The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 08-19
DOI 10.37547/tajet/Volume07Issue10-02

Check for updates

A Proposed Hybrid Blockchain-DID-ZKP Approach to Secure, Auditable, and Private Healthcare Interoperability

Sahil Fruitwala
Software Engineer, USA

Purva Desai
Data Analyst, USA

OPEN ACCESS

SUBMITED 27 August 2025
ACCEPTED 29 September 2025
PUBLISHED 06 October 2025
VOLUME Vol.07 Issue 10 2025

CITATION
Sahil Fruitwala, & Purva Desai. (2025). A Proposed Hybrid Blockchain-DID-ZKP Approach to Secure, Auditable, and Private Healthcare Interoperability. *The American Journal of Engineering and Technology*, *7*(10), 08–19. https://doi.org/10.37547/tajet/Volume07Issue10-02

Abstract: Traditionally, health records are kept in siloed data storages of different health organizations. Today, all patients' EHRs (Electronic Health Records) are used and shared with different institutes and research facilities without their consent. To protect and overcome pitfalls of generic systems, we introduce a new hybrid system called Hybrid Patient Data Vault (HPDV). This hybrid system can help patients securely share their health information in a manner that could allow them to share only what is necessary or in need-to-know basis. We detail the system's components, workflows, and emergency protocols, emphasizing patient-centric design. Through a STRIDE-based threat model and simulations of key metrics like transaction latency and ZKP generation time, we demonstrate HPDV's security and feasibility. Our evaluation shows it outperforms monolithic approaches in auditability and privacy, with ZKP proofs generated in under 7 seconds on standard devices. This work demonstrates a practical modern approach for secure, patient-controlled health data exchange.

Keywords: Patient-Controlled Data Sharing, Blockchain, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), Zero-Knowledge Proofs (ZKPs), FHIR, Healthcare Interoperability, Privacy-Preserving Architecture.

Introduction

The rapid digitization of healthcare systems has revolutionized patient care. This exponential growth has enabled seamless access to medical records for both patients and healthcare providers. However, this transition towards digital ecosystem has introduced unimaginable risks to patient's data privacy and security. In 2024 alone, over 190 million individuals were impacted by healthcare data breaches. This incident made it one of the largest cybersecurity crises after 2015 [1]. Data breaches are very expensive emotionally as well as financially. IBM reported incident occurred in 2024 cost them over $4.9 millions [2]. These kind of large scale security failures undermine the public's trust in healthcare organization and eventually jeopardizing the essential trust between patients and their healthcare providers.

Even though encryption is consider one of the most important aspect of new age systems. Many organizations rely on outdated or cheaper — easy to break cryptography practices. Main reason behind this negligence are either computation overhead or cost constraints, particularly among smaller healthcare providers such as small private clinics. While some organizations make use of modern encryption technology for better security, patient data remains siloed within EHR (Electronic Health Record) system of these organizations. Patients may have little or no control over how their data is being used, shared or even who can access their data. This creates a significant imbalance in data governance. Emerging technologies like blockchain promises a decentralized and tamper-proof data management. Blockchain's adoption in healthcare has been hampered by inherent limitations. Traditional blockchain architectures prioritize immutability at the expense of scalability and cost, rendering them impractical for real-time clinical workflows [3].

This paper addresses these challenges by proposing, a hybrid architecture that combines the auditability of permissioned blockchains, the sovereignty of decentralized identifiers (DIDs), and the privacy-preserving capabilities of zero-knowledge proofs (ZKPs). Unlike monolithic approaches, this hybrid solution decouples data storage from consent management system. This decoupled system, enables patients to cryptographically control access while maintaining compliance with FHIR stan- dards. By integrating ZKPs for selective data disclosure, the system minimizes exposure of sensitive health records without compromising clinical utility.

This paper makes three key contributions. First, we provide a detailed system architecture, explaining how its components fit together and interact. Second, we walk through the full operational workflows that covers everything from patient onboarding to secure data access including emergency protocols. Lastly, we explain our security model. We'll test it out with simulations to prove our combined method is useful and secure in practice.

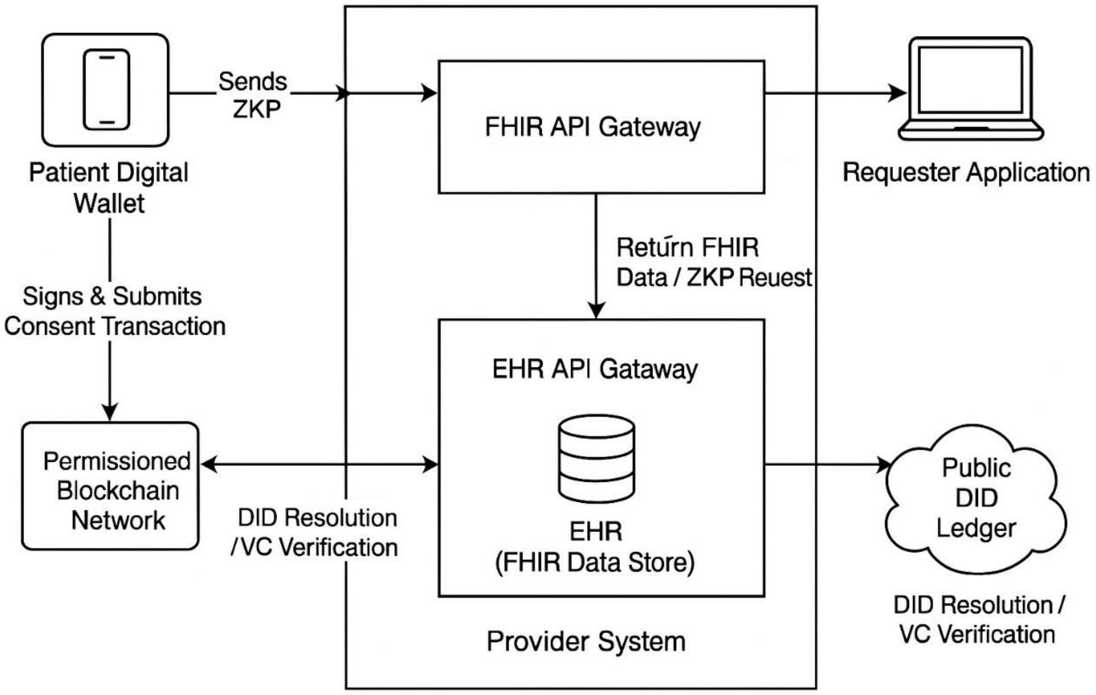


Fig. 1. High-Level Architecture Diagram

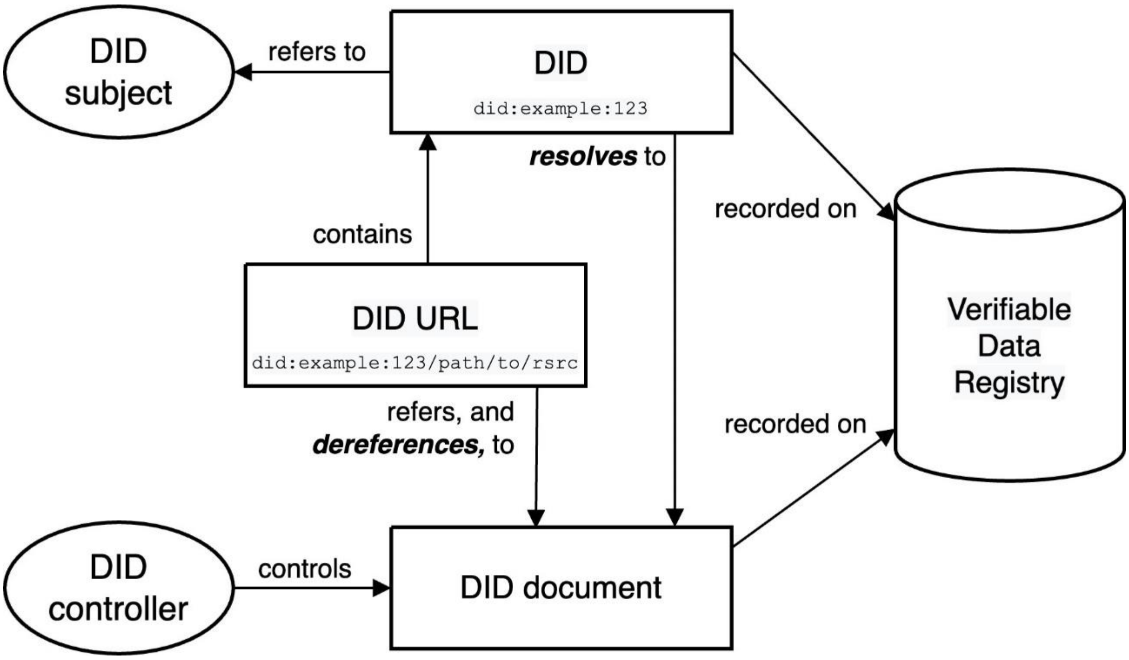


Fig. 2. Overview of DID architecture and the relationship of the basic components. (Source: Adapted from W3C Decentralized Identifiers Data Model v1.0 [7])

II. Background And Literature Review

The secure and efficient exchange of health information is not just a technical goal, it's a fundamental patient right and a critical component of modern healthcare. Yet today's systems remain fragmented across institutional silos, creating significant challenges in interoperability, privacy, and patient control [4]. To address these issues, researchers have turned to advanced cryptographic and decentralized technologies like blockchain.

In this section, we review key technologies and analyze current blockchain-based healthcare models. We highlight where these approaches fall short, and how our proposed hybrid architecture aims to address those gaps using permissioned blockchain, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Zero-Knowledge Proofs (ZKPs).

Fast Healthcare Interoperability Resources (FHIR)

Fast Healthcare Interoperability Resources (FHIR), developed by Health Level Seven International (HL7), is a widely adopted standard for sharing healthcare data using modular, web-based formats like JSON or XML [5]. It defines "resources" such as Patient, Observation, or Medication and enables interaction through RESTful APIs.

FHIR is a major step forward compared to older standards like HL7v2, which used rigid formats and lacked web compatibility. Its real-time capabilities make it ideal for apps, like pulling up a patient's allergy history in an emergency. However, FHIR primarily focuses on how data is formatted and exchanged, not who controls it or how secure it is. It assumes trust between systems but doesn't inherently enforce access restrictions or consent.

In blockchain-based models, FHIR data is often encrypted or hashed off-chain (e.g., using IPFS), while only metadata is stored on-chain; a practice common in hybrid systems [6].

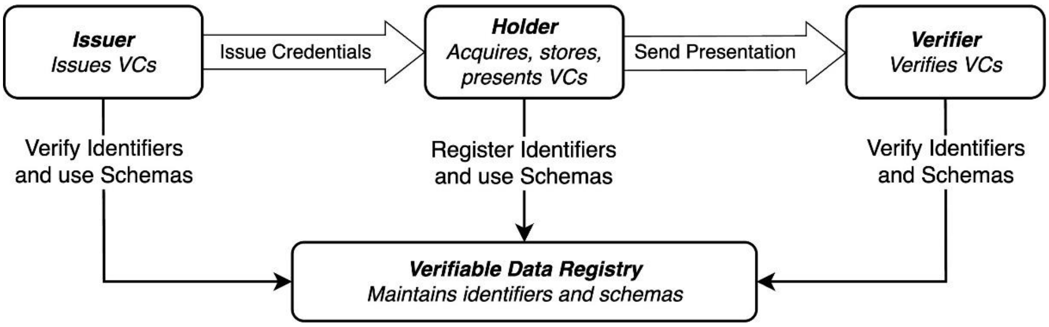


Fig. 3. Overview of the Verifiable Credential Exchange Flow. (Source: Adapted from W3C Verifiable Credentials Data Model v1.1 [8])

TABLE I Comparison of Related Architectures

Approach	Key Features	Gaps	Citation
Tripartite Chains	BLS aggregation, IPFS, 5-level classification	No DIDs/VCs/ZKPs; provider-centric	Han et al. (2025) [6]
DHR Privacy Survey	Smart contracts, cases (e.g., MedRec)	No tech depth; mismatched refs	Hamzah et al. (2025) [4]
IoMT-Edge hChain	Multi-factor auth, RBAC	No VCs/ZKPs; limited emergencies	Alruwaill et al. (2025) [10]
Our Hybrid	DIDs/VCs + ZKPs + Chains	N/A	This work

B. Self-Sovereign Identity: Empowering the Patient

Traditional digital identity in healthcare is either siloed (a different ID at every hospital) or federated (using third-party logins like Google). Self-Sovereign Identity (SSI) changes this by giving individuals direct control over their digital identities.

The foundation of SSI, as defined by the W3C, includes:

1. These are globally unique, verifiable IDs that belong entirely to the individual—not issued by a central authority. A DID (e.g., did:ethr:0x123...abc) links to a DID Document, which holds public keys and endpoints for secure interaction [7]. A patient can carry this identity across systems and over time.
2. Verifiable Credentials (VCs): These are digital statements (e.g., "You have Type A+ blood") issued by a trusted party like a hospital. Patients store these credentials in a secure wallet and share them with third parties (like a new clinic or a researcher) without needing to contact the original issuer. Cryptographic proofs ensure the VC's validity.

By using DIDs and VCs together, our system moves beyond static access controls and into a model where patients have full ownership and portability of their digital health identity.

C. Permissioned Blockchains for Healthcare

Permissioned blockchains, such as Hyperledger Fabric, are particularly well-suited for healthcare because they restrict network access to verified participants and offer efficient consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT). These chains are ideal for storing immutable metadata (like audit logs or patient consent) while keeping sensitive health data off-chain to maintain compliance with privacy laws. For example, an EHR sharing system might log a consent transaction—"Patient grants Lab Y access"—with a timestamp. These logs ensure traceability and accountability. Han et al. (2025) demonstrated this with a tripartite architecture (patient, provider, and social chains) and used Boneh-Lynn-Shancham (BLS) signature aggregation for efficient cross-chain operations [6].

Still, many of these systems manage identity through provider-controlled keys, which limits true patient autonomy.

D. Zero-Knowledge Proofs (ZKPs) for Privacy

To provide the strongest level of privacy, our architecture incorporates Zero-Knowledge Proofs (ZKPs). A ZKP is a cryptography protocol that allow users to share some verifiable truth without exposing underling data [9]. For example, patients can use a ZKP provide that they are over 18 years old without reveling their exact age or birthdate. This principle of data minimization is a significant improvement over standard encryption, which protects data in transit but still requires the recipient to access the decrypted data.

E. Review of Related Architectural Proposals

Some of the recent academic literature argues and validated that hybrid architecture are most promising approach for secure EHR sharing. Many of this modern age architectures has gaps in identity sovereignty and privacy. Table I compares key works. The work by Han et al. (2025) illustrate this trend with a sophisticated tripartite (three-chain) architecture. Their model segregates data across a patient chain, a provider chain, and a "social chain". For data sharing, it suggested to use the InterPlanetary File System (IPFS) for off-chain storage. A key contribution is their use of a cross-chain aggregate signature scheme to enhance efficiency. This work provides a strong foundation for a multi-system off-chain approach. However, their suggested model is based on a traditional Public Key Infrastructure (PKI). In this infrastructure keys are managed by the system or providers and its privacy relies on encryption and access control policies.

Another relevant proposal is “hChain” by Alruwaill et al. (2025), which focuses on securing data from the Internet of Medical Things (IoMT) and edge devices. The hChain framework introduces a practical multi-factor authentication system. To protect user’s data, hChain framework uses location-based verification with efficient symmetric encryption to protect real-time data streams. While highly effective for its specific use case, its identity model remains institutional. This internalized database from provider’s lacks the portability.

Though, these work have made significant progress in establishing auditable and secure system, they suffer from common limitations. Many of these models depend on institutional identity model that do not allow patients to have full sovereignty. Moreover, privacy mechanism used in many of these models protects data but do not minimize the exposure of a actual data. Hamzah et al. (2025) suggests, the full potential of blockchain in healthcare lies in empowering patients with direct control and robust privacy.

A clear gap exists for a holistic framework that natively integrates true self-sovereign identity with advanced privacy- preservation. Our proposed architecture is designed to fill this gap, building upon the strengths of previous works. This paper introduces solution with next-generation identity and privacy layers to create a more robust, private, and truly patient-centric ecosystem for health data exchange.

III. The Proposed Architecture

Most of architecture that we reviewed lacked one thing — user control. Most of the blockchain based approaches that are fast were good for audit logs and some small data chunk. But as size increase of medical record these systems failed in perform and scale. Moreover, patients data that were being shared, were done without patients knowledge or consent. HPDV design addresses the limitations of monolithic systems by providing a multi-layered approach to security, scalability, and patient empowerment.

A. Architectural Principles

To make HPDV a patient-centric system, we developed it around five core principles.

- **Patient-Centricity:** The patients must have control over their data and identity. DIDs allow patients to own and manage their identity independent to any entity and VCs which enables patients to do selective sharing without relying on centralized authorities.
- **Zero-Trust Security:** No component implicitly trusts another. Every interaction, small or big, from an API call to a data request, must be cryptographically verified using decentralized identifiers and verifiable credentials.
- **Data Minimization by Design:** Following the privacy-by-design paradigm, the system aims to minimize data exposure at every step. The integration of Zero-Knowledge Proofs is at core of this principle which enables verification of patient’s record without revelation of actual data.
- **Immutable Auditability:** All events critical or non-critical related to consent and data access must be recorded in a tamper-proof and permanent manner. The permissioned blockchain serves as the non-repudiable source of truth for all audit trail.
- **Interoperability through Standards:** The system leverages existing open standards for data representation, such as FHIR and W3C standards like DIDs and VCs, to ensure compatibility without any vendor lock-in.

B. System Components and Diagram

HPDV comprises of mainly four components — Patient Digital Wallet, Provider EHR & FHIR API Gateway, Permissioned Blockchain Network, DID Ledger. This multi-layered system interconnects component for a privacy preserving data exchange.

1) *Patient Digital Wallet:* The Patient Digital Wallet is a client-side application (e.g., mobile or desktop) that serves as the patient’s primary interface to the ecosystem. Patients can manage their DID (e.g., did:ethr:patientPublicID), store VCs issued by healthcare providers, generates ZKPs using local cryptographic libraries (e.g., snarkjs), and signs blockchain transactions for consent management. This digital wallet can interact with secure APIs for ZKP generation through FHIR data. Most significant benefit of this digital wallet is, all data that are being stored locally are in Verifiable Credentials format

with minimal metadata. This will help in privacy preservation of user incase someone else get hold of patient's device.

2) *Provider System: EHR and FHIR API Gateway:* This component represents the existing infrastructure of healthcare providers. The EHR (Electronic Health Record) is the secure, centralized database where patient health data is stored as FHIR resources. The FHIR API Gateway is a guard rails for EHR. It is responsible for: (a) receiving authenticated data requests from requesters; (b) querying the permissioned blockchain to verify the existence and validity of patient consent; (c) logging all access events to the blockchain; and (d) retrieving the authorized FHIR data from the EHR to send to requester.

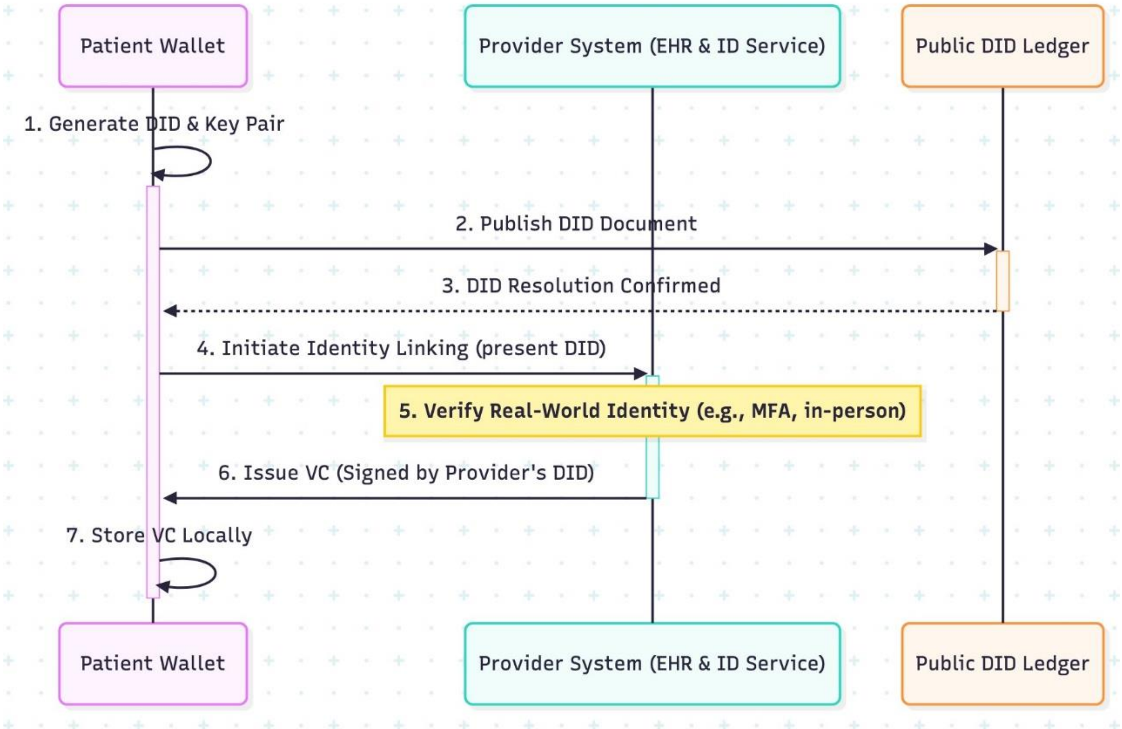

Patient Wallet
Provider System (EHR & ID Service)
Public DID Ledger
1. Generate DID & Key Pair
2. Publish DID Document
3. DID Resolution Confirmed
4. Initiate Identity Linking (present DID)
5. Verify Real-World Identity (e.g., MFA, in-person)
6. Issue VC (Signed by Provider's DID)
7. Store VC Locally
Patient Wallet
Provider System (EHR & ID Service)
Public DID Ledger

Fig. 4. Consent Granting

Healthcare providers stores raw health data in a secure and in centralized fashion as FHIR resource. The FHIR API Gateway acts as a secure intermediary: it verifies consent by querying the blockchain to check for a valid grantConsent transaction and authenticates requests using DIDs before releasing data. If a ZKP is involved, the gateway will proxy the raw data to the patient's wallet for proof generation.

3) *Permissioned Blockchain Network:* This is a decentralized network operated by a consortium of trusted healthcare entities such as hospitals, clinics. We propose using a framework like Hyperledger Fabric whose sole purpose is to serve as an immutable audit log. This permissioned blockchain will store the Consent Management Smart Contracts, which holds rules for granting, revoking, and checking consent. Crucial part of this layer is it does not store any Protected Health Information (PHI). It only stores trail of consent directives and access logs linked to patient and requester DIDs to ensure scalability and privacy. Unlike many traditional public blockchains, consensus here is achieved via Practical Byzantine Fault Tolerance (PBFT) which offers decentralization without the high energy costs.

4) *Public DID Ledger:* This is a public, decentralized registry where DID documents are anchored. These documents contain public keys, service endpoints, and verification methods. When a component needs to verify someone's identity or find their public key, it resolves their DID using this public ledger. This decouples identity from any single institution.

HPDV smartly integrates several technologies: DIDs for secure identity, blockchain for immutable audit trail and ZKPs enhance privacy for data verification, all while actual health records remain securely stored off-chain in EHRs.

C. ***Detailed Operational Workflows***

The interaction between the layered components of our system is governed by well-defined workflows as shown in Figure

1. These workflows assume that nodes of permissioned blockchain are online and patient will interact with system via their internet connected digital wallet. The following sections detail the primary workflows, illustrated with sequence diagrams.

A. Onboarding & Identity Linking:

- The patient downloads the Digital Wallet app and generates a DID (e.g., did:ethr:patientPublicID) with a cryptographic key pair.
- The patient visits a healthcare provider and undergoes secure enrollment via a login portal.
- The provider verifies the patient's real-world identity and issues VCs (e.g., "This DID is linked to Patient ID #123 in our EHR") to the wallet.
- The wallet stores the VCs locally.

This identity linking process is illustrated in Figure 4.

2) Consent Granting:

- A health care provider (e.g., clinic, hospital) sends a consent request to the patient's wallet via a secure channel (e.g., DID-linked messaging).
- The wallet displays the incoming request with details such as data requested, purpose and duration.
- The patient approves, and the wallet signs a smart contract transaction with their private key.
- The transaction is submitted to the blockchain to invoke grantConsent method for audit trail.
- Blockchain nodes validate and commit the transaction via consensus.

Consent granting workflow is depicted in Figure 5, ensures that all consent directives are auditable and immutable.

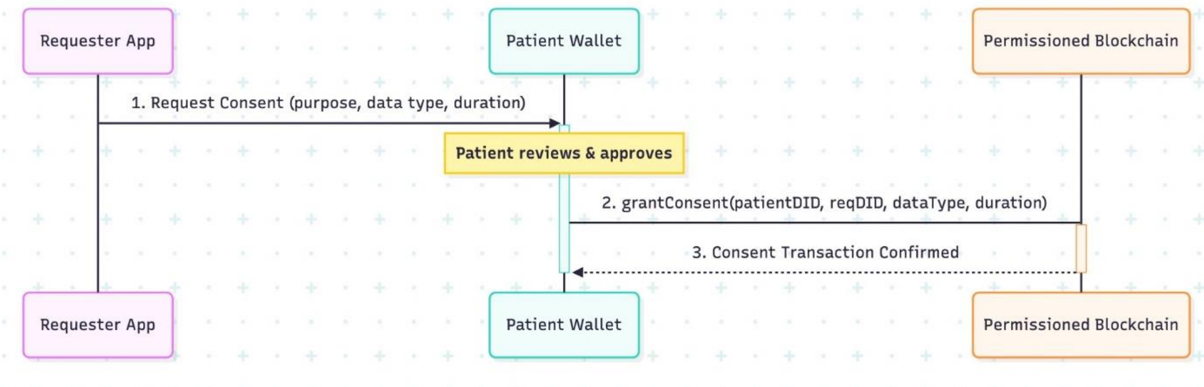

Requester App
Patient Wallet
Permissioned Blockchain
1. Request Consent (purpose, data type, duration)
Patient reviews & approves
2. grantConsent(patientDID, reqDID, dataType, duration)
3. Consent Transaction Confirmed
Requester App
Patient Wallet
Permissioned Blockchain

Fig. 5. Consent Granting

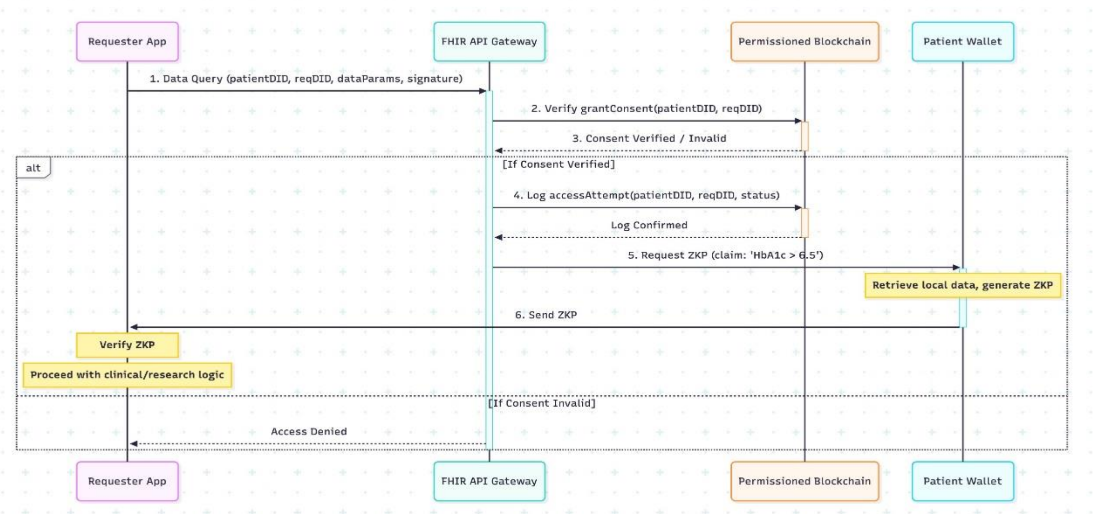

Requester App
FHIR API Gateway
Permissioned Blockchain
Patient Wallet
1. Data Query (patientDID, reqDID, dataParams, signature)
2. Verify grantConsent(patientDID, reqDID)
3. Consent Verified / Invalid
alt
[If Consent Verified]
4. Log accessAttempt(patientDID, reqDID, status)
Log Confirmed
5. Request ZKP (claim: 'HbA1c > 6.5')
Retrieve local data, generate ZKP
6. Send ZKP
Verify ZKP
Proceed with clinical/research logic
[If Consent Invalid]
Access Denied
Requester App
FHIR API Gateway
Permissioned Blockchain
Patient Wallet

Fig. 6. ZKP-based Data Access

3) Privacy-Preserving Data Access via ZKP: This workflow as represented in Figure 6 enables a requester to verify a fact about a patient's data without accessing the raw data itself.

- The requester queries the FHIR API Gateway for the patient's data, including their DID.
- The gateway checks the blockchain for valid consent.
- If consent exists, the gateway retrieves raw FHIR data from the EHR and proxies it to the patient's wallet (or the patient pulls it directly if online).
- The wallet runs a ZKP circuit: *proof* = *zkSNARK*(*privateData, publicStatement*), generating a proof (e.g., "HbA1c>6.5").
- The wallet sends the proof to the requester.
- The requester verifies the proof using the public verifier key.
- The gateway logs the access on the blockchain: logAccess(patientDID, requesterDID, timestamp).

4) *Access Revocation:* This straightforward workflow, depicted in Figure 7, ensures that patient can immediatly revoke access at any time.

- The patient selects the consent to revoke in their wallet.
- The wallet signs and submits a revokeConsent(recipientDID, dataType) transaction to the blockchain.
- Nodes validate and commit the revocation.
- Future access attempts by the requester fail the blockchain consent check.

D. Emergency Access Protocol

The strength of HPDV architecture is its biggest flaw as well - patient control. In emergency situations where patient is offline or do not have access to digital wallet to grant access, system must have an emergency access protocol. This emergency protocol should prioritizes patient's data safety while maintaining the auditability.

Currently, there are two approaches that we taken into consideration for emergency situations. The workflow can be seen in Figure 8

1) *Break-Glass Access:* The primary mechanism is the "break-glass" procedure, a standard practice in existing EHR systems. In emergency situations, an authorized provider can bypass the standard consent checks to access the patient's record directly from the EHR. HPDV accomplishes this by requiring the FHIR API Gateway to automatically submit a **logEmergencyAccess** transaction to the permissioned blockchain. This creates a non-repudiable, immutable record of the emergency access that is visible to the patient post-event, ensuring transparency and accountability.

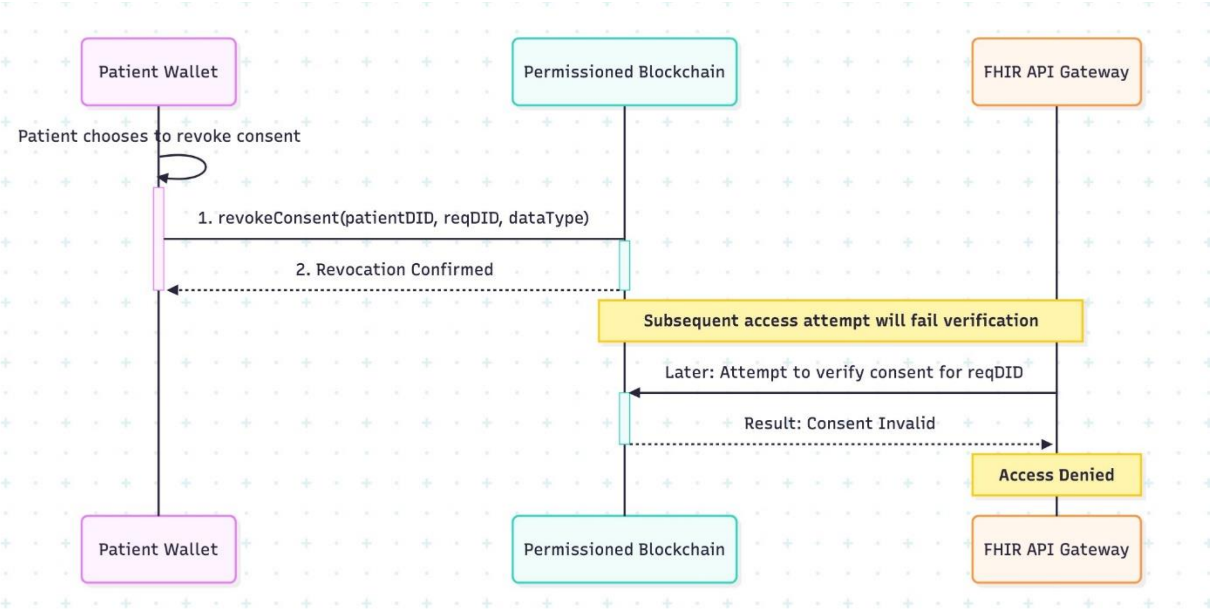
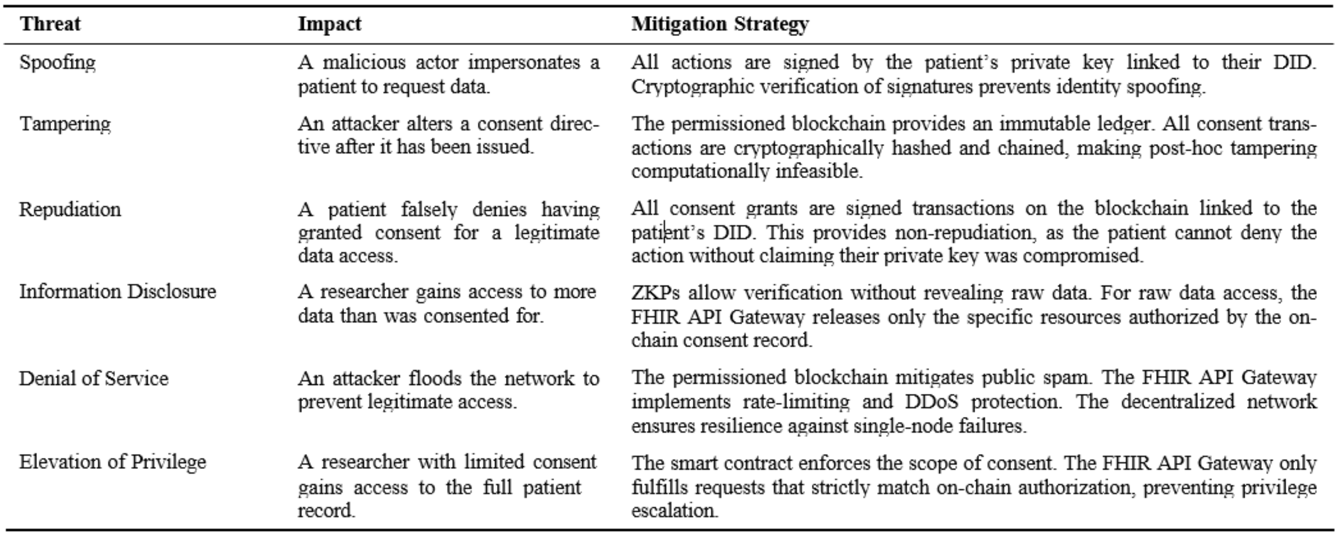

Patient Wallet
Permissioned Blockchain
FHIR API Gateway
Patient chooses to revoke consent
1. revokeConsent(patientDID, reqDID, dataType)
2. Revocation Confirmed
Subsequent access attempt will fail verification
Later: Attempt to verify consent for reqDID
Result: Consent Invalid
Access Denied
Patient Wallet
Permissioned Blockchain
FHIR API Gateway

Fig. 7. Access Revocation

TABLE II

Analysis of Potential Security Threats, Their Associated Impacts, and Proposed Mitigation Strategies in Decentralized Health

Data Systems



Threat	Impact	Mitigation Strategy
Spoofing	A malicious actor impersonates a patient to request data.	All actions are signed by the patient's private key linked to their DID. Cryptographic verification of signatures prevents identity spoofing.
Tampering	An attacker alters a consent directive after it has been issued.	The permissioned blockchain provides an immutable ledger. All consent transactions are cryptographically hashed and chained, making post-hoc tampering computationally infeasible.
Repudiation	A patient falsely denies having granted consent for a legitimate data access.	All consent grants are signed transactions on the blockchain linked to the patient's DID. This provides non-repudiation, as the patient cannot deny the action without claiming their private key was compromised.
Information Disclosure	A researcher gains access to more data than was consented for.	ZKPs allow verification without revealing raw data. For raw data access, the FHIR API Gateway releases only the specific resources authorized by the on-chain consent record.
Denial of Service	An attacker floods the network to prevent legitimate access.	The permissioned blockchain mitigates public spam. The FHIR API Gateway implements rate-limiting and DDoS protection. The decentralized network ensures resilience against single-node failures.
Elevation of Privilege	A researcher with limited consent gains access to the full patient record.	The smart contract enforces the scope of consent. The FHIR API Gateway only fulfills requests that strictly match on-chain authorization, preventing privilege escalation.

2) *Designated Proxy Access:* Alternatively, patients can choose trusted proxies to keep control over theirs data. A patient can use their wallet to grant a specific DID, possibly belonging to a family member, proxy rights. This authorization is recorded as a smart contract rule on the blockchain. In an emergency, the designated proxy can use their own DID to authenticate and gain access to the patient's records on their behalf, following a fully audited and pre-approved pathway.

This balances control with necessity but introduces risks like potential misuse.

IV. Evaluation And Security Model

To validate practicality of HPDV, we conducted a comprehensive evaluation focusing on security and performance. We used STRIDE threat model to do qualitative security analysis of our proposed system, followed by quantitative performance simulation of the architecture's most critical workflows.

A. Threat Model and Mitigations

We analyze potential threats using the industry standard STRIDE model. Table II summarizes the threats, their potential impact in a healthcare context and their respective mitigations.

B. Performance Evaluation

To assess the system's performance, we developed a simulation using Python script. This script was responsible for simulating the two most critical user-facing workflows: (1) Consent Granting via a blockchain transaction and (2) ZKP Generation. The test environment was a standard laptop with an Apple M2 processor and 16GB RAM. Our simulation uses following reasonable assumptions for a conceptual evaluation:

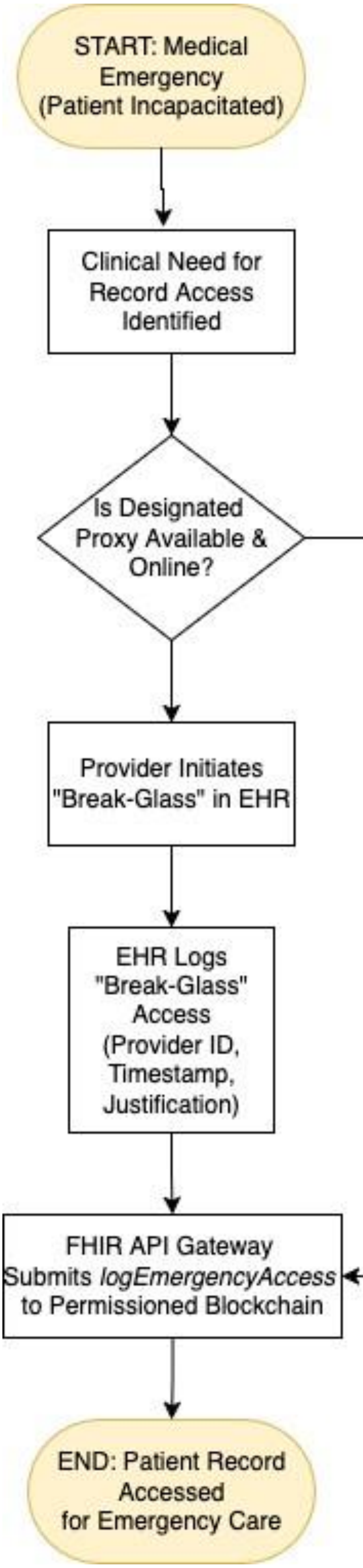
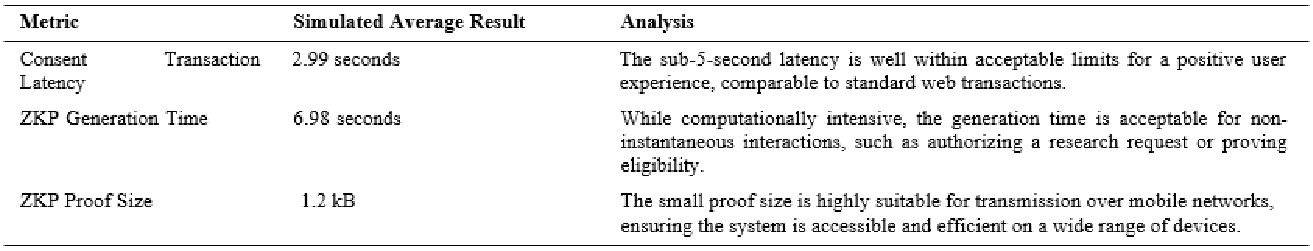

START: Medical Emergency (Patient Incapacitated)
Clinical Need for Record Access Identified
Is Designated Proxy Available & Online?
EHR Logs "Break-Glass" Access (Provider ID, Timestamp, Justification)
Provider Initiates "Break-Glass" in EHR
EHR Logs "Break-Glass" Access (Provider ID, Timestamp, Justification)
FHIR API Gateway Submits *logEmergencyAccess* to Permissioned Blockchain
END: Patient Record Accessed for Emergency Care

Fig. 8. Emergency Access Protocol

TABLE III

Analysis of Potential Security Threats, Their Associated Impacts, and Proposed Mitigation Strategies in Decentralized Health

Data Systems



Metric	Simulated Average Result	Analysis
Consent Transaction Latency	2.99 seconds	The sub-5-second latency is well within acceptable limits for a positive user experience, comparable to standard web transactions.
ZKP Generation Time	6.98 seconds	While computationally intensive, the generation time is acceptable for non-instantaneous interactions, such as authorizing a research request or proving eligibility.
ZKP Proof Size	1.2 kB	The small proof size is highly suitable for transmission over mobile networks, ensuring the system is accessible and efficient on a wide range of devices.

- The permissioned blockchain operates with a consensus mechanism that results in a block confirmation time between 2 and 4 seconds.
- Based on current industry benchmarks, ZKP generation takes 5-9 seconds for complex statements on modern smartphones. We assume these will be the primary device in most cases.
- The simulation was executed 100 times to derive a stable average performance metrics.

C. Simulation Results

The results of the simulation, presented in Table III, demonstrate the real-world feasibility of the proposed architecture. The results confirm our hypothesis that our architecture is performant enough for general adoption.

V. Discussion

Our design offers a clear path to a truly patient-first healthcare system. It combines strong security, meaningful privacy, and modern tech standards.

A. Analysis of Findings

Our STRIDE model and simulation highlight the strengths of our hybrid architecture and reinforce our commitment to security-by-design. By combining blockchain with zero-knowledge proofs (ZKPs), we've created a system that offers both immutable auditability and complete privacy, outperforming traditional monolithic approaches. While the cryptographic processes do introduce some overhead, our performance tests show that they don't compromise usability on modern devices. In fact, achieving sub-three-second consent latency sets a solid benchmark, making it ideal for securely sharing sensitive health data when time really matters.

B. Limitations

Despite its strengths, HPDV has several limitations of its own that must be addressed.

1. Technical Complexity: Integrating various components of our hybrid system, like blockchain, decentralized identifiers (DIDs), and zero-knowledge proofs (ZKPs), requires specialized knowledge. Developers may face challenges, especially when designing circuits for complex ZKP scenarios.
2. Key Management Burden: The system's security relies heavily on patients being able to securely manage their private keys. Without a reliable recovery mechanism, losing a key could mean permanently losing access to their personal health data.
3. Adoption Barriers: Establishing a permissioned blockchain consortium is a challenge on its own. Cooperation among competing healthcare providers is essential for success of the system. Achieving this consensus on technical standards, operational costs, and legal liabilities is a major non-technical hurdle.
4. Offline and Usability Issues: Even with an emergency "break-the-glass" protocol, patients still need internet access to maintain full control over their data.
5. Scalability Constraints: While the system runs efficiently in tests (around 7 seconds), generating ZKPs for larger datasets can be slow on lower-end devices. Plus, in its current form, blockchain throughput tops out at about 100 transactions per second.

These challenges point to the need for more intuitive user experiences and further system optimizations.

C. *Future Work*

This system opens up several exciting directions for future work:

- **Build and Test in the Real World:** The next step is to build a full working prototype and try it out with a small group of real patients in a pilot study.
- **Smarter Privacy Tools:** We can improve privacy even further by exploring tools like homomorphic encryption, which allows data to be analyzed without ever being decrypted.
- **Consortium Governance:** We also need to explore how the system would be managed across multiple organizations, such as using token-based rewards to encourage hospitals and clinics to run blockchain nodes.

VI. Conclusion

Right now, most health data is controlled by separate hospitals and systems, which limits both patient freedom and data sharing. This paper tackled that problem by introducing a new hybrid system that puts patients back in control.

By combining:

- Blockchains for secure audit trails,
- DIDs and Verifiable Credentials for digital identity, and
- Zero-Knowledge Proofs for private data sharing,

we've created a system that's secure, transparent, and truly patient-first.

Our tests show the idea is practical, but challenges, like technical complexity, still remain. Even so, this hybrid design is a promising step toward a future where patients can safely and easily control how their health data is used.

As technology continues to improve, systems like this could play a major role in driving personalized healthcare, better research, and more secure data exchange.

References

1. S. Alder, "Healthcare data breach statistics," The HIPAA Journal, accessed: Jul. 20, 2025. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/
2. "Cost of a data breach 2024 — ibm," accessed: Jul. 20, 2025. [Online]. Available: https://www.ibm.com/reports/data-breach
3. K. Li, A. R. Sai, and V. Urovi, "Do you need a blockchain in healthcare data sharing? a tertiary review," *Explor Digit Health Technol.*, vol. 2, no. 3, p. Art. no. 3, Jun. 2024.
4. F. H. et al., "Blockchain and digital health records: Improving privacy and patient control."
5. "Overview - fhir v5.0.0," accessed: July 23, 2025. [Online]. Available: https://www.hl7.org/fhir/overview.html
6. G. Han, Y. Ma, Z. Zhang, and Y. Wang, "A hybrid blockchain-based solution for secure sharing of electronic medical record data," *PeerJ Computer Science*, vol. 11, p. e2653, Jan. 2025.
7. "Decentralized identifiers (dids) v1.0," accessed: July 23, 2025. [Online]. Available: https://www.w3.org/TR/did-1.0/
8. "Verifiable credentials data model v2.0," accessed: July 23, 2025. [Online]. Available: https://www.w3.org/TR/vc-data-model/
9. "Zero knowledge proofs: An illustrated primer," a Few Thoughts on Cryptographic Engineering. Accessed: July 20, 2025. [Online]. Available: https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/
10. M. Alruwaill, S. Mohanty, and E. Kougianos, "hchain: Blockchain based large scale ehr data sharing with enhanced security and privacy," may 19, 2025, arXiv: arXiv:2505.12610.