# BAB V
# PENUTUP

## 5.1 Kesimpulan

Berdasarkan analisis 27 studi literatur, penelitian ini menyoroti tujuh prinsip fundamental yang menjadikan teknologi blockchain sebagai solusi keamanan inovatif dalam perlindungan data dan transaksi digital. Pertama, desentralisasi menghilangkan ketergantungan pada otoritas sentral, mengurangi risiko *single-point failure* dan meningkatkan ketahanan sistem terhadap serangan terpusat atau manipulasi. Kedua, kriptografi berperan sebagai tulang punggung keamanan melalui penerapan fungsi hash, tanda tangan digital, dan sistem kunci publik-privat yang menjamin autentisitas, kerahasiaan, dan integritas data. Ketiga, imutabilitas memastikan data yang tercatat dalam *ledger* bersifat permanen, sehingga melindungi catatan kritis seperti transaksi keuangan dan dokumen KYC dari upaya pemalsuan atau penghapusan.

Prinsip keempat, mekanisme konsensus (seperti *Proof-of-Work* dan *Proof-of-Stake*) memungkinkan validasi transaksi secara kolektif oleh seluruh jaringan tanpa melibatkan pihak ketiga, memperkuat kepercayaan dalam sistem. Kelima, transparansi dan auditabilitas memfasilitasi verifikasi publik terhadap seluruh riwayat transaksi tanpa mengungkap identitas pengguna, berkat enkripsi asimetris yang canggih. Keenam, integritas data terjaga melalui struktur blockchain yang saling terhubung dengan fungsi hash. Setiap perubahan pada satu blok akan mengganggu keseluruhan rantai, membuat manipulasi data secara tersembunyi menjadi mustahil. Terakhir, blockchain menunjukkan ketahanan tinggi terhadap ancaman siber seperti *Denial-of-Service (DoS)* melalui kombinasi arsitektur desentralisasi, penggunaan hash unik, dan lapisan enkripsi multi-level.

Secara holistik, prinsip-prinsip ini tidak hanya mengatasi kelemahan sistem terpusat konvensional tetapi juga menetapkan standar baru dalam keamanan digital. Dengan demikian, blockchain terbukti sebagai teknologi yang andal, revolusioner, dan adaptif untuk meningkatkan perlindungan data serta transaksi di berbagai sektor, mulai dari keuangan hingga manajemen rantai pasok.

## 5.2 Saran

Berdasarkan hasil penelitian mengenai prinsip dasar keamanan dalam blockchain, terdapat beberapa rekomendasi yang dapat dipertimbangkan untuk meningkatkan efektivitas dan implementasi teknologi ini:

1. **Inovasi Protokol Konsensus Berkelanjutan**

   Meskipun mekanisme konsensus seperti *Proof-of-Work (PoW)* dan *Proof-of-Stake (PoS)* telah terbukti efektif, perlu dilakukan eksplorasi mendalam terhadap metode yang lebih hemat energi dan berkelanjutan. Pendekatan hibrid (gabungan algoritma) atau integrasi kecerdasan buatan dapat dijadikan alternatif untuk meningkatkan efisiensi energi dan skalabilitas jaringan tanpa mengorbankan keamanan sistem.

2. **Optimalisasi Skalabilitas dengan Prinsip Desentralisasi**

   Untuk mengatasi hambatan skalabilitas, diperlukan eksplorasi teknologi pendukung seperti *Layer-2 solutions* (misalnya *rollups*) dan *sharding*. Implementasi ini harus tetap mempertahankan prinsip desentralisasi sebagai inti keamanan blockchain serta memastikan integritas data dalam jaringan terdistribusi.

3. **Antisipasi Ancaman Teknologi Kuantum pada Kriptografi**

   Kemajuan komputasi kuantum berpotensi mengganggu sistem enkripsi konvensional. Oleh karena itu, penelitian terkait algoritma kriptografi pasca-kuantum (*post-quantum cryptography*) perlu diprioritaskan. Pengembang blockchain dan lembaga riset disarankan berkolaborasi dalam merancang sistem enkripsi yang tahan terhadap ancaman komputasi masa depan.

4. **Penerapan Regulasi dan Standarisasi Internasional**

   Interoperabilitas dan keamanan blockchain memerlukan kerangka regulasi yang terintegrasi di tingkat internasional. Pemerintah, akademisi, dan pelaku industri perlu memperkuat kolaborasi untuk merumuskan kebijakan yang mendukung inovasi teknologi sekaligus menjamin perlindungan data dan kepatuhan hukum.

5. **Peningkatan Literasi Teknologi bagi Pengguna**

   Rendahnya pemahaman pengguna terhadap mekanisme blockchain meningkatkan risiko kesalahan operasional dan kerentanan terhadap serangan *social engineering*. Solusinya, diperlukan program edukasi berbasis praktik, seperti pelatihan dan workshop, untuk meningkatkan kesadaran keamanan di kalangan pengguna korporasi maupun individu.

6. **Implementasi Terarah pada Sektor Prioritas**

   Penelitian lanjutan disarankan fokus pada integrasi blockchain di sektor strategis, seperti layanan kesehatan, keuangan digital, logistik, dan pemerintahan. Pengembangan kasus penggunaan yang mengadaptasi prinsip keamanan blockchain sesuai dengan kebutuhan industri dapat mempercepat adopsi teknologi ini secara luas.

7. **Mitigasi Proaktif Risiko Keamanan Siber**

   Walaupun blockchain memiliki ketahanan terhadap serangan terpusat, beberapa risiko seperti celah keamanan pada smart contract dan serangan 51% masih menjadi perhatian. Oleh karena itu, diperlukan pengujian keamanan yang ketat serta pengembangan smart contract yang lebih andal untuk meminimalkan potensi eksploitasi.