

Spesifikasi Tugas Besar IF4035 Blockchain

Implementasi Aplikasi Berbasis Blockchain

Semester 1 Tahun 2025/2026

Tujuan

Tugas besar ini bertujuan agar mahasiswa dapat:

1. Mengembangkan kemampuan dalam mengimplementasikan aplikasi berbasis blockchain (dApps).
2. Melatih keterampilan dalam mendesain arsitektur aplikasi berbasis blockchain.

Learning Outcomes:

1. Mendesain dan mengimplementasikan sistem dApps yang berjalan di atas private blockchain.
2. Mengintegrasikan komponen on-chain dan off-chain secara aman.
3. Mengidentifikasi potensi celah keamanan dan menerapkan mitigasinya sesuai OWASP Smart Contract Top 10.

Requirement

Mahasiswa wajib mengajukan topik dApps pada file “Tubes Group.xlsx“ untuk disetujui dosen pengampu. Setelah disetujui, kelompok wajib membuat dApps dengan memenuhi persyaratan berikut:

1. Menentukan Platform Blockchain

Mahasiswa diperbolehkan memilih platform apapun yang sesuai dengan permasalahan yang diangkat, dengan implementasi dilakukan pada **private blockchain**. Platform yang direkomendasikan:

- Private Ethereum: <https://geth.ethereum.org/>
- Hyperledger Fabric: <https://hyperledger-fabric.readthedocs.io/en/release-2.5/>
- (Opsional) Quorum atau Polygon Edge untuk use case enterprise.

2. Membangun Frontend

Frontend dapat berupa web, mobile, atau desktop menggunakan framework/library (mis. React, Flutter, Electron) untuk mempermudah proses pengembangan antarmuka. Minimal harus:

- Menampilkan status transaksi dan hasil query blockchain.
- Memfasilitasi interaksi pengguna dengan smart contract.

3. Integrasi dengan Wallet

Aplikasi wajib terintegrasi dengan wallet sesuai platform (contoh: Metamask untuk Ethereum). Integrasi alternatif seperti WalletConnect diperbolehkan untuk mobile. Proses

integrasi ini harus dilakukan agar pengguna tidak mengalami kesulitan dalam melakukan berbagai transaksi yang berkaitan dengan blockchain.

4. Membangun Smart Contract

Smart contract harus:

- Mengimplementasikan proses bisnis dari aplikasi yang dibangun.
- Diperbolehkan menggunakan framework seperti Hardhat atau Truffle.
- Memperhatikan aspek keamanan berdasarkan OWASP Smart Contract Top 10.

Contoh: Dalam sistem voting, smart contract menangani pendaftaran pemilih, pencatatan suara, dan perhitungan hasil.

5. Offchain Information Gathering (Oracle)

Setiap dApps harus melibatkan **transaksi dengan data off-chain**. Gunakan oracle untuk mengambil data eksternal. Sebagai ilustrasi, Bob akan membeli sebuah properti kepada Alice dengan menggunakan smart contract. Untuk membeli properti ini, tentu akan melibatkan informasi perpajakan yang berlaku pada daerah tersebut. Oleh karena itu, Smart Contract perlu mengambil informasi ini dari eksternal. Hal ini dapat dicapai dengan menggunakan oracle.

- Framework dan bahasa pemrograman yang digunakan untuk mengimplementasikan oracle dibebaskan.
- Sebutkan API endpoint dan struktur data JSON di laporan.
- Implementasikan error handling (mis. fallback atau retry mechanism).
- Pertimbangkan serangan oracle manipulation (lihat <https://scsfg.io/hackers/oracle-manipulation/>).
- Contoh implementasi oracle: Medium - Implementing a Blockchain Oracle

6. Mengimplementasikan Token (Bonus)

- Fungible Token (ERC-20) atau Non-Fungible Token (ERC-721/ERC-1155).
- Gunakan OpenZeppelin: <https://docs.openzeppelin.com/contracts/4.x/>
- Nilai bonus maksimal: +10% dari nilai akhir.

7. Integrasi dengan IPFS (Bonus)

Anda dapat memanfaatkan IPFS untuk menyimpan file seperti gambar, video, atau file lainnya. Ingat bahwa IPFS bersifat publik dan dapat diakses oleh siapapun.

- Layanan yang disarankan: <https://web3.storage/>
- Perhatikan aspek keamanan dan privasi karena IPFS bersifat publik.

Deliverables

Mahasiswa wajib mengumpulkan:

1. Codebase

- Repository publik (GitHub/GitLab) dengan struktur:
`frontend/, smart-contract/, oracle/, docs/`.
- Sertakan: LICENSE, README.md, dan konfigurasi Hardhat/Truffle.
- README harus memuat:
 1. Deskripsi aplikasi
 2. System requirement untuk deployment dApps dan menjalankan private chain.
 3. Langkah menjalankan private chain
 4. Cara melakukan deployment smart contract pada private chain
 5. Cara melakukan deployment dan integrasi oracle
 6. Link/Snippet video demonstrasi cara menggunakan aplikasi

Catatan: Diperbolehkan untuk membuat script agar proses deployment menjadi lebih mudah

2. Video Demonstrasi (maks. 15 menit)

- Jelaskan use case dan fitur utama.
- Tampilkan interaksi pengguna, hasil transaksi, dan log di blockchain.
- Gunakan screen recording dengan audio penjelasan.

3. Video Presentasi (maks. 15 menit)

Selain video demonstrasi penggunaan aplikasi, setiap kelompok wajib membuat **video presentasi** yang menjelaskan keseluruhan proyek secara konseptual dan teknis. Video ini berfungsi untuk menilai pemahaman mahasiswa terhadap proses pengembangan dApps yang telah dilakukan.

Isi minimal video presentasi:

1. **Latar belakang dan pentingnya proyek** — jelaskan permasalahan yang diselesaikan dan relevansinya dengan blockchain.
2. **Requirement dan use case** — paparkan requirement awal, target pengguna, serta ilustrasi use case.
3. **Desain sistem dan arsitektur** — tunjukkan diagram arsitektur (frontend, smart contract, oracle, dan integrasi wallet).
4. **Penjelasan smart contract** — uraikan fungsi utama, variabel state, dan hubungan dengan proses bisnis.
5. **Implementasi oracle dan off-chain data** — jelaskan sumber data, mekanisme pengambilan, serta antisipasi kegagalan.
6. **Tech stack dan design pattern** — paparkan framework, bahasa, dan pattern yang digunakan beserta alasan pemilihannya.
7. **Kendala dan solusi teknis** — sebutkan tantangan yang dihadapi dan cara penyelesaiannya.
8. **Kesimpulan dan refleksi kelompok** — simpulkan hasil akhir, pembelajaran utama, dan rencana pengembangan lanjutan.

Ketentuan:

- Durasi maksimal: 15 menit.
- Format: bebas (screen recording, slide narration, atau kombinasi).
- Setiap anggota kelompok wajib muncul atau berbicara minimal satu bagian.

- Video diunggah ke platform publik (YouTube Unlisted atau Google Drive) dan tautannya dicantumkan dalam README serta Project Report.

Pertanyaan dan panduan tambahan:

Silakan merujuk ke dokumen berikut untuk daftar pertanyaan presentasi:

Blockchain Final Project QnA

4. Project Report (PDF)

Isi minimal:

1. Problem statement dan use case. Anda dapat melengkapi bagian ini dengan use case diagram.
2. Pemilihan platform blockchain dan justifikasinya
3. Tech stack yang digunakan untuk membangun dApps dan alasan pemilihan
4. High-level design terkait interaksi antar komponen yang terlibat dalam dApps. Berikan penjelasan terkait peran komponen pada aplikasi anda.
5. Properti dan method yang ada pada smart contract. Anda dapat menggambarkannya dengan menggunakan Class diagram
6. Penjelasan terkait dengan implementasi *Oracle* dan integrasinya dengan *smart contract*. Lengkapi penjelasan Anda dengan informasi berikut:
 - i. Deskripsi dan struktur data yang diambil.
 - ii. Mekanisme pengambilan data dari API eksternal serta integrasinya dengan *smart contract*. Anda dapat menggambarkannya dengan menggunakan *sequence diagram*.
 - iii. Jelaskan terkait dengan skenario buruk yang mungkin terjadi pada saat pengambilan data eksternal dengan mekanisme yang Anda pilih. Berikan juga solusi yang Anda implementasikan untuk mengatasi hal tersebut.
7. Design pattern yang anda gunakan dalam mengimplementasikan smart contract dan oracle. Jelaskan alasan anda menggunakan pattern tersebut
8. Implementasi oracle dan sequence diagram
9. Antisipasi skenario buruk (mis. API gagal, oracle delay)
10. Design pattern dan alasan penggunaan
11. Optimasi smart contract (jika ada)
12. Daftar anggota dan pembagian tugas
13. Refleksi akhir kelompok: kendala dan pembelajaran
14. Daftar referensi

4. Report Akhir dalam Format IEEE (Paper)

Selain Project Report dalam format PDF, setiap kelompok diwajibkan untuk menyusun versi **paper ilmiah** dengan format IEEE. Paper ini bertujuan untuk melatih mahasiswa menulis laporan penelitian terstruktur dan dapat dikembangkan menjadi publikasi ilmiah di masa depan.

Format dan Template:

- Gunakan template resmi IEEE Conference (2 kolom), tersedia di: <https://www.ieee.org/conferences/publishing/templates.html>
- Panjang paper maksimal 6 halaman (tidak termasuk referensi).
- Format file akhir: PDF dan .tex (beserta semua sumber gambar/diagram).

Struktur Paper (mengikuti format IEEE):

- a. **Abstract** – Ringkasan singkat (maks. 200 kata) yang mencakup tujuan, metode, dan hasil utama proyek.
- b. **Keywords** – 3–5 kata kunci terkait blockchain, smart contract, oracle, dan dApps.
- c. **Introduction** – Jelaskan latar belakang masalah, motivasi penggunaan blockchain, serta gap yang diselesaikan oleh proyek.
- d. **Related Work** – Paparkan karya atau sistem sejenis yang relevan dan tunjukkan perbedaan atau keunggulan proyek Anda.
- e. **Methodology / System Design** – Sajikan arsitektur sistem, komponen utama (frontend, smart contract, oracle, wallet integration), serta diagram pendukung.
- f. **Implementation and Evaluation** – Jelaskan implementasi teknis, hasil uji coba, serta analisis performa atau keamanan sistem.
- g. **Discussion** – Bahas tantangan, solusi teknis, serta keterbatasan proyek.
- h. **Conclusion and Future Work** – Simpulkan hasil, kontribusi utama, dan arah pengembangan selanjutnya.
- i. **References** – Gunakan gaya citasi IEEE (mis. `bibliographystyle{IEEEtran}`). Minimal 5 referensi akademik (buku, jurnal, atau konferensi).

Catatan Penting:

- Gunakan bahasa ilmiah dan objektif.
- Setiap gambar atau tabel wajib diberi keterangan dan dirujuk dalam teks.
- Paper wajib mencantumkan daftar anggota dan afiliasi (contoh: *School of Electrical Engineering and Informatics, Institut Teknologi Bandung*).
- Paper dikumpulkan bersamaan dengan Project Report dan Video Presentasi.

Penilaian

Penilaian dilakukan berdasarkan aspek desain, implementasi teknis, dokumentasi, serta kemampuan presentasi dan komunikasi ilmiah. Setiap kelompok akan dinilai secara menyeluruh dengan bobot sebagai berikut:

Aspek	Bobot	Kriteria
Ketepatan desain dApps	20%	Arsitektur sesuai problem dan platform
Implementasi Smart Contract	20%	Fungsional, aman, efisien, teruji
Integrasi Offchain dan Oracle	15%	API eksternal berfungsi dan error-handling baik
Frontend dan Wallet Integration	10%	Interaktif, sinkron dengan blockchain dan wallet
Project Report (PDF)	10%	Lengkap, jelas, sesuai struktur laporan
Video Demonstrasi	5%	Menampilkan seluruh fitur utama aplikasi
Video Presentasi	10%	Menjelaskan latar belakang, desain, implementasi, kendala, dan refleksi tim
Report Akhir Format IEEE	10%	Mengikuti struktur IEEE dan berisi analisis ilmiah
Total Nilai Utama	100%	—
Bonus (Opsional)	+10% maksimal	Token, IPFS, optimasi gas/keamanan, atau deployment otomatis

Keterangan Tambahan:

- Nilai bonus hanya berlaku jika seluruh deliverables utama telah terpenuhi.
- Plagiarisme kode atau laporan akan mengakibatkan pembatalan nilai tugas besar.
- Penilaian individu dalam kelompok dapat dilakukan berdasarkan kontribusi (misalnya dari log commit, pembagian tugas, atau bagian presentasi).

Batas Waktu

- Pengumpulan: **30 Desember 2025 pukul 23.59 (inklusif)**.
- Format pengumpulan: link repository GitHub dan link video demonstrasi.