

Guardian Key Protocol: A Multi-Party Recovery Framework for Owner Incapacity in Blockchain-Based Land Registry Systems

Anjali Avasthi¹, Shriram Sendapriyar², Shubha Rawat³, Rohit Labade⁴

¹Computer Department, Bharati Vidyapeeth's College of Engineering, Lavale (Pune)

²Computer Department, Bharati Vidyapeeth's College of Engineering, Lavale (Pune)

³Computer Department, Bharati Vidyapeeth's College of Engineering, Lavale (Pune)

⁴Computer Department, Bharati Vidyapeeth's College of Engineering, Lavale (Pune)

Abstract - Blockchain-based land registry systems improve transparency and security in property management but assume the owner is always available to sign using their private key. This assumption fails in cases of key loss, temporary incapacity, or death. This paper proposes the Guardian Key Protocol (GKP), a recovery mechanism built atop a dual-signature blockchain land registry. GKP combines Shamir's Secret Sharing for distributed key custody, government-authorized oracle verification to authenticate off-chain trigger events, and time-locked smart contract finalization to prevent fraudulent recovery attempts. Three guardian nodes pre-registered by the owner hold key shards, and recovery requires a 2-of-3 threshold together with a mandatory government escrow shard, ensuring no single party can unilaterally recover the key. The protocol aligns with Indian legal instruments including the Information Technology Act of 2000, the Registration Act of 1908, and the Indian Succession Act of 1925. GKP extends the security model of dual-signature land registries to cover succession, guardianship, and key-loss scenarios without compromising routine operation.

Key Words: Guardian Key Protocol, blockchain land registry, Shamir's Secret Sharing, key recovery, smart contracts, digital inheritance.

1. INTRODUCTION

Land registries constitute one of the most critical types of public infrastructure, defining ownership, inheritance procedures, asset security, and the legal validity of each registration record. Paper-based registries are highly susceptible to fraud, delays, and fragmentation, which has motivated the use of blockchain technology to enhance land administration. Among the most prominent approaches is the dual-signature model, wherein a transfer is authorized only after cryptographic approval by both the property owner and the designated registrar, reducing the risk of unilateral manipulation [4][5].

A fundamental limitation of such systems, however, is their dependency on the continuous availability of the owner's private key. In cases of key loss, temporary incapacity due to health or legal reasons, or the owner's death, the registry becomes frozen and no transfers can proceed. This directly conflicts with the legal reality that property transactions must remain possible regardless of the owner's personal availability. Indian legislation, including the Indian Succession Act of 1925, the Information Technology Act (IT Act) of 2000, and the Registration Act of 1908, explicitly provides mechanisms that

permit legitimate transactions when the owner cannot personally sign [2][3][1].

This paper proposes the Guardian Key Protocol (GKP), a recovery layer designed to operate on top of an existing dual-signature blockchain land registry. GKP addresses three distinct failure scenarios — key loss, temporary incapacity, and death — using a combination of distributed key sharing, government-authorized oracle verification, and time-locked smart contract finalization, ensuring both cryptographic security and compliance with applicable law [3][1][2].

2. BACKGROUND

Prior work on blockchain-based land registries has consistently identified three key properties: transparency, immutability, and multi-party approval coordination between the landowner and the registrar. Research into multi-tier blockchain architectures demonstrates the potential of blockchain as an effective audit layer for land transactions. India's legislative recognition of electronic signatures under the IT Act further supports the practical feasibility of blockchain-based land management [6][1].

In the domain of cryptographic recovery, Shamir's Secret Sharing (SSS) is an established technique that splits a secret into n shares such that any k shares ($k \leq n$) are sufficient to reconstruct it, while fewer than k shares reveal no information about the secret. Although SSS is well studied for protecting cryptocurrency wallets and personal accounts, its application to government-managed property records with legally recognized inheritance implications has not been thoroughly explored [1].

Existing digital inheritance and dead-man-switch protocols address postmortem transactions but are limited in scope, lacking integration with court orders, hospital certificates, civil registration records, and registrar-managed workflows. GKP addresses this gap by bridging formal land administration processes with modern cryptographic recovery methods [3][1].

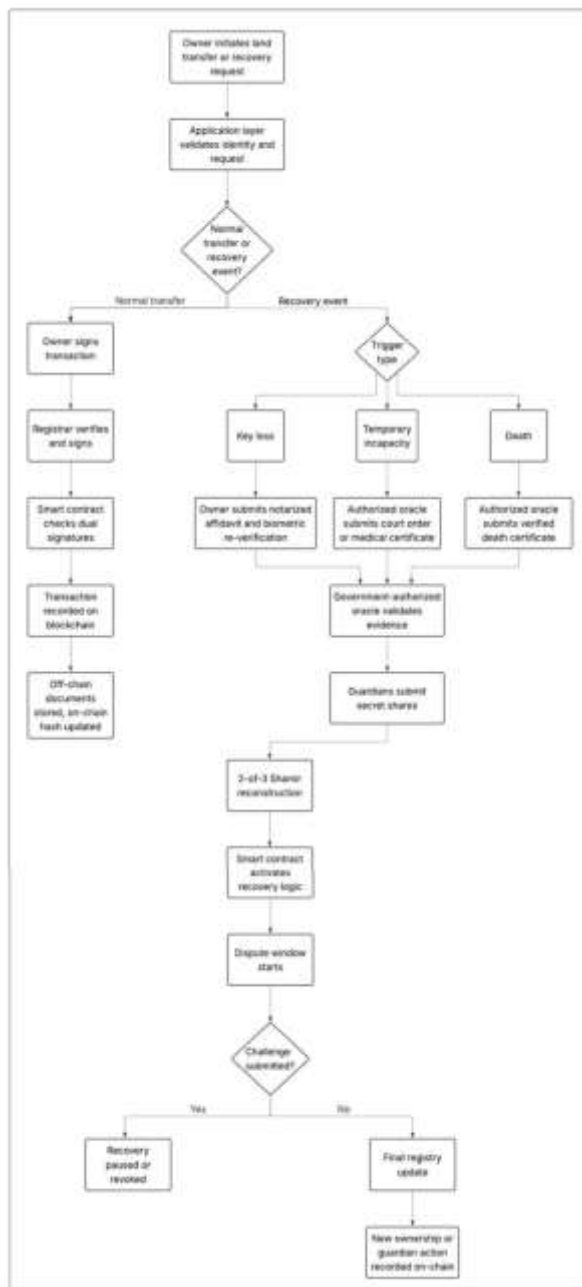
3. PROBLEM STATEMENT

Three distinct operational failures arise in dual-signature blockchain land registry systems. First, in a key loss scenario, a legally capable and living owner is permanently unable to access the private key required to authorize a transfer. Second, in a temporary incapacity scenario, the owner is unable to act due to health or legal reasons, despite the continued need for property management. Third, in the event of death, ownership must be transferred through succession or probate procedures;

however, the blockchain has no mechanism to recognize a death certificate or judicial order [2][3].

Across all three scenarios, the underlying technical problem is identical: a transfer must be authorized despite the owner's inability to sign. Any solution must simultaneously satisfy three requirements: cryptographic integrity (the recovery process must not weaken the security model), legal anchoring (recovery triggers must correspond to recognized legal events), and resistance to unauthorized recovery attempts (the protocol must not create a new attack surface) [1][2].

4. GUARDIAN KEY PROTOCOL



GKP implements a recovery layer that operates above the standard dual-signature transfer flow. Under normal operating

conditions, the registry functions unchanged: the owner and registrar must jointly authorize each transfer. The recovery layer activates exclusively upon a verified trigger event. The protocol comprises four components described below.

Guardian Pre-Registration: The owner designates up to three guardians, typically relatives or legal representatives, at the time of registry enrollment. Under normal conditions these guardians hold no authority over the property. Their role is limited strictly to participation in a verified recovery event.

Distributed Key Sharding via SSS: The owner's private key is split into three shares using Shamir's Secret Sharing with a 2-of-3 threshold. One share is held by each guardian, and a fourth mandatory shard is placed in escrow with the government registry. Reconstruction requires any two guardian shares plus the government shard. This means that even full collusion among all three guardians is insufficient to recover the key without government participation, providing a structural check against unauthorized restoration.

Government-Authorized Oracle Verification: Recovery is initiated only after an off-chain trigger is validated by an authorized government oracle node. For key loss, the owner submits a notarized affidavit and undergoes biometric re-verification. For temporary incapacity, a court-issued guardianship order or certified medical certificate is required. For death, a verified death certificate from an authorized civil registration authority is required. Only upon validation of the appropriate off-chain document does the smart contract commence the on-chain recovery sequence.

Time-Locked Smart Contract Finalization: Once a recovery transfer is triggered on-chain, the smart contract enforces a mandatory dispute window before finalizing the ownership update. During this window, any interested party — including a living owner disputing a falsified death certificate — may raise a challenge and halt the transfer. This time-lock acts as the last line of defense against fraudulent recovery attempts and ensures reversibility prior to finalization.

5. SECURITY PROPERTIES

GKP is designed to defend against several threat classes common to high-value registry systems. Regarding shard theft, a single compromised share reveals no information about the private key by the information-theoretic properties of SSS. An attacker who compromises one guardian device still requires an additional guardian share and the government escrow shard, making shard-only attacks insufficient [1].

Fake-death attacks are mitigated by the oracle model, which requires verification documents to originate from authorized institutional nodes rather than being submitted freely. Even if a fraudulent death trigger were somehow introduced, the mandatory time-lock dispute window provides a further opportunity for the living owner or a legitimate party to challenge and revoke the transfer before finalization [2][1].

Guardian collusion is structurally prevented: all three guardians together cannot reconstruct the key without the government escrow shard. Replay attacks are neutralized by binding each recovery trigger to a unique combination of parcel identifier and transaction hash, ensuring a triggered recovery event cannot be resubmitted. These layered controls make the recovery process fully auditable on-chain [3][1].

6. LEGAL ALIGNMENT

GKP's design is grounded in three Indian statutes. The Information Technology Act of 2000 confers legal recognition on digital signatures and electronic authentication procedures, establishing the legal validity of cryptographic identity within registry workflows [2][1]. The Registration Act of 1908 defines the requirements for valid property registration, and blockchain entries satisfying these requirements may therefore be treated as part of the formal registration process [2].

The Indian Succession Act of 1925 governs inheritance and provides the legal basis for GKP's death-triggered recovery path, enabling ownership transfer when the private key holder is deceased. For incapacity scenarios, court-supervised guardianship procedures under applicable Indian law authorize property management on behalf of the incapacitated owner. These statutes collectively provide the legal legitimacy that elevates GKP from a purely technical mechanism to a legally anchored institutional procedure [3][1].

Land is a legally protected asset, not an abandoned commodity. Registry systems are therefore obligated to support succession, guardianship, and transfer even in the absence of the registered owner. GKP satisfies this obligation by anchoring every recovery trigger to a corresponding legal instrument [3][2].

7. DISCUSSION

The primary strength of GKP is that it preserves the trusted dual-signature transfer mechanism for routine operations while introducing a tightly controlled recovery path for emergency scenarios. Guardians hold no ongoing authority, and state participation is mandatory for any extraordinary transfer — a design property that is essential for legal process integrity [1][2].

The principal practical challenge is administrative. Implementing oracle governance, onboarding guardians, managing shard custody, and resolving disputes all require clearly defined procedures and institutional capacity. In communities with limited digital literacy or infrastructure, a custodial model in which the registry office bears part of the recovery burden may be necessary, representing a deliberate trade-off between decentralization ideals and operational feasibility [3].

Privacy is a further consideration. Recovery events involve sensitive documents such as medical certificates and death certificates. Committing only pre-computed hashes of these documents to the blockchain, rather than the documents themselves, mitigates exposure while maintaining verifiability. Production deployments may require additional privacy-preserving measures, such as zero-knowledge proofs or role-based access controls, to meet data protection obligations.

8. CONCLUSIONS

This paper has proposed the Guardian Key Protocol (GKP), a recovery framework that addresses a fundamental vulnerability in blockchain-based land registry systems: the implicit assumption that the property owner is always available and capable of signing transactions. By integrating Shamir's Secret Sharing for distributed key custody, government-authorized

oracle verification for legally anchored trigger authentication, and time-locked smart contract finalization for fraud resistance, GKP provides a comprehensive response to the failure scenarios of key loss, temporary incapacity, and owner death. Unlike general-purpose cryptographic key recovery schemes, GKP is purpose-built for the institutional, legal, and operational context of state-managed property records. It is not merely a technological contribution but a legal and institutional innovation, enabling blockchain-based land registries to reliably support succession, guardianship, and recovery without immobilizing ownership or compromising the security of the underlying registry. Future work should address prototype implementation, formal security proofs, and pilot evaluation within a government land registry environment [3][1].

ACKNOWLEDGEMENT

The authors would like to acknowledge the support of their respective institutions and colleagues who contributed feedback during the preparation of this manuscript.

REFERENCES

- [1] [General blockchain land registry and cryptographic recovery reference — full citation to be supplied by authors]
- [2] Government of India, "The Information Technology Act, 2000," Ministry of Electronics & Information Technology, New Delhi, 2000.
- [3] Government of India, "The Indian Succession Act, 1925," Ministry of Law and Justice, New Delhi, 1925.
- [4] Government of India, "The Registration Act, 1908," Ministry of Law and Justice, New Delhi, 1908.
- [5] Drishti Judiciary, "Digital Signature and Electronic Signature," [Online]. Available: <https://www.drishtijudiciary.com> [Accessed: 2024].
- [6] [Land registry blockchain research / case studies reference — full citation to be supplied by authors]