BAB V
SIMPULAN DAN SARAN

5.1. Simpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan pada proyek "Impelementasi Teknologi *Blockchain* Dalama Penerbitan dan Verifikasi Keaslian *E-Certificate* Berbasis *Website*," dapat ditarik beberapa kesimpulan utama:

1. Implementasi serta integrasi teknologi *blockchain* dengan Web3 dalam penerbitan sertifikat elektronik (*e-certificate*) mampu mewujudkan mekanisme distribusi dan verifikasi sertifikat yang bersifat aman, transparan, dan terdesentralisasi. Penerapan *smart contract* memberikan kepastian terhadap validitas serta integritas data sertifikat, sedangkan penggunaan Web3 berfungsi sebagai penghubung antara aplikasi dengan jaringan blockchain sehingga proses penerbitan dan verifikasi dapat dilakukan secara efisien dan terpercaya.
2. Hasil evaluasi terhadap aspek keamanan, keandalan, dan transparansi menunjukkan bahwa penerapan *smart contract* dan pemanfaatan penyimpanan terdistribusi berbasis *blockchain*, seperti IPFS, mampu memberikan jaminan keaslian sertifikat dengan pengujian korelasi pearson yang di mana pengujian tersebut menyebutkan bahwa antara input dan hash tidak ada korelasi sama sekali, mencegah potensi manipulasi data, serta meningkatkan tingkat kepercayaan pengguna. Dengan demikian, sistem e-certificate berbasis blockchain dapat menjadi solusi efektif untuk mengatasi permasalahan pemalsuan dan meningkatkan akuntabilitas dalam proses sertifikasi digital.

5.2. Saran

Berdasarkan hasil penelitian dan kesimpulan yang telah diperoleh, berikut adalah beberapa saran yang dapat dijadikan masukan untuk pengembangan sistem CertiChain di masa depan:

1. Untuk meningkatkan fleksibilitas, sistem dapat dilengkapi dengan fitur desain sertifikat yang dinamis. Fitur ini akan memungkinkan User/Organisasi untuk mengunggah *template* sertifikat mereka sendiri dan menyesuaikan elemen-elemen seperti logo, warna, dan tata letak secara mandiri. Hal ini akan membuat platform lebih profesional dan dapat digunakan oleh berbagai institusi dengan identitas visual yang berbeda.
2. Sistem dapat diperkuat dengan menerapkan mekanisme notifikasi otomatis (misalnya melalui email atau notifikasi *on-chain*) kepada User/Organisasi dan penerima sertifikat. Notifikasi ini dapat berisi informasi penting seperti status persetujuan, konfirmasi penerbitan sertifikat, atau tautan verifikasi.
3. Perlu dilakukan pengujian keamanan lanjutan, seperti *brute force attack* terhadap kode unik atau *stress testing* terhadap *smart contract*, untuk memastikan ketahanan sistem terhadap serangan siber dan penggunaan dalam skala besar. Pengujian ini akan membantu mengidentifikasi dan memperbaiki potensi kerentanan, sehingga meningkatkan integritas dan kepercayaan terhadap sistem.