RANCANG BANGUN SIMULASI SISTEM HAK CIPTA DIGITAL TERDESENTRALISASI BERBASIS ALGORITMA SHA-256 DAN *BLOCKCHAIN* (*PROOF OF DESIGN*)

Disusun Oleh:

1 Deviana Ainul Riqoh (230202741)
2 Fajar Saputro (230202749)
3 Raffly Ardya Putra (230202775)
4 Reza Dwi Nugroho (230202781)
5 Vera Indryawanti (230202791)

A. PENDAHULUAN

1. Latar Belakang

Di era digital, kemudahan menduplikasi asset visual (seperti logo atau design grafis) tanpa penurunan kualitas menimbulkan masalah serius terkait hak cipta. Metode perlindungan konvensional (seperti *watermark* atau metadata EXIF) mudah dimanipulasi atau dihapus oleh pihak yang tidak bertanggung jawab. Selain itu, sistem pendaftaran hak cipta yang bersifat terpusat (*centralized*) memiliki kelemahan berupa titik kegagalan tunggal (*single point of failure*), kerentanan terhadap peretasan basis data, dan birokrasi yang cenderung lambat. Oleh karena itu, diperlukan sebuah mekanisme baru yang memanfaatkan kriptografi untuk menjamin integritas data dan pembuktian kepemilikan yang tak terbantahkan secara matematis.

2. Tujuan Proyek

Proyek ini bertujuan untuk membangun sebuah *Proof of Concept* (PoC) system simulasi pendaftaran hak cipta digital yang menerapkan:

a. Fungsi Hash Kriptografi untuk memastikan integritas file secara mutlak.
b. Konsep Blockchain untuk pencatatan Riwayat kepemilikan yang kekal (*immutable*).
c. Logika Smart Contract sederhana untuk mendeteksi dan mencegah plagiarisme (pendaftaran ganda) secara otomatis.

B. DESKRIPSI SISTEM

Sistem yang dibangun adalah aplikasi berbasis web (*client-side*) yang mensimulasikan cara kerja *Decentralized Application* (DApp). Alur kerja system adalah sebagai berikut:

1. Identitas Terdesentralisasi: Pengguna melakukan autentikasi menggunakan dompet kripto (MetaMask), menggantikan metode login email/password tradisional.
2. Hashing (*Digital Fingerprint*): Saat pengguna mengunggah file gambar, system memproses file tersebut menjadi *digest* atau sidik jari digital yang unik.
3. Validasi Otomatis: Sistem memeriksa apakah *digest* tersebut sudah ada di dalam *ledger* (buku besar).
4. Pencatatan Blok: Jika data unik, informasi (Hash, Waktu, Pemilik) disimpan ke dalam blok baru yang terhubung secara kriptografis dengan blok sebelumnya. Data disimpan secara persisten menggunakan *Local Storage* browser untuk menyimulasikan persistensi node blockchain.

C. ALGORITMA DAN PROTOKOL KRIPTOGRAFI

Sistem ini mengintegrasikan beberapa konsep kriptografi utama sebagai fondasi keamanan:

1. Secure Hash Algorithm 256-bit (SHA-256)
   Algoritma ini digunakan sebagai inti verifikasi untuk menghasilkan “sidik jari digital” dari file gambar.

- Sifat *One-Way*: Hash yang dihasilkan tidak dapat dikembalikan menjadi gambar asli (*irreversible*).
- Sifat *Collision Resistance*: Sangat sulit secara komputasi untuk menemukan dua gambar berbeda yang menghasilkan hash yang sama.
- Efek *Avalanche*: Perubahan sekecil apapun pada input (missal: penambahan satu titik piksel pada logo) akan menghasilkan perubahan drastis pada output hash. Sifat ini menjamin orisinalitas mutlak.

2. Public Key Infrastructure (PKI) – Via MetaMask
   Sistem tidak menyimpan *username* atau *password*. Autentikasi dilakukan melalui mekanisme tanda tangan digital dari dompet MetaMask. Alamat dompet (*Public Address*) bertindak sebagai identitas public, sementara kendali penuh atas akun berada pada pengguna yang memegang Private Key secara local di perangkat mereka.
3. Chain Linking (Hash Pointers)
   Integritas urutan data dijamin dengan menyertakan prevHash (Hash dari blok sebelumnya) ke dalam struktur blok baru. Jika penyerang mencoba memodifikasi data di Blok #1, maka Hash Blok #1 akan berubah. Hal ini menyebabkan ketidakcocokan pada prevHash di Blok #2, sehingga rantai menjadi tidak valid (putus).

D. URAIAN SINGKAT IMPLEMENTASI

1. Teknologi (Tech Stack)
   - Frontend: HTML5 & CSS3 untuk antarmuka pengguna yang responsive.
   - Logic: JavaScript (Vanilla ES6+) untuk logika kriptografi dan simulasi struktur data blockchain.
   - Cryptography: Web Crypto API (crypto.subtle) bawaan browser untuk eksekusi algoritma SHA-256 yang efisien dan aman di sisi klien.
2. Struktur Data Blok
   Setiap blok dalam sistem direpresentasikan sebagai Objek JSON yang memuat property:
   - Index: Nomor urut blok
   - Timestamp: Waktu pencatatan transaksi
   - Owner: Alamat heksadesimal dompet pendaftar
   - Hash: Output SHA-256 dari file gambar
   - PreHashs: Referensi ke hash blok sebelumnya
3. Mekanisme Persistensi
   Untuk menyimulasikan sifat distributed ledger yang tidak hilang saat refresh atau restart, system memanfaatkan fitur local storage browser untuk menyimpan array rantai blok (blockchain) dan tabel hash (registeredHashes) secara persisten di sisi klien.

E. HASIL PENGUJIAN DAN DEMONSTRASI

Berdasarkan serangkaian pengujian yang dilakukan, system berhasil menangani scenario sebagai berikut:

Skenario Pengujian	Input Data	Hasil yang Diharapkan	Hasil Aktual	Status
Pendaftaran Valid	Logo A (belum terdaftar)	Blok baru terbentuk, Hash dicatat	Blok #1 terbentuk di UI	Berhasil
Uji Plagiarisme	Logo A (di upload ulang)	Sistem menolak dengan pesan error	Alert: “Logo sudah terdaftar”	Berhasil
Uji Integritas (Avalanche)	Logo A + 1 titik pixel (edit)	Sistem menganggap sebagai file baru	Hash berubah total sukses daftar	Berhasil
Persistensi Data	Refresh Browser	Data blok tidak hilang	Riwayat blok tetap tampil	Berhasil

F. ANALISIS KEAMANAN

1. Integritas Data (Data Integrity): Terjamin oleh penggunaan SHA-256. Tidak ada cara komputasi praktis saat ini untuk memalsukan gambar agar memiliki hash yang sama dengan gambar asli yang sudah terdaftar (Pre-image resistance).
2. Penyangkalan (Non-Repudiation): Dengan integritasi MetaMask, setiap pendaftaran terikat secara matematis pada alamat dompet unik. Pengguna tidak dapat menyangkal bahwa akun merekalah yang mendaftar karya tersebut (dengan asumsi private key pengguna tetap aman).
3. Ketersediaan (Availability): Dalam simulasi ini, ketersediaan bergantung pada penyimpanan local perangkat (local device storage). Namun, dalam implementasi nyata (mainnet), ketersediaan akan dijamin oleh ribuan node yang tersebar di seluruh dunia, membuat sistem tahan terhadap penyensoran atau server down.

G. KESIMPULAN

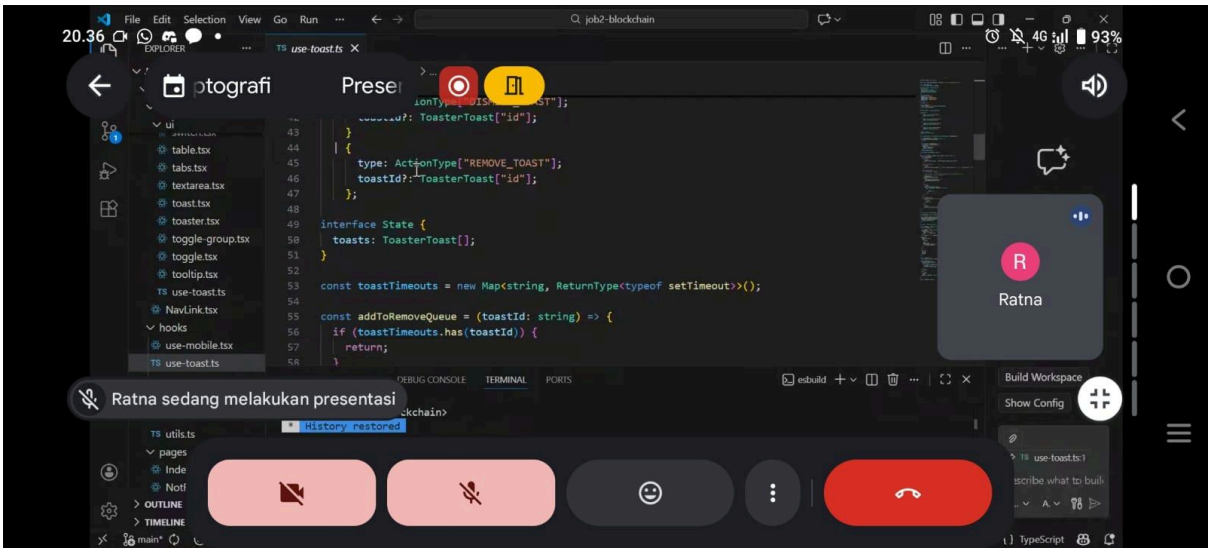
Proyek ini berhasil membuktikan bahwa integrasi kriptografi (SHA-256) dan struktur data Blockchain dapat menjadi solusi efektif untuk perlindungan hak cipta digital. Sistem mampu mendeteksi duplikasi secara otomatis (anti-plagiasi) dan menjamin integritas karya hingga level piksel (efek avalanche). Meskipun dikembangkan dalam bentuk simulasi Proof of Concept, logika dasar keamanan yang diterapkan telah mencerminkan standar arsitektur sistem tersentralisasi modern.

LAMPIRAN BUKTI PENDUKUNG

A. File Slide Presentasi

[Terlampir]

B. Bukti Pelaksanaan Presentasi



C. Manual Book (Panduan Pengguna Singkat)

[Terlampir]

D. Tautan Repositori

https://github.com/Reja016/Proof-of-Design

E. Bukti Implementasi (Kode Inti)

Implementasi SHA-256 Menggunakan Web Crypto API (JavaScript):

```
async function calculateHash(file) {
    const arrayBuffer = await file.arrayBuffer();
    // Menggunakan Web Crypto API untuk performa dan keamanan
    const hashBuffer = await crypto.subtle.digest('SHA-256', arrayBuffer);
    const hashArray = Array.from(new Uint8Array(hashBuffer));
    // Konversi ke format Heksadesimal
    return hashArray.map(b => b.toString(16).padStart(2, '0')).join('');
}
```

F. Pembagian Peran Tim (Sumbangsih)

No	Nama Anggota	Peran & Kontrubusi
1	Deviana Ainul Riqoh (230202741)	Project Manager & UI Designer: Merancang antarmuka dan alur UX.
2	Reza Dwi Nugroho (230202781)	Lead Programer: Mengimplementasikan fungsi Hashing dan logika validasi javascript.
3	Fajar Saputro (230202749)	Blockchain Architect: Merancang struktur data Blok, Linked-List, dan integrasi LocalStorage.
4	Vera Indryawanti (230202791))	Tester & Integration: Melakukan uji coba skenario plagiarisme (QA) dan integrasi WalletMask.
5	Raffly Ardya Putra (230202775)	Documentation: Menyusun laporan akhir, slide presentasi, dan analisis keamanan sistem.