BLOCK CHAIN TECHNOLOGY

DIPLOMA WALLAH

OPEN ELECTIVE

Jharkhand University Of Technology (JUT)

UNIT V: Blockchain Technology for Government and Cryptography

1. Blockchain for Government Applications

A. Digital Identity

Definition

Digital identity refers to an electronic representation of an individual's identity that can be verified and authenticated using blockchain technology.

Problems with Traditional Digital Identity Systems

- **Centralization Risks**: Single point of failure; vulnerable to hacks and breaches; limited user control.
- **Inefficiency**: Multiple redundant verification processes; time-consuming; bureaucratic.
- **Paper-Based Issues**: Physical documents lost, damaged, or forged.
- **Privacy Concerns**: Excessive data collection, surveillance risks, no control for users.
- **Corruption**: Bribes for certificates, fake documents, unfair service delivery.

Blockchain Solution: Self-Sovereign Identity (SSI)

- Users own and control their digital identities without centralized authorities.
- **Decentralized Identifiers (DID)**: Unique, user-controlled identifiers recorded immutably on blockchain.
- **Verifiable Credentials (VCs)**: Digitally signed attestations issued by trusted authorities.
- **Selective Disclosure**: Users share only necessary information, preserving privacy through cryptographic proofs.

- **Instant Verification**: Verification of credentials in seconds, lower cost, enhanced interoperability.

Process

1. User generates cryptographic key pair and creates DID.
2. Trusted issuer (government) verifies and issues verifiable credential.
3. User holds credential in digital wallet.
4. When needed, user presents credential; verifier checks validity via blockchain.
5. User controls which information to disclose.

Benefits

- User control and privacy.
- Enhanced security.
- Faster identity verification.
- Lower costs and fraud.
- Interoperability across services.
- Inclusion of unbanked and undocumented populations.

Real-World Example

India's National Blockchain Framework has verified over 340 million documents digitally using blockchain-based identity management integrated with Aadhaar.

B. Land Records

Problems with Traditional Land Registry

- Fraud and forgery: Fake ownership documents, multiple sales.
- Slow transactions: Months to years due to manual searches and bureaucratic delays.
- Corruption: Bribes and manipulation in document processing.
- Lack of transparency: Difficulty verifying title and encumbrances.
- High cost and complexity.

Blockchain Land Registry Solution

- Immutable, transparent, cryptographically verifiable land ownership records.

- Complete ownership history accessible on blockchain.
- Automated smart contract-based ownership transfers.
- Fraud detection via cryptographic signatures.
- Instant transaction settlements.

Blockchain Land Registry Process

1. Digitize and verify existing paper records; record them immutably on blockchain.
2. Seller lists property details along with verified documents and photos on blockchain.
3. Buyer searches properties with full ownership history.
4. Seller accepts offer; government inspector verifies property physically and digitally.
5. Smart contract executes simultaneous payment and ownership transfer.
6. Immutable records prevent fraud, multiple sales, and disputes.

Benefits

- Fraud prevention and transparency.
- Reduced transaction time from months to minutes.
- Lower costs.
- Better governance and land market stability.

Examples

- Georgia implemented a blockchain land registry reducing fraud and transaction times.
- Sweden pilots blockchain-based property transfers.
- India is expanding state-level blockchain land registry projects integrated with the National Blockchain Framework.

C. Record Keeping Between Government Entities

- Blockchain enables shared, real-time data access across government departments.
- Eliminates data silos and duplications.
- Automates inter-agency workflows with smart contracts.

- Improves transparency and accountability.
- Example: Automated business registration processes with instant tax and labor registration notifications.

D. Public Distribution System (PDS) / Social Welfare Systems

Current Challenges

- Major leakages and diversion of subsidized goods (up to 80% lost).
- Corruption at warehouses, transport, and Fair Price Shops.
- Ghost and duplicate beneficiaries.
- Lack of transparency and accountability.
- Inefficient targeting and delivery.

Blockchain PDS Solution

- Track every gram of subsidized food from farmer to beneficiary using blockchain and IoT sensors.
- Farmer registration with biometric identity.
- Real-time monitoring of storage conditions and stock levels.
- Secure transport tracking with GPS and tamper-proof seals.
- Beneficiary identification with Aadhaar-linked biometric authentication.
- Real-time recording of distribution quantities on blockchain.
- Smart contracts to prevent duplicate and fraudulent distributions.
- Direct benefit transfer options reduce physical diversion.

Impact

- Leakage reduced from 80% to under 5%.
- Thousands of crores of rupees saved annually.
- Improved food security and trust among beneficiaries.
- Faster, transparent government welfare delivery.

---

2. Cryptography: Privacy and Security on Blockchain

A. Zero-Knowledge Proofs (ZKPs)

Overview

ZKPs allow one party to prove the truth of a statement without revealing any underlying data beyond the validity itself.

Properties

- **Completeness**: True statements can be proven reliably.
- **Soundness**: False statements cannot be proved.
- **Zero-knowledge**: No additional information is leaked.

Example

Proving "I am over 18" without revealing birth date using complex cryptographic methods.

Types of ZKPs

- **zk-SNARKs**: Succinct, non-interactive proofs requiring a trusted setup; used in privacy coins like Zcash.
- **zk-STARKs**: Scalable, transparent proofs with no trusted setup and quantum resistance.

Applications

- Private identity verification (age, income).
- Secure voting systems.
- Financial privacy in transactions.
- Scalability solutions (zk-Rollups) for blockchain networks.

B. Ring Signatures

Concept

A group signature in which anyone in a set can sign a message anonymously, making it impossible to determine which specific member signed.

Features

- Signer anonymity and unlinkability.
- No central authority or group manager needed.
- Complex signature includes all group members' public keys.

Application Example

Monero cryptocurrency uses ring signatures to hide sender identities, ensuring untraceable transactions and strong privacy.

C. Blockchain Security Attacks and Preventive Measures

1. 51% Attack

- Occurs when one entity controls over half the computing or staking power.
- Allows double-spending and rewriting recent blocks.
- Economically impractical on large networks like Bitcoin and Ethereum.

2. Sybil Attack

- Creating numerous fake identities to manipulate consensus or network behavior.
- Prevented through Proof of Work or Proof of Stake economic barriers, reputation systems, and Proof of Personhood.

Summary

Unit V covers how blockchain transforms government functionalities and privacy/security mechanisms:

- Blockchain enables **self-sovereign digital identity** giving control and privacy to citizens.
- Immutable **land registries** prevent fraud, speed transactions, and promote transparency.
- Inter-agency record keeping is streamlined and automated on shared ledgers.
- Public welfare systems like **PDS** use blockchain and biometrics to eliminate corruption and improve efficiency.
- Cryptographic innovations like **Zero-Knowledge Proofs** and **Ring Signatures** secure privacy and enable trustless verification.
- Network security is reinforced against attacks by economic incentives and cryptographic designs.

This unit lays the foundation for trustworthy, efficient, and inclusive government services powered by blockchain and cryptography, addressing long-standing issues of fraud, inefficiency, and privacy.

Diploma Wallah

Made with ❤ by Sangam