Secure IP Ownership Management System using Blockchain Technology

A Vinil - 2022A3PS1648H
Abhinav Reddy Kallem - 2021B4A32408H
Himanshu Singh - 2022AAPS0306H
Nishant Raut - 2022B5AA0689H

November 2024

INTRODUCTION

What is Intellectual Property (IP)?

- **Definition:** Intellectual Property (IP) refers to the creations of the mind, including inventions, ideas, and artistic works.
- **Management:** IP can be transferred, licensed, or registered to protect and commercialize rights.
- **Record Keeping:** A ledger is maintained to store details of IP ownership and transactions.
- **Example:** Like a bank tracks monetary assets, an IP ledger tracks ownership and usage of intellectual assets.

Disadvantages of Centralised Intellectual Property (IP) Management System:

- Lack of Transperency
- Difficulty Verifying Authenticity
- Risk of Duplicates
- Need for Trusted Intermediaries

SYSTEM STRUCTURE

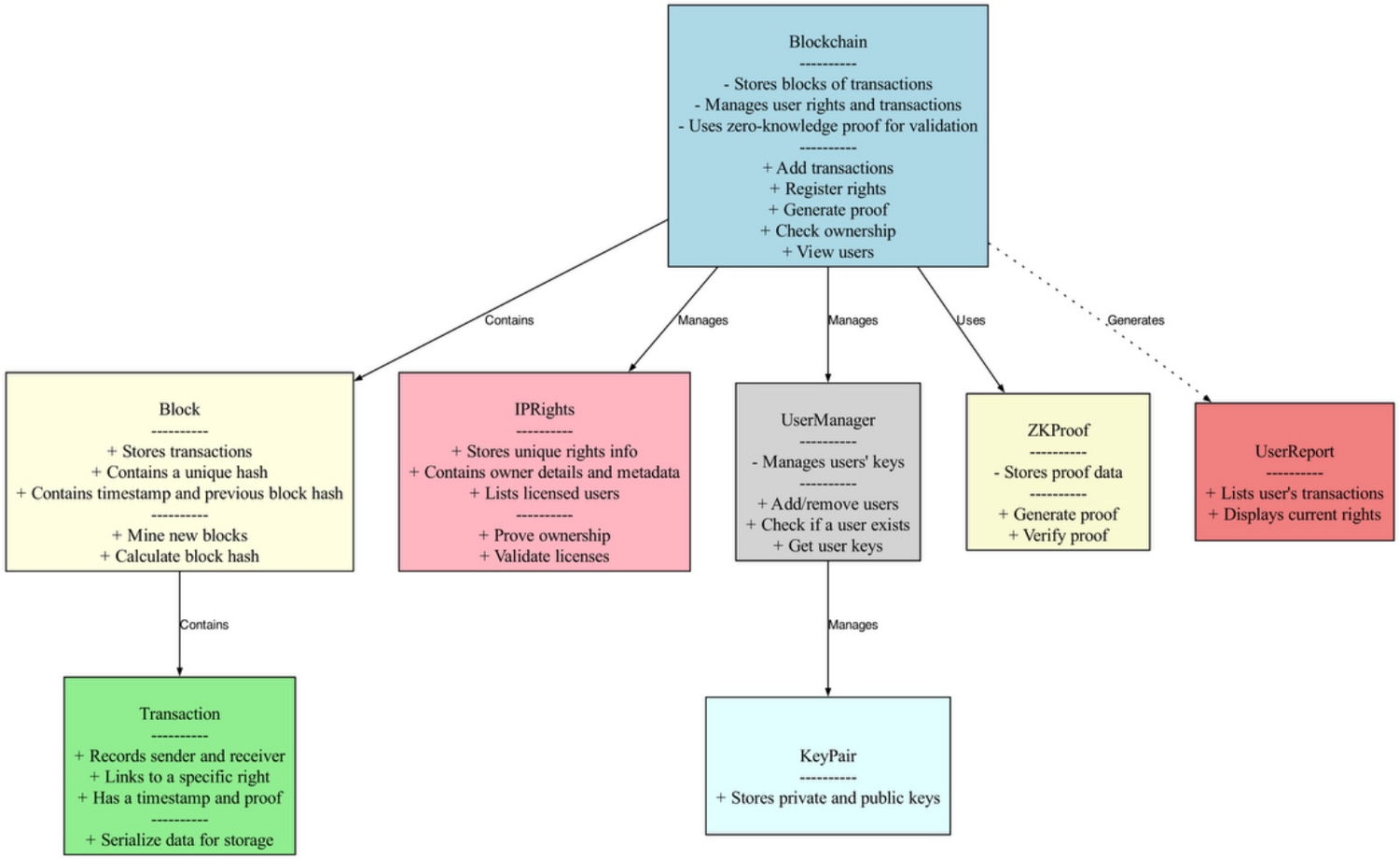

Figure: Class Diagram for IP Right Management System

Implementing Blockchain

- **Cryptographic Components:**
  1. Hash function
  2. Public Key Infrastructure
- **Blockchain:** A chain of blocks that stores data securely in a decentralized manner.
- **Block:** Previous hash,vector of 10 Transactions, Current Hash
- **Transaction:** fromUser, toUser, IP, timestamp, Type
- **Problem:** Transparency of Confidential Information
  - Solution: ZKP.

ZKP

- Prove Ownership of IP Rights without revealing Private Key
- The key security properties are
  1. Zero-Knowledge: The proof doesn't reveal Owner's private key
  2. Soundness: Only someone who knows the private key can generate valid proofs
  3. Completeness: Valid proofs are always accepted

- Implementation
  1. Setup
     - Large Prime Number p and Generator g
     - Private key x and corresponding Public key $y = g^x mod(p)$ of each user
  2. Proof Generation
     - Create a random value r
     - Compute $t = g^r mod(p)$
     - Generate challenge c using hash of commitment t reduced to $modulo(p-1)$ to fit the group
     - Calculate response $s = r + c * xmod(p-1)$
     - Send (t, s) to verifier
  3. Verification
     - Receive Public Key y and (t, s)
     - Rederive c from t
     - Verify $g^s = t * y^c mod(p)$