Workflow

Figure 3 shows the proposed hybrid PoA–PBFT blockchain architecture's operational workflow for electronic passport authentication. The figure is divided into three major functional sections —PoA, PBFT operation, and distributed ledger— each representing a sequential phase of the validation and recording process.

The PoA section begins the workflow with the Authority Registration phase. Institutional participants, such as the Directorate General of Immigration and the, Ministry of Immigration and Corrections, register as validator nodes. Each node receives a digital certificate issued by the National Certificate Authority (CA), which serves as its immutable credential for participating in block validation. This process ensures that only verified governmental

entities are eligible to join the network, eliminating the possibility of untrusted or anonymous participants. Thus, the PoA layer establishes the system's institutional trust foundation, binding every node's cryptographic identity to its legal authority. The transaction proceeds to the PBFT operation block following registration, which represents the core consensus process. When an authorized operator initiates a passport-related transaction—such as issuance, renewal, or revocation—the request is sent to the primary node. The primary node aggregates verified data and triggers the multi-phase PBFT process, which starts with the request message. Then, a Pre-Prepare message is broadcast to all replica validators, ensuring that each receives an identical validation proposal. Each Validator Node independently examines the cryptographic integrity of the block, verifying the transaction signatures and timestamps. Then, the validates exchange Prepare and Commit messages, ensuring agreement through cross-validation. A consensus is reached when a quorum of 2f+1 matching commit messages is reached, guaranteeing deterministic and fault-tolerant agreement even in the presence of faulty or malicious nodes.

Finally, in the Distributed Ledger section, the validated block is permanently appended to the blockchain. Each block comprises a block header, validator signatures, transaction data, and smart contract logs. The block header contains a hash pointer linking it to the previous block, maintaining the immutability and chronological integrity of the ledger. Validator signatures provide cryptographic proof of consensus, while the transaction field records details of the passport operation. Smart contract logs document the automated validation and policy enforcement actions performed during the process. Together, these components establish an auditable and tamper-resistant ledger that supports transparent verification across all authorized institutions.

4. Discussion

This operational workflow demonstrates how the proposed system harmonizes institutional trust with the Distributed Consensus System (DCS). The PoA layer enforces access control and node legitimacy, whereas the PBFT mechanism ensures synchronization, fault tolerance, and deterministic finality across validator nodes. The system transforms the e-passport into a self-verifiable digital identity asset that can be authenticated in real-time across ministries and border agencies without relying on centralized verification authorities by combining these mechanisms.

The proposed PoA–PBFT blockchain architecture incorporates a multilayer security and governance model that ensures institutional trust, cryptographic integrity, and operational accountability across all participating authorities. As illustrated in Figure 4, the framework integrates three principal domains—governance authentication, consensus operation, and application interoperability—within a unified and verifiable security structure that mirrors real-world governmental hierarchy.

Figure 4 shows that the proposed e-passport blockchain architecture integrates three primary layers: the governance and validation layer, the blockchain network layer, and the application interoperability layer. At the top level, the CA acts as the root of trust, issuing cryptographic certificates that authorize participation in the network. Validator legitimacy is governed by the Proof-of-Authority (PoA) mechanism, ensuring that only certified government entities—such as the Ministry of Immigration and Corrections and the Directorate General of Immigration—are allowed to operate as validator nodes (VA Node01 and VA Node02). This mechanism replaces anonymous participation with institutional accountability, thereby forming the foundation for a secure verification of national identity.

The second layer represents the blockchain network, where the primary node initiates transactions and the PBFT consensus mechanism validates them through structured message exchanges. Each validator node verifies the transaction and confirms agreement once at least 2f + 1 validators reach quorum. The Distributed Ledger permanently stores the validated data, while Smart Contracts automate validation rules, manage access control, and ensure that all e-passport records remain immutable and auditable.

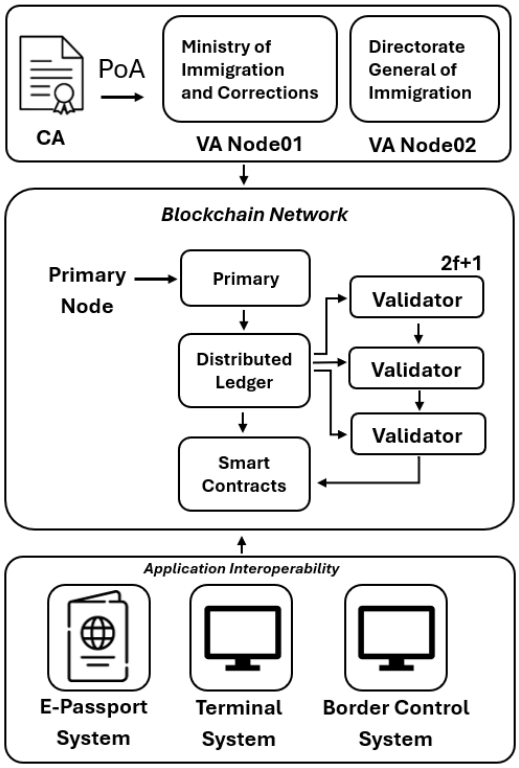

Figure 4: Application interoperability layer

The bottom layer, the Application Interoperability Layer, enables seamless communication between the blockchain network and government application systems. This layer connects the E-Passport Issuance System, Embassy or Terminal Systems, and Border Control Systems, allowing real-time travel document authentication and verification across national and diplomatic authorities. Through this integration, the system achieves secure, interoperable, and verifiable e-passport management while maintaining compliance with international standards, such as ICAO Doc 9303 (Edition, 2021).

This paper proposes a hybrid PoA and PBFT blockchain architecture for securing the authentication and verification processes in national e-passport systems. The model integrates the institutional legitimacy of PoA with the deterministic fault tolerance of PBFT, creating a permissioned blockchain framework capable of ensuring data integrity, immutability, and real-time interoperability among government agencies. The design eliminates single points of failure, enhances transparency, and enables automated validation through smart contracts, making it suitable for large-scale e-governance applications. The findings demonstrate that the proposed blockchain model can be feasibly implemented within Indonesia's e-passport infrastructure and can be extended to support cross-border authentication in compliance with the International Conference on Authentication and Privacy (ICAO) standards. The hybrid PoA–PBFT mechanism provides a practical balance between governance control and distributed trust, offering a secure foundation for sovereign digital identity systems. Future work will focus on developing a prototype implementation using Hyperledger Fabric to evaluate system performance, including consensus latency, throughput, and network resilience under operational conditions.

Author Contributions: All authors contributed to this research.

Funding: This research was funded by Politeknik Pengayoman Indonesia, The Ministry of Law of The Republic of Indonesia.

Conflicts of Interest: The authors declare no conflict of interest.

Informed Consent Statement/Ethics approval: Not applicable.

Declaration of Generative AI and AI-assisted Technologies: AI-based text assistance was used to improve grammar, clarity, translation, and overall readability. All research design, experimental work, analysis, and conclusions were conducted independently, and the AI tool was specifically used as a language support.

References

Butera, A., Gatteschi, V., Member, S., Gabriele, F., Novaro, D., & Vianello, D. (2023). *Blockchain and NFTs-based Trades of Second-hand Vehicles*. 1–18. https://doi.org/10.1109/ACCESS.2023.3284676

Diego, S. D. E., & Gutierrez-aguero, I. (2025). Decentralized Digital Product Passport Building Blocks for Enhancing Supply Chain Sovereignty and Circular Economy Practices. *IEEE Access*, *PP*, 1. https://doi.org/10.1109/ACCESS.2025.3594826

Edition, E. (2021). *ICAO Doc 9303 Part 8: Emergency Travel Documents*.

Hasan, H. R., Salah, K., Member, S., Jayaraman, R., & Ellahham, S. (2020). *Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates*. 222093–222108. https://doi.org/10.1109/ACCESS.2020.3043350

Jahan, N., Reno, S., & Ahmed, M. (2023). Securing E-Passport Management Using Private-Permissioned Blockchain and IPFS. *3rd International Conference on Electrical, Computer and Communication Engineering, ECCE 2023*. https://doi.org/10.1109/ECCE57851.2023.10101496

KOCAOĞULLAR, C., YILDIRIM, K., SAKAOĞULLARI, M. A., & KÜPÇÜ, A. (2025). BasGit: a secure digital ePassport alternative. *Turkish Journal of Electrical Engineering and Computer Sciences*, *33*(5), 631–646. https://doi.org/10.55730/1300-0632.4148

Kuperberg, M. (2020). *Blockchain-based Identity Management : A Survey from the Enterprise and Ecosystem Perspective*. *November*. https://doi.org/10.1109/TEM.2019.2926471

Medina, J., Member, S., Cessa-rojas, R., Member, S., & Umpaichitra, V. (2021). Reducing COVID-19 Cases and Deaths by Applying Blockchain in Vaccination Rollout Management. *IEEE Open Journal of Engineering in Medicine and Biology*, *PP*, 1. https://doi.org/10.1109/OJEMB.2021.3093774

Papatheodorou, N., Hatzivasilis, G., & Papadakis, N. (2025). The YouGovern Secure Blockchain-Based Self-Sovereign Identity (SSI) Management and Access Control. *Applied Sciences (Switzerland)*, *15*(12). https://doi.org/10.3390/app15126437

Ricci, L., Di Francesco Maesa, D., Favenza, A., & Ferro, E. (2021). Blockchains for covid-19 contact tracing and vaccine support: A systematic review. *IEEE Access*, *9*, 37936–37950. https://doi.org/10.1109/ACCESS.2021.3063152

Terkes, M., Demirci, A., Gokalp, E., & Cali, U. (2024). Battery Passport for Second-Life Batteries: Potential Applications and Challenges. *IEEE Access*, *12*, 128424–128467. https://doi.org/10.1109/ACCESS.2024.3450790

Vinoth Kumar, C., Selvaprabhu, P., Baska, N., Vivek Menon, U., Babu Kumaravelu, V., Chinnadurai, S., & Ali, F. (2024). Ethereum Blockchain Framework Enabling Banks to Know Their Customers. *IEEE Access*, *12*, 101356–101365. https://doi.org/10.1109/ACCESS.2024.3427805