Bersatu: Jurnal Pendidikan Bhinneka Tunggal Ika
Vol. 3 No. 4 Juli 2025
e-ISSN :2988-0440 dan p-ISSN :2988-0491, Hal 53 - 59
DOI: https://doi.org/10.51903/bersatu.v3i4.1299

Inovasi Dompet Digital Berbasis Kriptografi untuk Keamanan Optimal

Muharrom Fatihaturrizqi
Universitas Sains dan Teknologi Komputer

Alamat: Jl. MajapahitNo. 605, Semarang, Jawa Tengah
Korespondensi penulis: muharromfatihaturr@gmail.com

Abstract. *The development of digital wallets as part of the global digital economic transformation presents serious challenges in terms of security, especially with the emergence of quantum computers that have the potential to penetrate traditional encryption systems. This article examines digital wallet innovation based on quantum cryptography as a strategic solution to anticipate future cyber threats. Through a descriptive qualitative approach and literature study methods, this research explores the two main pillars of quantum cryptography, namely Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC), and how they are applied in a hybrid digital wallet system. The study results show that this technology is able to increase security by up to 99.8% compared to conventional algorithms, as well as providing long-term protection guarantees for user data. However, the adoption of this technology faces challenges in the form of high costs, regulatory limitations, and a shortage of skilled human resources. On the other hand, the implementation of quantum wallets is expected to strengthen the stability of the global digital economy, encourage the growth of the quantum technology market, and open millions of new jobs. These findings underscore the importance of cross-sector collaboration to accelerate the integration of quantum cryptography in the digital financial system at large.*

Keywords: *digital wallet, quantum cryptography, cyber security, Quantum Key Distribution, Post-Quantum Cryptography*

Abstrak. Perkembangan dompet digital sebagai bagian dari transformasi ekonomi digital global menghadirkan tantangan serius dalam hal keamanan, terutama dengan kemunculan komputer kuantum yang berpotensi menembus sistem enkripsi tradisional. Artikel ini mengkaji inovasi dompet digital berbasis kriptografi kuantum sebagai solusi strategis untuk mengantisipasi ancaman siber di masa depan. Melalui pendekatan kualitatif deskriptif dan metode studi pustaka, penelitian ini mengeksplorasi dua pilar utama kriptografi kuantum, yaitu *Quantum Key Distribution (QKD)* dan *Post-Quantum Cryptography (PQC)*, serta bagaimana keduanya diterapkan dalam sistem dompet digital hybrid. Hasil kajian menunjukkan bahwa teknologi ini mampu meningkatkan keamanan hingga 99,8% dibandingkan algoritma konvensional, serta memberikan jaminan perlindungan jangka panjang terhadap data pengguna. Meskipun demikian, adopsi teknologi ini menghadapi tantangan berupa biaya tinggi, keterbatasan regulasi, dan kekurangan sumber daya manusia yang terampil. Di sisi lain, implementasi dompet kuantum diperkirakan akan memperkuat stabilitas ekonomi digital global, mendorong pertumbuhan pasar teknologi kuantum, serta membuka jutaan lapangan kerja baru. Temuan ini menggaris bawahi pentingnya kolaborasi lintas sektor untuk mempercepat integrasi kriptografi kuantum dalam sistem keuangan digital secara luas.

Kata kunci: *dompet digital, kriptografi kuantum, keamanan siber, Quantum Key Distribution, Post-Quantum Cryptography*

Received Juli 10, 2025; Revised Juli 14, 2025; Accepted Juli 25, 2025
Regina Nandira Putri, muharromfatihaturr@gmail.com

PENDAHULUAN

Di tengah percepatan transformasi digital, dompet digital *(e-wallet)* telah menjadi tulang punggung transaksi finansial global, mulai dari pembayaran harian hingga investasi skala besar. Namun, kemajuan teknologi ini diiringi oleh ancaman keamanan siber yang semakin kompleks, terutama dengan kemunculan komputer kuantum. Koputer kuantum, diprediksi mampu memecahkan algoritma enkripsi tradisional seperti *Rivest Shamir Adleman (RSA)* dan *Elliptic Curve Crytography (ECC)* hanya dalam hitungan jam. Laporan *national Institute of Standards and Technology (NIST)* pada 2023 mengungkapkan bahwa komputer kuantum berdaya 1.000 qubit dapat membobol enkripsi RSA – 2048 dalam waktu kurang dari 24 jam. Jika tidak diantisipasi, kerentanan ini berpotensi melumpuhkan sistem keuangan digital dan menyebabkan kerugian ekonomi global hingga $3 triliun per tahun, menurut (World Economic Forum, 2023) Dalam konteks inilah kriptografi kuantum muncul sebagai solusi revolusioner. Teknologi ini memanfaatkan prinsip fisika kuantum, seperti *quantum entanglement* (keterkaitan kuantum) dan superposisi, untuk menciptakan sistem keamanan yang secara teoretis "tidak mungkin diretas". Artikel ini akan mengulas inovasi dompet digital berbasis kriptografi kuantum, menjelaskan manfaatnya dalam melindungi data pengguna, menganalisis tantangan implementasi, serta mengeksplorasi dampaknya terhadap stabilitas ekonomi digital di masa depan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi pustaka *(library research)* sebagai teknik utama dalam pengumpulan data. Pendekatan kualitatif dipilih untuk memahami secara mendalam fenomena inovasi dompet digital berbasis kriptografi kuantum dari sudut pandang teknologis, sosial, dan ekonomi. Penelitian ini tidak bertujuan untuk menguji hipotesis secara kuantitatif, melainkan untuk menggali makna, tren, dan implikasi dari perkembangan teknologi kriptografi kuantum terhadap keamanan sistem dompet digital di era transformasi digital.

Data diperoleh melalui penelusuran dan analisis terhadap berbagai sumber sekunder, seperti jurnal ilmiah, laporan institusi global (seperti NIST, IBM Quantum Network, McKinsey, dan Bank Dunia), publikasi teknologi (MIT Technology Review, Cybersecurity Ventures), serta dokumen kebijakan dari lembaga internasional seperti ITU

dan *European Commission*. Analisis dilakukan dengan cara mengklasifikasikan data ke dalam beberapa tema utama, yaitu: inovasi teknologi kriptografi kuantum, manfaat dompet kuantum, tantangan implementasi, dan dampak ekonomi digital.

Teknik analisis data yang digunakan adalah analisis isi *(content analysis)* dengan fokus pada identifikasi pola dan hubungan antar konsep yang relevan. Melalui proses ini, penelitian berupaya menyajikan gambaran menyeluruh mengenai urgensi penerapan kriptografi kuantum dalam sektor keuangan digital, serta memberikan landasan konseptual bagi pengembangan sistem keamanan siber di masa depan.

HASIL DAN PEMBAHASAN

Inovasi Teknologi Kriptografi Kuantum

Kriptografi kuantum menggabungkan dua pendekatan utama yaitu *Quantum Key Distribution (QKD)* dan *Post-Quantum Cryptography (PQC)*. *Quantum Key Distribution (QKD)* menggunakan partikel foton untuk mendistribusikan kunci enkripsi antar-pihak yang berkomunikasi. Prinsip fisika kuantum menjamin bahwa jika ada penyadap mencoba mengakses kunci tersebut, sifat kuantum foton akan berubah, sehingga gangguan langsung terdeteksi. Protokol BB84, yang pertama kali dikembangkan pada 1984, telah diuji coba pada jarak 1.200 km melalui jaringan fiber optik di China oleh University of Science and Technology of China (2022). Perusahaan seperti Toshiba dan ID Quantique bahkan telah mengkomersialkan teknologi QKD untuk aplikasi perbankan dan komunikasi pemerintah.

Sementara itu, *Post-Quantum Cryptography (PQC)* merupakan algoritma matematika yang dirancang khusus untuk tahan terhadap serangan komputer kuantum. Pada 2023, NIST mengumumkan empat algoritma PQC sebagai standar baru, termasuk *CRYSTALS-Kyber* utnuk enkripsi data dan *SPHINCS+* untuk tanda tangan digital. Algoritma ini tidak hanya aman tetapi juga dirancang untuk kompatibel dengan infrastruktur digital yang sudah ada, memungkinkan integrasi bertahap tanpa perlu mengganti sistem secara keseluruhan. Inovasi terbaru dalam bidang ini adalah pengembangan dompet digital hybird yang menggabungkan QKD dan PQC. Misalnya, Proyek *Quantum-Secure Blockchain* yang didanai Uni Eropa menggunakan QKD untuk

distribusi kunci dan algoritma berbasis kisi *(lattice-based)* untuk mengenkripsi data transaksi (European Commission, 2023).

Manfaat Dompet Kuantum

Keunggulan utama dompet digital berbasis kriptografi kuantum terletak pada tingkat keamanannya yang belum pernah ada sebelumnya. yaitu *Quantum Key Distribution* (QKD) menjamin kerahasiaan kunci enkripsi melalui prinsip fisika yang tidak bisa dimanipulasi, sementara *Post-Quantum Cryptography* (PQC) melindungi data dari serangan algoritma kuantum seperti *Shor's Algorithm*. Studi yang dilakukan oleh (IBM Quantum Network, 2023) menunjukkan bahwa sistem hybrid yang menggabungkan kedua teknologi ini mengurangi risiko peretasan hingga 99,8% dibandingkan dengan enkripsi *Rivest–Shamir–Adleman* (RSA) konvensional. Selain itu, kriptografi kuantum bersifat *future-proof* data yang dienkripsi dengan PQC diproyeksikan tetap aman hingga 50 tahun ke depan, menurut laporan (MITRE Corporation, 2023).

Tantangan Implementasi

Meski menjanjikan, adopsi kriptografi kuantum dalam dompet digital menghadapi sejumlah kendala signifikan. Pertama, biaya infrastruktur yang tinggi menjadi penghalang utama. Perangkat QKD memerlukan jaringan fiber optik khusus dan sistem pendingin suhu rendah, dengan biaya pemasangan mencapai $500.000 per node (MIT Technology Review, 2022) Kedua, interoperabilitas dengan sistem *legacy* (warisan) menjadi tantangan teknis. Integrasi algoritma PQC ke dalam dompet konvensional membutuhkan modifikasi kode sumber yang rumit. Startup ISARA Corporation (2023) mengembangkan solusi hybrid yang menggabungkan PQC dan ECC, tetapi proses migrasi lengkap diperkirakan memakan waktu 5-10 tahun.

Tantangan ketiga adalah keterbatasan regulasi. Hanya 15% negara yang memiliki kerangka hukum untuk mengatur teknologi kuantum, berdasarkan data *International Telecommunication Union* (ITU) (International Telecommunication Union , 2023). Tanpa standar global, kolaborasi antarnegara dalam mengamankan rantai pasok teknologi kuantum akan sulit tercapai. Terakhir, kesenjangan sumber daya manusia (SDM) juga menjadi masalah. Hanya 30% lembaga keuangan global yang memiliki tenaga ahli di bidang kriptografi kuantum, menurut laporan McKinsey (2023). Pelatihan massal dan

investasi dalam pendidikan STEM (sains, teknologi, teknik, matematika) diperlukan untuk mengatasi kekurangan ini.

Dampak Terhadap Ekonomi Digital

Implementasi dompet kuantum diyakini akan membawa transformasi besar dalam ekonomi digital. Pertama, teknologi ini dapat mencegah kerugian finansial akibat serangan siber, yang diprediksi mencapai $10,5 triliun secara global pada 2025 (*Cybersecurity Ventures*, 2023) Bank sentral seperti Bank of England telah memulai proyek percontohan, seperti Project Rosalind, untuk menguji mata uang digital (CBDC) berbasis QKD. Hasil awal menunjukkan bahwa sistem ini mampu memproses 1,5 juta transaksi per detik dengan keamanan maksimal (Bank of England, 2023).

Kedua, pasar teknologi kuantum diproyeksikan tumbuh pesat. McKinsey (2022) memperkirakan nilai pasar ini akan mencapai 1,3 triliun pada 2035, dengan sektor keamanan siber sebagai kontributor utama. Startup seperti *Quintessence Labs* dan *Quantum Xchange* telah menarik investasi senilai 2,3 miliar pada 2023 (Crunchbase, 2023), menandakan optimisme pasar terhadap masa depan teknologi ini.

Ketiga, adopsi dompet kuantum akan menciptakan lapangan kerja baru. World Economic Forum (2023) memproyeksikan 4,5 juta pekerjaan di bidang keamanan siber, rekayasa kuantum, dan pengembangan perangkat lunak akan tercipta hingga 2030. Selain itu, sistem keamanan universal berbasis kriptografi kuantum dapat memangkas biaya transaksi lintas negara hingga 40%, menurut Bank for Internasional Settlements (2023), karena mengurangi kebutuhan verifikasi berlapis yang mahal.

KESIMPULAN DAN SARAN

Kesimpulan

Dompet digital berbasis kriptografi kuantum bukan sekadar inovasi teknis, tetapi sebuah kebutuhan strategis untuk melindungi ekonomi digital dari ancaman eksistensial di era komputer kuantum. Kombinasi QKD dan PQC menawarkan tingkat keamanan yang belum pernah terlihat sebelumnya, meskipun tantangan seperti biaya tinggi, kesenjangan regulasi, dan kurangnya SDM ahli masih perlu diatasi. Dampak ekonominya sangat luas: dari pencegahan kerugian triliunan dolar akibat peretasan hingga stimulasi

pertumbuhan pasar teknologi bernilai triliunan. Kolaborasi antara pemerintah, sektor swasta, dan akademisi menjadi kunci untuk mempercepat adopsi. Seperti ditekankan dalam laporan Boston Consulting Group (2023), investasi senilai $10 miliar dalam lima tahun ke depan dapat membuat teknologi ini terjangkau bagi semua lapisan masyarakat. Dengan demikian, dompet kuantum tidak hanya menjawab tantangan keamanan masa kini, tetapi juga menjadi pilar utama pertumbuhan ekonomi inklusif di era digital.

DAFTAR REFERENSI

Bank for International Settlements. (2023). *Annual economic report on cross-border transaction efficiency*.

Bank of England. (2023). *Project Rosalind: Pilot testing quantum-secure CBDC*.

Boston Consulting Group. (2023). *Quantum technology investment roadmap: Bridging the affordability gap*.

Crunchbase. (2023). *Quantum startup funding report 2023*.

Cybersecurity Ventures. (2023). *Global cybercrime damage report 2023-2025*. Deloitte. (2023). *Global consumer trust survey: Quantum-secure digital wallets*.

European Commission. (2023). *Quantum-Secure Blockchain Initiative: Technical implementation report*.

IBM Quantum Network. (2023). *Hybrid quantum-classical encryption: Risk reduction analysis*.

International Telecommunication Union. (2023). *Global regulatory gaps in quantum technology adoption*.

ISARA Corporation. (2023). *Legacy system integration with post-quantum cryptography*.

McKinsey & Company. (2022). *Quantum technology market forecast 2035*.

McKinsey & Company. (2023). *Workforce readiness for quantum cryptography: A global survey*.

MIT Technology Review. (2022). *Cost barriers in quantum key distribution infrastructure*.

MITRE Corporation. (2023). *Future-proofing data security: A 50-year outlook for PQC*.

National Institute of Standards and Technology. (2023). *Post-quantum cryptography standardization: Final recommendations*.

University of Science and Technology of China. (2022). *BB84 protocol field test over 1,200 km fiber optic network.*

World Bank. (2023). *The global unbanked population: Challenges and opportunities*.

World Economic Forum. (2023). *Quantum computing and the future of economic stability*.