Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas Besar II (Tubes II) IF4020 Kriptografi Sem. I Tahun 2025/2026

Sistem Pencatatan Ijazah Digital Berbasis *Blockchain* atau *Centralized Immutable Ledger*

Batas pengumpulan	:	Minggu, 28 Desember 2025, Pukul 23.59 WIB
Tempat pengumpulan	:	Form Pengumpulan
Anggota kelompok	:	3 orang
QnA	:	Sheet QnA
Revisi 1 (10 Des)	:	Pembaruan *signature* menjadi URL/QR code ijazah dalam contoh ijazah
Revisi 2 (12 Des)	:	Penegasan format Ijazah boleh PDF, Image, ataupun Text (.txt)
Revisi 3 (14 Des)	:	Penegasan bahwa cukup ada 2 entitas saja, Admin Institusi dan Publik, hanya Admin Institusi yang wajib diimplementasikan dengan autentikasi
Revisi 4 (22 Des)	:	Perpanjangan deadline

Berkas pengumpulan :

a. **Tautan video demo** yang menjalankan program *step-by-step* mulai dari git clone, menginstal dependensi, hingga menjalankan fungsi-fungsi yang ada. Tunjukkan git log dan sebutkan (jalankan) bonus yang diimplementasi.
b. **Tautan kode program** dengan README minimal berisi daftar fungsi, cara menjalankan, dan pembagian tugas. Berikan juga daftar dependensi (*dependency management*) dalam sebuah file, seperti requirements.txt atau file lain yang serupa.

Latar Belakang

Maraknya kasus penggunaan ijazah palsu untuk karir pekerjaan menuntut tersedianya sistem pencatatan ijazah yang transparan. Teknologi blockchain dapat digunakan untuk masalah ini. Perguruan tinggi menerbitkan ijazah dalam bentuk dokumen digital. Ijazah ditandatangani oleh rektor menggunakan algoritma kriptografi kunci publik dan fungsi hash.

Penjelasan Implementasi

Pada tugas kali ini, mahasiswa diminta merancang dan mengimplementasikan prototipe sistem penerbitan, penyimpanan, dan verifikasi ijazah digital berbasis blockchain. Sistem harus menerapkan kombinasi kriptografi kunci publik + fungsi hash (untuk tanda tangan digital & verifikasi) dan kriptografi simetri (untuk enkripsi data sensitif di *off-chain storage*).

Dapat dipilih salah satu platform Ethereum, blockchain *centralized*/*decentralized* lain, atau blockchain yang dikembangkan sendiri. Dalam arsitektur ini, hanya metadata ijazah yang disimpan dalam blockchain. Informasi lengkap seperti nama mahasiswa, NIM, dan dokumen ijazah dalam bentuk PDF disimpan pada *off-chain storage* seperti IPFS, *cloud object storage*, atau penyimpanan dalam server lokal.

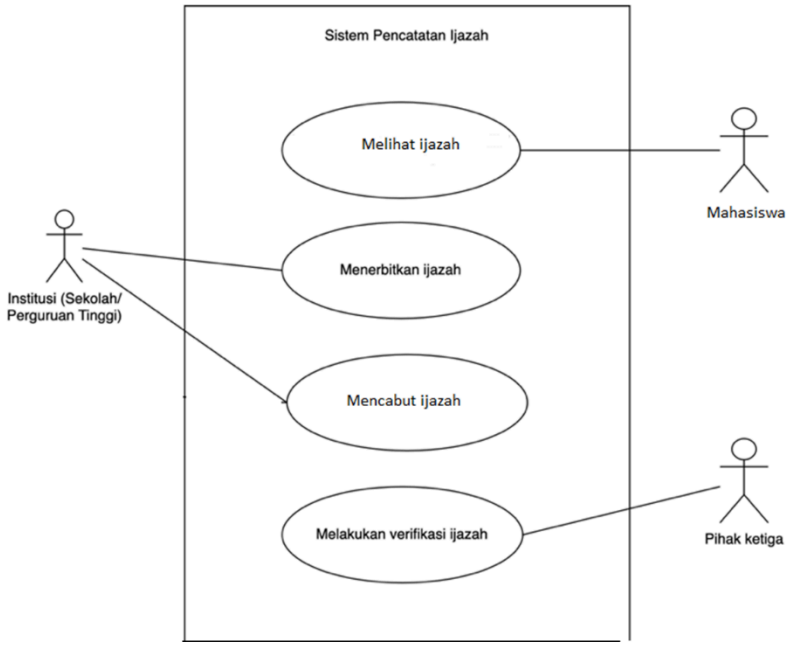
Pendekatan ini digunakan karena file PDF ijazah (ukuran 100-50kB) dinilai terlalu besar dan tidak efisien untuk disimpan secara *on-chain*. Penyimpanan *off-chain* akan menghemat biaya gas, yang meningkat seiring jumlah byte yang disimpan. Selain itu, pendekatan ini juga mempertahankan privasi dengan tidak mempublikasikan identitas mahasiswa pada *ledger* yang bersifat terbuka. Dengan pendekatan ini, verifikasi ijazah dapat dilakukan dengan memanfaatkan sifat transparansi dan *immutability* dari blockchain tanpa mengorbankan privasi mahasiswa.

Penandatanganan ijazah menggunakan algoritma ECDSA dan fungsi hash SHA. Ijazah digital disimpan dalam bentuk terenkripsi, menggunakan algoritma AES.

Pengguna sistem adalah

- Admin (kantor registrasi kampus): menerbitkan & mencabut ijazah.
- Publik: Verifier seperti (perusahaan / publik) yang memverifikasi keaslian ijazah atau Student yang dapat melihat ijazahnya sendiri
- ~~Student: melihat ijazah (menerima link ke ijazah digital).~~

Diagram berikut menjelaskan peran pengguna sistem:



Dalam sistem ini, terdapat dua jenis transaksi wajib:

1. **Penerbitan Ijazah (*Issue Certificate*)**

   Transaksi ini berfungsi untuk menambahkan entitas ijazah baru ke dalam sistem blockchain. Melalui transaksi ini, diperoleh ID tertentu untuk entitas ijazah baru. Data yang dicatat dalam transaksi antara lain adalah

   - hash dokumen ijazah (SHA-256),
   - CID IPFS atau URL file PDF ijazah yang disimpan di *off-chain storage*,
   - *issuer* atau alamat institusi penerbit,
   - tanda tangan digital (*signature*) dari *issuer*
   - *timestamp* waktu penerbitan.

2. **Pencabutan Ijazah (*Revoke Certification*)**

   Transaksi ini berfungsi untuk mengubah status ijazah dari “aktif” menjadi “dibatalkan”. Transaksi ini dilakukan ketika ijazah harus dicabut atau dinyatakan tidak sah. Data yang dicatat dalam transaksi ini adalah

   - ID ijazah yang dicabut,
   - alasan pencabutan,
   - tanda tangan dari *issuer*.

Ketentuan Spesifikasi

1. ***Blockchain* atau *Centralized Immutable Ledger***

   Gunakan ***Blockchain*** publik dengan kapabilitas publikasi *smart contract* seperti Ethereum, Solana, dan lainnya (cukup gunakan testnet atau devnet) dengan spesifikasi:

   - Gunakan *blockchain* publik yang memiliki kapabilitas publikasi *smart contract* dan memiliki platform *blockchain explorer* publik seperti Etherscan Sepolia (https://sepolia.etherscan.io/), Solscan Testnet (https://solscan.io/?cluster=testnet), dan lainnya
   - Buat website sebagai interfacenya
   - Gunakan dompet kripto sebagai metode autentikasi (gunakan metode signature nonce challenge, seperti tubes 1)
   - Buat page *upload* dan *revoke* ijazah untuk institusi
   - Sisipkan URL ke *blockchain explorer* di website untuk melihat daftar transaksi dari kontrak tersebut. Contoh: https://sepolia.etherscan.io/address/0x7b79995e5f793A07Bc00c21412e50Ecae098E7f9

   atau boleh juga membuat sendiri ***centralized immutable ledger*** sederhana dengan spesifikasi:

   - Buat website sebagai interfacenya
   - Autentikasi dapat menggunakan dompet kripto atau *input field private key* (gunakan metode signature nonce challenge, seperti tubes 1). *Public key issuer* boleh *hardcoded* di *software*.
   - Tidak perlu implementasi blok untuk mengumpulkan transaksi
   - Untuk hash transaksi pada ledger, lakukan *chaining hash function*, implementasi dibebaskan, namun tetap pastikan perubahan pada tx ke-n akan menginvalidasi tx ke-n + 1, contoh:

     Hash TX #1: hash(genesis tx constant, misal 0x000000 + metadata transaksi #1)

     Hash TX #2: hash(previous tx hash + metadata transaksi #2) dan seterusnya
   - Tidak perlu implementasi proof-of-work
   - Buat page *upload* dan *revoke* untuk *issuer*, dan daftar transaksi ledger untuk publik

- Pastikan transaksi yang terpublikasi tidak dapat diubah lagi

2. **Sertifikat Ijazah**
    - Hash yang disimpan di blockchain adalah hash ijazah yang belum ditandatangani
    - Ijazah yang belum ditandatangani disimpan di storage (IPFS, cloud block storage, atau storage lainnya) dalam keadaan terenkripsi oleh AES
    - Buat page *unlisted* agar mahasiswa dan publik dapat mengakses dan memverifikasi ijazah yang telah ditandatangani oleh *issuer*. URL ijazah mengandung URL dari file ijazah yang terinkripsi dengan AES, kunci AES nya, dan transaction hash di blockchain. Setelah mengunduh (dari storage), mendekripsi, dan memverifikasi ijazah, front-end menambahkan URL ijazah ke file ijazah tersebut yang selanjutnya dapat diunduh.
    - Ijazah boleh dalam bentuk **PDF**, **Image** ataupun **Text** (.txt)

Format ijazah kira-kira sebagai berikut:

Kementerian Pendidikan Tinggi, Sains, dan Teknologi

Institut Teknologi Bandung

dengan ini menyatakan bahwa

RIVALDO THAMRIN NASUTION

NIM 11223029

lahir di Sibolga, tanggal 17 Juli 2010, telah menyelesaikan dengan baik dan sudah memenuhi semua persyaratan pada Program Studi Teknik Sipil

Oleh sebab itu kepadanya diberikan gelar

SARJANA TEKNIK

beserta hak dan segala kewajiban yang melekat pada gelar tersebut. Diberikan di Bandung tanggal 26 Maret 2026

Rektor

[URL Ijazah dalam bentuk Teks / QR code]

Prof. Dr. Ir. Tatacipta Dirgantara, M.T.

NIP: 1243568790

BONUS

1. **Transaksi pembaruan Data**

   Transaksi ini memungkinkan institusi mengubah atau menambah informasi dalam sistem. memperbolehkan institusi memperbarui *public key* milik *issuer* maupun menambah *issuer* tambahan sebagai bagian dari mekanisme *multi-signature*.