Journal of Research Technology and Engineering
www.jrte.org

BlooDChain: Design and Analytical Evaluation of a Privacy-Preserving Blockchain Framework with Steganography for Anonymous Blood Donor Matching

*W.D.J.I. Senarathna, T. A. H. Dilpriya

Department of Computer and Data Science, Faculty of Computing
NSBM Green University
Mahenwatta, Pitipana, Homagama, Sri Lanka
*Corresponding Author Email: janakaishansenarathna@outlook.com

Received: 28 June 2026; Revised: 05 August 2026; Accepted: 05 September 2026; Available online: 10 Oct 2026

Abstract: BlooDChain is a novel blockchain-enabled privacy-preserving blood donation platform that addresses critical challenges in donor-recipient coordination while maintaining robust privacy protection. The system integrates a multi-layered security architecture combining blockchain immutability, steganographic data concealment, hardware-based encryption, and zero-knowledge anonymous matching protocols to provide unprecedented donor privacy protection. BlooDChain introduces a three-tier privacy model accommodating varying donor risk profiles, representing a significant advancement over one-size-fits-all approaches. The anonymous matching protocol enables compatibility verification without identity disclosure during matching, addressing critical gaps in existing platforms, particularly valuable for rare blood type donors facing targeted risks. An ethical gift-based incentive mechanism encourages participation while maintaining non-commercial principles aligned with healthcare ethics. Hardware-based physical encryption keys provide additional security resistant to purely digital attacks, demonstrating a defense-in-depth approach. Comprehensive security analysis demonstrates resistance to diverse attack vectors, including identity disclosure, data extraction, cryptographic attacks, smart contract exploits, consensus attacks, and hardware compromises. Performance evaluation shows acceptable throughput (~358 TPS), low matching latency (~200 ms), and reasonable registration times (~3-5 seconds) suitable for blood donation coordination. BlooDChain advances state-of-the-art through the first comprehensive integration of blockchain, steganography, and hardware encryption for blood donation, a novel zero-knowledge matching protocol, an ethical incentive mechanism, a multi-tier privacy framework, and a practical implementation roadmap. The platform demonstrates the potential for advanced cryptographic techniques and blockchain technology to create blood donation systems simultaneously achieving high privacy, strong security, efficient coordination, and ethical incentive alignment.

Index Terms: Anonymous Matching, Blockchain, Blood Donation, Hardware Encryption, Privacy-Preserving Systems, Steganography

1 INTRODUCTION

1.1 Background and Motivation

Blood donation remains critical for modern healthcare, with millions depending on timely access to compatible supplies. Despite technological advancements, blood donation platforms face significant

challenges in efficient matching while maintaining privacy and security standards. Traditional centralized systems are vulnerable to single points of failure, data breaches, and unauthorized access to sensitive donor information [1].

Blockchain technology has revolutionized healthcare domains by providing decentralized, immutable, and transparent data management [2]. Recent implementations demonstrate significant potential in protecting patient privacy and ensuring data integrity [3]. However, existing blockchain healthcare applications often overlook specific requirements of blood donation systems, particularly donor anonymity for rare blood types and protection against targeted attacks [4].

Privacy concerns extend beyond general data protection. Individuals with rare blood types face unique risks when information is exposed, potentially becoming targets for coercion or exploitation [7]. Traditional encryption methods, while effective for data protection, do not adequately conceal the existence of sensitive information itself [8]. This necessitates advanced privacy-preserving techniques combining encryption with steganographic concealment [9].

1.2 Research Objectives and Contributions

This paper presents BlooDChain, a comprehensive solution addressing the identified research gaps in privacy-preserving blood donation management. The primary objective is to design a decentralized blockchain architecture that ensures transparency, immutability, and resistance to single-point failures while integrating steganographic data concealment techniques to hide sensitive donor information within blockchain structures. The system develops an anonymous matching protocol that enables compatibility searches without privacy compromise and implements hardware-based physical encryption keys to provide enhanced security against sophisticated attacks. Additionally, BlooDChain creates an ethical incentive mechanism to encourage rare blood type donor participation while maintaining non-commercial principles, supported by comprehensive security analysis demonstrating resistance to diverse attack vectors.

The main contributions of this research represent significant advancements in privacy-preserving healthcare systems. First, we introduce a novel blockchain architecture with integrated steganographic concealment specifically designed for blood donation management, combining distributed ledger immutability with multi-layered data hiding techniques. Second, we present an anonymous donor-recipient matching protocol utilizing zero-knowledge proofs that enables blood type compatibility verification without revealing participant identities during the matching phase. Third, we develop a multi-layered security framework that synergistically combines blockchain technology, steganographic concealment, and hardware-based encryption to provide defense-in-depth protection for sensitive donor information. Fourth, we design an ethical gift-based incentive mechanism that encourages participation from donors with rare blood types while maintaining adherence to healthcare ethical standards and regulatory guidelines. Fifth, we implement automated smart contract solutions for matching processes and incentive distribution, eliminating the need for centralized authority intervention while ensuring transparent and fair operations. Finally, we conduct comprehensive comparative evaluation demonstrating that BlooDChain achieves superior privacy protection and security characteristics compared to existing blood donation management systems.

2 RELATED WORK

2.1 Blockchain in Healthcare

Blockchain has emerged as transformative for healthcare data management. Li et al. [1] conducted systematic review of privacy preservation in blockchain-based healthcare, identifying key challenges requiring additional privacy-enhancing technologies beyond basic blockchain features. Shaikh et al. [2] proposed a framework using proof of authority consensus for ethical healthcare asset management, demonstrating improved accountability while maintaining data integrity. Adeniyi et al. [3] developed blockchain-based smart healthcare systems addressing centralized database vulnerabilities through multiple security layers including encryption and access control. Kasyapa and Vanmathi [4] examined blockchain integration challenges, identifying scalability, interoperability, and regulatory compliance as primary concerns requiring careful system design [10]. Senarathna [5] presented a comprehensive review of blockchain architecture, consensus mechanisms, security properties, and scalability solutions for distributed systems, characterising the throughput and finality trade-offs that govern permissioned deployments in regulated domains. Senarathna [6] further demonstrated a decentralized blockchain-based platform for mental health nature therapy, illustrating how distributed ledgers can underpin patient-facing healthcare services while preserving participant autonomy and consent.

2.2 Encryption and Privacy Technologies

Advanced encryption frameworks continue evolving for healthcare protection. Gandhi and Rathod [7] developed blockchain-driven protocols with advanced encryption for patient data security [11]. Abasaheb et al. [8] proposed blockchain-integrated systems using advanced Blowfish encryption with optimal key generation, demonstrating enhanced confidentiality while maintaining acceptable performance [12]. Hybrid encryption approaches have been developed for IoT-enabled healthcare environments. Popoola et al. [9] designed optimized frameworks ensuring data confidentiality in smart home healthcare, combining symmetric and asymmetric encryption efficiency [16]. Ravichandran et al. [10] developed efficient medical data encryption using selective shuffling for resource-constrained devices [17]. Senarathna and Dilpriya [13] analysed the role of cryptography in blockchain, detailing how cryptographic hash chaining and digital signatures jointly establish immutability, transparency, and verifiable integrity. Senarathna [14] examined the specific cryptographic primitives on which blockchain systems depend, and Senarathna [15] assessed cryptographic techniques for protecting cloud-resident data, a consideration directly relevant to the off-chain storage tier employed in BlooDChain.

2.3 Steganography in Medical Systems

Steganography integration with blockchain has emerged for healthcare data protection. Recent studies presented StegoSec-EHR, a blockchain-enabled IoT framework for secure electronic health record sharing via steganography in genetic disease diagnosis [16], demonstrating effective concealment within medical images stored on blockchain networks. Riaz et al. [17] proposed robust steganography techniques for medical record protection, employing adaptive embedding strategies maintaining image quality while maximizing hiding capacity [18]. Deep learning approaches have advanced capabilities, with Issac and Kumar [18] developing steganography using squeeze and excitation architectures achieving higher hiding capacity and better security than traditional methods [19].

Combined steganography and cryptography provide enhanced security for medical image transmission [19], first encrypting images then embedding encrypted data within cover images using steganographic techniques

[20]. Muhammad et al. [20] introduced MedProtect, protecting electronic patient data using interpolation-based medical image steganography [21].

2.4 Blood Donation Systems

Blockchain applications in organ and tissue donation provide relevant precedents. Igboanusi et al. [26] developed BOMS (Blockchain-enabled Organ Matching System), demonstrating effective smart contracts for automating matching algorithms while maintaining cryptographic privacy. Le et al. [27] introduced BloodChain, a Hyperledger Fabric-based network that manages detailed blood information, including consumption and disposal, among participating organizations. Hawashin et al. [28] proposed a private Ethereum solution that automates blood donation management with traceability and auditability while storing large data off chain in IPFS. Agarwal et al. [29] used smart contracts to automate the donation procedure while preserving donor and recipient anonymity, and Singh et al. [30] proposed a blockchain application for managing the blood supply chain and recommended RFID to prevent transfusion errors.

2.5 Smart Contracts and IPFS Integration

Smart contracts demonstrate significant potential for sustainable healthcare. Marino and Diaz Paz [31] conducted systematic review identifying applications in healthcare process automation and compliance [24]. Comparative analysis of Hyperledger Fabric and Ethereum revealed performance trade-offs for healthcare contexts [32], with Fabric demonstrating superior throughput while Ethereum provided broader developer support [25]. Integration of blockchain and IPFS enables efficient healthcare data management. Ma and Zhang [36] integrated blockchain with ZK-ROLLUP for healthcare data privacy via IPFS [33], storing large files on IPFS while recording cryptographic hashes on blockchain [34]. Kumari et al. [38] developed HealthRec-Chain, a patient-centric blockchain-enabled IPFS system for privacy-preserving health data management [35].

2.6 Privacy-Preserving Approaches

Contemporary privacy engineering addresses threats in anonymized healthcare data [43], identifying re-identification, linkage, and inference attacks as primary concerns [36]. Ko and Hwang [44] proposed self-sovereign management schemes with personal data stores and decentralized identifiers, enabling patient control without centralized identity providers [37]. Choudhury et al. [46] implemented Personal Health Train using federated deep learning for privacy-preserving analytics, training models on distributed data without centralization [38]. Prasser et al. [47] systematized privacy-preserving data sharing infrastructures for medical research, evaluating architectures and governance models [39].

2.7 Attribute-Based Encryption

Attribute-based encryption offers fine-grained access control. Nekouie et al. [48] compared ABE schemes in healthcare systems, demonstrating ciphertext-policy ABE effectiveness for scenarios where data owners define policies based on user attributes [40]. Zeng et al. [49] enhanced smart healthcare networks integrating ABE for optimization and anti-corruption mechanisms [41]. Yang et al. [50] developed HA-Med, a blockchain solution for sharing medical data with hidden policies and attributes, concealing access control policies from unauthorized parties [42]. Recent studies proposed attribute encryption for high-dimensional medical data using fuzzy algorithms enabling approximate matching [51], and blockchain-based electronic health records with fine-grained ABE and decentralized storage [52].

2.8 Research Gap Analysis

Analysis of existing literature reveals several critical gaps that motivate the development of BlooDChain. Current blockchain blood donation systems [27]–[30] primarily focus on supply chain transparency and donation tracking but lack comprehensive privacy protection mechanisms for rare blood type donors who face heightened security risks. While medical steganography research [16]–[25] demonstrates effective data concealment techniques, these approaches have not been systematically integrated with blockchain platforms to provide multi-layered privacy protection. Privacy-preserving healthcare systems [43]–[47] employ advanced cryptographic techniques but do not adequately address the specific requirements of anonymous donor-recipient matching where both parties require privacy protection during compatibility verification.

Smart contract implementations in healthcare [31]–[35] successfully automate various processes but lack specific designs for ethical incentive mechanisms that maintain non-commercial principles while encouraging rare blood type donor participation. Attribute-based encryption systems [48]–[52] provide fine-grained access control but do not integrate hardware-based physical keys for enhanced security in scenarios where digital key compromise poses severe risks. Furthermore, existing IPFS-blockchain integration frameworks [36]–[42] address scalability for general healthcare data but do not optimize for the specific data structures and access patterns inherent in blood donation matching systems. BlooDChain addresses these gaps by providing the first comprehensive framework that integrates blockchain technology, steganographic data concealment, hardware-based encryption, and ethical incentive mechanisms specifically designed for privacy-preserving blood donation coordination.

3 SYSTEM ARCHITECTURE

3.1 Overview

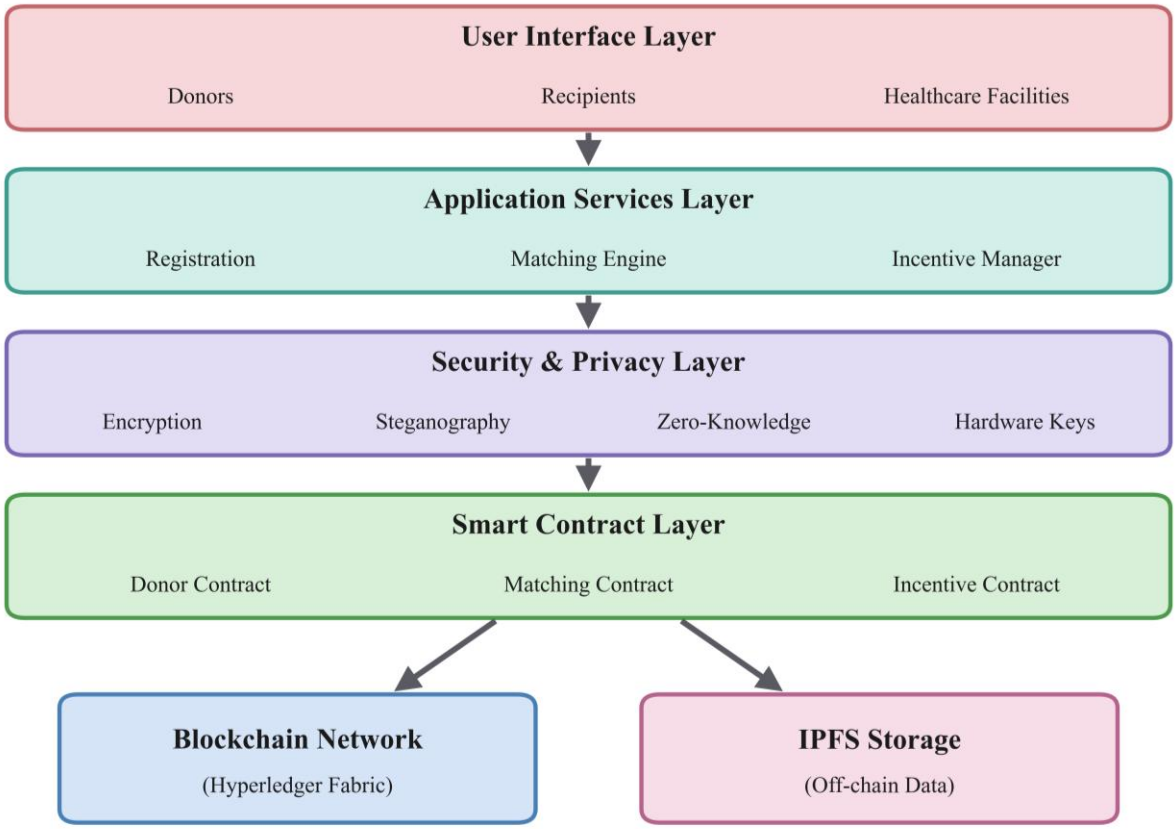

Fig. 1. BlooDChain System Architecture Overview

BlooDChain operates on a permissioned blockchain network where participants include donors, recipients, healthcare facilities, blood banks, and regulatory authorities. Unlike centralized systems maintaining vulnerable databases, BlooDChain distributes data across blockchain nodes with multi-layered cryptographic protection. Donor information is encrypted using advanced algorithms, then concealed within binary structures using steganography before blockchain storage. The platform introduces anonymous matching enabling recipients to search compatible donors based on blood type, location, and availability without revealing identities during initial matching. Zero-knowledge proof techniques verify compatibility without disclosing actual donor identities. Only after mutual consent does controlled identity disclosure occur through secure channels. Fig. 1 presents the layered architecture of BlooDChain. Donors, recipients, and healthcare facilities interact with the platform through the user interface layer, and their requests are handled by three application services: registration, the matching engine, and the incentive manager. Each request then passes through the security and privacy layer, which applies encryption, steganography, zero-knowledge proofs, and hardware keys, before the smart contract layer executes the donor, matching, and incentive contracts. The contracts record transactions on the Hyperledger Fabric network and keep large data objects in IPFS off-chain storage.

Hardware-based physical encryption keys (USB tokens or smart cards) provide additional authentication for accessing sensitive data. This hardware component protects against digital key theft and unauthorized access

even if blockchain nodes or communications are compromised. Physical keys store cryptographic credentials required to decrypt steganographically concealed data.

3.2 Key Components

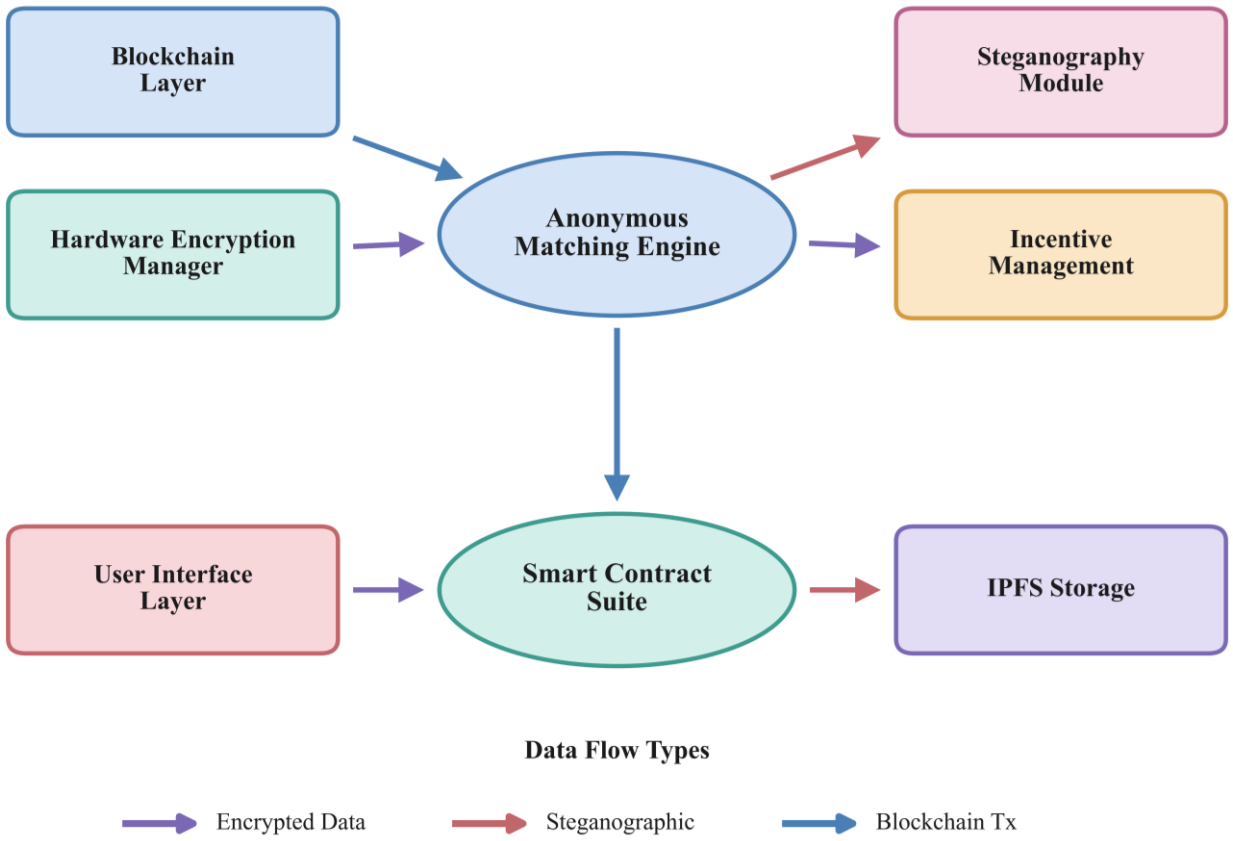

Fig. 2. BlooDChain Component Architecture

The BlooDChain platform comprises eight integrated components, whose interactions are shown in Fig. 2. The blockchain layer implements a permissioned network with PBFT consensus, storing encrypted and steganographically concealed records. The steganography module conceals donor data within binary structures using LSB replacement, spread spectrum, and deep learning techniques. The hardware encryption manager oversees physical keys (USB tokens, smart cards) for multi-factor authentication. The anonymous matching engine employs zero-knowledge proofs and homomorphic encryption for compatibility verification without identity disclosure. The smart contract suite automates registration, matching, and incentive distribution without centralized control. The incentive management system calculates ethical rewards for rare blood type donors based on rarity metrics. The user interface layer provides intuitive web and mobile access abstracting cryptographic complexity. Finally, IPFS integration handles large data objects with cryptographic hashes recorded on blockchain for integrity verification. In Fig. 2, the anonymous matching engine is the central component: it receives blockchain transactions from the blockchain layer and encrypted credentials from the hardware encryption manager, sends data to the steganography module for concealment, passes encrypted results to incentive management, and submits matching outcomes to the smart contract suite. The smart contract suite also receives requests from the user interface layer and stores large objects in IPFS, while the arrow colors distinguish encrypted data, steganographic, and blockchain transaction flows.

3.3 System Workflows

Donor Registration: Prospective donors initiate registration by providing personal information, blood type, medical history, and contact details while selecting their preferred privacy level (public, semi-anonymous, or fully anonymous). The system encrypts submitted information using strong cryptographic algorithms, converts encrypted data to binary format, and conceals it using steganographic techniques before storing on the blockchain via smart contract execution. A hardware encryption key is generated and securely provided to the donor, who receives confirmation with a unique platform identifier for subsequent access and authentication. Fig. 3 summarizes this workflow in nine steps: the donor accesses the platform, enters personal information, and selects a privacy level (steps 1–3); the data are encrypted, concealed using steganography, and stored on the blockchain (steps 4–6); and a hardware key is generated and delivered to the donor before registration completes (steps 7–9).

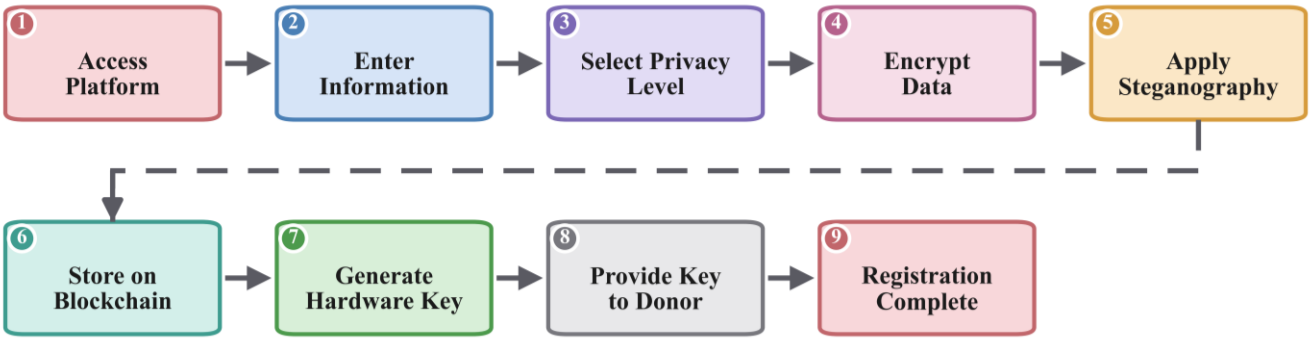

Fig. 3. Donor Registration Workflow

Donor Response and Coordination: Eligible donors receive encrypted notifications about matching requests and review anonymous recipient information including blood type needed, urgency, and general location. Upon acceptance, smart contracts facilitate controlled identity disclosure between parties, establishing secure communication channels for coordination details. Donation appointments are scheduled through the platform or associated healthcare facilities, with completion recorded immutably on blockchain through timestamped transactions. Both parties provide feedback and ratings stored on the blockchain for quality assurance and reputation management. Fig. 4 shows this process in nine steps: an eligible donor is notified and reviews the anonymous request (steps 1–2); after the donor accepts, identity is disclosed in a controlled way and a secure channel is opened (steps 3–5); and the appointment is scheduled, the donation is completed and recorded on the blockchain, and both parties give feedback (steps 6–9).

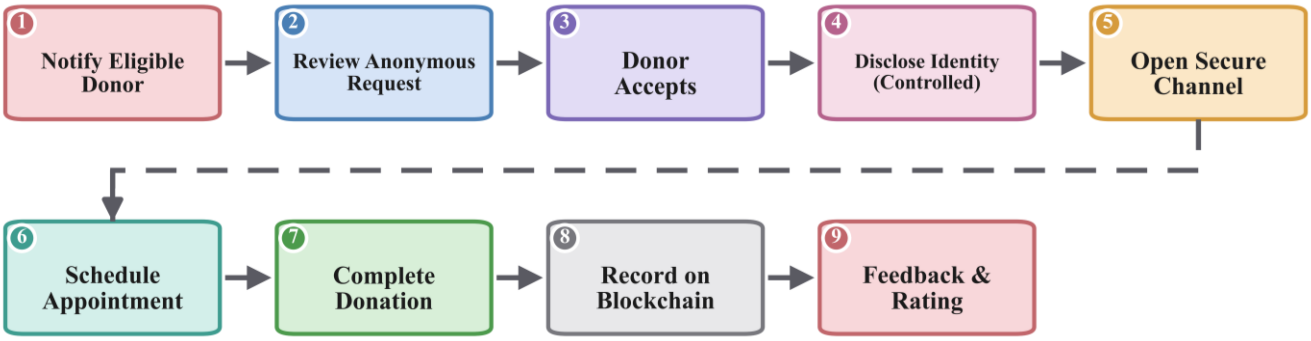

Fig. 4. Donation Coordination and Recording Workflow

Blood Search and Request: Recipients specify required blood type, quantity, urgency level, and location through the platform interface. The anonymous matching engine searches the blockchain for compatible donors without identity disclosure, calculating compatibility scores based on blood type, proximity, and availability. Matching results are presented as anonymous donor profiles, allowing recipients to select preferred donors and submit connection requests. All request transactions are recorded immutably on the blockchain with cryptographic commitments ensuring transparency and tamper resistance. Fig. 5 illustrates this workflow: the recipient specifies and submits the blood requirement (steps 1–2); the matching engine searches for compatible donors, verifies compatibility using zero-knowledge proofs, and scores and ranks the anonymous profiles (steps 3–6); and the recipient selects a donor and sends a connection request that is committed to the blockchain (steps 7–9).

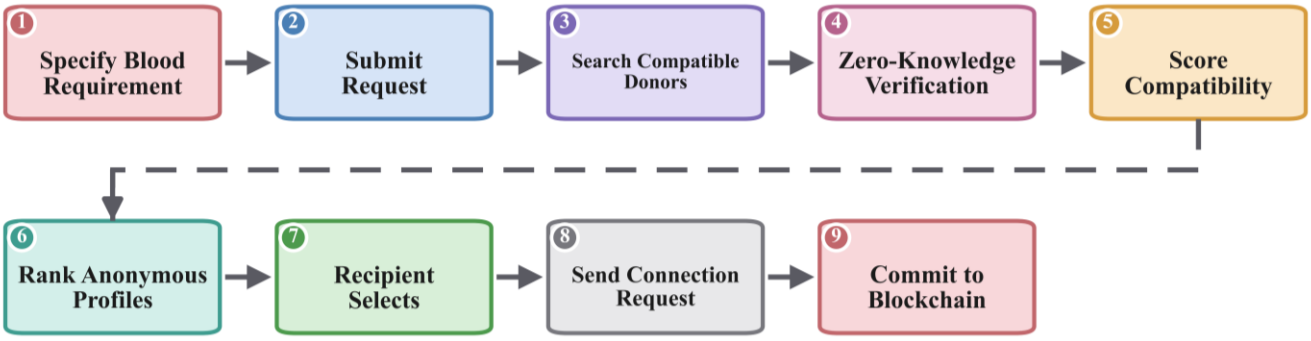

Fig. 5. Blood Request and Anonymous Matching Workflow

3.4 Privacy Levels

BlooDChain implements three privacy tiers: Public profiles enable direct identity visibility for verified recipients, suitable for common blood types. Semi-anonymous profiles conceal identity during matching until explicit donor acceptance. Fully anonymous profiles employ zero-knowledge matching with healthcare facility intermediaries, recommended for rare blood types facing heightened security risks.

4 DETAILED DESIGN

4.1 Blockchain Layer

Platform Selection: Hyperledger Fabric selected for modular architecture, private data collections, pluggable consensus, and fine-grained access control. Channel architecture enables separate communication channels for geographical regions while maintaining interoperability.

Consensus Mechanism: PBFT consensus ensures transaction finality, fast confirmation, and energy efficiency. PBFT tolerates up to ⌊(n-1)/3⌋ Byzantine nodes in n-validator network, providing robust security. Multi-endorsement requires approval from multiple healthcare organization nodes before ledger commitment. The tolerance bound and the corresponding safety condition are given in (1) and (2).

$$f = \left\lfloor \frac{n-1}{3} \right\rfloor \tag{1}$$

$$n \geq 3f + 1 \tag{2}$$

where n is the number of validator nodes and f the maximum number of simultaneously Byzantine nodes the network tolerates.

Data Structures: Blockchain stores donor records (encrypted and steganographically concealed profiles in private data collections), recipient requests (specifications with cryptographic commitments), matching transactions (compatibility scores and acceptance status), donation events (completed donations with verification signatures), and incentive allocations (reward distributions with timestamps).

Smart Contract Architecture: Modular contracts implement specific functionalities including DonorRegistrationContract (manages enrollment, profile updates, privacy settings), RecipientRequestContract (handles blood request submission, validation, prioritization), AnonymousMatchingContract (implements privacy-preserving matching using zero-knowledge proofs), DonationRecordingContract (records completed donations with verifiable signatures), and IncentiveDistributionContract (calculates rarity metrics, determines eligibility, allocates rewards). As shown in Fig. 6, the five contracts run as separate chaincode modules on the Hyperledger Fabric chaincode layer and write to a shared permissioned ledger, with sensitive donor data kept in private data collections. Keeping the contracts separate allows each function to be updated or audited without affecting the others.

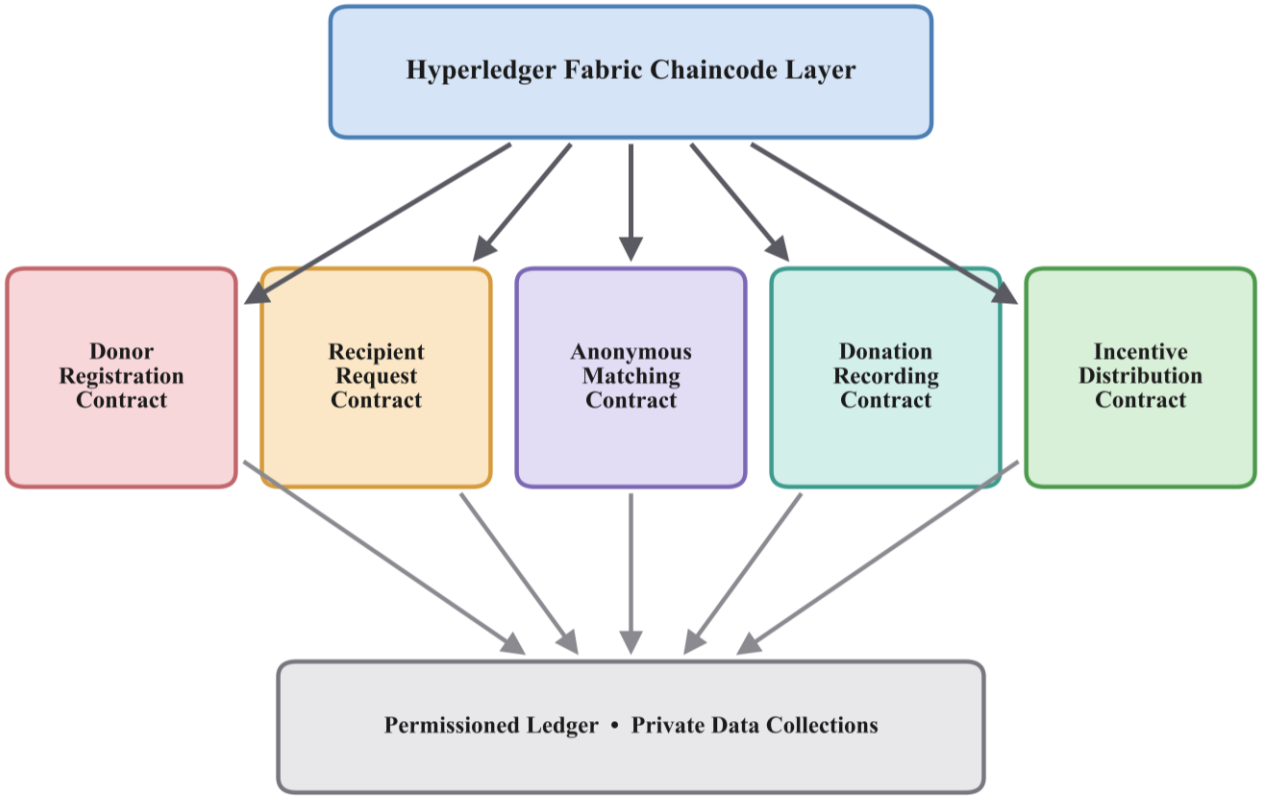

Fig. 6. Smart Contract Architecture

4.2 Steganography Integration

Technique Selection: Hybrid approach combining least significant bit (LSB) replacement for high capacity and computational efficiency, spread spectrum steganography spreading secret data across frequency spectrum for detection resistance, and deep learning-based adaptive steganography using neural networks learning optimal embedding strategies minimizing statistical detectability.

Concealment Workflow: Process encrypts donor data using AES-256, converts to binary representation, generates carrier data with appropriate expansion factor, calculates embedding positions using steganographic key, embeds encrypted data using hybrid LSB and spread spectrum approach, applies deep learning obfuscation, and verifies concealment quality against steganalysis tests.

Extraction Workflow: Authorized parties verify hardware key possession, apply deep learning extraction, calculate extraction positions using steganographic key, extract binary data from LSB and reverse spread spectrum, convert from binary representation, decrypt using hardware-derived key, verify data integrity, and log access event.

Security Properties: Steganographic layer conceals sensitive data existence, creates multi-layer security requiring defeat of both steganography and cryptography, resists statistical analysis through hybrid deep learning adaptation, and separates steganographic keys from encryption keys requiring attackers to compromise multiple independent secrets. Fig. 7 summarizes the complete concealment pipeline: donor data are encrypted with AES-256, converted to binary, placed into generated carrier data, embedded using the hybrid LSB and spread spectrum method under the steganographic key, obfuscated by the deep learning model, and checked against steganalysis tests before being stored on the blockchain.

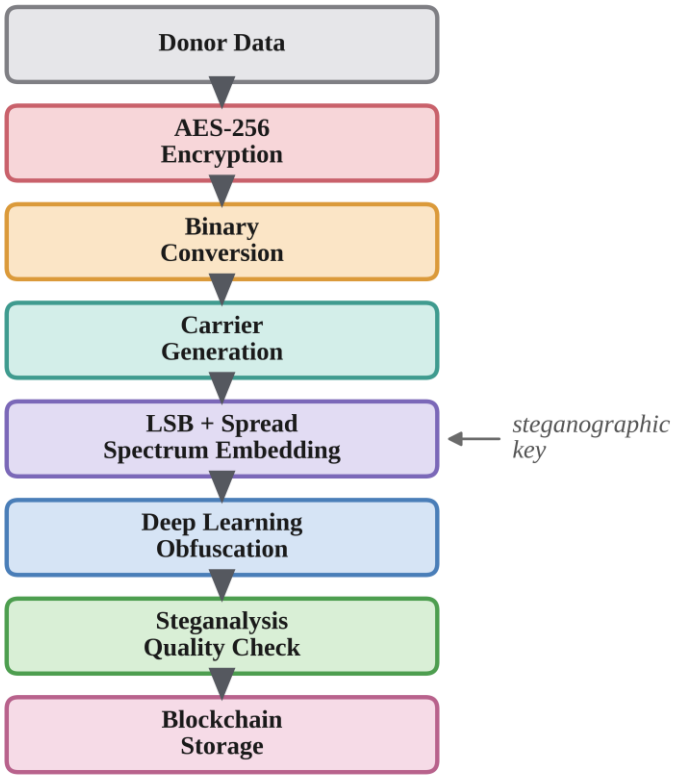

Fig. 7. Steganographic Concealment Process

4.3 Hardware-Based Encryption

Hardware Key Architecture: USB security tokens or smart cards store cryptographic credentials providing physical possession requirement (preventing purely remote attacks), tamper-resistant storage (protecting against extraction attempts), secure cryptographic operations (performing encryption/decryption internally without exposing keys), and multi-factor authentication (combining hardware tokens with PINs or biometrics). Fig. 8 maps these properties to the token: physical possession, tamper-resistant storage, and on-device cryptographic operations protect the keys themselves, while multi-factor authentication and PIN or biometric unlock control who can use them.

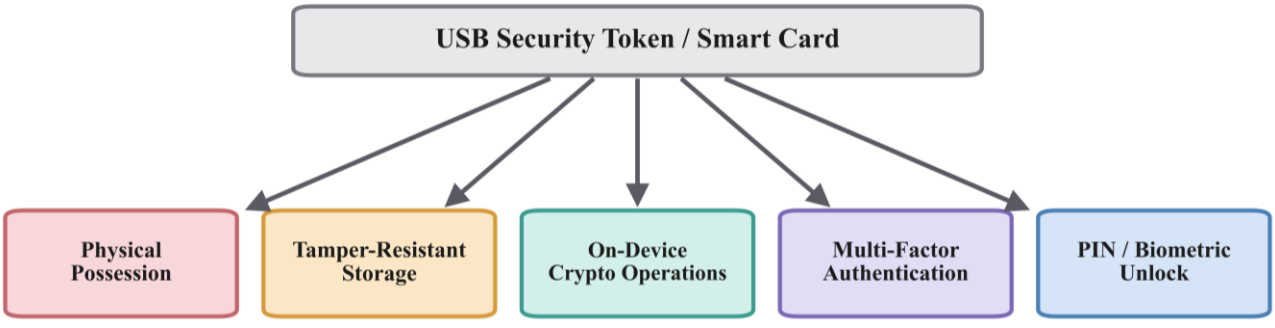

Fig. 8. Hardware Encryption Key Architecture

Initialization Process: During registration, system generates RSA keypair (4096-bit), symmetric encryption key (AES-256), and steganographic key (256-bit). Keys packaged and encrypted with PIN protection, written to hardware token, with public key hash registered on blockchain and encrypted backup stored securely.

Access Control: Data access requires hardware token authenticity verification, PIN verification with limited attempts before lockout, key retrieval from hardware token, concealed data retrieval from blockchain, extraction and decryption using hardware keys, successful access logging, and failed attempt tracking with automatic lockout after maximum attempts.

Recovery Mechanisms: Backup recovery uses encrypted backup codes requiring identity verification. Social recovery enables trusted contacts to collectively authorize key recovery through multi-signature scheme. Emergency revocation allows immediate key revocation via blockchain transaction. Re-keying protocol supports periodic key rotation with data re-encryption without disrupting operations.

4.4 Anonymous Matching Protocol

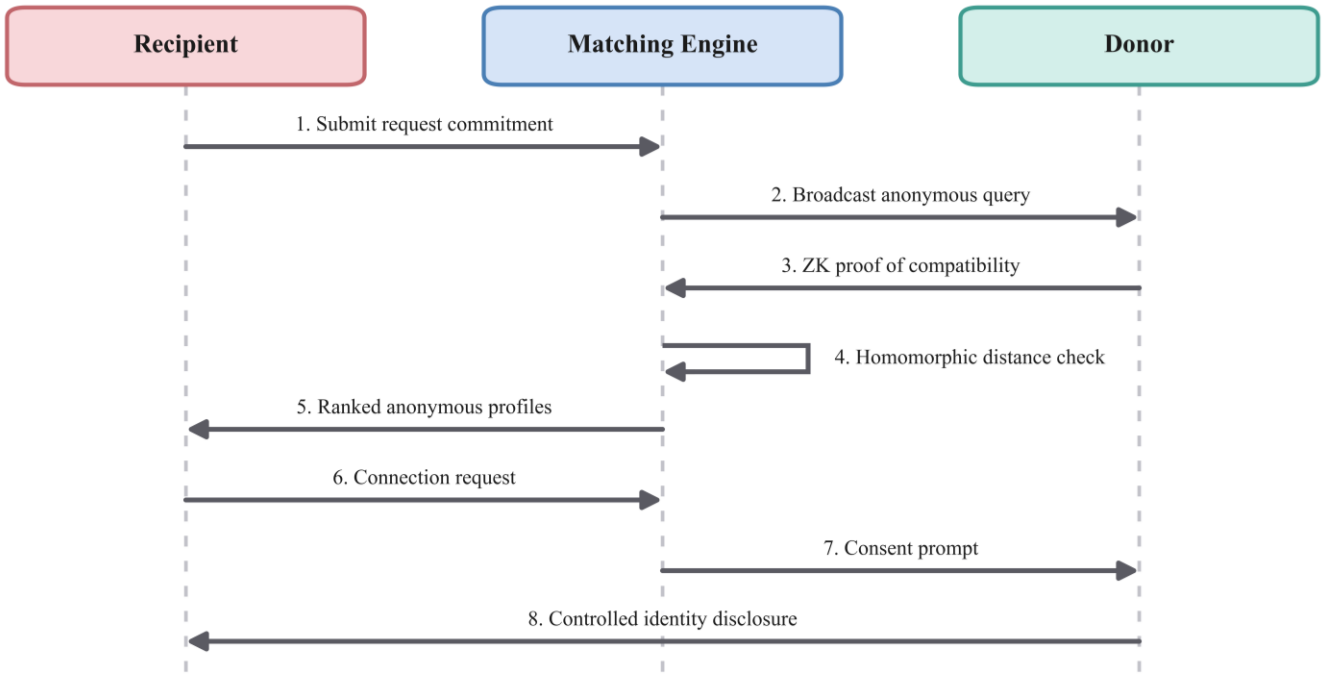

Fig. 9. Anonymous Matching Protocol Flow

The anonymous matching protocol involves three parties, the recipient, the matching engine, and the donor, who exchange the eight messages shown in Fig. 9. The recipient first submits a commitment to the blood request (1), which the matching engine broadcasts as an anonymous query to eligible donors (2). Each donor replies with a zero-knowledge proof of blood type compatibility (3), and the engine performs a homomorphic distance check (4) before returning ranked anonymous profiles to the recipient (5). When the recipient sends a connection request (6), the engine asks the donor for consent (7), and identity is disclosed in a controlled way only after the donor agrees (8). The mechanisms behind these steps are described below.

Zero-Knowledge Blood Type Verification: Protocol defines compatibility matrix, checks compatibility between donor and requested blood types, generates cryptographic commitment to donor blood type, and

creates zero-knowledge proof demonstrating "I know a blood type compatible with requested type" without revealing actual blood type. Verification confirms proof validity without learning donor blood type.

Privacy-Preserving Location Proximity: Uses homomorphic encryption for distance calculation. Donor and recipient coordinates encrypted using homomorphic encryption, encrypted distance calculated using Haversine formula on encrypted values, distance decrypted, and rounded to privacy radius preventing exact location inference. The great-circle separation is evaluated as in (3) and quantised as in (4).

$$d \;=\; 2R\,\arcsin\left(\sqrt{\sin^2\left(\frac{\varphi_D-\varphi_R}{2}\right)\;+\;\cos\varphi_R\,\cos\varphi_D\,\sin^2\left(\frac{\lambda_D-\lambda_R}{2}\right)}\right) \tag{3}$$

$$d_\rho \;=\; \rho\;\cdot\;\left\lfloor\frac{d}{\rho}\;+\;\frac{1}{2}\right\rfloor \tag{4}$$

where φ and λ denote the latitude and longitude of the donor (D) and recipient (R), R is the Earth radius, d_ρ is the quantised distance, and ρ is the privacy radius to which the decrypted distance is rounded.

Secure Multi-Party Matching: For fully anonymous profiles, implements secure multi-party computation where matching decisions computed without any party learning sensitive information. Each party holds shares of donor and request attributes. Computation proceeds through secure blood type compatibility checking, secure distance computation, and secure score aggregation, with only final match score revealed publicly.

Controlled Identity Disclosure: Upon mutual consent, system verifies donor and recipient consent for specific matching. For fully anonymous privacy level, identities disclosed only to healthcare facility intermediary. For semi-anonymous level, contact information disclosed for direct coordination. For public profiles, full information sharing occurs between parties.

4.5 Incentive Mechanism

Rarity Calculation: System continuously calculates blood type rarity metrics using registered donor statistics (total donors and donors by blood type), historical demand data (total requests and requests by blood type), and regional adjustment factors. Rarity score computed as (demandRatio / frequency) × normalizationFactor × regionalFactor, updated regularly in rarity database. The rarity score is defined in (5).

$$R_b \;=\; \frac{\frac{Q_b}{Q}}{\frac{N_b}{N}}\;\cdot\;\alpha\;\cdot\;\gamma_r \tag{5}$$

where Q_b and N_b are the request count and registered donor count for blood type b, Q and N are the corresponding totals, α is a normalisation constant, and γ_r is the regional adjustment factor.

Allocation Logic: Smart contracts determine incentives by calculating current rarity score, checking eligibility against minimum threshold, analyzing donor history for frequency bonus, calculating urgency multiplier based on donation urgency level, determining base incentive value from rarity tier mapping, computing total value as baseValue × (1 + frequencyBonus) × urgencyMultiplier, selecting incentive type based on value, recording allocation on blockchain, and notifying donor. The resulting incentive value is computed as in (6).

$$V \;=\; V_{\text{base}}(R_b)\;\cdot\;\left(1\;+\;\beta_f\right)\;\cdot\;\mu_u \tag{6}$$

where $V_{base}(R_b)$ is the rarity-tier base value, β_f the donation-frequency bonus, and μ_u the urgency multiplier.

Incentive Types: Non-monetary rewards include recognition (certificates, badges, honor roll with consent), priority access (priority matching if requiring blood in future), gift vouchers (health-related services, wellness programs, retail), community benefits (health screening, wellness workshops, educational resources), and symbolic gifts (medals, commemorative items for multiple rare type donations).

Ethical Safeguards: System implements value caps limiting maximum incentive values, non-transferability tying incentives to donor identity, transparency recording all allocations on blockchain for audit, regulatory compliance aligning with regional healthcare regulations and ethical guidelines, and voluntary nature allowing opt-out while maintaining platform access. Fig. 10 summarizes the incentive mechanism: donor statistics, historical demand, and regional factors feed the rarity score engine defined in (5); the allocation logic applies the eligibility, frequency bonus, and urgency rules of (6); and the resulting value is mapped to one of five reward types, all subject to value caps, non-transferability, and blockchain auditing.

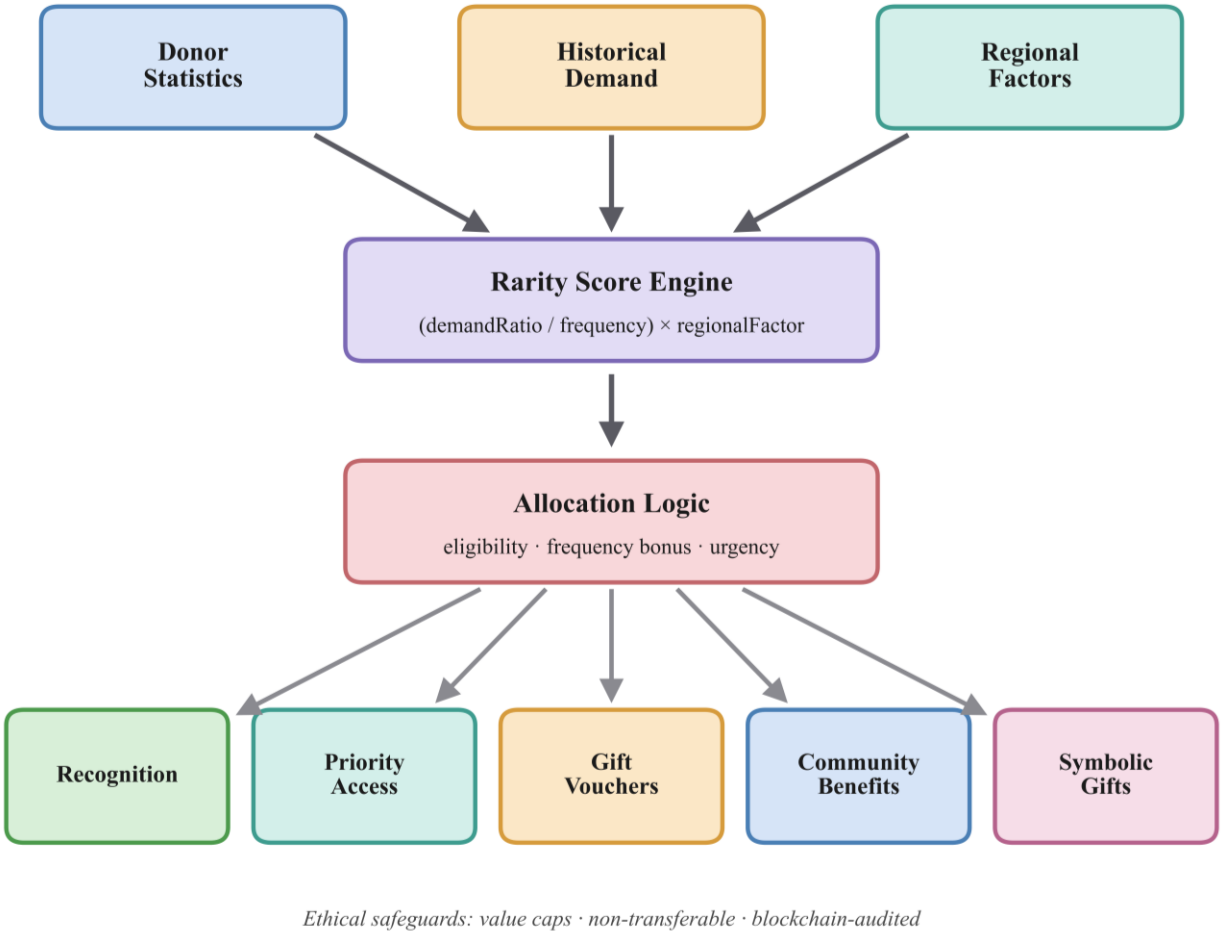

Fig. 10. Incentive Mechanism Architecture

5 Security Analysis

5.1 Threat Model

Adversary Types: External attackers attempting unauthorized access through network attacks or cryptanalysis, compromised blockchain validator nodes manipulating transactions, malicious insiders abusing privileges, curious recipients attempting to learn donor identities beyond protocol permissions, and colluding parties pooling information for re-identification attacks.

Attack Vectors: Identity disclosure attacks linking anonymous profiles to real identities, data extraction attacks extracting steganographically concealed information, cryptographic attacks breaking encryption through brute force or cryptanalysis, smart contract exploitation manipulating matching results or stealing incentives, consensus attacks compromising blockchain through 51% or eclipse attacks, hardware key theft through physical theft or cloning, and re-identification attacks correlating anonymized attributes with external datasets. To counter these adversaries and attack vectors, BlooDChain arranges its defenses in the five layers shown in Fig. 11: hardware, cryptographic, steganographic, blockchain, and governance. Because the layers use independent mechanisms, an attacker must defeat several of them to reach donor data; the resistance of each layer is analyzed in Section 5.3.

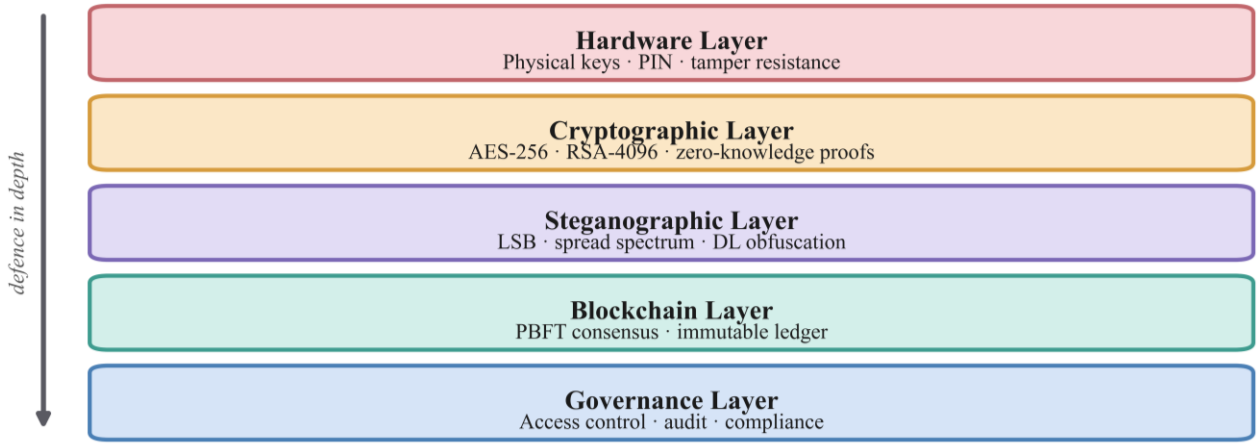

Fig. 11. Security Architecture Layers

5.2 Security Properties

Confidentiality: Donor information remains accessible only to authorized parties possessing appropriate credentials. Multi-layered protection through encryption, steganography, and hardware keys ensures data protection even if individual layers compromised. Formal property: P(A learns D | A lacks K_e, K_s, K_h) ≤ ε where ε is negligibly small.

$$\Pr[A \rightarrow D \mid K_e, K_s, K_h \notin A] \leq \varepsilon \tag{7}$$

where D is the protected donor record and K_e, K_s, K_h are the encryption, steganographic and hardware keys respectively, and ε is negligible in the security parameter.

Anonymity: Donor identities remain anonymous during matching with disclosure only after mutual consent. Formal property: P(O identifies D from M | O observes M) ≤ 1/n + ε where n is total potential donors.

$$\Pr[O \rightarrow \mathrm{id}(D) \mid M] \leq \frac{1}{n} + \varepsilon \tag{8}$$

where n is the size of the anonymity set of potential donors and M the matching transcript observed by O.

Integrity: All blockchain records are tamper-proof with attempted modifications detectable through cryptographic hash verification. Formal property: P(A produces B' where B' ≠ B and H(B') = H(B)) ≤ ε.

$$\Pr[H(B') = H(B) \wedge B' \neq B] \leq \varepsilon \tag{9}$$

where B is a committed block, B′ any distinct forgery, and H the collision-resistant ledger hash function.

Availability: Decentralized architecture ensures system operation even when individual nodes fail. System remains operational with at least f+1 correct nodes in network designed to tolerate f Byzantine failures.

Authenticity: All transactions cryptographically signed by creators enabling verification and non-repudiation. Verifier confirms transaction originated from holder of corresponding private key.

Unlinkability: Multiple donations by same donor remain unlinkable to observers without authorization. Formal property: P(A links T1 and T2 | both from D) ≤ 1/2 + ε.

$$\Pr[\text{Link}(T_1, T_2) \mid D] \leq \frac{1}{2} + \varepsilon \tag{10}$$

where T_1 and T_2 are two donation transactions originating from the same donor D.

5.3 Attack Resistance

Identity Disclosure Resistance: Traffic analysis mitigated through encrypted communications, mixing networks obscuring origins, and randomized transaction timing. Timing correlation defeated by batch processing, randomized submission delays, and decoy transactions. Auxiliary information attacks prevented through minimal attribute disclosure, fuzzing quasi-identifiers, and k-anonymity enforcement.

Data Extraction Resistance: Statistical steganalysis resisted by deep learning adaptive steganography, randomized embedding positions, and hybrid techniques. Machine learning steganalysis encounters training on normal blockchain patterns, adversarial examples confusing classifiers, and regular model updates. Known-plaintext attacks limited by unique encryption keys per donor, key rotation, and independent steganographic keys.

Cryptographic Attack Resistance: Brute force attacks computationally infeasible due to 256-bit AES and 4096-bit RSA requiring 2^256 and equivalent operations respectively, with hardware rate limiting preventing rapid guessing. Side-channel attacks resisted through constant-time operations, timing randomization, and electromagnetic shielding. Quantum computing threats addressed through post-quantum algorithm readiness and lattice-based encryption.

Smart Contract Attack Resistance: Reentrancy attacks prevented by checks-effects-interactions pattern and reentrancy guards. Integer overflow/underflow protection via SafeMath libraries and bounds validation. Access control violations prevented through role-based enforcement, multi-signature requirements, and time-locked administrative functions.

Consensus Attack Resistance: 51% attacks mitigated through permissioned network limiting validators, high economic cost of controlling 2/3 validators, validator diversity across organizations and regions, and continuous misbehavior monitoring. Eclipse attacks defended by diverse network connections, authenticated peers, topology monitoring, and redundant paths.

Hardware Key Attack Resistance: Physical theft limited impact through PIN/biometric protection, limited access attempts before lockout, remote revocation capability, and tamper-evident packaging. Cloning attempts resisted by tamper-resistant hardware preventing extraction, cryptographic attestation of authentic hardware, and challenge-response protocols detecting clones.

6 Performance Evaluation

6.1 Theoretical Analysis

Transaction Throughput: For Hyperledger Fabric with 2-second block generation, 2 MB maximum block size, and 2 KB average transaction size, theoretical maximum throughput is TPS_max = 2048 KB / (2 KB × 2s) = 512 TPS. Accounting for consensus overhead and network latency with 0.7 efficiency factor yields TPS_effective ≈ 358 TPS, sufficient for blood donation platform serving millions with average rates below peak capacity. Peak and effective throughput are given by (11) and (12).

$$\mathrm{TPS}_{\max} = \frac{S_{\mathrm{block}}}{S_{\mathrm{tx}} \cdot T_{\mathrm{block}}} = \frac{2048}{2 \cdot 2} = 512\ \mathrm{TPS} \tag{11}$$

$$\mathrm{TPS}_{\mathrm{eff}} = \eta \cdot \mathrm{TPS}_{\max} = 0.7 \cdot 512 \approx 358\ \mathrm{TPS} \tag{12}$$

where S_{block} is the maximum block size (2048 KB), S_{tx} the mean transaction size (2 KB), T_{block} the block interval (2 s), and $\eta = 0.7$ the consensus-and-network efficiency factor.

Fig. 12 compares this effective throughput, and the matching latency estimated in the latency analysis below, with a traditional centralized system and two blockchain-based blood donation systems [27], [28]. Throughput is read on the left axis and matching latency on the right, logarithmic axis; the BlooDChain values are analytical estimates from (12) and the latency analysis, and the comparison is discussed in Section 6.2.

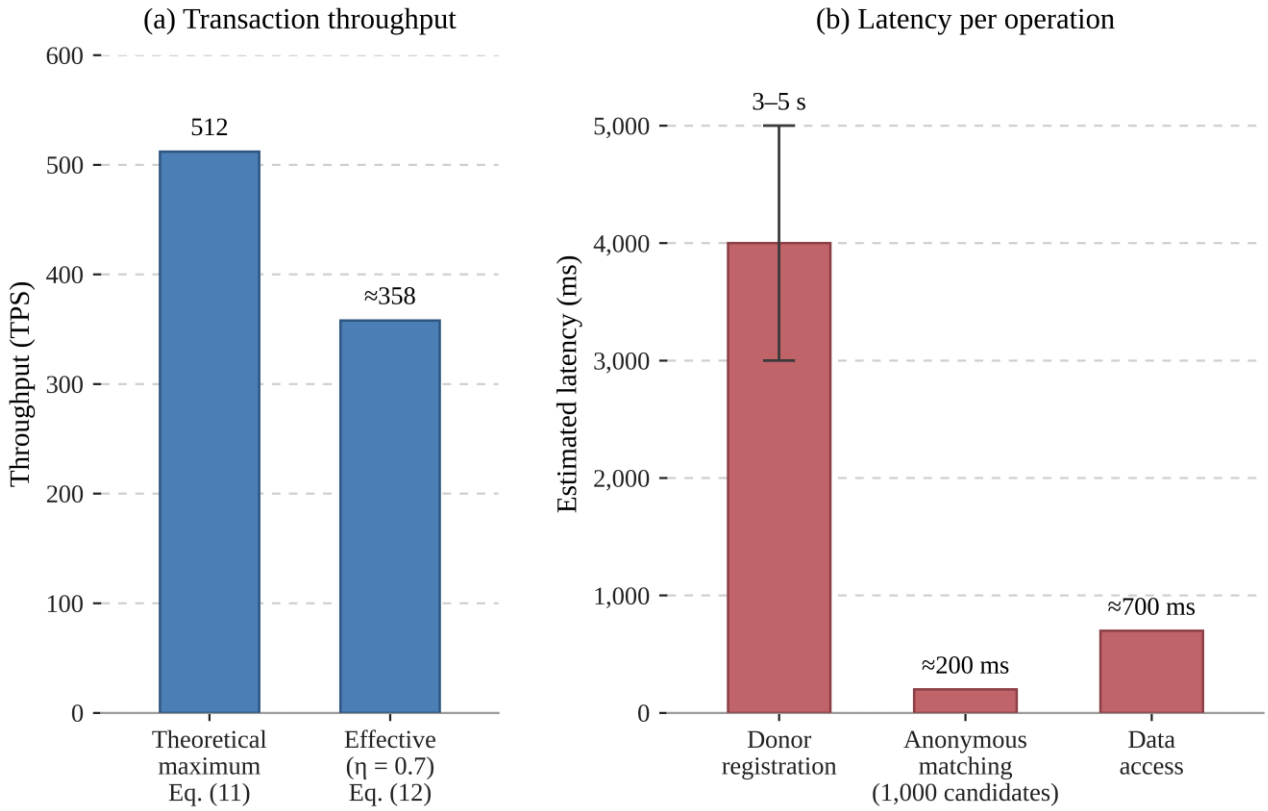

Fig. 12. Performance Metrics Comparison

Latency Analysis: Donor registration latency totals approximately 3-5 seconds (AES-256 encryption ~2 ms, deep learning steganography ~150 ms, blockchain transaction confirmation ~2-4 seconds, hardware key generation ~500 ms). Matching query latency approximately 200 ms for 1000 candidate donors (database query ~100 ms, zero-knowledge proof ~50 ms per donor with optimization, ranking algorithm ~20 ms). Data access latency totals approximately 700 ms (hardware authentication ~100 ms, blockchain retrieval ~500 ms, steganographic extraction ~100 ms, decryption ~2 ms).

Storage Requirements: Per-donor storage includes personal information (~1 KB), medical history (~5 KB), encryption overhead (~200 bytes), and steganographic expansion (10× factor) totaling ~62 KB per donor. For 1 million donors, approximately 62 GB blockchain storage required, with replication factor of 10 validators totaling ~620 GB network storage. Transaction history (5 donations per donor lifetime, 500 bytes per transaction) adds ~2.5 GB, yielding total system storage of ~65 GB primary data plus replication. Per-donor and network-wide storage follow (13) and (14).

$$S_{\text{donor}} = \left(S_{\text{pi}} + S_{\text{mh}} + S_{\text{enc}}\right) \cdot \kappa \approx 62\ \text{KB} \tag{13}$$

$$S_{\text{net}} = N \cdot S_{\text{donor}} \cdot \rho \approx 620\ \text{GB} \tag{14}$$

where S_{pi}, S_{mh} and S_{enc} are the personal-information, medical-history and encryption-overhead components, κ is the steganographic expansion factor (10×), N the donor population, and ρ the validator replication factor.

Computational Complexity: Donor registration exhibits O(n log n) complexity where n is data size (encryption O(n), steganography O(n log n) with deep learning). Matching query shows O(m log k) complexity where m is candidates and k is attributes, with typical query for 10,000 donors requiring ~13 ms. Zero-knowledge proof generation exhibits O(1) constant time per proof (~50 ms per compatibility proof). Incentive calculation shows O(log n) complexity where n is donation history length, efficiently computable even for extensive histories.

6.2 Comparative Analysis

Table 1 compares BlooDChain with a traditional centralized system and two blockchain-based blood donation systems [27], [28]. The first six rows compare privacy and security features, and the last three compare throughput, matching latency, and storage per donor. BlooDChain is the only system that combines zero-knowledge matching, multi-layer concealment, customizable privacy tiers, and an incentive mechanism, at the cost of higher storage per donor. Each dimension is discussed below.

Table 1. Feature Comparison with Existing Systems

Feature	Traditional	BloodChain	Aljuhani	BlooDChain
Donor Anonymity	None	Basic Pseudonyms	Encryption Only	Zero-Knowledge Matching
Data Concealment	Encryption at Rest	Standard Encryption	Blockchain Encryption	Multi-Layer (Encryption + Steganography + Hardware)
Privacy Levels	One-Size-Fits-All	Single Setting	No Customization	Three-Tier Customizable
Authentication	Username/Password	Digital Signatures	Blockchain-Based	Multi-Factor Hardware

Feature	Traditional	BloodChain	Aljuhani	BlooDChain
Anonymous Matching	Not Supported	Basic Matching	No Anonymity	Zero-Knowledge Protocol
Incentive Mechanism	None	Not Implemented	Not Implemented	Ethical Gift-Based
Throughput (TPS)	~1000+	~100	~300	~358
Matching Latency	~50 ms	~5-10 s	~3-5 s	~200 ms
Storage per Donor	~5 KB	~8 KB	~10 KB	~62 KB

Privacy Protection Comparison: BlooDChain provides superior protection through zero-knowledge anonymous matching versus basic pseudonyms [27] or encryption-only approaches [28]. Multi-layer concealment (encryption + steganography + hardware keys) significantly enhances security over standard encryption. Three-tier privacy levels accommodate varying requirements versus one-size-fits-all traditional approaches. Re-identification protection through k-anonymity, differential privacy, and noise addition surpasses limited protections in existing systems. Fig. 13 converts the features in Table 1 into capability levels from 0 (absent) to 5 (comprehensive), assigned by the authors across six dimensions. BlooDChain reaches the highest level on every dimension, and the largest gaps appear in anonymous matching and incentive mechanisms, which the existing systems provide only partially or not at all.

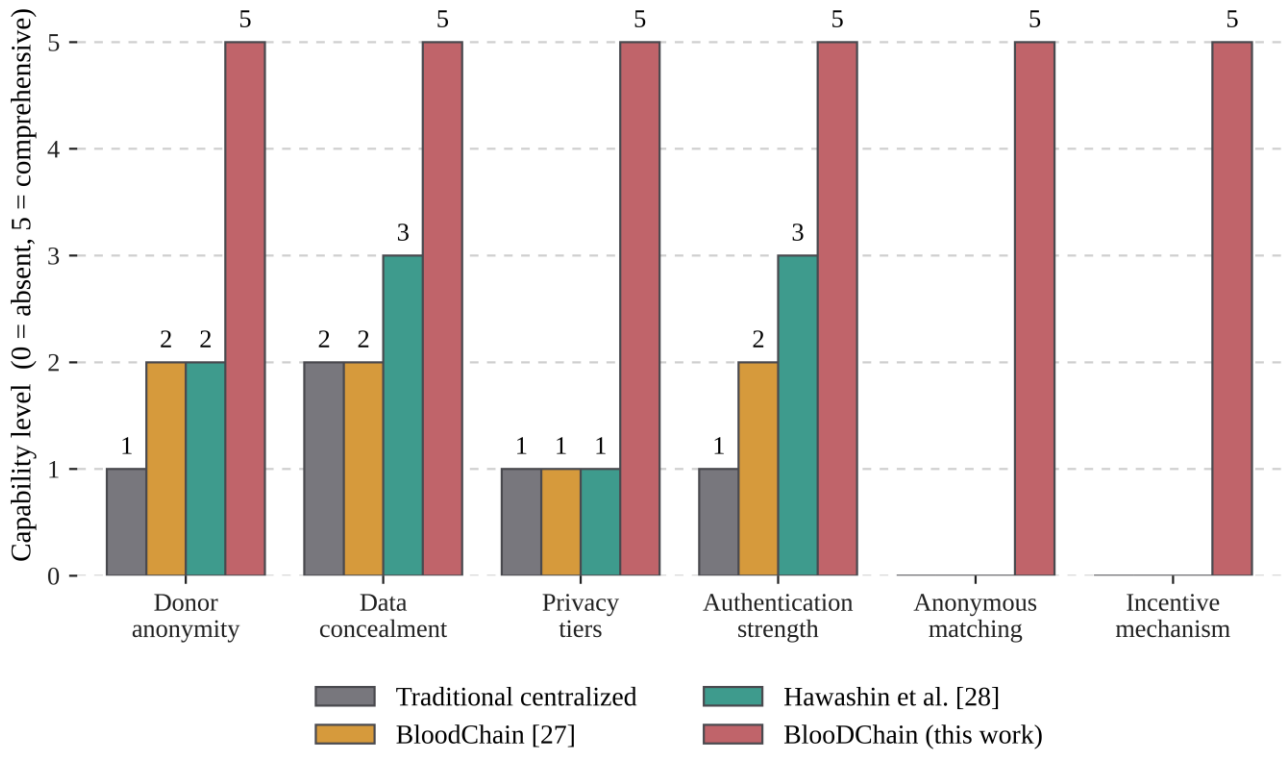

Fig. 13. Comparative Analysis Results

Security Features Comparison: Multi-factor authentication combining hardware keys, biometrics, and cryptographic methods provides stronger protection than username/password [traditional], digital signatures

[27], or blockchain-based authentication [28]. Attribute-based access control with smart contracts and hardware verification offers finer granularity than centralized role-based [traditional] or basic blockchain permissions [27], [28]. Multi-layered threat resistance addresses identity disclosure, steganalysis, cryptographic, consensus, and hardware attacks beyond basic data tampering resistance.

Functionality Comparison: Zero-knowledge anonymous matching protocol represents unique capability not found in traditional systems or existing blockchain blood donation platforms [27]–[30]. Ethical gift-based incentives for rare blood types address participation challenges unaddressed by prior work. Automated smart contract prioritization improves upon manual prioritization [traditional] or basic urgency flags [28]. Multi-channel architecture with regional customization enhances single network [27] or isolated database [traditional] approaches.

Performance Trade-offs: BlooDChain achieves competitive throughput (358 TPS) versus private blockchain systems (300 TPS [28]) despite additional security layers, though lower than centralized databases (1000+ TPS). Optimized matching latency (200 ms) significantly improves upon blockchain-based systems (3-10 seconds [27], [28]) while slightly higher than centralized query (50 ms). Storage overhead (~62 KB per donor) represents trade-off prioritizing privacy over efficiency versus ~5-10 KB in other systems, justifiable given decreasing storage costs and critical privacy importance.

6.3 Advantages and Limitations

Key Advantages: Superior multi-layered privacy architecture critical for rare blood type donors, flexible three-tier privacy model accommodating different risk profiles, unique zero-knowledge matching capability enabling compatibility verification without identity disclosure, systematic ethical incentive mechanism encouraging participation while maintaining non-commercial principles, hardware-enhanced security resistant to purely digital attacks, comprehensive threat resistance across diverse attack vectors, and optimized performance through algorithmic and architectural choices maintaining acceptable latency.

Acknowledged Limitations: Steganographic expansion increases storage requirements (~62 KB vs 5-10 KB), justified by decreasing storage costs and critical privacy importance. Zero-knowledge proofs and steganography add computational overhead, mitigated through optimizations keeping latency within acceptable ranges for non-real-time coordination. Hardware key management adds user burden, addressed through user-friendly interfaces, backup mechanisms, and optional deployment for highest-risk donors. Implementation complexity integrating multiple advanced technologies managed through modular architecture and comprehensive documentation. Novel privacy techniques may face regulatory scrutiny requiring education and compliance demonstration.

7 Implementation Considerations

7.1 Technology Stack

Table 2 lists the technology selected for each BlooDChain component and the reason for each choice. Hyperledger Fabric with Go chaincode forms the permissioned ledger, Python with TensorFlow implements the deep learning steganography, FIDO2/WebAuthn tokens provide the hardware keys, IPFS stores off-chain objects, React provides the user interface, and PostgreSQL indexes ledger data for fast queries.

Table 2. Technology Stack Selection

Component	Selection	Rationale
Blockchain	Hyperledger Fabric	Modular architecture, permissioned model, channel segregation, private data collections, PBFT consensus, enterprise-grade with healthcare deployments
Smart Contracts	Go (Chaincode)	Native Fabric support, strong typing, high performance, extensive cryptographic libraries, large developer community
Steganography	Python with TensorFlow	Rich ecosystem, TensorFlow for deep learning steganography, NumPy for binary manipulation, blockchain API integration
Hardware Security	FIDO2/WebAuthn Tokens	Industry-standard protocol, wide device support, strong cryptography, cost-effective, browser/OS integration
Off-Chain Storage	IPFS	Decentralized alignment, content-addressing integrity, scalability for large documents, active development
User Interface	React with Web3	Component-based architecture, healthcare UI libraries, Web3.js blockchain integration, mobile responsiveness
Indexing Database	PostgreSQL	Efficient blockchain indexing, ACID properties, advanced encryption, full-text search, proven scalability

7.2 Deployment Architecture

Multi-Tier Topology: User applications tier (web, mobile, administrative dashboards, API clients), application servers tier (RESTful APIs, WebSocket servers, authentication services, hardware key management), blockchain network tier (Hyperledger Fabric peers, ordering service nodes, certificate authority, chaincode containers), storage layer tier (IPFS nodes, PostgreSQL databases, backup systems), and security infrastructure tier (hardware security modules, key management, intrusion detection/prevention, SIEM).

Geographic Distribution: Multi-region deployment for resilience and compliance includes North America cluster (US/Canada compliance), European Union cluster (GDPR compliance), and Asia-Pacific cluster (regional regulations). Each region operates Hyperledger Fabric channel with cross-region replication for disaster recovery and data sovereignty maintained per regional requirements.

Scalability Strategies: Horizontal scaling through additional peer nodes for endorsement capacity, ordering nodes for consensus throughput, application server load balancing, and read replicas for query workloads. Vertical scaling through optimized peer hardware (CPU, RAM, SSD), database query optimization and indexing, caching layers, and content delivery networks. Sharding through geographic donor partitioning, separate channels for healthcare networks, and microservices architecture for functional decomposition.

7.3 Regulatory Compliance

HIPAA Compliance: Access controls limiting PHI access, encryption at rest and in transit, comprehensive audit trails, integrity controls preventing unauthorized alterations, and disaster recovery procedures.

GDPR Compliance: Right to access (donors retrieve stored information), right to rectification (update incorrect data), right to erasure (cryptographic erasure rendering data unrecoverable through key destruction), data minimization (only essential collection), privacy by design (built-in features), and data portability (export functionality).

Blood Donation Regulations: FDA regulations enforcement including donor eligibility criteria, record keeping requirements, traceability, and adverse event reporting. WHO guidelines adherence including voluntary non-remunerated donation principles, quality management, donor selection protocols, and safe blood program integration.

Blockchain-Specific Considerations: Immutability versus right to erasure addressed through cryptographic erasure where key destruction renders blockchain data unrecoverable, meeting functional erasure requirements. Data localization through multi-channel architecture with regional segregation satisfying sovereignty regulations.

7.4 Cost Benefit Analysis

Benefits include reduced donor search time saving healthcare costs, prevented privacy breaches avoiding regulatory fines (millions), improved rare blood type availability saving lives (invaluable), reduced administrative overhead through automation, and enhanced donor trust increasing donation rates. Return on investment expected within 3-5 years for large healthcare networks, with cost per donor decreasing with scale and privacy protection value substantial though difficult to quantify.

8 Future Recommendations and Work

While BlooDChain presents a comprehensive framework, several promising directions warrant further investigation. Post-quantum cryptographic algorithms require full integration and performance evaluation to ensure long-term security against quantum computing threats. Layer-2 scaling solutions including state channels and rollup technologies should be explored to enhance transaction throughput beyond current 358 TPS limitations for global deployment scenarios. Advanced machine learning techniques could optimize matching algorithms through predictive blood demand forecasting and intelligent donor mobilization during emergency situations. Integration with existing healthcare information systems through HL7 FHIR standards and cross-chain interoperability protocols would facilitate seamless adoption across diverse healthcare networks. Dynamic incentive optimization mechanisms using real-time supply-demand analytics could further encourage rare blood type donor participation. Additionally, longitudinal studies evaluating privacy preservation effectiveness, donor participation rates, and health outcomes in real-world deployments would provide valuable insights for iterative system refinement and inform best practices for privacy-preserving healthcare coordination platforms.

9 Conclusion

This paper presented BlooDChain, a comprehensive blockchain-enabled privacy-preserving blood donation platform addressing critical challenges in donor-recipient coordination while maintaining robust privacy protection. The multi-layered security architecture combining blockchain immutability, steganographic data concealment, hardware-based encryption, and zero-knowledge anonymous matching protocols provides unprecedented donor privacy protection. The three-tier privacy model accommodates varying donor risk profiles, representing significant advancement over one-size-fits-all approaches. The anonymous matching protocol enables compatibility verification without identity disclosure during matching, addressing critical gaps in existing platforms particularly valuable for rare blood type donors facing targeted risks. The ethical gift-based incentive mechanism encourages participation while maintaining non-commercial principles aligned with healthcare ethics.

Hardware-based physical encryption keys provide additional security resistant to purely digital attacks, demonstrating defense-in-depth approach. Comprehensive security analysis demonstrated resistance to diverse attack vectors including identity disclosure, data extraction, cryptographic attacks, smart contract exploits, consensus attacks, and hardware compromises. Formal verification of security properties provides mathematical assurance of system guarantees. Performance evaluation showed acceptable throughput (~358 TPS), low matching latency (~200 ms), and reasonable registration times (~3-5 seconds) suitable for blood donation coordination. Comparative analysis revealed superior privacy protection and security features compared to existing systems [27]–[30] while maintaining competitive performance.

The implementation roadmap, technology stack recommendations, and deployment architecture provide practical guidance for real-world adoption. Consideration of regulatory compliance (HIPAA, GDPR, FDA) and operational challenges demonstrates production deployment feasibility. BlooDChain advances state-of-the-art through: (1) first comprehensive integration of blockchain, steganography, and hardware encryption for blood donation; (2) novel zero-knowledge matching protocol for healthcare coordination; (3) ethical incentive mechanism design for rare resource allocation; (4) multi-tier privacy framework; and (5) practical implementation roadmap. The platform demonstrates that advanced cryptographic techniques, blockchain technology, and thoughtful design can create blood donation systems simultaneously achieving high privacy, strong security, efficient coordination, and ethical incentive alignment, with potential to increase participation particularly among rare blood type donors through credible privacy guarantees.

ACKNOWLEDGMENT

The authors acknowledge the Ethereum Foundation, OpenZeppelin, IPFS Protocol Labs, and the broader open-source blockchain community for providing foundational technologies and libraries that enabled this research.

REFERENCES

[1] K. Li, A. Lohachab, M. Dumontier, V. Urovi, Privacy preservation in blockchain-based healthcare data sharing: A systematic review, Peer-to-Peer Networking and Applications, 18 (6), 302, 2025, https://doi.org/10.1007/s12083-025-02148-9.

[2] M.F. Shaikh, S.H. Hassan, A. Maccaro, G. Pratesi, D. Piaggio, A blockchain framework using proof of authority and smart contracts for ethical and secure healthcare asset management, Frontiers in Public Health, 13, 1638546, 2025, https://doi.org/10.3389/fpubh.2025.1638546.

[3] J.K. Adeniyi et al., A blockchain-based smart healthcare system for data protection, iScience, 28 (4), 112109, 2025, https://doi.org/10.1016/j.isci.2025.112109.

[4] M.S.B. Kasyapa, C. Vanmathi, Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies, Frontiers in Digital Health, 6, 1359858, 2024, https://doi.org/10.3389/fdgth.2024.1359858.

[5] J.I. Senarathna, Blockchain technology: A comprehensive review of architecture, consensus mechanisms, security, scalability solutions, and real-world applications for distributed systems, TechRxiv, 2025, https://doi.org/10.36227/techrxiv.176617589.93522339/v1.

[6] J.I. Senarathna, EcoTherapistVR: Design and proof-of-concept implementation of a decentralized blockchain-based virtual reality platform for mental health nature therapy, OSF Preprints, 2026, https://doi.org/10.31234/osf.io/6rwm7_v1.

[7] P. Gandhi, D. Rathod, Securing patient data in the healthcare industry: A blockchain-driven protocol with advanced encryption, Journal of Education and Health Promotion, 13, 94, 2024, https://doi.org/10.4103/jehp.jehp_984_23.

[8] S. Abasaheb et al., Blockchain-integrated secure healthcare information sharing via advanced Blowfish encryption standard with optimal key generation, Transactions on Emerging Telecommunications Technologies, 36 (4), e70077, 2025, https://doi.org/10.1002/ett.70077.

[9] O. Popoola et al., An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security, Internet of Things, 27, 101255, 2024, https://doi.org/10.1016/j.iot.2024.101255.

[10] D. Ravichandran et al., An efficient medical data encryption scheme using selective shuffling and inter-intra pixel diffusion IoT-enabled secure E-healthcare framework, Scientific Reports, 15, 3847, 2025, https://doi.org/10.1038/s41598-025-85539-5.

[11] A. Haddad, M.H. Habaebi, E2EE enhanced patient-centric blockchain-based system for EHR management, PLOS ONE, 19 (5), e0301371, 2024, https://doi.org/10.1371/journal.pone.0301371.

[12] S. Pandey, B. Bhushan, Improving data security and privacy in health care: Cryptographic techniques and security protocols, Studies in Systems, Decision and Control, 549, 209–228, 2025, https://doi.org/10.1007/978-981-95-2129-6_11.

[13] J.I. Senarathna, H. Dilpriya, The role of cryptography in blockchain: Ensuring immutability, transparency and security, Preprints.org, 2025, https://doi.org/10.20944/preprints202504.1814.v1.

[14] J.I. Senarathna, Blockchain and how it relies on cryptographic methods, Preprints.org, 2025, https://doi.org/10.20944/preprints202504.1170.v1.

[15] J.I. Senarathna, Cryptography in secure cloud computing, Preprints.org, 2025, https://doi.org/10.20944/preprints202504.1371.v1.

[16] StegoSec-EHR: A blockchain-enabled IoT framework for secure HER sharing via steganography in genetic disease diagnosis, Peer-to-Peer Networking and Applications, 18 (1), 19, 2025, https://doi.org/10.1007/s12083-025-02147-w.

[17] H. Riaz et al., Robust steganography technique for enhancing the protection of medical records in healthcare informatics, IEEE Journal of Biomedical and Health Informatics, 29 (5), 2215–2226, 2025, https://doi.org/10.1109/JBHI.2025.3554032.

[18] B.M. Issac, S.N. Kumar, Deep learning steganography for big data security using squeeze and excitation with inception architectures, Scientific Reports, 15 (1), 31193, 2025, https://doi.org/10.1038/s41598-025-16394-7.

[19] Secure medical image transmission via steganography and cryptography, Computers, Materials and Continua, 84 (1), 1077–1092, 2025, https://doi.org/10.32604/cmc.2025.061659.

[20] A.R. Muhammad et al., MedProtect: Protecting electronic patient data using interpolation-based medical image steganography, Journal of Electronics, Electromedical Engineering, and Medical Informatics, 7 (1), 25–34, 2025, https://doi.org/10.35882/jeeemi.v7i1.363.

[21] M.A. Hameed et al., A novel medical steganography technique based on adversarial neural cryptography and digital signature using least significant bit replacement, International Journal of Cognitive Computing in Engineering, 5, 369–383, 2024, https://doi.org/10.1016/j.ijcce.2024.08.002.

[22] EHR-protect: A steganographic framework based on data-transformation to protect electronic health records, Intelligent Systems with Applications, 25, 200493, 2025, https://doi.org/10.1016/j.iswa.2025.200493.

[23] Ali et al., Optimize image steganography based on distinction disparity value and HMPSO to ensure confidentiality and integrity, Journal of Computer Networks and Communications, 2024, 2516567, 2024, https://doi.org/10.1155/2024/2516567.

[24] Medical steganography: Enhanced security and image quality, and new S-Q assessment, Signal Processing, 224, 109597, 2024, https://doi.org/10.1016/j.sigpro.2024.109597.

[25] A comparative analysis of chaos theory based medical image steganography to enhance data security, Procedia Computer Science, 235, 2264–2273, 2024, https://doi.org/10.1016/j.procs.2024.04.213.

[26] I.S. Igboanusi et al., BOMS: Blockchain-enabled organ matching system, Scientific Reports, 14, 16069, 2024, https://doi.org/10.1038/s41598-024-66375-5.

[27] H.T. Le, T.T.L. Nguyen, T.A. Nguyen, X.S. Ha, N. Duong-Trung, BloodChain: A blood donation network managed by blockchain technologies, Network, 2 (1), 21–35, 2022, https://doi.org/10.3390/network2010002.

[28] D. Hawashin, D.A.J. Mahboobeh, K. Salah, R. Jayaraman, I. Yaqoob, M. Debe, S. Ellahham, Blockchain-based management of blood donation, IEEE Access, 9, 163016–163032, 2021, https://doi.org/10.1109/ACCESS.2021.3133953.

[29] A. Agarwal, A.M. Jain, S.N. Rathod, S.P. Shah, N.Y. Suvarna, Blood management system using blockchain, Mapana – Journal of Sciences, 22 (Special Issue 2), 349–361, 2023, https://doi.org/10.12723/mjs.sp2.20.

[30] S. Singh, S. Kumar, H.P. Olasiuk, R.K. Revulagadda, N.S. Vihari, A blockchain technology application for managing blood supply chain, 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), 2023, https://doi.org/10.1109/ICIPTM57143.2023.10118148.

[31] C.A. Marino, C. Diaz Paz, Smart contracts and shared platforms in sustainable health care: Systematic review, JMIR Medical Informatics, 13, e58575, 2025, https://doi.org/10.2196/58575.

[32] Scalability and efficiency analysis of Hyperledger Fabric and private Ethereum in smart contract execution, Computers, 14 (4), 132, 2025, https://doi.org/10.3390/computers14040132.

[33] A. Khatoon, A blockchain-based smart contract system for healthcare management, Electronics, 9 (1), 94, 2020, https://doi.org/10.3390/electronics9010094.

[34] K.N. Griggs et al., Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, Journal of Medical Systems, 42, 130, 2018, https://doi.org/10.1007/s10916-018-0982-x.

[35] Review: Smart contracts, blockchain and health, Preprints, 2025081589, 2025, https://doi.org/10.20944/preprints202508.1589.v1.

[36] S. Ma, X. Zhang, Integrating blockchain and ZK-ROLLUP for efficient healthcare data privacy protection system via IPFS, Scientific Reports, 14, 11746, 2024, https://doi.org/10.1038/s41598-024-62292-9.

[37] Zero-trust medical image sharing: A secure and decentralized approach using blockchain and the IPFS, Symmetry, 17 (4), 551, 2025, https://doi.org/10.3390/sym17040551.

[38] D. Kumari et al., HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy-preserving scalable health data, Computer Networks, 250, 110550, 2024, https://doi.org/10.1016/j.comnet.2024.110550.

[39] S. Rani et al., A secure framework for IoT-based healthcare using blockchain and IPFS, Security and Privacy, 7 (3), e348, 2024, https://doi.org/10.1002/spy2.348.

[40] J. Jayabalan, N. Jeyanthi, Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy, Journal of Parallel and Distributed Computing, 164, 152–167, 2022, https://doi.org/10.1016/j.jpdc.2022.03.009.

[41] R.K. Mishra et al., Integration of blockchain and IPFS: Healthcare data management & sharing for IoT environment, Multimedia Tools and Applications, 84, 27229–27250, 2025, https://doi.org/10.1007/s11042-024-20092-3.

[42] M.K. Singh et al., A Blockchain-IPFS framework for secure, scalable, and interoperable healthcare data management, SN Computer Science, 6, 400, 2025, https://doi.org/10.1007/s42979-025-03936-z.

[43] Addressing contemporary threats in anonymised healthcare data using privacy engineering, npj Digital Medicine, 8, 145, 2025, https://doi.org/10.1038/s41746-025-01520-6.

[44] T. Ko, B.W. Hwang, Self-sovereign management scheme of personal health record with personal data store and decentralized identifier, Computational and Structural Biotechnology Journal, 23, 3943–3956, 2024, https://doi.org/10.1016/j.csbj.2024.11.036.

[45] A secure and privacy-preserving approach to healthcare data collaboration, Symmetry, 17 (7), 1139, 2025, https://doi.org/10.3390/sym17071139.

[46] A. Choudhury et al., Advancing privacy-preserving health care analytics and implementation of the personal health train: Federated deep learning study, JMIR AI, 4, e60847, 2025, https://doi.org/10.2196/60847.

[47] F. Prasser et al., Privacy-preserving data sharing infrastructures for medical research: Systematization and comparison, BMC Medical Informatics and Decision Making, 21, 242, 2021, https://doi.org/10.1186/s12911-021-01602-x.

[48] A. Nekouie et al., Comparison of attribute-based encryption schemes in securing healthcare systems, Scientific Reports, 14, 7147, 2024, https://doi.org/10.1038/s41598-024-57692-w.

[49] Y. Zeng et al., Enhancing smart healthcare networks: Integrating attribute-based encryption for optimization and anti-corruption mechanisms, Heliyon, 11 (1), e39462, 2025, https://doi.org/10.1016/j.heliyon.2024.e39462.

[50] Yang et al., HA-Med: A blockchain-based solution for sharing medical data with hidden policies and attributes, IET Information Security, 2498245, 2024, https://doi.org/10.1049/2024/2498245.

[51] Attribute encryption access control method of high-dimensional medical data based on fuzzy algorithm, PLOS ONE, 20 (3), e0317119, 2025, https://doi.org/10.1371/journal.pone.0317119.

[52] H.M. Hussien, S.M. Yasin, N.I. Udzir, M.I.H. Ninggal, Blockchain-based access control scheme for secure shared personal health records over decentralised storage, Sensors, 21 (7), 2462, 2021, https://doi.org/10.3390/s21072462.