



PROOF OF DESIGN (POD)

PLATFORM AUTENTIKASI KREATOR VIA BLOCKCHAIN



>>

ANGGOTA KELOMPOK

- » **DEVIANA AINUL RIQOH**
- » **FAJAR SAPUTRO**
- » **RAFFLY ARDYA PUTRA**
- » **REZA DWI NUGROHO**
- » **VERA INDRIYAWANTI**



LATAR BELAKANG MASALAH

- Era Digital & Kemudahan Duplikasi: Karya seni digital (seperti logo) sangat mudah dicuri dengan "Klik Kanan > Save As" atau screenshot.
- Masalah Pembuktian: Metadata gambar tradisional mudah dimanipulasi. Sulit membuktikan siapa pemilik asli pertama kali.
- Kelemahan Sistem Terpusat: Pendaftaran hak cipta konvensional seringkali birokratis, lambat, dan datanya tersimpan di satu server pusat yang rawan peretasan.

TUJUAN & SOLUSI YANG DITAWARKAN

Tujuan: Membangun sistem Proof of Concept (simulasi) untuk membuktikan kepemilikan karya digital secara terdesentralisasi.

Solusi:

- Kriptografi (Digital Fingerprint): Menggunakan matematika untuk memastikan keaslian file.
- Blockchain Ledger: Mencatat riwayat kepemilikan yang transparan dan tidak bisa diubah.
- Web3 Identity: Menggunakan dompet kripto (MetaMask) sebagai identitas pemilik, bukan sekedar email/password.

ARSITEKTUR & ALUR SISTEM



- » **CONNECT WALLET:** USER LOGIN MENGGUNAKAN METAMASK
- » **UPLOAD & HASHING:** USER MENGUNGGAH FILE. SISTEM MENGHITUNG SHA-256 HASH
- » **VERIFIKASI (SMART CONTRACT):** SISTEM MENGECEK DATABASE
 - JIKA HASH ADA: TOLAK (PLAGIAT)
 - JIKA HASH BARU: LANJUT
- » **MINING BLOCK:** DATA (HASH, OWNER, WAKTU) DIBUNGKUS DALAM BLOK BARU
- » **STORAGE:** BLOK DITAMBAHKAN KE RANTAI BLOCKCHAIN PERMANEN

TEKNOLOGI YANG DIGUNAKAN

» FRONTEND

HTML5, CSS3, JavaScript (ES6)

» CRYPTOGRAPHY

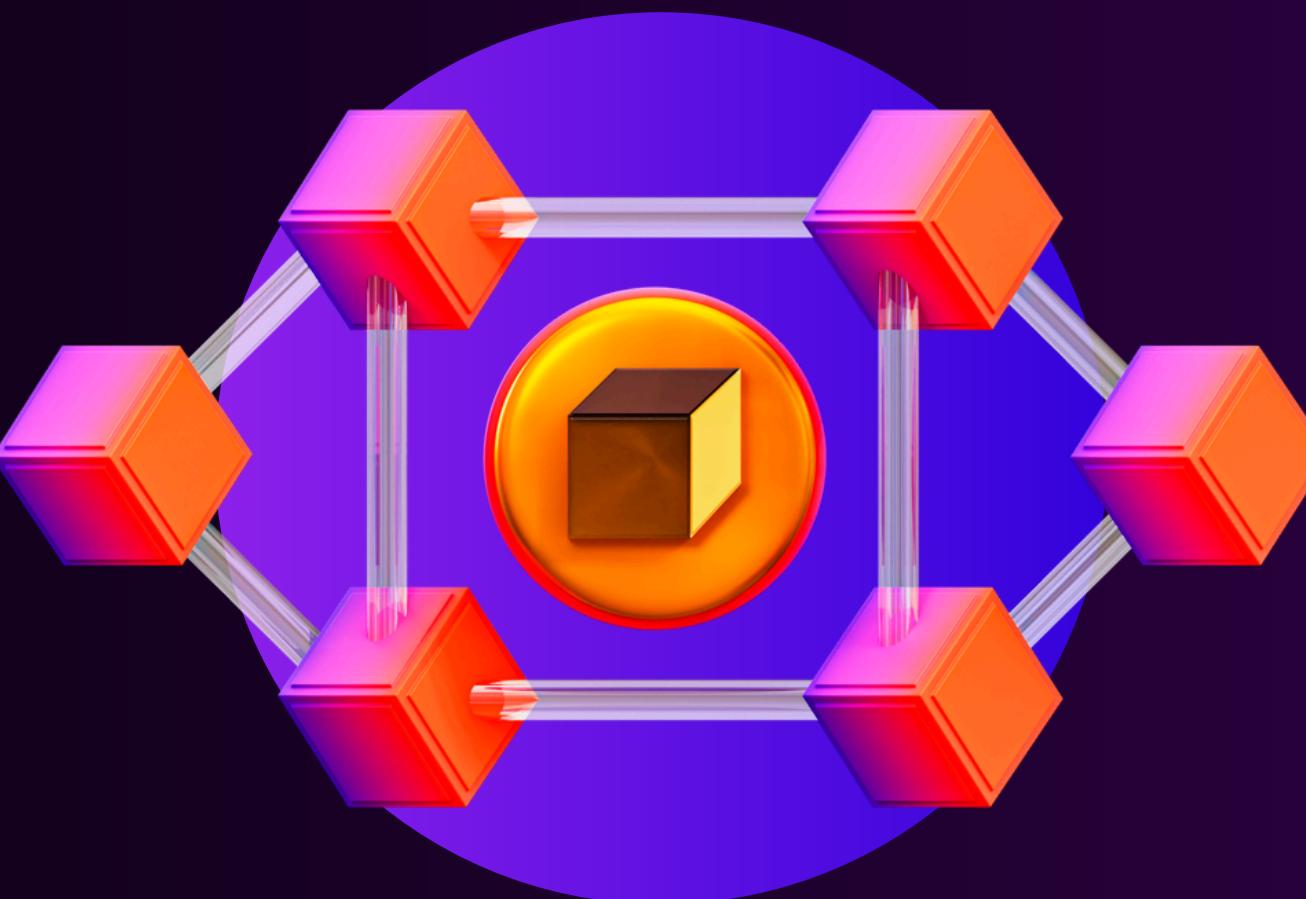
API `crypto.subtle` (SHA-256 Algorithm). Untuk mengubah input gambar apapun menjadi string 64 karakter heksadesimal

» AUTHENTICATION

Web3 Injection (MetaMask
Window.ethereum)

» STORAGE SIMULATION

Browser LocalStorage
(Persistence Data)



KRIPTOGRAFI & EFEK AVALANCHE

FUNGSI HASH SHA-256

Mengubah input data (gambar) sebesar apapun menjadi string 64 karakter yang tetap

INTEGRITAS MUTLAK (AVALANCHE EFFECT)

Perubahan input yang sangat kecil menyebabkan perubahan output yang drastis

CONTOH KASUS

- Gambar Logo Asli → Hash: e3b0c4...
- Gambar Logo + Perbedaan Kecil → Hash: f9a1d2...
(Berubah Total)

KESIMPULAN TEKNIS

Sistem ini menjamin bahwa file yang terdaftar adalah 100% orisinil tanpa modifikasi satu bit pun

STRUKTUR BLOCKCHAIN & SMART CONTRACT

SIMULASI STRUKTUR BLOK

Setiap blok data yang disimpan berisi:

- Timestamp: Waktu pencatatan
- Owner Address: Alamat dompet pemilik (misal: 0xAb5...)
- Image Hash: Sidik jari file gambar
- Previous Hash: Pengunci yang menghubungkan dengan blok sebelumnya (membentuk rantai)

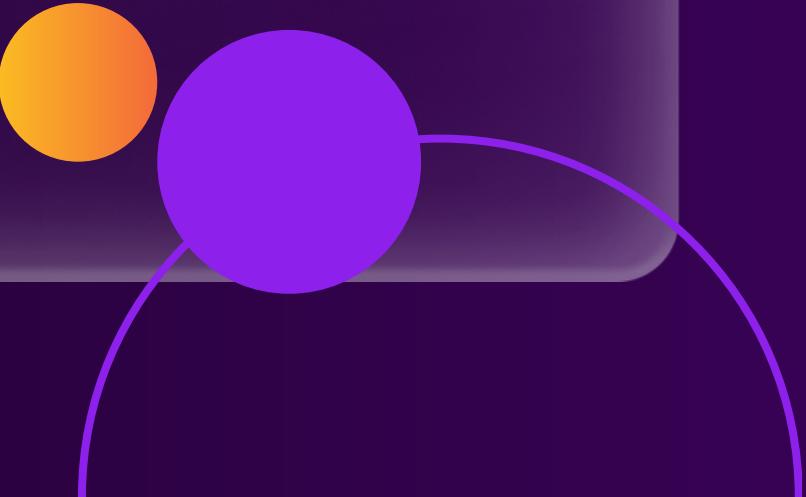
SIMULASI SMART CONTRACT

Menggunakan logika pemrograman (Javascript) untuk mencegah pendaftaran ganda terhadap Hash yang sama (Mencegah klaim hak cipta ganda)

BATASAN PROYEK

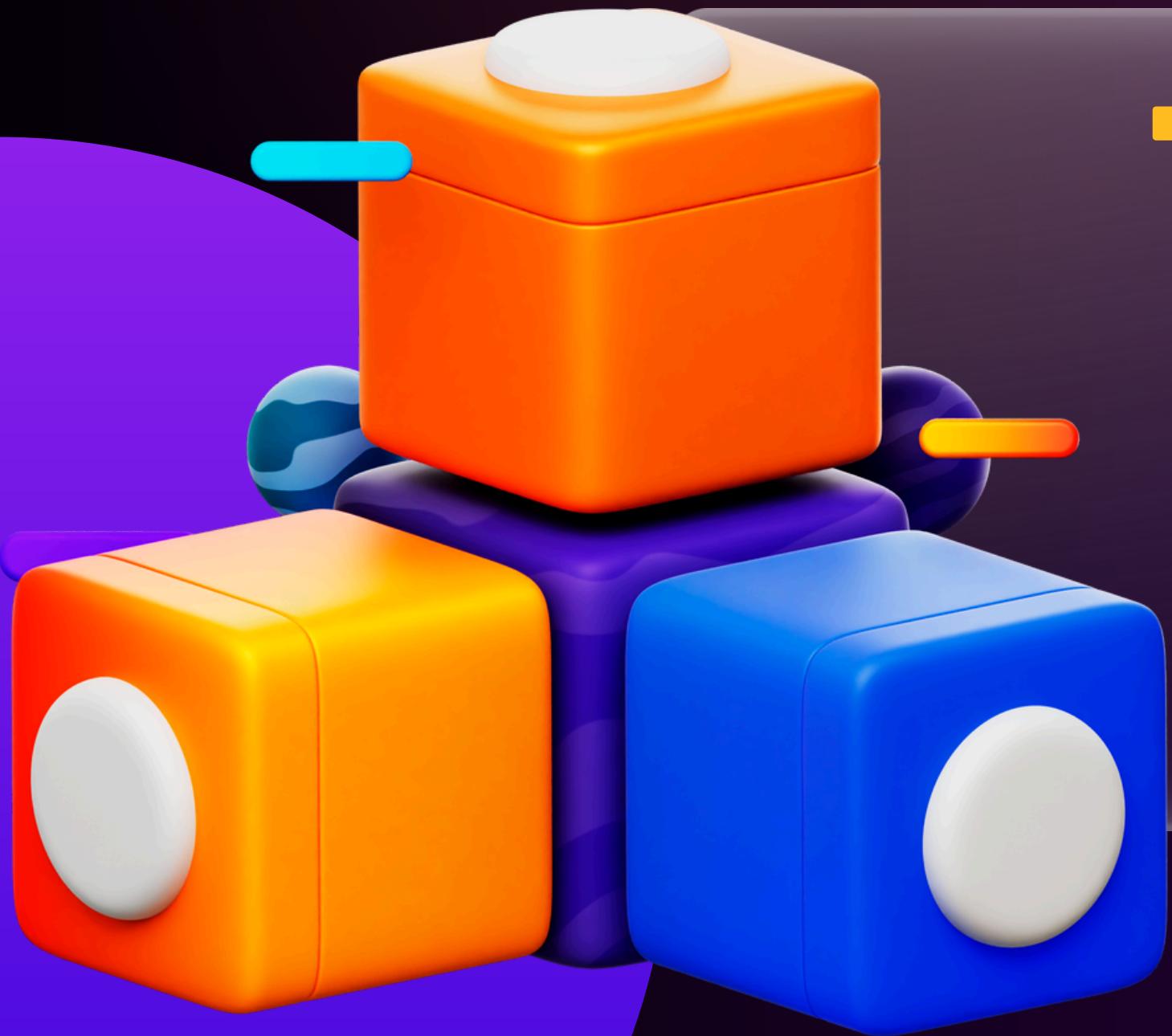
Karena ini adalah proyek simulasi (Proof of Concept), terdapat beberapa perbedaan dengan aplikasi Minnet (Production):

Fitur	Simulasi Ini	Aplikasi Nyata (Mainnet)
Penyimpanan Data	Browser LocalStorage (Lokal disatu perangkat)	Ribuan Node Jaringan Blockchain (Terdesentralisasi Global)
Biaya Transaksi	Gratis	Membutuhkan Gas Fee (ETH/MATIC)



KESIMPULAN

- Sistem simulasi ini berhasil mendemonstrasikan alur kerja pendaftaran hak cipta digital yang transparan
- Penggunaan SHA-256 terbukti efektif menjamin integritas file secara matematis
- Integritas dengan MetaMask memberikan pengalaman pengguna Web3 yang autentik dalam mengololan indentitas digital



TERIMA KASIH

SILAHKAN BERTANYA JIKA ADA HEHE...

