SCBX QUANTUM OUTLOOK 2026:
The Unfiltered Truth of Quantum

SPECIAL EDITION
NOVEMBER 2026





คำนำ (Foreword)

เรากำลังยืนอยู่ ณ จุดเริ่มต้นของยุคใหม่แห่งการประมวลผล ตลอดหลายทศวรรษที่ผ่านมา เศรษฐกิจโลกถูกขับเคลื่อนด้วยความก้าวหน้าอย่างต่อเนื่องของการประมวลผลแบบคลาสสิก (Classical Computing) และในระยะหลังคือการเติบโตอย่างก้าวกระโดดของปัญญาประดิษฐ์ (Artificial Intelligence) ทว่าเมื่อความท้าทายในภาคการเงิน โลจิสติกส์ และการค้นพบทางวิทยาศาสตร์ทวีความซับซ้อนยิ่งขึ้น ปัญหาบางส่วนเหล่านี้ก็กำลังเติบโตเกินกว่าที่คอมพิวเตอร์แบบคลาสสิก (Classical Computer) ที่ทรงพลังที่สุดจะรับมือได้ในทางปฏิบัติ

การประมวลผลเชิงควอนตัม (Quantum Computing) ไม่ใช่เพียงการอัปเกรด หากแต่เป็นการเปลี่ยนกระบวนทัศน์ขั้นพื้นฐาน (Fundamental paradigm shift) คำถามไม่ใช่อีกต่อไปว่า Quantum Computing ที่ขยายสเกลได้จะเกิดขึ้นจริง “หรือไม่” แต่เป็น “เมื่อใด” — และใครจะเป็นผู้ที่เตรียมพร้อมสำหรับการใช้ประโยชน์จากศักยภาพของมัน

ไม่ว่าท่านจะเป็นผู้นำองค์กรที่แสวงหาความได้เปรียบในการแข่งขัน นักลงทุนที่กำลังประเมินภูมิทัศน์ของเทคโนโลยีนี้ หรือผู้ที่ใฝ่รู้และต้องการเข้าใจอนาคตของเทคโนโลยี รายงานฉบับนี้ได้รับการออกแบบมาเพื่อมอบความชัดเจนที่จำเป็นต่อการเปลี่ยนผ่านจาก “ความสนใจใคร่รู้ในควอนตัม” (Quantum curiosity) ไปสู่ “ความพร้อมด้านควอนตัม” (Quantum readiness)

สารบัญ (Table of Contents)

CHAPTER 1
บทสรุป (Summary)

หน้า **4-7**

1.1 บทสรุปสำหรับผู้บริหาร (Executive Summary)

1.2 คำถามที่จุดประกายความคิดเรื่องควอนตัม: จะเกิดอะไรขึ้นหากบริษัทเทคโนโลยียักษ์ใหญ่ประกาศความสำเร็จของ Quantum Computer ที่ใช้งานได้จริงและ Scale ได้ในวันพรุ่งนี้?

1.3 ความพร้อมด้านควอนตัม (Quantum Readiness)

1.4 โอกาสที่เป็นไปได้จริงของ Quantum Computing

CHAPTER 2
Quantum Computing สำหรับบุคคลทั่วไป

หน้า **8-11**

2.1 ความเข้าใจคลาดเคลื่อนที่พบได้บ่อย

2.2 คอมพิวเตอร์ควอนตัมคืออะไร?

2.3 Quantum Algorithms: เครื่องยนต์แห่งนวัตกรรม

CHAPTER 3
ความคืบหน้าสู่ความได้เปรียบเชิงควอนตัม

หน้า **12-24**

3.1 ความได้เปรียบเชิงควอนตัมคืออะไร? (What is the Quantum Advantage?)

3.2 ก้าวสู่การประมวลผลเชิงควอนตัมแบบทนทานต่อข้อผิดพลาด (Towards Fault-Tolerant Quantum Computing)

3.3 การพัฒนา Algorithm และความต้องการทรัพยากร

3.4 กรณีการใช้งานเทียบกับความได้เปรียบเชิงควอนตัมที่แท้จริง (Use cases versus actual quantum advantages)

3.5 ศักยภาพการประยุกต์ใช้งานในภาคการเงิน (Potential Applications in Finance)

3.6 Quantum AI: ความคาดหวังและความเป็นจริง (Quantum AI: Promise and Reality)

CHAPTER 4
Post Quantum Cryptography Update (2026)

หน้า **25-28**

4.1 เหตุใดองค์กรจึงต้องเตรียมพร้อมตั้งแต่วันนี้

4.2 กรอบเวลาการเปลี่ยนผ่านชัดเจนขึ้น และใกล้เข้ามา

4.3 ความเสี่ยงจากควอนตัมมีอยู่จริง แม้ยังไม่ทราบว่าจะเกิดขึ้นเมื่อใด

4.4 จากมาตรฐานสู่การนำไปใช้จริง

4.5 บทเรียนที่ภาคการเงินเริ่มได้รับจากการนำไปใช้จริง

4.6 ทิศทางในภูมิภาคชัดเจนขึ้น

4.7 การเตรียมเข้าสู่ระยะนำไปใช้จริง

CHAPTER 5
ภูมิทัศน์การลงทุนระดับโลกและความพยายามในการสร้างคอมพิวเตอร์ควอนตัม

หน้า **29-33**

5.1 จาก Research Ecosystem สู่ Quantum Supply Chain

5.2 การคาดการณ์ผลกระทบทางเศรษฐกิจ: วิธีตีความตัวเลขอย่างระมัดระวัง (Economic impact projections: how to read the numbers carefully)

CHAPTER 6
Thailand Positioning

หน้า **34-38**

6.1 จุดเปลี่ยนเชิงยุทธศาสตร์ระดับชาติ (National Strategic Pivot)

6.2 Siam Quantum Square (SQ^2)

6.3 ผู้ขับเคลื่อนหลักจากภาคธุรกิจอุตสาหกรรม (Key players from industrial sector)

6.4 ระบบนิเวศการวิจัยด้านควอนตัมของไทยแบบกระจายศูนย์ (A Distributed Thai Quantum Research Ecosystem)

6.5 การขับเคลื่อนไปข้างหน้าร่วมกัน (Moving forwards together)

บทสรุปส่งท้าย:
ความจำเป็นเร่งด่วนเชิงยุทธศาสตร์ด้านควอนตัม (Ending Remarks: The Quantum Imperative)

หน้า **39**

ภาคผนวก (Appendix)

หน้า **40-41**

ภาคผนวก ก: อภิธานศัพท์ (Appendix A: Glossary of Terms)

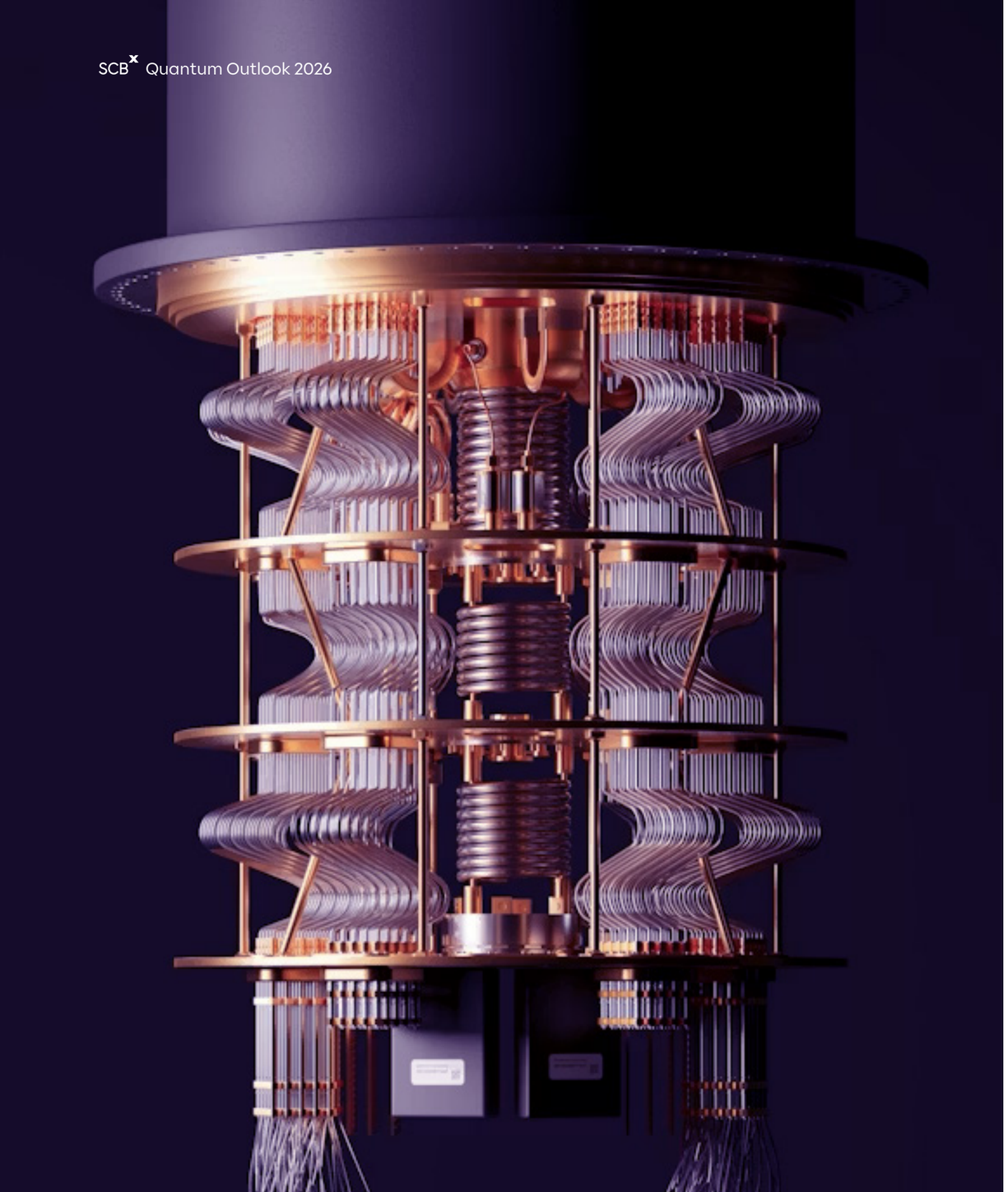
ภาคผนวก ข: เจาะลึกเชิงเทคนิค – งานวิจัยการหาค่าเหมาะสมที่สุดของพอร์ตโฟลิโอโดย SCBX (Appendix B: Technical Deep-Dive – SCBX Portfolio Optimization Research)

ภาคผนวก ค: รายการตรวจสอบความพร้อมสู่ยุคควอนตัม (Appendix C: The Quantum Readiness Checklist)

CHAPTER 1

บทสรุป (SUMMARY)





1.1 บทสรุปสำหรับผู้บริหาร (Executive Summary)

เศรษฐกิจโลกในปัจจุบันพึ่งพาระบบประมวลผลสารสนเทศแบบดั้งเดิมเป็นหลัก ตลอดหลายทศวรรษที่ผ่านมา คอมพิวเตอร์แบบคลาสสิก และ ปัญญาประดิษฐ์ได้ขับเคลื่อนการเติบโตทั้งทางเศรษฐกิจและเทคโนโลยีอย่างมหาศาล อย่างไรก็ตาม คอมพิวเตอร์ดั้งเดิมทำงานบนพื้นฐานของหน่วยข้อมูลที่เรียบง่าย นั่นคือ “Bit” ซึ่งมีค่าเป็น 0 หรือ 1 อย่างใดอย่างหนึ่ง และไม่สามารถเป็นทั้งสองค่าพร้อมกันได้

เมื่อภาคอุตสาหกรรมพยายามแก้ไขโจทย์ที่ซับซ้อนยิ่งขึ้น ตั้งแต่การพยากรณ์สภาพอากาศ ห่วงโซ่อุปทาน การคิดค้นยา การออกแบบวัสดุ การแพทย์แม่นยำ ไปจนถึงการจำลองระบบนิเวศคอมพิวเตอร์แบบดั้งเดิม มักเผชิญข้อจำกัดในการรองรับขนาดและความซับซ้อนของงานภายใต้กรอบเวลาและต้นทุนที่นำไปใช้ได้จริง ซึ่งปัญหาเหล่านี้จำนวนมากจะยากขึ้นแบบทวีคูณเมื่อจำนวนตัวแปรและขนาดของปัญหาเพิ่มขึ้น ทำให้การหาคำตอบที่แม่นยำแทบเป็นไปไม่ได้ในทางปฏิบัติ แม้แต่กับคอมพิวเตอร์ความสามารถสูงสุด (Supercomputer) ที่ทรงพลังที่สุดและ AI ก็ตาม นี่คือเหตุผลที่นักวิจัยและภาคอุตสาหกรรมกำลังศึกษาวิธีประมวลผลข้อมูลแบบใหม่ที่อาศัยกฎพื้นฐานที่สุดของธรรมชาติ นั่นคือ การประมวลผลควอนตัม (Quantum Computation หรือ QC) ซึ่งมีหน่วยพื้นฐานคือคิวบิต (Qubit หรือ Quantum Bit) โดยคิวบิตสามารถแทนค่า 0 และ 1 ได้ในแบบที่ต่างออกไปจากเดิม ทำให้เครื่องสามารถก้าวข้ามข้อจำกัดของคอมพิวเตอร์แบบดั้งเดิมได้

ในรายงาน SCBX Quantum Outlook: Post-Quantum Cryptography ฉบับก่อนหน้า (ธันวาคม 2025)[2] ได้กล่าวถึงยุทธศาสตร์เชิงรับที่จำเป็นสำหรับการปกป้องข้อมูลและการเข้ารหัสจากภัยคุกคามของคอมพิวเตอร์ควอนตัมในอนาคต สำหรับรายงานฉบับนี้จะปรับมุมมองสู่ยุทธศาสตร์เชิงรุก ได้แก่ ความพร้อมด้านควอนตัม (Quantum Readiness) และ การสร้างมูลค่า (Value Creation) แสดงให้เห็นว่าเทคโนโลยีควอนตัมกำลังเปลี่ยนผ่านจากความสนใจทางวิทยาศาสตร์ สู่แพลตฟอร์มที่เป็นรูปธรรมและนำไปปฏิบัติได้จริงสำหรับนวัตกรรมระดับองค์กร ซึ่งทำให้คำถามเปลี่ยนจาก “เราจะสร้างมันขึ้นมาได้หรือไม่?” เป็น “เราต้องเตรียมพร้อมให้เร็วแค่ไหน?” [1] เราได้ก้าวล่วงวิสัยทัศน์ดั้งเดิมของ ริชาร์ด พี. ไฟน์แมน (Richard P. Feynman) เกี่ยวกับการประมวลผลเชิงควอนตัมไปไกลมากแล้ว:

“ธรรมชาติไม่ได้เป็นแบบคลาสสิก และหากคุณต้องการจำลองธรรมชาติ คุณก็ควรทำให้การจำลองนั้นเป็นเชิงกลศาสตร์ควอนตัม”

เอกสารฉบับนี้สรุปความสำคัญของความพร้อมด้านควอนตัม โอกาสในการประยุกต์ใช้ข้ามอุตสาหกรรมที่เป็นไปได้จริง อธิบายเทคโนโลยีด้วยภาษาที่เข้าใจง่าย และวางรากฐานให้องค์กรสามารถเริ่มเตรียมพร้อมเพื่อสร้างมูลค่าทางธุรกิจเมื่อการประมวลผลเชิงควอนตัม พัฒนาจนสามารถใช้ศักยภาพได้อย่างเต็มที่

1.2 คำถามที่จุดประกายความคิดเรื่องควอนตัม: จะเกิดอะไรขึ้นหากบริษัทเทคโนโลยียักษ์ใหญ่ประกาศความสำเร็จของ Quantum Computer ที่ใช้งานได้จริงและ Scale ได้ในวันพรุ่งนี้?

จะเป็นอย่างไร? ถ้าคุณตื่นขึ้นมา พร้อมข่าวที่ว่าบริษัทเทคโนโลยีรายใหญ่ประสบความสำเร็จในการเปิดให้บริการคอมพิวเตอร์ควอนตัม (Quantum Computer) ที่สามารถทนทานต่อความผิดพลาด (fault-tolerant) และสเกลได้ ผ่านระบบ Cloud นัยสำคัญที่ลึกซึ้งที่สุดต่ออุตสาหกรรมโลกที่อยู่เบื้องหลังพาดหัวข่าวนั้นคือ การปรากฏขึ้นอย่างฉับพลันของความได้เปรียบด้านข้อมูล (Information Advantage) ที่ไม่อาจต้านทานได้

ข้อมูลหรือคำตอบประเภทใดที่ยังอยู่เหนือความสามารถของเราในปัจจุบันหากปราศจากคอมพิวเตอร์ควอนตัมที่ใช้งานได้จริง?

ในบริบทสำคัญหลายประการ อุตสาหกรรมต้องเผชิญกับปัญหาที่ซับซ้อนอย่างรุนแรงเมื่อจำนวนตัวแปรเพิ่มขึ้น ตัวอย่างเช่น การจำลองปฏิสัมพันธ์ระดับโมเลกุลอย่างแม่นยำเพื่อพัฒนาวัคซีนหรือวัสดุชนิดใหม่ การหาค่าที่เหมาะสมที่สุด (Optimization) ในห่วงโซ่อุปทานขนาดใหญ่ที่มีข้อจำกัดเปลี่ยนแปลงตลอดเวลา หรือการหาเส้นทางที่มีประสิทธิภาพสูงสุดสำหรับยานพาหนะนับพันคันและจุดหมายปลายทาง ในกรณีเช่นนี้ คอมพิวเตอร์แบบดั้งเดิมมักไม่สามารถตรวจสอบความเป็นไปได้ทั้งหมดโดยตรง จึงต้องอาศัยทางลัด การประมาณค่า และวิธีการโดยประมาณตามหลักเหตุผลเชิงประสบการณ์ หรือ วิธีฮิวริสติก (Heuristics) หากไม่มีคอมพิวเตอร์ควอนตัมที่ใช้งานได้จริง เราก็หาคำตอบที่ใกล้เคียงคำตอบที่ดีที่สุดได้เพียงระดับหนึ่งเท่านั้น โดยเฉพาะในระบบที่ซับซ้อนมาก ตัวอย่างเช่น การจำลองปฏิสัมพันธ์ระดับโมเลกุลที่เกี่ยวข้องทั้งหมดอย่างแม่นยำบนคอมพิวเตอร์แบบดั้งเดิมอาจใช้เวลานานจนไม่สามารถนำไปใช้ได้จริง [PNAS2017] ยิ่งไปกว่านั้น สำหรับองค์กรขนาดใหญ่ แม้แต่การปรับปรุงคุณภาพของคำตอบเพียงเล็กน้อย เช่น ผลตอบแทนเพิ่มขึ้น 2% (ซึ่งเป็นการประเมินที่อนุรักษ์นิยมอย่างยิ่ง) ก็สามารถสร้าง ROI อย่างมีนัยสำคัญในอุตสาหกรรมอย่างการเงิน โลจิสติกส์ และวัสดุศาสตร์

คอมพิวเตอร์ควอนตัมที่ใช้งานได้จริงอาจช่วยแก้ปัญหาบางอย่างที่ในปัจจุบันไม่สามารถแก้ไขได้ ด้วยการประมวลผลข้อมูลที่ซับซ้อนในลักษณะที่เป็นธรรมชาติกว่า เนื่องจากคอมพิวเตอร์ควอนตัมใช้ปรากฏการณ์ทางกลศาสตร์ควอนตัม จึงอาจทำให้การคำนวณบางอย่างที่เคยทำไม่ได้ในทางปฏิบัติ สามารถเข้าถึงได้มากขึ้น อย่างไรก็ตาม คอมพิวเตอร์ควอนตัมไม่ใช่เครื่องมือวิเศษที่แก้ได้ทุกปัญหา

สำหรับงานบางประเภท คอมพิวเตอร์ควอนตัมทำได้รวดเร็วกว่าวิธีที่ดีที่สุดที่เราใช้กันในปัจจุบัน ตัวอย่างเช่น การใช้อัลกอริทึมของชอร์ (Shor's algorithm) เจาะระบบเข้ารหัสแบบกุญแจสาธารณะ (Public-key Cryptography) ที่ใช้กันอย่างแพร่หลาย ความได้เปรียบด้านความเร็วนี้เป็นที่ยอมรับในวงวิชาการแล้ว [Shor] แต่สำหรับปัญหาการหาค่าที่เหมาะสมที่สุดจำนวนมากในโลกความเป็นจริง เรื่องกลับซับซ้อนกว่านั้น ปัญหาบางประเภทยากมาก จนถึงตอนนี้ก็ยังไม่มีวิธีใดที่เรารู้จัก ทั้งแบบดั้งเดิมและแบบควอนตัม ที่รับประกันคำตอบที่ดีที่สุดได้อย่างมีประสิทธิภาพเมื่อปัญหามีขนาดใหญ่ขึ้น [Kempe2006] ในทางปฏิบัติ หมายความว่าการประมวลผลเชิงควอนตัมอาจมีประโยชน์อย่างมากในบางด้าน แต่ไม่น่าจะแก้ปัญหาการหาค่าที่เหมาะสมที่สุดให้ทุกปัญหาได้โดยอัตโนมัติ ดังนั้น คำถามที่ว่า "อัลกอริทึมควอนตัมจะสร้างความได้เปรียบที่ใช้ได้จริงและถึงขั้นพลิกโฉมกับปัญหาธุรกิจหลายประเภทหรือไม่?" เรื่องนี้ยังอยู่ระหว่างการวิจัยอย่างจริงจัง [Preskill2018] รายงานฉบับนี้จะพิจารณาความคาดหวังเหล่านี้อย่างสมจริง แต่สำหรับปัญหา Optimization ในโลกจริงจำนวนมากภาพรวมกลับซับซ้อนกว่านั้น ปัญหาบางประเภทมีความยากเสียจนไม่มีวิธีการใด ทั้งคลาสสิกหรือควอนตัม ที่สามารถรับประกันคำตอบที่สมบูรณ์แบบได้อย่างมีประสิทธิภาพเมื่อขนาดของปัญหาใหญ่ขึ้น [Kempe2006] ในทางปฏิบัติ นั่นหมายความว่า Quantum Computing อาจให้ประโยชน์อย่างมากในบางพื้นที่ที่คัดสรรแล้ว แต่ไม่น่าจะแก้ปัญหา Optimization ที่ยากทุกประเภทได้โดยอัตโนมัติ คำถามที่ว่า Quantum Algorithms จะสร้าง Practical Edge ที่พลิกโฉมธุรกิจในวงกว้างหรือไม่ ยังคงเป็นหัวข้อการวิจัยที่เข้มข้น [Preskill2018] และรายงานฉบับนี้จะอภิปรายความคาดหวังดังกล่าวอย่างสมจริง

1.3 ความพร้อมด้านควอนตัม (Quantum Readiness)

คำถามสำคัญสำหรับองค์กรในวันนี้ไม่ใช่ว่าคอมพิวเตอร์ควอนตัมจะถูกสร้างขึ้นได้ในที่สุดหรือไม่ หากแต่เป็นคำถามว่าใครจะพร้อมเมื่อวันนั้นมาถึง สำหรับอุตสาหกรรมส่วนใหญ่ ความเสี่ยงเชิงกลยุทธ์ที่ใหญ่ที่สุดไม่ใช่ความล้มเหลวทางเทคโนโลยี หากแต่เป็นความล่าช้าเชิงกลยุทธ์

- **ความพร้อมต้องใช้เวลาบ่มเพาะ:** การกลายเป็น Quantum-ready ไม่ใช่แค่เรื่องของการซื้อฮาร์ดแวร์เมื่อมีจำหน่าย แต่ต้องอาศัยความเชี่ยวชาญใหม่ข้ามศาสตร์ทั้งฟิสิกส์ คณิตศาสตร์ วิทยาการคอมพิวเตอร์ และความรู้เฉพาะทางของธุรกิจ (Domain knowledge) รวมถึงการ Re-skilling ทีมวิศวกรรมอย่างมีนัยสำคัญ ต่างจาก AI ที่มักผนวกเข้ากับไปป์ไลน์ซอฟต์แวร์เดิมได้ ควอนตัมมักต้องการการตั้งโจทย์ปัญหาใหม่ตั้งแต่พื้นฐาน และพัฒนาขั้นตอนการทำงานแบบควอนตัมใหม่ องค์กรที่รอจนกว่าฮาร์ดแวร์ขนาดใหญ่จะมาถึงย่อมเสี่ยงต่อการเผชิญช่องว่างด้านทักษะและความรู้ (Competency Gap) ที่สำคัญ
- **การประยุกต์ใช้ควอนตัมที่มีคุณค่ากำลังอยู่ระหว่างการค้นพบ:** แม้แต่ในชุมชนวิทยาศาสตร์ระดับโลก ก็ยังไม่ชัดเจนว่าปัญหาใดจะส่งมอบความได้เปรียบทางเศรษฐกิจสูงสุด การระบุกรณีศึกษาที่ถูกต้องต้องอาศัยการทดลองและการมีส่วนร่วมตั้งแต่เนิ่น ๆ องค์กรที่เริ่มสำรวจแอปพลิเคชันควอนตัมในวันนี้ ไม่ได้แค่ทดสอบเทคโนโลยีใหม่ แต่กำลังค้นพบว่ามูลค่าที่แท้จริงอยู่ที่ใด และพัฒนาอัลกอริทึมที่เป็นกรรมสิทธิ์ (Proprietary algorithms) เฉพาะอุตสาหกรรมของตน นวัตกรรมเหล่านี้สามารถได้รับการปกป้องเป็นทรัพย์สินทางปัญญา และอาจกลายเป็นความได้เปรียบทางการแข่งขัน ที่มีความหมายเมื่อฮาร์ดแวร์ควอนตัมขนาดใหญ่พร้อมใช้งาน

- **การเข้าถึงฮาร์ดแวร์อาจมีข้อจำกัด:** อีกปัจจัยที่มักถูกมองข้ามคือการเข้าถึงตัวฮาร์ดแวร์เอง ในช่วงปีแรก ๆ ของยุค Fault-Tolerant Quantum Computing โปรเซสเซอร์ขนาดใหญ่มีแนวโน้มที่จะหายากและมีราคาแพง การเข้าถึงจะถูกจัดการผ่านผู้ให้บริการระบบคลาวด์และพันธมิตรด้านการวิจัย องค์กรที่ร่วมมือกับผู้ให้บริการฮาร์ดแวร์อยู่แล้วจะย้ายไปอยู่แถวหน้าทันทีเมื่อระบบใหม่พร้อมใช้งาน ผู้ที่รอก็อาจพบว่าการเข้าถึงระบบที่ล้ำสมัยถูกจำกัด ล่าช้า หรือแพงเกินไป

- **หน้าต่างแห่งโอกาสกำลังแคบลง:** เมื่อไม่กี่ปีก่อน มีการคาดการณ์ว่าคอมพิวเตอร์ควอนตัมที่ทนทานต่อความผิดพลาดและใช้ประโยชน์ได้จริงจะเกิดขึ้นในช่วงปลายทศวรรษ 2030 หรืออาจถึงทศวรรษ 2040 แต่ความก้าวหน้าอย่างรวดเร็วด้านวิศวกรรมฮาร์ดแวร์ การแก้ไขข้อผิดพลาด และการปรับปรุงอัลกอริทึม ทำให้กรอบเวลาเหล่านี้สั้นลงอย่างมาก ส่งผลให้ในปัจจุบัน แผนงานของหลายบริษัทในอุตสาหกรรมชี้ว่า ความได้เปรียบเชิงควอนตัมที่ใช้ประโยชน์ได้จริงในงานบางประเภทอาจเกิดขึ้นได้ระหว่างช่วงปลายทศวรรษ 2020 ถึงต้นทศวรรษ 2030 องค์กรที่ยังวางแผนโดยคาดว่าเทคโนโลยีนี้จะมาถึงช่วงปลายทศวรรษ 2030 อาจจะกำลังเตรียมตัวรับความล้าสมัยไปแล้ว

Executive TL;DR: ความเสี่ยงเชิงกลยุทธ์ที่ใหญ่ที่สุดในการประมวลผลเชิงควอนตัม ไม่ใช่ว่าเทคโนโลยีมาถึงช้าเกินไป แต่คือการที่มันมาถึงอย่างกะทันหันและองค์กรของคุณยังไม่พร้อม การประมวลผลเชิงควอนตัมไม่สามารถนำมาใช้ได้ในชั่วข้ามคืน มันต้องการความเชี่ยวชาญใหม่ อัลกอริทึมใหม่ และบุคลากรที่สามารถคิดในโมเดลการคำนวณที่แตกต่างไปจากเดิมอย่างสิ้นเชิง การสร้างขีดความสามารถนี้ใช้เวลาเป็นปี สถาบันที่เพิ่งเริ่มต้นเมื่อฮาร์ดแวร์ควอนตัมขนาดใหญ่พร้อมใช้งานจะเผชิญกับช่องว่างด้านทักษะและความรู้ที่รุนแรง ในขณะที่ผู้ริเริ่มกลุ่มแรก จะมีทั้งบุคลากร ทรัพย์สินทางปัญญา และประสบการณ์การดำเนินงานที่จำเป็นในการปรับใช้เทคโนโลยีทันที ยิ่งไปกว่านั้น การเข้าถึงฮาร์ดแวร์ควอนตัมที่ล้ำสมัยในช่วงแรกจะถูกจำกัด และผู้ที่มีส่วนร่วมในระบบนิเวศอยู่แล้วจะได้อยู่หน้าแถว ดังนั้น การชะลอการเตรียมตัวไม่ใช่แค่เลื่อนการลงทุน แต่มันก่อให้เกิดค่าเสียโอกาสที่แท้จริง ที่ซึ่งความรู้ พันธมิตร และความได้เปรียบที่สำคัญที่สุดถูกผู้อื่นคว้าไปก่อน

1.4 โอกาสที่เป็นไปได้จริงของ Quantum Computing

คอมพิวเตอร์ควอนตัมไม่ได้มาแทนที่คอมพิวเตอร์แบบคลาสสิก เมื่อพูดถึงการแก้ไขปัญหา จะเข้าใจได้ดีกว่าหากมองว่ามันเป็นตัวเร่งการประมวลผลเฉพาะทาง (Specialized Accelerators) สำหรับงานบางประเภท ตามข้อมูลของ World Economic Forum (WEF) การประยุกต์ใช้จริงกำลังปรากฏขึ้นแล้วผ่านแนวทางแบบผสมผสานระหว่างคอมพิวเตอร์ควอนตัมกับคอมพิวเตอร์แบบคลาสสิก (Hybrid Quantum-Classical) ในหลายภาคส่วนสำคัญ โดยคาดการณ์ว่ามูลค่าทางเศรษฐกิจที่จะเข้าถึงได้สูงถึงหลายแสนล้านดอลลาร์ภายในปี 2035 จากการประมวลผลเชิงควอนตัมเพียงอย่างเดียว [WEF1]

โอกาสเพิ่มขีดความสามารถของอุตสาหกรรมที่เห็นภาพได้ชัดเจน ตัวอย่างเช่น:

- **Combinatorial Optimization (โลจิสติกส์และปฏิบัติการ):** การค้นหาตารางเวลา เส้นทาง หรือการจัดสรรทรัพยากรที่มีประสิทธิภาพสูงสุดในสภาพแวดล้อมที่เปลี่ยนแปลงมักจะเป็นเรื่องยากมากสำหรับระบบคลาสสิก ตัวอย่างเช่น ท่าเรือลอสแอนเจลิสเพิ่งทดลองใช้การเพิ่มประสิทธิภาพด้วยควอนตัมแบบผสมผสาน (Hybrid Quantum Optimization) สำหรับสถานการณ์การจัดการสินค้า ซึ่งช่วยลดระยะทางการเดินทางของเครนลงประมาณ 30% ช่วยปรับปรุงผลผลิตในการดำเนินงาน [WEF2] ในขณะที่Ford Otosan ใช้แนวทางการประมวลผลแบบผสมผสาน (Hybrid Computing) เพื่อหาค่าที่เหมาะสมสำหรับกำหนดการผลิต ซึ่งลดเวลาในการจัดกำหนดการเหลือไม่ถึงห้านาที [WEF2]

- **Advanced Chemical Simulation (วัสดุศาสตร์และ Healthcare):** คอมพิวเตอร์ดั้งเดิมประสบปัญหาอย่างมากเมื่อพยายามจำลองระบบควอนตัมขนาดใหญ่อย่างแม่นยำ รวมถึงโมเลกุลและวัสดุ ควอนตัมคอมพิวเตอร์มีแนวโน้มทำได้ดีกว่า เพราะวิชาเคมีเป็นเรื่องของกลศาสตร์ควอนตัมที่แก่นแท้อยู่แล้ว สิ่งนี้อาจช่วยเร่งการค้นพบแบตเตอรี่ที่ดีกว่า วัสดุที่ยั่งยืน และเภสัชภัณฑ์ ตัวอย่างเช่น Moderna ที่กำลังร่วมมือกับ IBM เพื่อคาดการณ์ว่าลำดับ mRNA พับตัวเป็นรูปทรงที่ทำงานได้อย่างไร การทดลองเหล่านี้ยังอยู่ในระยะเริ่มต้นและมีสเกลเล็ก แต่ก็แสดงให้เห็นว่าในอนาคตวิธีการเชิงควอนตัมอาจสามารถจำลองโมเลกุลเหล่านี้ได้โดยใช้การลดรูปแบบจำลองน้อยกว่าที่เครื่องมือคลาสสิกต้องใช้ [WEF3]

- **The Financial Sector Imperative (ความจำเป็นเร่งด่วนของภาคการเงิน):** ในบรรดาอุตสาหกรรมทั้งหมด บริการทางการเงินอาจเป็นหนึ่งในผู้ได้รับผลประโยชน์กลุ่มแรก ๆ ที่ชัดเจนที่สุดจากการประมวลผลเชิงควอนตัม เพราะการเงินพึ่งพาโมเดลที่ซับซ้อน การจำลองสถานการณ์หาค่าที่เหมาะสมที่สุด และการตรวจจับรูปแบบอย่างมาก World Economic Forum คาดการณ์ว่ากรณีศึกษาของการประมวลผลเชิงควอนตัมในบริการทางการเงินอาจสร้างมูลค่าสูงถึง 6.22 แสนล้านดอลลาร์ภายในปี 2035 [WEF4] สถาบันการเงินชั้นนำกำลังก้าวข้ามทฤษฎีไปสู่การพิสูจน์แนวคิด (Proof of Concept) แล้ว ตัวอย่างเช่น ธนาคาร Yapı Kredi ของตุรกี ได้ทดลองใช้ควอนตัมแอนนีลลิง (Quantum Annealing) เพื่อวิเคราะห์ความเสี่ยงทางการเงินแบบลูกโซ่ (Cascading financial risks) ในกลุ่มตัวอย่างลูกค้าองค์กร 4,297 ราย ซึ่งคัดเลือกจากเครือข่ายลูกค้ากว่า 600,000 ราย โดยรายงานว่าการคำนวณสำหรับสถานการณ์นำร่องดังกล่าวใช้เวลาเพียงเจ็ดวินาที [WEF4] นอกจากนี้ สถาบันอย่าง Intesa Sanpaolo และ Santander ก็กำลังทดลองวิธี Quantum และ Quantum-inspired สำหรับการตรวจจับการฉ้อโกงและการปรับปรุง Dynamic Bond-Hedging Optimization [WEF4] หากใช้ในลักษณะนี้เป็นตัวเร่งความเร็วเฉพาะทางสำหรับงานที่เน้นคณิตศาสตร์ การประมวลผลควอนตัมอาจกลายเป็นเครื่องมือแข่งขันที่มีความหมายสำหรับสถาบันการเงิน

CHAPTER 2

QUANTUM COMPUTING สำหรับบุคคลทั่วไป

การประมวลผลเชิงควอนตัมไม่ใช่แค่คอมพิวเตอร์ที่เร็วขึ้น แต่เป็นวิธีการประมวลผลข้อมูลที่แตกต่างออกไป
โดยอาศัยกฎของกลศาสตร์ควอนตัมแทนตรรกะแบบคลาสสิก



2.1 ความเข้าใจที่คลาดเคลื่อนที่พบได้บ่อย

ก่อนจะพูดถึงโอกาส เราควรแยกข้อเท็จจริงออกจากกระแสที่เกินจริงเกี่ยวกับเทคโนโลยีนี้เสียก่อน เพราะการรู้ว่าคอมพิวเตอร์ควอนตัมทำอะไรไม่ได้ สำคัญไม่แพ้การรู้ว่ามันอาจทำอะไรได้ดีในอนาคต

ความเข้าใจที่คลาดเคลื่อน 1: **“ควอนตัมคอมพิวเตอร์สามารถแก้ปัญหาได้ทุกอย่าง”**

ข้อเท็จจริง: แม้ว่าควอนตัมคอมพิวเตอร์จะสามารถแก้ปัญหาบางประเภทได้อย่างมีประสิทธิภาพกว่าคอมพิวเตอร์คลาสสิกอย่างมาก แต่ก็ไม่ใช่ ‘จินนี่วิเศษ’ ยังมีงานอีกจำนวนมากที่คาดว่าคอมพิวเตอร์ควอนตัมจะไม่สามารถแก้ได้อย่างมีประสิทธิภาพ เช่น วิทยาการเข้ารหัสลับหลังยุคควอนตัม (Post-Quantum Cryptography: PQC) ซึ่งเป็นการเข้ารหัสที่ออกแบบมาเพื่อต้านทานการโจมตีทางควอนตัม เป็นเครื่องพิสูจน์ถึงความเฉพาะเจาะจงนี้ในตัวเอง: PQC อาศัยโจทย์ทางคณิตศาสตร์ที่ในปัจจุบันยังไม่มีใครรู้จักวิธีคำนวณเชิงควอนตัมที่มีประสิทธิภาพสำหรับแก้โจทย์เหล่านั้น [1]

ความเข้าใจที่คลาดเคลื่อน 2: **“คอมพิวเตอร์ควอนตัมหาคำตอบที่ดีที่สุดโดยการลองตัวเลือกทุกอย่างพร้อมกัน”**

ข้อเท็จจริง: แม้ว่า สภาวะซ้อนทับ (Superposition) จะช่วยให้คอมพิวเตอร์ควอนตัมสำรวจเส้นทางคำตอบหลายทางได้ในเวลาเดียวกัน แต่ความท้าทายก็คือเราไม่สามารถแค่อ่านคำตอบเหล่านั้นออกมาทั้งหมดพร้อมกันได้ตามกฎของกลศาสตร์ควอนตัม เมื่อเราดูผลลัพธ์ ระบบจะ ‘ยุบตัว’ (Collapses) กลายเป็นคำตอบเดียวอันเนื่องมาจากการวัดเชิงควอนตัม (Quantum Measurement) หากเราไม่ระมัดระวังในการออกแบบอัลกอริทึม คำตอบนั้นก็จะเป็นการสุ่ม ซึ่งความน่าฉงนของอัลกอริทึมควอนตัมไม่ใช่แค่การสำรวจทุกเส้นทาง แต่เป็นการใช้การสอดแทรกเชิงควอนตัม (Quantum Interference) อย่างชาญฉลาด เพื่อทำให้คำตอบที่ถูกต้องมีโอกาสปรากฏมากกว่าคำตอบที่ผิด เปรียบเหมือนระลอกคลื่นบนสระน้ำอัลกอริทึมควอนตัม ต้องจัดระเบียบคลื่นความน่าจะเป็นให้คำตอบที่ผิดหักล้างกันไป ในขณะที่คำตอบที่ถูกขยายจนเป็นยอดคลื่นขนาดใหญ่ที่วัดได้ การสร้างความสอดแทรกควอนตัมที่แม่นยำในตัวแปรนับพันตัวนั้นยากเป็นพิเศษ ทำให้การค้นพบอัลกอริทึมควอนตัมที่มีประโยชน์เป็นความท้าทายอย่างลึกซึ้ง

ความเข้าใจที่คลาดเคลื่อน 3: **“ตัวเลขเดียวที่สำคัญคือจำนวน Qubits”**

ข้อเท็จจริง: จำนวนไม่ได้บอกคุณภาพ การมีคิวบิตคุณภาพต่ำที่มีสัญญาณรบกวนสูง (Noisy Qubit) 1,000 ตัว ก็เหมือนมีพนักงานเยอะแต่สื่อสารกันไม่รู้เรื่องและทำงานผิดพลาดตลอด สุดท้ายงานก็ไม่เสร็จ เป้าหมายที่แท้จริงคือการแก้ไขข้อผิดพลาด (Error Correction) ซึ่งเป็นการนำคิวบิตทางกายภาพ (Physical Qubit) จำนวนมากมารวมกัน เพื่อสร้างคิวบิตเชิงตรรกะ (Logical Qubit) ที่เสถียรและเชื่อถือได้พอจะใช้ประมวลผลงานจริง แต่แม้จะสร้างคิวบิตเชิงตรรกะได้แล้ว เวลาอ่านประกาศใหญ่ ๆ จากบริษัทควอนตัมก็ยังต้องดูรายละเอียดให้ดี นี่เป็นเพียงเกริ่นนำ และเราจะอธิบายเพิ่มเติมในส่วนถัดไป [ดู Section 3.2]

ความเข้าใจที่คลาดเคลื่อนที่ 4: **“นักวิทยาศาสตร์รู้ศักยภาพสูงสุดของเครื่องเหล่านี้แล้ว”**

ข้อเท็จจริง: ลองนึกถึงตอนที่คอมพิวเตอร์คลาสสิกเครื่องแรก “ENIAC” เปิดตัวในทศวรรษ 1940 ไม่มีใครทำนายถึงการมีอยู่ของอินเทอร์เน็ต AI หรือโซเชียลมีเดียอย่างที่เราเห็นในปัจจุบัน เราอยู่ใน “ยุค ENIAC” ของการประมวลผลเชิงควอนตัม เครื่องจักรพื้นฐานมีอยู่และใช้งานได้ แต่เรายังห่างไกลจากระบบที่เชื่อถือได้และปรับขนาดได้ซึ่งจะพลิกโฉมอุตสาหกรรมและผสานเข้ากับชีวิตประจำวันของเราอย่างราบรื่น เรารู้เครื่องมือทางเทคนิคและวิทยาศาสตร์ แต่นวัตกรรมที่พลิกโฉมจะมาจากการทำงานร่วมกันอย่างสร้างสรรค์ระหว่างวิทยาศาสตร์ควอนตัมและธุรกิจ ซึ่งเป็นการสำรวจที่เราต้องเริ่มตั้งแต่วันนี้

2.2 คอมพิวเตอร์ควอนตัมคืออะไร?

การบรรยายที่แพร่หลายมักเสนอว่าคอมพิวเตอร์ควอนตัมเป็นเพียงทางเลือกที่แตกต่างไปจากเครื่องคลาสสิกที่เราใช้ในปัจจุบัน แม้จะแม่นยำ แต่คำอธิบายนี้ก็ยังกล่าวไม่หมด ในทางวิทยาศาสตร์กายภาพกลศาสตร์คลาสสิกแท้จริงแล้วเป็นเพียงสับเซตที่มีข้อจำกัดและเข้าใจง่ายกว่าภายใต้กฎที่กว้างขึ้นของกลศาสตร์ควอนตัม

ดังนั้น ควอนตัมคอมพิวเตอร์จึงไม่ควรถูกมองว่าเป็นเทคโนโลยีต่างสายพันธุ์ แต่เป็นรูปแบบการประมวลผลที่เป็นสากลและครอบคลุมมากกว่า มันมีความสามารถโดยกำเนิดที่จะจำลองการคำนวณแบบคลาสสิกได้ และสำหรับงานบางประเภทที่คัดสรรแล้ว ยังสามารถคำนวณได้อย่างมีประสิทธิภาพกว่าวิธีคลาสสิกที่ดีที่สุดเท่าที่รู้จักอย่างมาก

ท้ายที่สุดแล้ว คอมพิวเตอร์ควอนตัมสร้างขึ้นจากหน่วยข้อมูลพื้นฐานที่สุดเรียกว่า คิวบิต ซึ่งใช้ประโยชน์จากคุณสมบัติทางควอนตัมที่แปลกประหลาดสามประการ:

Superposition (พลังของคำว่า “และ”): คิวบิตไม่ใช่แค่ 0 หรือ 1 มันสามารถอยู่ในสถานะที่เป็นทั้งสองอย่างพร้อมกันได้ ลองนึกภาพเหรียญที่กำลังหมุนอยู่บนโต๊ะ ในขณะที่มันหมุน มันเป็นได้ทั้งหัวและก้อยในเวลาเดียวกัน สิ่งนี้ทำให้คอมพิวเตอร์สามารถเก็บและจัดการสถานะจำนวนมากได้พร้อม ๆ กัน แม้ว่าการดึงคำตอบที่เป็นประโยชน์จากสถานะนั้นจะต้องใช้อัลกอริทึมที่ออกแบบอย่างพิถีพิถัน ดังที่อธิบายไว้ในส่วนความเข้าใจผิดด้านบน

Quantum Measurement (คอขวด): นี่คือช่วงเวลาที่เราหยุดเหรียญเพื่อดูผลลัพธ์ และเมื่อถูกวัด สถานะควอนตัมนั้นก็จะหายไป ความไม่อาจย้อนกลับได้นี้คือหนึ่งในข้อจำกัดหลักที่อัลกอริทึมควอนตัมต้องถูกออกแบบให้ล้อมรอบ



Entanglement (ความสัมพันธ์ที่มองไม่เห็น): Entanglement เชื่อมโยงสองคิวบิตเพื่อให้การวัดตัวหนึ่งกำหนดสถานะของอีกตัวหนึ่งในทันที ไม่ว่าจะอยู่ห่างกันแค่ไหน นี่ไม่ใช่ช่องทางการสื่อสาร ไม่มีข้อมูลเดินทางระหว่างพวกมัน แต่มันสร้างความสัมพันธ์ (Correlations) ที่ไม่มีตัวเทียบเท่าในการประมวลผลแบบคลาสสิก ด้วยการทำให้เกิดความสัมพันธ์เหล่านี้ควอนตัมคอมพิวเตอร์สามารถแก้ปัญหาบางประเภทที่คอมพิวเตอร์แบบคลาสสิกแก้ได้ยาก

ด้วยการใช้คุณสมบัติเหล่านี้ คิวบิตจึงทำหน้าที่เป็นการขยายความหมายของ บิตแบบคลาสสิกอย่างทรงพลังขยายแกนหลักแบบเลขฐานสองของเทคโนโลยีดิจิทัลในปัจจุบันไปสู่กระบวนทัศน์การประมวลผลควอนตัมที่ซับซ้อนอย่างมากมาย

2.3 Quantum Algorithms: เครื่องยนต์แห่งนวัตกรรม

ฮาร์ดแวร์ควอนตัมเพียงอย่างเดียวไม่สามารถสร้างมูลค่า สะพานเชื่อมระหว่างฟิสิกส์ควอนตัมที่อธิบายไว้ข้างต้นกับผลกระทบทางธุรกิจในโลกแห่งความเป็นจริงคืออัลกอริทึมควอนตัม ชุดคำสั่งทางคณิตศาสตร์ที่ใช้ประโยชน์จาก การซ้อนทับเชิงควอนตัม (Superposition), ความพัวพันเชิงควอนตัม (Entanglement) และ การแทรกสอดเชิงควอนตัม (Interference) เพื่อแก้ปัญหาเฉพาะกลุ่มในแบบที่ไม่มีโปรแกรมคลาสสิกใดทัดเทียมได้

เพื่อสำรวจภูมิทัศน์นี้ การคิดเป็นสามเลเยอร์จะช่วยได้มาก:

- **Algorithm (เครื่องยนต์):** รูปแบบเฉพาะหรือชุดคำสั่งที่คอมพิวเตอร์ควอนตัมต้องปฏิบัติตาม
- **Problem (โจทย์):** อุปสรรคทางคณิตศาสตร์ที่เครื่องยนต์นี้ถูกออกแบบมาให้ข้ามผ่าน (เช่น “จงหาตัวประกอบจำนวนเฉพาะของตัวเลขขนาดใหญ่นี้”)
- **Application (ผลกระทบ):** สถานการณ์ในโลกแห่งความเป็นจริงที่ความเร็วในการแก้ปัญหาเหล่านั้นอาจแปลงเป็นความได้เปรียบในการแข่งขันหรือเชิงกลยุทธ์

ตัวอย่าง อัลกอริทึมควอนตัมที่เป็นที่รู้จักในยุค Fault-Tolerant อัลกอริทึมที่เน้นด้านล่างนี้แสดงถึงเกณฑ์มาตรฐาน (Benchmarks) ที่ชัดเจนของยุค Fault-Tolerant [รายละเอียดเพิ่มเติมในส่วน 3.3] ประสิทธิภาพเชิงทฤษฎีของอัลกอริทึมเหล่านี้ได้รับการพิสูจน์อย่างเข้มงวดภายใต้สมมติฐานที่กำหนด ในขณะที่ขนาดของความได้เปรียบขึ้นอยู่กับโจทย์ปัญหา การเตรียมข้อมูลนำเข้า ผลลัพธ์ที่ต้องการ และวิธีคลาสสิกที่นำมาเปรียบเทียบ อย่างไรก็ตาม การทำให้ความได้เปรียบเหล่านี้เกิดขึ้นจริงในทางปฏิบัติต้องใช้ฮาร์ดแวร์ที่เต็มประสิทธิภาพโดยเฉพาะคอมพิวเตอร์ควอนตัมที่ติดตั้งคิวบิตเชิงตรรกะ (Logical Qubits) ที่มีเสถียรภาพซึ่งสามารถดำเนินการที่มีความแม่นยำสูง (High-fidelity Operations) นับล้านครั้งโดยไม่มีข้อผิดพลาดทางกายภาพ แม้ว่าฮาร์ดแวร์ที่ต้องใช้รันอัลกอริทึมเหล่านี้ในสเกลที่สามารถดิสรัปต์เชิงพาณิชย์ได้นั้นยังอยู่ระหว่างการพัฒนาทางวิศวกรรม แต่ความได้เปรียบในทางปฏิบัติจะต้องได้รับการประเมินเป็นรายแอปพลิเคชัน

Algorithm	ปัญหาทางคณิตศาสตร์	ผลกระทบที่เป็นไปได้ในโลกจริง
Shor's [2]	แยกตัวประกอบจำนวนขนาดใหญ่ให้เป็นองค์ประกอบจำนวนเฉพาะในเวลา Polynomial time — ซึ่งเป็นการเร่งความเร็วแบบทวีคูณ (Exponential Speedup) เหนือวิธีคลาสสิกที่ดีที่สุด	Cybersecurity: เหตุผลที่เราต้องอัปเกรดมาตรฐานการเข้ารหัสระดับชาติของเราตั้งแต่วันนี้
Quantum Phase Estimation (QPE) [3]	แยกแยะระดับพลังงานของระบบควอนตัม — คุณสมบัติพื้นฐานที่กำหนดว่าโมเลกุลมีพฤติกรรม ทำปฏิกิริยา และยึดเกาะกันอย่างไร — ด้วยความแม่นยำสูงมาก — ซึ่งกลายเป็นสิ่งที่ทำไม่ได้ในทางปฏิบัติสำหรับคอมพิวเตอร์คลาสสิกเมื่อโมเลกุลมีขนาดใหญ่เกินกว่าโมเลกุลขนาดค่อนข้างเล็ก (โดยมีเงื่อนไขว่าต้องมีการคาดเดาสถานะเริ่มต้นของโมเลกุลที่สมเหตุสมผล)	Pharma & Materials: จำลอง Active Sites ที่โมเลกุลยาเข้าไปเกาะกับเป้าหมายทางชีวภาพอย่างแม่นยำ; ออกแบบวัสดุ Cathode แบตเตอรี่ใหม่; และอธิบายกลไกตัวเร่งปฏิกิริยาที่ซับซ้อน — เช่น คลัสเตอร์ FeMoco ทางชีววิทยาทำให้เกิดการตรึงไนโตรเจนที่อุณหภูมิห้องได้อย่างไร ซึ่งอาจปฏิวัติการผลิตปุ๋ยอุตสาหกรรม [5] QPE คืออัลกอริทึมที่เป็นพื้นฐานของความได้เปรียบด้านควอนตัมทางเคมีในระยะยาวที่น่าเชื่อถือทางวิทยาศาสตร์ที่สุด
Harrow–Hassidim–Lloyd [4]	แก้ระบบสมการเชิงเส้นขนาดใหญ่มาก — โครงสร้างทางคณิตศาสตร์หลักของการจำลอง, Optimization และ Machine Learning — ด้วยการเร่งความเร็วที่อาจเป็นแบบทวีคูณ (Exponential) แต่เฉพาะภายใต้เงื่อนไขที่จำกัดเท่านั้น (ตัวอย่างเช่น ข้อมูลต้องสามารถโหลดเข้าสู่ระบบได้อย่างมีประสิทธิภาพ และต้องการเพียงข้อมูลสรุปของคำตอบเท่านั้น)	Finance & Engineering: เร่งการคำนวณความเสี่ยงของพอร์ตโฟลิโอ, ออปติไมซ์เครือข่ายโลจิสติกส์ขนาดใหญ่ และเร่งงานเทรนนิ่งโมเดล Machine Learning ที่เกี่ยวข้องกับการแก้ระบบสมการเชิงเส้น

The Expanding Frontier of Quantum Algorithmic Discovery (พรมแดนที่กำลังขยายตัวของการค้นพบ Quantum Algorithm): แม้ว่า Shor's, QPE และ HHL จะเป็นเสาหลักพื้นฐานของวิทยาการคอมพิวเตอร์ควอนตัม แต่ภูมิทัศน์ของซอฟต์แวร์ควอนตัมในภาพกว้างนั้นมีการพัฒนาอย่างรวดเร็ว หากดึงการเปรียบเทียบก่อนหน้านี้มาใช้ ทุก ๆ อัลกอริทึมใหม่จะต้องหาวิธีที่ไม่ซ้ำใครในการออกแบบ "คลื่นความน่าจะเป็น" ทางคณิตศาสตร์สำหรับโจทย์ปัญหาเฉพาะใหม่ การค้นพบอัลกอริทึมเหล่านี้อย่างต่อเนื่องนั้นยังคงเป็นหนึ่งในแนวพรมแดนที่คึกคักและน่าตื่นเต้นที่สุดในสาขานี้ โดยจะขยายขอบเขตของสิ่งที่คอมพิวเตอร์ควอนตัมจะสามารถแก้ปัญหาได้ในที่สุด ซึ่งความก้าวหน้าทางทฤษฎีและการเพิ่มความเร็วทางควอนตัมที่เพิ่มขึ้นเรื่อย ๆ นี้ถูกติดตามอย่างจริงจังโดยชุมชนวิทยาศาสตร์เช่น Quantum Algorithm Zoo [6]

CHAPTER 3

ความคืบหน้า สู่ความได้เปรียบเชิงควอนตัม



3.1 ความได้เปรียบเชิงควอนตัมคืออะไร? (What Is The Quantum Advantage?)

แม้ว่าคลังอัลกอริทึมควอนตัมที่เพิ่มขึ้นอย่างต่อเนื่องจะเป็นเสมือนพิมพ์เขียวเชิงทฤษฎีสำหรับศักยภาพในการบรรลุความได้เปรียบในการประมวลผลเชิงควอนตัม แต่อัลกอริทึมเพียงอย่างเดียวนั้นยังคงเป็นเพียงแนวคิดทางคณิตศาสตร์ การจะแปลงอัลกอริทึมควอนตัมเหล่านี้ให้เกิดเป็นมูลค่าทางเศรษฐกิจที่จับต้องได้ จำเป็นต้องเชื่อมช่องว่างระหว่างวิทยาศาสตร์เชิงทฤษฎีกับวิศวกรรมกายภาพประยุกต์ในการพัฒนาฮาร์ดแวร์

การประมวลผลเชิงควอนตัมมุ่งเน้นการแก้ปัญหาที่มีความซับซ้อนและส่งผลกระทบอย่างยิ่งใหญ่ ซึ่งมีศักยภาพในการพลิกโฉมเศรษฐกิจและเทคโนโลยีของโลกดังที่ได้กล่าวไว้ข้างต้น การจะขับเคลื่อนศักยภาพดังกล่าวให้เกิดขึ้นจริงถือเป็นความท้าทายแบบคู่ขนาน โดยจำเป็นต้องอาศัยความก้าวหน้าแบบก้าวกระโดดไปพร้อม ๆ กัน ทั้งในด้านฮาร์ดแวร์ทางกายภาพที่สามารถควบคุมสถานะควอนตัมอันเปราะบาง และซอฟต์แวร์เฉพาะทางที่จำเป็นต่อการประมวลผล แม้ปัจจุบันจะยังอยู่ในระยะก่อนเชิงพาณิชย์ (Pre-commercial phase) แต่อุตสาหกรรมนี้ก็กำลังพัฒนาไปอย่างรวดเร็ว การรอคอยอย่างนิ่งเฉย เพื่อรอให้ควอนตัมมาถึงแบบสมบูรณ์ อาจจะเป็นข้อผิดพลาดทางกลยุทธ์ เนื่องจากอัตราเร่งของการพัฒนาในปัจจุบันกำลังบ่งชี้ว่า การเปลี่ยนผ่านจากการทดลองในห้องปฏิบัติการไปสู่การพลิกโฉมตลาด (Market disruption) จะเกิดขึ้นอย่างฉับพลัน ซึ่งจะสร้างความได้เปรียบและให้ผลตอบแทนอย่างมหาศาลแก่องค์กรที่เตรียมความพร้อมไว้ล่วงหน้า

ในการเดินทางสู่เศรษฐกิจที่ขับเคลื่อนด้วยควอนตัม สิ่งสำคัญคือการแยกความแตกต่างระหว่างหมุดหมายทางวิทยาศาสตร์ (Milestones) กับมูลค่าทางธุรกิจที่จับต้องได้ ข้อได้เปรียบไม่ได้ถูกสร้างมาเท่าเทียมกันทั้งหมด และการทำความเข้าใจความก้าวหน้าสามระดับที่แตกต่างกันนั้นจำเป็นสำหรับการตั้งความคาดหวังในการลงทุนที่สมจริง

- **Quantum Supremacy (ระดับที่ 1: Milestone การพิสูจน์แนวคิด):** นี่ถือเป็นความสำเร็จทางเทคนิคที่สำคัญ ซึ่งอุปกรณ์ควอนตัมสามารถประมวลผลการคำนวณเฉพาะทางได้เร็วกว่าซูเปอร์คอมพิวเตอร์ที่ทรงพลังที่สุดในโลกอย่างก้าวกระโดด กล่าวคือ ใช้เวลาเพียงหลักนาทีเมื่อเทียบกับหลายปี ซึ่งถือว่าเกินกว่าขีดจำกัดของคอมพิวเตอร์แบบคลาสสิกในทางปฏิบัติ บริษัทเทคโนโลยียักษ์ใหญ่ อย่าง Google ได้ประกาศความสำเร็จนี้เป็นครั้งแรกในปี 2019 และการสาธิตในระยะเวลาต่อมาโดยบริษัทและสถาบันวิจัยด้านควอนตัมอื่น ๆ ได้สนับสนุนหลักฐานนี้ให้น่าเชื่อถือขึ้นอย่างต่อเนื่อง [2][4] ที่น่าสนใจคือ ในเวลาต่อมานักวิจัยฝั่งคลาสสิกได้ค้นพบวิธีที่เร็วกว่ามากสำหรับงานเดิมของ Google ในปี 2019 ทำให้ตัวเลขประมาณการอันโด่งดังที่ว่า “10,000 ปี” หดสั้นลงอย่างมากซึ่งเป็นเครื่องเตือนใจที่ดีว่าคำกล่าวอ้างเช่นนี้เป็นเป้าหมายที่เคลื่อนที่อยู่เสมอ (Moving target) แม้การทดลองเหล่านี้จะพิสูจน์ได้ว่า ฮาร์ดแวร์ควอนตัมในปัจจุบันมีศักยภาพทางกายภาพมากพอที่จะแก้ปัญหาที่คอมพิวเตอร์คลาสสิกไม่สามารถจัดการได้ (Classically intractable tasks) ในระดับสเกลที่ใหญ่ ทว่าตัวงานประมวลผลเหล่านั้นยังคงขาดอรรถประโยชน์เชิงพาณิชย์โดยตรง สิ่งเหล่านี้จึงถือเป็นเพียงการพิสูจน์แนวคิดที่จำเป็นเพื่อยืนยันว่ากฎทางฟิสิกส์อันซับซ้อนของควอนตัมนั้นสามารถทำงานได้จริง แต่ยังไม่ใช่ผลิตภัณฑ์ที่พร้อมนำไปปรับใช้ในเชิงพาณิชย์ทันที
- **Quantum Utility (ระดับที่ 2: มองเห็นคุณค่าในโลกจริงครั้งแรก):** สิ่งนี้เกิดขึ้นเมื่อคอมพิวเตอร์ควอนตัมสามารถประมวลผลการคำนวณด้วยระดับความแม่นยำและความซับซ้อนที่ก้าวข้ามขีดความสามารถของอัลกอริทึมคลาสสิกที่มีอยู่ในปัจจุบัน ทำให้ได้ข้อมูลที่น่าเชื่อถือซึ่งนักวิทยาศาสตร์และวิศวกรสามารถนำไปใช้งานและตรวจสอบความถูกต้องได้จริง ในระยะนี้ เราไม่ได้มุ่งเน้นว่าคอมพิวเตอร์ควอนตัมจะต้องทำงานได้เร็วกว่าซูเปอร์คอมพิวเตอร์เสมอไป (ซึ่งนั่นคือความคาดหวังในระดับ 3 ความได้เปรียบเชิงควอนตัม) แต่ประเด็นสำคัญคือคอมพิวเตอร์ควอนตัมมีความแม่นยำเพียงพอที่จะเป็นเครื่องมือที่เชื่อถือได้ ในการสำรวจปัญหาสำคัญที่คอมพิวเตอร์คลาสสิกทำได้เพียงแค่คาดเดาหรือประเมินค่าโดยประมาณเท่านั้น คำนี้ได้รับความนิยมแพร่หลายจาก IBM ในปี 2023 [5]

ณ เดือนตุลาคม 2026 วงการนี้กำลังอยู่ในช่วงเปลี่ยนผ่าน (Transition period) ในเดือนกรกฎาคม 2026 IBM และมหาวิทยาลัยชิคาโกรายงานผลการคำนวณบนคิวบิตที่มีการป้องกันข้อผิดพลาด (Logical Qubits) จำนวน 70 ตัว ซึ่งพวกเขาระบุว่าอยู่เหนือขีดความสามารถของวิธีจำลองแบบคลาสสิกชั้นนำ พร้อมกลไกในตัวสำหรับตรวจสอบว่าคำตอบนั้นน่าเชื่อถือหรือไม่ [6] ทว่าภายในเวลาไม่กี่สัปดาห์ นักวิจัยกลุ่มอื่นก็แสดงให้เห็นว่าคลัสเตอร์ GPU ขนาดใหญ่สามารถทำได้ทัดเทียมกันซึ่งสะท้อนให้เห็นว่าวิธีคลาสสิกตอบโต้กลับได้รวดเร็วเพียงใด [7] และยังมีการทดลอง “Quantum Echoes” ของ Google (2025) เป็นอีกหนึ่งการสาธิตที่ตรวจสอบได้บนโจทย์ทางวิทยาศาสตร์ อย่างไรก็ตาม อุตสาหกรรมยังไม่บรรลุอรรถประโยชน์เชิงควอนตัมในเชิงพาณิชย์อย่างกว้างขวางสำหรับการใช้งานอเนกประสงค์ในสเกลขนาดใหญ่

- **ความได้เปรียบเชิงควอนตัม หรือ Quantum Advantage (ระดับ 3):** นี่คือจุดเปลี่ยนที่สำคัญที่สุด (Ultimate inflection point) โดยถูกคาดการณ์ว่าจะเกิดขึ้นเมื่อคอมพิวเตอร์ควอนตัมสามารถแก้ปัญหาที่ตอบโจทย์เชิงพาณิชย์ได้อย่างแท้จริงตัวอย่างเช่น การจำลองโมเลกุลยาที่ซับซ้อนซึ่งคอมพิวเตอร์แบบคลาสสิกไม่สามารถสร้างแบบจำลองได้อย่างแม่นยำ หรือการหาค่าเหมาะสมที่สุดสำหรับเครือข่ายโลจิสติกส์ที่ระดับใหญ่มากซึ่งเกินกว่าขีดจำกัดของระบบคลาสสิก โดยสามารถทำได้รวดเร็วกว่า ประหยัดต้นทุนกว่า หรือมีความแม่นยำสูงกว่าวิธีการแบบคลาสสิกใด ๆ ที่มีอยู่ กรณีการใช้งานที่น่าเชื่อถือที่สุดและมีโอกาสบรรลุระดับ 3 ได้ในอนาคตอันใกล้ (โดยมีข้อมูลสนับสนุนจากการประเมินทรัพยากรที่ได้รับการตีพิมพ์พร้อมระบุจำนวนคิวบิตที่แน่ชัด) ได้แก่ เคมีควอนตัมและวัสดุศาสตร์ (เช่น FeMoco และการจำลองโมเลกุลยา) [8] ส่วนการถอดรหัส (เช่น RSA-2048 ผ่านอัลกอริทึมของชอร์ (Shor's algorithm)) ก็มีการประเมินทรัพยากรที่ได้รับการศึกษาอย่างละเอียดไม่แพ้กัน แต่นั่นถือเป็นภัยคุกคามด้านความมั่นคงปลอดภัยมากกว่าจะเป็นแหล่งที่มาของมูลค่าทางธุรกิจ (ดูหัวข้อ 3.3.2)

ในมุมมองของเรา ขณะนี้วงการกำลังก้าวเข้าสู่ระดับ 2 และจากแผนงานของบริษัทฮาร์ดแวร์ชั้นนำ ระดับ 3 สำหรับปัญหาบางประเภทก็มีโอกาสเกิดขึ้นได้ภายในหนึ่งทศวรรษ ที่ต้องย้ำคือ ระดับ 2 ไม่ใช่เหตุการณ์ที่เกิดขึ้นครั้งเดียวแล้วจบ แต่เป็นช่วงที่ค่อย ๆ ขยายกว้างขึ้นเรื่อย ๆ องค์กรที่มองข้ามระดับนี้ว่าเป็นแค่ทางผ่าน อาจพลาดสัญญาณแรก ๆ ที่สำคัญ ซึ่งจะเป็นตัวชี้ว่าบริษัทใดพร้อมจะได้ประโยชน์จากระดับ 3 เมื่อถึงเวลานั้น

3.2 ก้าวสู่การประมวลผลเชิงควอนตัมแบบทนทานต่อข้อผิดพลาด (Towards Fault-Tolerant Quantum Computing)

เพื่อให้บรรลุความได้เปรียบเชิงควอนตัมในเชิงพาณิชย์ เราจำเป็นจะต้องมีระบบที่ทั้งใหญ่และเสถียรเพื่อให้สามารถทำงานได้อย่างน่าเชื่อถือ ซึ่งเป้าหมายสูงสุดของการพัฒนาฮาร์ดแวร์ควอนตัมเป็นที่รู้จักกันในชื่อของ คอมพิวเตอร์ควอนตัมแบบทนทานต่อข้อผิดพลาด (Fault-Tolerant Quantum Computer หรือ FTQC) ซึ่งเป็นเครื่องจักรที่มีขีดความสามารถในการตรวจจับและแก้ไขข้อผิดพลาดของตนเองได้แบบเรียลไทม์ และสามารถประมวลผลคำสั่งทุกรูปแบบได้ตามที่คาดหวัง แม้ฮาร์ดแวร์จะก้าวหน้าแบบทวีคูณ แต่เรายังไปไม่ถึงยุคของ FTQC และหนทางข้างหน้ายังอีกยาวไกล การแข่งขันระดับโลกเพื่อสร้างเครื่องที่เชื่อถือได้เครื่องแรกจึงเปรียบได้กับการวิ่งมาราธอนทางวิศวกรรมดังนั้น สำหรับผู้บริหารจำเป็นต้องเข้าใจลำดับขั้นต่อไปนี้ เพื่อใช้ประเมินพาดหัวข่าวเรื่องความก้าวหน้าครั้งสำคัญ ที่มักเห็นตามสื่ออย่างรู้เท่าทัน

3.2.1 คอมพิวเตอร์ควอนตัมแบบทนทานต่อข้อผิดพลาด (Fault-Tolerant Quantum Computers) คืออะไร?

คิวบิตทางกายภาพ หรือ Physical Qubit เพียงหนึ่งหน่วย ซึ่งเป็นฮาร์ดแวร์พื้นฐาน เช่น วงจรตัวนำยวดยิ่ง ไอออนที่ถูกดักจับ หรืออะตอมเป็นกลาง มีธรรมชาติที่อ่อนไหวต่อสิ่งรบกวนแม้แต่คิวบิตที่ถูกออกแบบมาอย่างดีที่สุดก็อาจจะประมวลผลผิดพลาดได้ เพื่อก้าวข้ามข้อจำกัดนี้ เราจึงใช้กลยุทธ์ที่เรียกว่า การแก้ไขข้อผิดพลาดทางควอนตัม (Quantum Error Correction)

เราสามารถเปรียบเทียบการพัฒนาไปสู่ระบบ FTQC กับโครงสร้างขององค์กรธุรกิจได้ดังนี้:

- **คิวบิตทางกายภาพ หรือ Physical Qubit (เปรียบเสมือน พนักงานรายบุคคล):** พนักงานคนหนึ่งอาจมีทักษะสูง แต่ก็ยังมีโอกาสทำงานผิดพลาดได้ หากการดำเนินการทั้งหมดขององค์กรขึ้นอยู่กับคนเพียงคนเดียวที่ห้ามผิดพลาดเลย ระบบก็ย่อมล้มเหลวในท้ายที่สุด
- **คิวบิตเชิงตรรกะ หรือ Logical Qubit (เปรียบเสมือน ทีมงานที่มีประสิทธิภาพสูง):** คือกลุ่มของคิวบิตทางกายภาพคุณภาพสูงที่ทำงานสอดประสานกัน เปรียบเสมือนทีมงานมืออาชีพที่จะคอยตรวจสอบงานของกันและกัน และแก้ไขข้อผิดพลาดทันทีที่เกิดขึ้น แต่เพื่อให้ระบบนี้ทำงานได้ พนักงานรายบุคคลจะต้องมีระดับความสามารถขั้นต่ำถึงเกณฑ์มาตรฐานที่กำหนด หากพนักงานแต่ละคนมีแนวโน้มที่จะทำผิดพลาดมากเกินไป การเพิ่มจำนวนคนจะยิ่งสร้างความวุ่นวายให้กับระบบ
- **FTQC (เปรียบเสมือน องค์กรที่ขับเคลื่อนได้อย่างเต็มรูปแบบ):** การมีทีมงานที่ดีเพียงไม่กี่ทีมถือเป็นจุดเริ่มต้น แต่ก็ยังไม่เพียงพอที่จะขับเคลื่อนองค์กรขนาดใหญ่ได้ ตัวอย่างเช่น ธนาคาร คอมพิวเตอร์ควอนตัมแบบทนทานต่อข้อผิดพลาด เปรียบเสมือนบริษัทขนาดใหญ่ที่มีทีมงานมืออาชีพหลายร้อยทีมทำงานร่วมกันอย่างเป็นระบบ โดยได้รับการสนับสนุนจากโครงสร้างพื้นฐาน (Universal gates) ที่เอื้อให้สามารถดำเนินโปรเจกต์ระยะยาวที่ซับซ้อนได้ โดยที่ทั้งองค์กรจะไม่ล่มสลายลงเพียงเพราะความผิดพลาดเพียงครั้งเดียว

สถานะปัจจุบัน: ขณะนี้เรากำลังอยู่ในช่วงเปลี่ยนผ่านจากยุคของพนักงานรายบุคคล ไปสู่ ทีมงานมืออาชีพ ในระยะเวลา 5 ปีนับจากนี้ จะเป็นเครื่องพิสูจน์ว่าอุตสาหกรรมจะสามารถบูรณาการทีมงานเหล่านี้ให้กลายเป็นองค์กรที่ขับเคลื่อนได้อย่างเต็มรูปแบบ ได้อย่างไร?

3.2.2 หมุดหมายเชิงกลยุทธ์: สิ่งที่ต้องติดตาม (Strategic Milestones: What to Monitor)

สำหรับผู้บริหารที่ติดตามความคืบหน้าของฮาร์ดแวร์ควอนตัม หมุดหมาย 5 ประการต่อไปนี้ถือเป็นสัญญาณที่ชัดเจนที่สุดของความก้าวหน้าที่แท้จริง สิ่งเหล่านี้ไม่ใช่เพียงตัวชี้วัดทางการตลาด แต่มันคือความท้าทายทางวิศวกรรมและเทคโนโลยีที่ต้องได้รับการแก้ไขตามลำดับ ก่อนที่การประมวลผลแบบทนทานต่อข้อผิดพลาด (Fault-tolerant computation) จะเกิดขึ้นได้จริง

หมุดหมายที่ 1: อัตราข้อผิดพลาดทางกายภาพต่ำกว่าเกณฑ์ความทนทาน (Physical Error Rates Below the Fault-Tolerance Threshold)

สรุปสำหรับผู้บริหาร (Executive TL;DR): นี่คือจุด "คุ้มทุน (Break-even)" หากอัตราข้อผิดพลาดลดลงต่ำกว่าจุดนี้ การเพิ่มจำนวนคิวบิตจะยิ่งทำให้คอมพิวเตอร์ฉลาดขึ้นอย่างแท้จริง แทนที่จะยิ่งทำให้เกิดสัญญาณรบกวนมากขึ้น

ความหมายในทางปฏิบัติ: ทุกการดำเนินการทางควอนตัม ตั้งแต่การเตรียมคิวบิต เกตแบบคิวบิตเดี่ยว (Single-qubit gates), เกตแบบสองคิวบิต (Two-qubit gates) และการวัดผล จะต้องทำงานโดยมีอัตราข้อผิดพลาดต่ำกว่าเกณฑ์ของรหัสการแก้ไขข้อผิดพลาดที่เลือกใช้ สำหรับแนวทางที่ได้รับความนิยมสูงสุดอย่าง Surface codes เกณฑ์นี้จะอยู่ที่ประมาณ 1% ต่อการดำเนินการ หากต่ำกว่าเกณฑ์นี้ การเพิ่มคิวบิตจะช่วยเพิ่มประสิทธิภาพได้จริง แต่หากสูงกว่าเกณฑ์ การเพิ่มคิวบิตจะยิ่งทำให้ระบบแย่ลง ในทางปฏิบัติ วิศวกรตั้งเป้าอัตราข้อผิดพลาดไว้ที่ราว 0.1% ซึ่งต่ำกว่าเกณฑ์อย่างสบาย เพื่อให้การแก้ไขข้อผิดพลาดไม่ต้องใช้คิวบิตเพิ่มเติมในจำนวนที่มากจนจัดการไม่ได้

หมุดหมายที่ 2: คิวบิตเชิงตรรกะที่ต่ำกว่าเกณฑ์ / การลดข้อผิดพลาดตามสเกล (Below-Threshold Logical Qubits / Error Suppression With Scale)

สรุปสำหรับผู้บริหาร (Executive TL;DR): นี่คือการยืนยันว่าทฤษฎีสามารถนำมาใช้งานได้จริง เป็นการพิสูจน์ว่าเครื่องจักรสามารถสเกลได้ และไม่ใช่เพียงแค่ความสำเร็จโดยบังเอิญในห้องปฏิบัติการ

ความหมายในทางปฏิบัติ: ชี้ให้เห็นว่าอัตราข้อผิดพลาดเชิงตรรกะ (Logical error rates)จะลดลงแบบทวีคูณ เมื่อมีการเพิ่มคิวบิตทางกายภาพ เข้าไปในระบบรหัสแก้ไขข้อผิดพลาด นี่คือข้อพิสูจน์ว่าการแก้ไขข้อผิดพลาดทางควอนตัมทำงานได้ตามที่ทฤษฎีคาดการณ์ไว้ หมายความว่าระบบสามารถทำงานได้ต่ำกว่าเกณฑ์ความทนทานต่อข้อผิดพลาดในรูปแบบที่สเกลได้ ไม่ใช่จำกัดอยู่แค่บนอุปกรณ์ที่ถูกปรับแต่งมาเป็นพิเศษเพียงเครื่องเดียว

หมุดหมายที่ 3: ชุดเกตอเนกประสงค์ที่ทนทานต่อข้อผิดพลาด (A Universal Fault-Tolerant Gate Set)

สรุปสำหรับผู้บริหาร (Executive TL;DR): นี่คือสะพานเชื่อมไปสู่ซอฟต์แวร์ หากปราศจากสิ่งนี้ คอมพิวเตอร์จะแก้ปัญหาได้เฉพาะทางเท่านั้น แต่เมื่อมีสิ่งนี้ มันจะสามารถรันอัลกอริทึมใด ๆ ก็ได้ ตัวอย่างเช่น อัลกอริทึมของชอร์ (Shor's) หรือ HHL เป็นต้น

ความหมายในทางปฏิบัติ: การสาธิตให้เห็นว่าทุกประเภทของการดำเนินการทางควอนตัมที่จำเป็นสำหรับการประมวลผลแบบอเนกประสงค์ สามารถทำงานพร้อมกับการแก้ไขข้อผิดพลาดแบบแอคทีฟได้ตลอดกระบวนการ ซึ่งรวมถึงกลุ่มเกตที่ไม่ใช่เกตคลิฟฟอร์ด (Non-Clifford gates) ที่ขึ้นชื่อเรื่องความยาก โดยเฉพาะ T-gate ซึ่งไม่สามารถดำเนินการในรูปแบบที่เรียบง่ายและได้รับการป้องกันเช่นเดียวกับการดำเนินการอื่น ๆ ในโครงร่างการแก้ไขข้อผิดพลาดที่ใช้กันทั่วไป จึงมักต้องถูกสร้างขึ้นผ่านกระบวนการที่ใช้ทรัพยากรสูงที่เรียกว่า Magic state distillation หรือ Magic state cultivation



หมุดหมายที่ 4: Magic State Distillation / Cultivation at Scale

สรุปสำหรับผู้บริหาร (Executive TL;DR): ในการออกแบบยุคแรก คาดว่าคิวบิตส่วนใหญ่ของเครื่องจะถูกใช้ไปเพียงเพื่อผลิต 'Magic states' หมุดหมายที่ 4 นี้คือการทำให้เครื่องจักรมีประสิทธิภาพมากพอจนเกิดความคุ้มค่าในเชิงพาณิชย์

ความหมายในทางปฏิบัติ: การสร้าง 'Magic states' ที่มีคุณภาพสูง ซึ่งเป็นสถานะทรัพยากรทางควอนตัมพิเศษที่ต้องใช้ในการสร้าง T-gates แบบทนทานต่อข้อผิดพลาด อย่างมีประสิทธิภาพและเพียงพอที่จะทำให้ภาระส่วนเกินของคิวบิตกายภาพไม่ครอบงำการทำงานของเครื่องจักรทั้งหมด ในสถาปัตยกรรมแบบรหัสพื้นผิว (surface code) ปัจจุบัน Magic state distillation ต้องใช้จำนวนคิวบิตทางกายภาพเป็นสัดส่วนที่มากที่สุดในระบบแบบทนทานต่อข้อผิดพลาด โดยการประเมินในระยะแรกชี้ให้เห็นว่า สำหรับการคำนวณเพื่อถอดรหัส RSA คิวบิตทางกายภาพส่วนใหญ่อย่างยิ่งจะถูกใช้ไปกับการผลิต Magic states เพียงอย่างเดียว แทนที่จะใช้ในการคำนวณหลัก เทคนิคใหม่ ๆ เช่น Magic state cultivation (2024) ได้ช่วยลดภาระส่วนนี้ลงอย่างมีนัยสำคัญแล้ว

หมุดหมายที่ 5: Sustained Fault-Tolerant Operation at Industrially Relevant Scale and Runtime

สรุปสำหรับผู้บริหาร (Executive TL;DR): นี่คือเป้าหมายสูงสุด ซึ่งเป็นจุดที่คอมพิวเตอร์ควอนตัมมีความพร้อมเต็มที่สำหรับสร้างความได้เปรียบเชิงควอนตัมในเชิงพาณิชย์ (ระดับ 3)

ความหมายในทางปฏิบัติ: คือเครื่องจักรที่สามารถตอบสนองเงื่อนไขทั้ง 4 ประการต่อไปนี้ได้พร้อมกัน:

มีจำนวนคิวบิตเชิงตรรกะ เพียงพอสำหรับอัลกอริทึมที่เราต้องการนำไปใช้ โดยปัจจุบันถูกประเมินไว้ที่ราว 1,400 คิวบิตสำหรับการถอดรหัส RSA-2048 และประมาณ 1,000-2,500 คิวบิตสำหรับการจำลองเคมี FeMoco ขึ้นอยู่กับวิธีการ (ดูหัวข้อ 3.3.3)

1. อัตราข้อผิดพลาดเชิงตรรกะ ต่ำเพียงพอสำหรับวงจร ที่กำหนดอัลกอริทึมของชอร์ อยู่ที่ระดับประมาณ 10^{-12}

2. สามารถประมวลผลได้อย่างต่อเนื่องตลอดรอบเวลาการทำงาน อย่างสมบูรณ์ ซึ่งอาจกินเวลานานหลักชั่วโมงหรือเป็นวัน

3. มีระบบควบคุมแบบคลาสสิก ที่ประมวลผลได้เร็วพอที่จะถอดรหัสข้อผิดพลาดและปรับแก้ได้แบบเรียลไทม์ โดยต้องไม่ทำงานล่าช้ากว่าอัตราการเกิดข้อผิดพลาดของคิวบิต

4. ตอนนี้เราขอนำเสนอไทม์ไลน์ของฮาร์ดแวร์สำหรับบริษัทผู้เล่นหลักในฟิลด์นี้ โปรดทราบว่ารายชื่อบริษัทด้านควอนตัมนี้อาจไม่ครอบคลุมทั้งหมด

ความคืบหน้าที่ซึ่งครอบคลุมหมุดหมายทางวิศวกรรม 5 อย่าง (ณ ไตรมาสที่สามของปี 2026)

บริษัท	M1 — อัตราข้อผิดพลาด	M2 — Logical Qubit	M3 — Universal FT Gate Set	M4 — Magic State Large Scale	M5 — Sustained FT Operation
IBM	สำเร็จ Heron r2/r3 (~0.1-0.3%)	สำเร็จ สาธิต qLDPC codes และการถอดรหัสแบบเรียลไทม์ความเร็วสูงแล้ว; ชิปทดสอบ Loon (พ.ย. 2025) รวมองค์ประกอบ FT สำคัญ; ยังไม่มีการตีพิมพ์ผลการขยายสเกลต่ำกว่าเกณฑ์ด้วย qLDPC codes	สำเร็จบางส่วน Clifford ได้; T-gate อยู่ระหว่างทำ; ก.ค. 2026: รัน T gate เชิงตรรกะ 468 ครั้งบนคิวบิตเชิงตรรกะ 70 ตัว (รหัสป้องกันข้อผิดพลาดขนาดเล็ก)	สำเร็จบางส่วน แผน distillation สเกลใหญ่ปี 26-27	ยังไม่เริ่ม Starling (2029)
Google	สำเร็จ Willow (<0.5%)	สำเร็จ การลดข้อผิดพลาดแบบทวีคูณ (Nature)	สำเร็จบางส่วน แสดงการดำเนินการ Clifford ต่ำกว่าเกณฑ์แล้ว; เทคนิค T-gate (Non-Clifford) ที่ได้รับการป้องกันยังอยู่ในระยะเริ่มต้นและสเกลเล็ก	สำเร็จบางส่วน Magic state cultivation (ทางเลือกที่ถูกกว่า distillation ซึ่งพัฒนาโดย Google) ยังไม่ได้แสดงในสเกลที่ใช้งานได้จริง	ยังไม่สำเร็จ เป้าหมาย 2029; สร้างฮาร์ดแวร์อะตอมเป็นกลางควบคู่ด้วยตั้งแต่ มี.ค. 2026
Quantinuum	สำเร็จ Helios (>99.9%) (99.921% สูงสุดในทุกแพลตฟอร์ม)	สำเร็จ 48 LQ บน Helios ที่อัตราส่วน ~2:1 ด้วยรหัสขนาดเล็ก; รายงานความเที่ยงตรงเชิงตรรกะใกล้ระดับ “Five-nines” (ส.ค. 2026); ยังไม่แสดงในสเกลว่าข้อผิดพลาดลดลงเมื่อรหัสใหญ่ขึ้น	สำเร็จ ชุดเกตอเนกประสงค์ที่แก้ไขข้อผิดพลาดเต็มรูปแบบรวม T-gate รายแรก (มิ.ย. 2025) ที่รหัสขนาดเล็ก; ข้อผิดพลาด T-gate ต่ำกว่าอัตราทางกายภาพ	สำเร็จบางส่วน ตั้งเป้า Sol (2027)	ยังไม่สำเร็จ Apollo (2029); ชิปกับดัก Sol (2027) อยู่ระหว่างการตรวจสอบ
Microsoft	มีข้อโต้แย้ง ประกาศ Majorana 1 (ก.พ. 2025) และ Majorana 2 (มิ.ย. 2026); นักฟิสิกส์อิสระยังโต้แย้งว่าได้แสดงคิวบิตเชิงทอพอโลยีที่ใช้งานได้จริงหรือไม่; แผนสำรองระยะสั้น: เครื่องอะตอมเป็นกลาง “Magne” ร่วมกับ Atom Computing (ปลายปี 2026)	ยังไม่สำเร็จ	ยังไม่สำเร็จ ทางทฤษฎี	ยังไม่สำเร็จ สัญญาด้านการออกแบบว่าจะมี Overhead ต่ำกว่า Surface codes มาก; ยังไม่ได้รับการพิสูจน์	ยังไม่สำเร็จ ตั้งเป้าคอมพิวเตอร์ควอนตัมที่ขยายสเกลได้ภายในปี 2029 (ประกาศ มิ.ย. 2026); ออกแบบสำหรับ 1 ล้านคิวบิตบนชิปเดียว; อยู่ในขั้นประเมินรอบสุดท้ายของ DARPA
IonQ	สำเร็จ แพลตฟอร์ม Barium: ความเที่ยงตรง two-qubit >99.9%; รายงาน 99.99% ในปี 2025 ด้วยเทคโนโลยี Oxford Ionics	สำเร็จบางส่วน กำลังดำเนินการ	สำเร็จบางส่วน แยกรายเกต	ยังไม่สำเร็จ ตั้งเป้าปี 2027	ยังไม่สำเร็จ เป้าหมาย 2028
QuEra	สำเร็จ Harvard-MIT-QuEra 2025: การแก้ไขข้อผิดพลาดต่ำกว่าเกณฑ์บนอะเรย์สูงสุด 448 อะตอม	สำเร็จ ผลงานนำโดย Harvard 2025 (Nature): ประสิทธิภาพเชิงตรรกะต่ำกว่าเกณฑ์; รันอัลกอริทึมบน LQ สูงสุด 96 ตัว; ผล Harvard-MIT แยกต่างหาก: อะเรย์ 3,000 คิวบิตทำงานต่อเนื่อง 2+ ชม.	สำเร็จบางส่วน Distillation (2025)	สำเร็จบางส่วน ล้ำหน้าจุดนี้	ยังไม่สำเร็จ เป้าหมาย 2030; รายงานการเข้ารหัสแบบกะทัดรัด ~2:1 สำหรับหน่วยความจำควอนตัม (เม.ย. 2026)

M = Milestone | LQ = Logical Qubits | FT = Fault-Tolerant | Sources: company roadmaps and public announcements as of the third quarter of 2026. M3 partial credit requires Clifford gates demonstrated fault-tolerantly; full credit requires T-gate confirmed below physical error rate.



ประเด็นที่ควรเน้นจากการเปรียบเทียบข้ามบริษัท:

Quantinuum เป็นผู้นำทางวิทยาศาสตร์ที่ชัดเจนใน Milestone 1–3 Quantinuum เป็นบริษัทแรกที่สาธิตชุดเกตอเนกประสงค์ที่แก้ไขข้อผิดพลาดได้อย่างสมบูรณ์ (M3) แม้จะยังเป็นสเกลเล็ก และรายงานความเที่ยงตรงของเกตแบบสองคิวบิตสูงที่สุดในทุกแพลตฟอร์ม การเข้ารหัสแบบกะทัดรัดที่อัตราส่วน 2:1 บน Helios นั้นมีประสิทธิภาพสูง แต่ใช้รหัสขนาดเล็ก บททดสอบถัดไปคือข้อผิดพลาดจะยังคงลดลงต่อเนื่องหรือไม่เมื่อรหัสมีขนาดใหญ่ขึ้น ทั้งนี้ ทีมอะตอมเป็นกลาง (Harvard/QuEra) ได้รายงานการเข้ารหัสแบบกะทัดรัดในระดับใกล้เคียงกันแล้วเช่นกัน

Google และ QuEra เป็นผู้นำใน M2 ทั้งสองบริษัทได้ตีพิมพ์หลักฐาน (Peer-reviewed) ถึง Exponential Error Suppression ด้วยสเกลถือเป็นการตรวจสอบความถูกต้องทางทฤษฎีที่สำคัญที่สุดว่า FTQC สามารถสร้างได้จริงทางกายภาพ ผลงานการทำงานต่อเนื่อง 2 ชั่วโมงของอะเรย์ 3,000 อะตอมโดย Harvard–MIT โดยมี QuEra เป็นพันธมิตรใกล้ชิด คือการสาธิตเวลาการทำงานที่แข็งแกร่งที่สุดในขณะนี้

Microsoft คือตัวแปรอิสระ (Wildcard) ในทางทฤษฎี สถาปัตยกรรม Topological มอบเส้นทางที่มีประสิทธิภาพสูงสุดสู่ M4 และ M5 Overhead ในการแก้ไขข้อผิดพลาดที่ต่ำกว่าอย่างมากจะถือเป็นการพลิกโฉมวงการ แต่พวกเขาก็ตามหลังมากที่สุดในด้าน Milestone ที่ได้สาธิตไว้ และผลลัพธ์ Majorana 1 (2025) และ Majorana 2 (มิ.ย. 2026) ของพวกเขายังคงถูกโต้แย้งโดยนักฟิสิกส์อิสระ แม้ว่าขณะนี้ Microsoft จะตั้งเป้าสร้างเครื่องที่ขยายสเกลได้ภายในปี 2029 แล้วก็ตาม หากสถาปัตยกรรมนี้ใช้ได้ตามอ้าง Microsoft อาจก้าวข้ามทุกคน หากไม่เป็นเช่นนั้น พวกเขาจะตามหลังไปหลายปี โปรดทราบว่าเอกสารที่ตีพิมพ์ได้รับการวิจารณ์อย่างมากและต้องใช้ความระมัดระวังเป็นพิเศษในการตีความผลลัพธ์

IBM มีเส้นทางที่น่าเชื่อถือและละเอียดที่สุดสู่แผนงาน M5 ขององค์กรมีรายละเอียดที่ชัดเจนที่สุดและจัดส่งได้ตามกำหนดการอย่างสม่ำเสมอที่สุด Starling (2029) และ Blue Jay (2033+) ระบุเป้าหมายด้านประสิทธิภาพที่เป็นรูปธรรมอย่างที่ไม่มีบริษัทอื่นเทียบได้ในความเฉพาะเจาะจง IBM ตอกย้ำเส้นทางนี้ในเดือนพฤษภาคม 2026 ด้วยแผนลงทุนด้านควอนตัมมากกว่า 1 หมื่นล้านดอลลาร์ภายในห้าปี ซึ่งรวมถึงโรงงานผลิตชิปควอนตัมแห่งใหม่ในสหรัฐฯ (Anderon) ที่ได้รับการสนับสนุนจากกระทรวงพาณิชย์สหรัฐฯ [16]

ช่องว่างที่สำคัญที่สุดคือ M4 ทุกบริษัทบรรลุเพียงบางส่วนอย่างมากที่สุดในการผลิต Magic State ในระดับใหญ่ และนี่คือหมุดหมาย ที่ครอบงำภาระส่วนเกินของคิวบิตกายภาพ ความก้าวหน้าในจุดนี้ในปี 2026-2027 จะเป็นดัชนีชี้นำ ที่แข็งแกร่งที่สุดว่าบริษัทใดจะข้ามเส้น M5 ได้เป็นรายแรก

3.3 การพัฒนา Algorithm และความต้องการทรัพยากร

หากมุ่งความสำคัญไปที่ฮาร์ดแวร์ เราจะเห็นภาพเชิงกลยุทธ์เพียงครึ่งเดียว ช่องว่างควอนตัม คือระยะห่างระหว่างพลังของคอมพิวเตอร์ควอนตัมในปัจจุบัน กับพลังที่งานมูลค่าสูงต้องการ ช่องว่างนี้กำลังแคบลงจากแรงผลักดันสองด้านที่มาบรรจบกัน ด้านหนึ่งคือการสร้างเครื่องที่ทรงพลังขึ้น (ฮาร์ดแวร์) อีกด้านคือการเขียนคำสั่งที่มีประสิทธิภาพขึ้น (ซอฟต์แวร์)

3.3.1 การทดลองที่ล้ำสมัยที่สุด (ณ ไตรมาสที่สามของปี 2026)

หมุดหมายต่อไปนี้แสดงถึงการเปลี่ยนผ่านจากความสงสัยในห้องทดลองไปสู่ผลประโยชน์เชิงอุตสาหกรรม (Industrial utility)

การทดลอง	องค์กร / ฮาร์ดแวร์	สิ่งที่สาธิตได้	ผลลัพธ์สำคัญ	นัยสำคัญเชิงกลยุทธ์	แหล่งอ้างอิง
Random Circuit Sampling (RCS)	Google Quantum AI – Willow processor (105 คิวบิต)	ทดสอบมาตรฐาน Random circuit sampling	ทำงานสำเร็จในเวลา 5 นาที (ซูเปอร์คอมพิวเตอร์ต้องใช้ 10^{25} ปี)	ยืนยันการทำงานระดับควอนตัมในสเกลใหญ่	ประกาศ Willow ของ Google Quantum AI (ธ.ค. 2024)
อัลกอริทึม Quantum Echoes	Google Quantum AI – Willow chip	ศึกษาพลวัตควอนตัม (Quantum dynamics)	เร็วกว่าค่าประมาณคลาสสิกที่ดีที่สุด ราว 13,000 เท่าสำหรับการวัดเฉพาะนี้ (Nature, ต.ค. 2025); มี การพิสูจน์แนวคิดขนาดเล็กกว่าแยกต่างหากที่นำเทคนิคนี้ไปใช้กับโมเลกุลจริง 2 ชนิด	เปลี่ยนผ่านสู่อัลกอริทึมที่มีความหมายทางวิทยาศาสตร์	Google Quantum AI (ต.ค. 2025)
Universal Fault-Tolerant Gate Set	Quantinuum – H-series	ชุดเกตที่แก้ไขข้อผิดพลาดได้ครบถ้วน (Clifford, T-gate)	อัตราข้อผิดพลาด T-gate ต่ำกว่าระดับกายภาพ; แก้ไขแบบเรียลไทม์	เงื่อนไขสำคัญสุดท้ายสำหรับการประมวลผลแบบ Fault-tolerant	Quantinuum (มิ.ย. 2025)
การดำเนินงานอะตอมเป็นกลางต่อเนื่อง	Harvard-MIT (QuEra)	อะตอมในอะเรย์ 3,000 คิวบิต ทำงานต่อเนื่อง > 2 ชม.	ทำงานต่อเนื่องได้นานกว่า 2 ชั่วโมง (ในงานตีพิมพ์ปี 2025 ฉบับอื่น ทีม Harvard/QuEra รันอัลกอริทึมบน Logical qubits สูงสุด 96 ตัวด้วยประสิทธิภาพต่ำกว่าเกณฑ์และสาธิต Magic-state distillation เชิงตรรกะ)	แก้ไขปัญหาการสูญเสียอะตอมระหว่างการคำนวณ	Nature (2025) หลายฉบับ
เวิร์กโฟลว์ Hybrid QuantumHPC	RIKEN (Fugaku) + Quantinuum	เวิร์กโฟลว์รวมซูเปอร์คอมพิวเตอร์ + ควอนตัม	สำรวจปฏิกิริยาเคมีในชีวโมเลกุล	ควอนตัมในฐานะ Co-processor ภายในไปป์ไลน์ HPC	RIKEN & Quantinuum (2025)
Verified Quantum Advantage on Logical Qubits	IBM + มหาวิทยาลัยชิคาโก – โปรเซสเซอร์ IBM Heron	วงจรแบบมีโครงสร้าง (ไม่ใช่แบบสุ่ม) บน Logical qubits ที่มีการป้องกันข้อผิดพลาด 70 ตัว พร้อมกลไกในตัวสำหรับตรวจสอบว่าคำตอบเชื่อถือได้เพียงใด	~15 นาทีบนคอมพิวเตอร์ควอนตัม; การดำเนินการ two-qubit เชิงตรรกะ 2,415 ครั้ง และ T gate เชิงตรรกะ 468 ครั้ง; ข้อผิดพลาดเชิงตรรกะต่ำกว่าทางกายภาพ ~10 เท่า; ต่อมาคลัสเตอร์ GPU ขนาดใหญ่ทำได้ทัดเทียมใน ~37 นาที	แสดงให้เห็นว่าปัจจุบันคำกล่าวอ้างเรื่องความได้เปรียบถูกนำเสนอ—และถูกโต้แย้ง—อย่างเปิดเผยผ่าน “Quantum Advantage Tracker” แบบเปิดของ IBM; ผสานทั้งสเกล การป้องกันข้อผิดพลาด และความสามารถในการตรวจสอบ	IBM Newsroom (ก.ค. 2026); arXiv preprint
96 Verified Logical Qubits	QuEra Computing (448 อะตอม)	สร้าง 96 Logical Qubits (อัตราส่วน 4.7 Physical:1 Logical)	พิสูจน์ว่าอะตอมเป็นกลางสเกลได้เร็วกว่าและประหยัดกว่า	ก้าวสำคัญสู่ Fault-Tolerant เชิงพาณิชย์	Nature (ม.ค. 2026)
Record-breaking 2:1 Encoding	Quantinuum (Helios) + Microsoft	สร้าง 48 Logical Qubits (Color code/Iceberg)	ประสิทธิภาพการเข้ารหัสสูงสุด (2:1) ด้วยความแม่นยำ 99.92%	เหมาะสมที่สุดสำหรับ Enterprise ในระยะสั้น-กลาง	Quantinuum & Microsoft (พ.ย. 2025)
Quantum RNA Structure Prediction	IBM (Heron 156-qubit) ร่วมกับ Moderna	จำลองการพับตัวของ mRNA ขนาด 60 นิวคลีโอไทด์	กรอง Noise ออกจากวงจรความลึก 950 Non-local gates	Quantum Utility สร้างมูลค่าใน Drug Discovery ได้จริง	IBM / Moderna (มี.ค. 2026)

3.3.2 การปิดช่องว่างด้วยการออกแบบอัลกอริทึมที่ดีขึ้น

ดังที่ได้กล่าวไปข้างต้น ทรัพยากรควอนตัมที่จำเป็นในการดำเนินการอัลกอริทึมที่สำคัญสามารถลดลงได้มหาศาลเมื่อเวลาผ่านไป เนื่องจากนักวิจัยค้นพบวิธีการนำไปใช้งานที่มีประสิทธิภาพมากขึ้น การพัฒนาเหล่านี้อาจเกิดจากการออกแบบวงจร ที่ดีขึ้น การคำนวณทางเลขคณิตที่มีประสิทธิภาพกว่าเดิม การแก้ไขข้อผิดพลาดที่ได้รับการปรับปรุงหรือการคิดค้นเทคนิคอัลกอริทึมใหม่ทั้งหมด

ประเด็นเชิงกลยุทธ์ที่สำคัญคือ ความก้าวหน้าทางฮาร์ดแวร์ไม่ใช่ปัจจัยเดียวที่กำหนดขีดความสามารถทางควอนตัม แต่ความก้าวหน้าในการออกแบบอัลกอริทึมและการแก้ไขข้อผิดพลาดก็สามารถลดความต้องการจำนวนคิวบิตลงได้หลายลำดับขั้น กล่าวอีกนัยหนึ่งคือระยะห่างที่แท้จริงระหว่างฮาร์ดแวร์ในปัจจุบันกับการประยุกต์ใช้ควอนตัมที่มีประโยชน์เชิงพาณิชย์สามารถหดตัวลงได้อย่างรวดเร็ว เมื่อซอฟต์แวร์และทฤษฎีมีการพัฒนาอย่างต่อเนื่อง

ในช่วงทศวรรษที่ผ่านมา เราได้เห็นรูปแบบนี้เกิดขึ้นซ้ำแล้วซ้ำเล่า ข้อกำหนดด้านทรัพยากรสำหรับอัลกอริทึมควอนตัมระดับเรือธงหลายรายการลดลงอย่างมากเมื่อมีการแนะนำเทคนิคใหม่ ๆ เข้ามา ตัวอย่างที่เห็นได้ชัดเจนที่สุดคือ อัลกอริทึมของชอร์สำหรับการแยกตัวประกอบจำนวนเต็ม

กรณีศึกษา: วิวัฒนาการของทรัพยากรที่จำเป็นสำหรับการถอดรหัส RSA-2048

เหตุผลความสำคัญ: RSA-2048 เป็นหนึ่งในระบบเข้ารหัสแบบกุญแจสาธารณะที่ถูกนำไปใช้งานอย่างแพร่หลายที่สุด เช่น ในใบรับรองดิจิทัลและลายเซ็นดิจิทัล เมื่อรวมกับการเข้ารหัสแบบเส้นโค้งวงรี (Elliptic-curve cryptography หรือ ECC) ซึ่งรักษาความปลอดภัยให้กับการเชื่อมต่ออินเทอร์เน็ตส่วนใหญ่และคริปโทเคอร์เรนซีแทบทั้งหมด ระบบเหล่านี้ปกป้องโครงสร้างพื้นฐานทางดิจิทัลของโลกในสัดส่วนที่มหาศาล หากคอมพิวเตอร์ควอนตัมมีศักยภาพเพียงพอที่จะรัน Shor's algorithm ได้ ก็จะสามารถแยกตัวประกอบกุญแจ RSA-2048 ได้อย่างมีประสิทธิภาพ ส่งผลให้ระบบการเข้ารหัสที่เป็นมาตรฐานหลักนี้หมดความปลอดภัยลง ด้วยเหตุนี้ ความต้องการด้านทรัพยากรสำหรับการรันอัลกอริทึมของชอร์จึงถูกศึกษาและวิจัยอย่างเข้มข้นตลอดช่วงทศวรรษที่ผ่านมา ซึ่งผลลัพธ์แสดงให้เห็นถึงแนวโน้มที่ชัดเจน นั่นคือ จำนวนคิวบิตที่ประเมินว่าต้องใช้ลดลงอย่างรวดเร็ว

ปี	ทรัพยากรที่ประเมินไว้	ข้อมูลเชิงลึกสำคัญ
2012	วิเคราะห์โดย Surface-code analysis ของ Austin Fowler และคณะ: ~1 พันล้านคิวบิตทางกายภาพ	การประมาณค่า Fault-tolerant ในยุคแรกตั้งสมมติฐานเกี่ยวกับส่วนเผื่อ สำหรับการแก้ไขข้อผิดพลาดแบบอนุรักษ์นิยม
2019	การศึกษาโดย Craig Gidney และ Martin Ekerå (ตีพิมพ์ในวารสาร Quantum, 2021): ~20 ล้านคิวบิตทางกายภาพแบบมีสัญญาณรบกวน ใช้เวลาประมวลผล ~8 ชั่วโมง	การปรับปรุงครั้งใหญ่ในวงจรเลขคณิตแบบมอดูลาร์ (Modular arithmetic circuits) ช่วยลดต้นทุนทรัพยากรลงได้มหาศาล
2025	การวิเคราะห์ล่าสุดโดย Craig Gidney แห่ง Google Quantum AI: <1 ล้านคิวบิตทางกายภาพ แบบมีสัญญาณรบกวน และ ~1,400 คิวบิตเชิงตรรกะ ใช้เวลาประมวลผล <1 สัปดาห์	นวัตกรรมที่รวมถึง Approximate residue arithmetic, yoked surface codes, และ magic-state cultivation
2026	สถาปัตยกรรม "Pinnacle" โดย Iceberg Quantum สตาร์ทอัพจากซิดนีย์ (Preprint ฉบับปรับปรุง พ.ค. 2026): ใช้คิวบิตทางกายภาพน้อยกว่า 100,000 ตัว โดยใช้เวลารันราวหนึ่งเดือน~150,000 คิวบิตสำหรับเวลารันราวหนึ่งสัปดาห์	ใช้รหัสแก้ไขข้อผิดพลาดแบบ qLDPC แทน Surface codes ตั้งสมมติฐานอัตราข้อผิดพลาด 0.1% และการดำเนินการที่เร็วมาก ยากต่อการสร้างทางวิศวกรรมมากกว่า เพราะต้องเชื่อมต่อคิวบิตที่อยู่ห่างกัน
2026 (ECC)	Google Quantum AI ร่วมกับ Ethereum Foundation และ Stanford (White paper, มี.ค. 2026) เป้าหมาย เส้นโค้งวงรี 256 บิต Logical qubits น้อยกว่า 1,200–1,450 ตัว คิวบิตทางกายภาพน้อยกว่า 500,000 ตัว เวลารันหลักนาที	ถูกกว่าการประเมิน ECC ก่อนหน้าราว 10 เท่า Google ไม่เปิดเผยวงจรโจมตี แต่เผยแพร่ Zero-knowledge proof แทน เพื่อให้บุคคลภายนอกสามารถตรวจสอบคำกล่าวอ้างได้โดยไม่ต้องรู้วิธีโจมตี

การสอดคล้องกับแผนงานฮาร์ดแวร์ของอุตสาหกรรม: สิ่งที่น่าสนใจคือ การประเมินด้านอัลกอริทึมล่าสุดขณะนี้อยู่ในระดับที่ใกล้เคียงกับเป้าหมายการขยายสเกลที่ประกาศโดยบริษัทฮาร์ดแวร์ควอนตัมหลายแห่งแล้ว

- IonQ คาดการณ์ว่าจะมีระบบที่มีคิวบิตเชิงตรรกะประมาณ 1,600 ตัวภายในปี 2028 ล่าสุดบริษัทระบุว่าคาดว่าจะบรรลุจำนวนคิวบิตเชิงตรรกะที่เกี่ยวข้องกับการถอดรหัส RSA-2048 ได้ในปี 2028–2029
- สถาปัตยกรรม Blue Jay ระยะยาวของ IBM เป้าหมายช่วงต้นทศวรรษ 2030 มุ่งเป้าหมายที่คิวบิตเชิงตรรกะประมาณ 2,000 ตัว ซึ่งจะเกินกว่าความต้องการที่ถูกประเมินไว้

ข้อควรระวัง: จำนวนคิวบิตเชิงตรรกะของแต่ละบริษัทไม่สามารถนำมาเปรียบเทียบกันโดยตรงได้ เนื่องจากคิวบิตเชิงตรรกะของแต่ละบริษัทมีอัตราข้อผิดพลาดที่แตกต่างกันและการถอดรหัส RSA ยังต้องการอัตราข้อผิดพลาดที่ต่ำมากรวมถึงการทำงานที่ยาวนานและเสถียรด้วย ตัวอย่างเช่น Starling ของ IBM (2029, Logical qubits ~200 ตัว) ยังห่างไกลจากจำนวน ~1,200–1,400 คิวบิตเชิงตรรกะ ที่การประเมิน RSA และ ECC ล่าสุดต้องการอยู่มาก

จากแผนงานของบริษัทต่าง ๆ ที่เผยแพร่อยู่ตอนนี้ คอมพิวเตอร์ควอนตัมอาจเจาะระบบเข้ารหัส RSA-2048 ได้ในช่วงต้นถึงกลางทศวรรษ 2030 โดยไม่ต้องรอการค้นพบครั้งใหม่ เพียงแค่ต้องต่อยอดจากความรู้ที่มีอยู่แล้วในปัจจุบัน เพื่อให้เห็นภาพ ในปี 2026 Global Risk Institute สำรวจความเห็นผู้เชี่ยวชาญ 26 คน พบว่ามีโอกาส 28-49% ที่จะมีคอมพิวเตอร์ควอนตัมที่เจาะระบบเข้ารหัสได้ภายใน 10 ปี [12] ขณะเดียวกัน Google (มีนาคม 2026) และ Microsoft (มิถุนายน 2026) ต่างตั้งเป้าว่าจะเปลี่ยนระบบของตัวเองไปใช้การเข้ารหัสแบบใหม่ที่ทนต่อคอมพิวเตอร์ควอนตัมให้เสร็จภายในปี 2029

3.3.3 Resource requirements of the current day

เราขอยกตัวอย่างความต้องการทรัพยากรปัจจุบันของอัลกอริทึมควอนตัมที่เป็นที่รู้จักบางตัวเพื่อแก้ปัญหาที่นำไปใช้ได้จริง โปรดทราบว่าตัวเลขเหล่านี้เป็นการประเมินที่ตีพิมพ์สำหรับเครื่อง Fault-tolerant ในอนาคต ไม่ใช่ฮาร์ดแวร์ในปัจจุบัน และยังคงเปลี่ยนแปลงตามเทคนิคที่พัฒนาขึ้นอย่างต่อเนื่อง

อัลกอริทึม	โจทย์ปัญหาเป้าหมาย	ผลกระทบเชิงปฏิบัติ	ประมาณการ Logical Qubits	ประมาณการเวลาประมวลผล
Shor's Algorithm	การแยกตัวประกอบ RSA-2048 / ECC 256 บิต	ความมั่นคงปลอดภัยทางไซเบอร์: ทำให้มาตรฐานการเข้ารหัสระดับโลกในปัจจุบัน (RSA/ECC) หมดความปลอดภัย	~1,200–1,450 (ECC); ~1,400 (RSA)	หลักนาที (ECC) ถึง < 1 สัปดาห์ (RSA) บนคิวบิตทางกายภาพ ~0.1–1 ล้านตัว
Quantum Phase Estimation (QPE)	การจำลองโมเลกุล FeMoco	ความยั่งยืน/ESG: การค้นพบตัวเร่งปฏิกิริยาสำหรับปุ๋ยประสิทธิภาพสูงและการดักจับคาร์บอน	~1,000 – 2,500 (ขึ้นอยู่กับวิธีการ)	หลักชั่วโมงถึงหลักวัน (การประเมินปี 2021 ที่ถูกอ้างอิงอย่างกว้างขวางฉบับหนึ่ง: ~4 วัน) [8]
Quantum Amplitude Estimation	การกำหนดราคาอนุพันธ์ที่ซับซ้อนด้วยวิธีมอนติคาร์โล	การกำหนดราคาอนุพันธ์และการคำนวณความเสี่ยงที่รวดเร็วขึ้น [14]	~8,000–11,500 [14]	เป้าหมายสำหรับความได้เปรียบคือ ~1 วินาที ซึ่งต้องใช้ชั้น T-gate แบบลำดับราว 54–82 ล้านชั้นต่อวินาที—เกินกว่าฮาร์ดแวร์ปัจจุบันอย่างมาก [14]
Grover's Algorithm	การค้นหาข้อมูลแบบไม่มีโครงสร้าง	ข่าวกรอง/ข้อมูล: การเร่งความเร็วเชิงกำลังสอง (Quadratic speedup) สำหรับปัญหาการค้นหาแบบ Brute-force; ในทางปฏิบัติ Overhead จากการแก้ไขข้อผิดพลาดอาจหักล้างประโยชน์ส่วนใหญ่นี้ไป [13]	ขึ้นอยู่กับโจทย์ปัญหา	มักช้ากว่าทางเลือกแบบคลาสสิกที่ขนาดปัญหาตามจริง

3.4 กรณีการใช้งานเทียบกับความได้เปรียบเชิงควอนตัมที่แท้จริง (Use Cases Versus Actual Quantum Advantages)

กรณีศึกษาจำนวนมากที่ปรากฏในงานวิจัยด้านการประมวลผลควอนตัมทุกวันนี้ ควรมองว่าเป็นการสาธิตเพื่อสำรวจความเป็นไปได้ มากกว่าจะเป็นตัวอย่างของความได้เปรียบเชิงควอนตัมที่แท้จริง เพราะในกรณีส่วนใหญ่ปัญหาเดียวกันนี้สามารถแก้ไขได้ด้วยคอมพิวเตอร์แบบดั้งเดิม การสาธิตเหล่านี้จึงไม่ใช่หลักฐานว่าคอมพิวเตอร์ควอนตัมทำงานได้ดีกว่าคอมพิวเตอร์แบบดั้งเดิมแล้ว

ประเด็นนี้นำไปสู่คำถามสำคัญที่ผู้บริหารมักจะตั้งข้อสงสัยเสมอว่า: “ในเมื่อเครื่องจักรยังไม่สามารถทำงานได้อย่างเต็มประสิทธิภาพ แล้วทำไมเราถึงต้องเริ่มใช้งานตั้งแต่ตอนนี้?”

คำตอบของคำถามนี้อยู่ที่ ความพร้อมสู่ยุคควอนตัม (Quantum Readiness) [ดูเพิ่มเติมในส่วนที่ 1.3]

การทดลองด้านควอนตัมในปัจจุบันมักจะอยู่ในรูปแบบของกระบวนการทำงานแบบไฮบริด ซึ่งคอมพิวเตอร์คลาสสิกจะรับหน้าที่ประมวลผลงานส่วนใหญ่ ในขณะที่โปรเซสเซอร์ควอนตัมจะประมวลผลเฉพาะรูทีนย่อยที่มีความเฉพาะเจาะจงขนาดเล็ก ส่งผลให้เป้าหมายในขณะนี้ไม่ได้อยู่ที่การทำงานให้เหนือกว่าซูเปอร์คอมพิวเตอร์คลาสสิก แต่คือการเตรียมความพร้อมให้กับระบบ อัลกอริทึม และทีมงาน เพื่อรอรับช่วงเวลาที่ฮาร์ดแวร์ควอนตัมซึ่งสามารถสเกลได้ (Scalable quantum hardware) พร้อมออกสู่ตลาด

ในมุมมองนี้ โครงการต่าง ๆ ในปัจจุบันจึงทำหน้าที่หลักในการเป็นแพลตฟอร์มสำหรับการพัฒนาเพื่อพิสูจน์แนวคิด องค์กรต่าง ๆ ใช้โปรแกรมจำลองระบบควอนตัม (Quantum simulators) หรือฮาร์ดแวร์ขนาดเล็ก เพื่อออกแบบชิ้นส่วนในไปป์ไลน์การคำนวณ (Computational pipelines) ของตัวเองขึ้นใหม่ เพื่อให้สามารถทำงานร่วมกับโปรเซสเซอร์ควอนตัมในอนาคตได้ เมื่อเครื่องจักรขนาดใหญ่ เช่น โปรเซสเซอร์ที่มีคิวบิตคุณภาพสูงนับพันคิวบิต พร้อมใช้งาน สถาบันที่ได้พัฒนาความเชี่ยวชาญเหล่านี้ไว้ล่วงหน้าแล้ว จะสามารถบูรณาการเทคโนโลยีนี้เข้ากับองค์กรได้อย่างรวดเร็ว

สิ่งที่สำคัญไม่แพ้กันคือการพัฒนาทุนมนุษย์ การประมวลผลเชิงควอนตัมต้องการวิธีคิดเกี่ยวกับการประมวลผลที่แตกต่างไปจากเดิมอย่างสิ้นเชิง โดยต้องอาศัยการผสมผสานองค์ความรู้จากฟิสิกส์ คณิตศาสตร์ วิทยาการคอมพิวเตอร์ และความเชี่ยวชาญเฉพาะทางในอุตสาหกรรม การสร้างขีดความสามารถนี้ภายในองค์กรต้องใช้เวลา ดังนั้น การเปลี่ยนผ่านในครั้งนี้อาจสร้างการพลิกโฉม มากกว่าการเปิดรับเทคโนโลยี AI เสียด้วยซ้ำ เนื่องจากมันเรียกร้องให้องค์กรต้องรื้อระบบวิธีคิดใหม่ทั้งหมด ว่าโจทย์ปัญหาการคำนวณบางประเภทควรถูกตั้งสมมติฐานและแก้ไขปัญหาอย่างไร

3.4.1 กรณีศึกษา: การหาค่าเหมาะสมที่สุดของพอร์ตโฟลิโอภายใต้เงื่อนไขข้อจำกัดที่ SCBX (Case-study: Portfolio Optimization with Constraints at SCBX)

หนึ่งในตัวอย่างของโครงการริเริ่มเพื่อเตรียมความพร้อมสู่ยุคควอนตัม คืองานวิจัยเกี่ยวกับการหาค่าเหมาะสมที่สุดของพอร์ตโฟลิโอ (Portfolio optimization) ที่เรากำลังดำเนินการอยู่ ซึ่งถือเป็นโจทย์ปัญหาที่สถาบันการเงินระดับโลกให้ความสนใจศึกษาอย่างกว้างขวาง วัตถุประสงค์ของงานวิจัยนี้คือการสร้างพอร์ตการลงทุนที่สามารถรักษาสมดุลระหว่างผลตอบแทนที่คาดหวังกับระดับความเสี่ยง ในขณะเดียวกันก็ยังต้องตอบสนองต่อเงื่อนไขข้อจำกัดในทางปฏิบัติ ที่หลากหลายได้อย่างครบถ้วน

งานวิจัยในปัจจุบันของเรามุ่งเน้นไปที่การออกแบบวงจรควอนตัมที่มีประสิทธิภาพสูงขึ้นสำหรับกลุ่มโจทย์ปัญหาการหาค่าเหมาะสมที่สุดประเภทนี้ โดยเฉพาะอย่างยิ่ง เรากำลังศึกษาวิธีการฝัง ข้อจำกัดในโลกแห่งความเป็นจริง เช่น ขีดจำกัดด้านงบประมาณ (Budget limitation) หรือกฎเกณฑ์การจัดสรรสินทรัพย์ ลงไปในการดำเนินการทางควอนตัม (Quantum operations) โดยตรง เป้าหมายของผลงานชิ้นนี้ไม่ได้อยู่ที่การสร้างผลลัพธ์ที่เหนือกว่าอัลกอริทึมการหาค่าเหมาะสมที่สุดแบบคลาสสิกในทันที

แต่ในทางกลับกัน เป้าหมายที่แท้จริงคือการพัฒนาโครงสร้างการตั้งสมการโจทย์ปัญหาทางการเงินให้สอดคล้องกับธรรมชาติของเทคโนโลยีควอนตัม(Quantum-native formulations) เพื่อเป็นหลักประกันว่าเมื่อโปรเซสเซอร์ควอนตัมที่มีขนาดใหญ่ขึ้นและมีความน่าเชื่อถือสูงขึ้น พร้อมให้ใช้งาน อัลกอริทึมและกระบวนการทำงานที่จำเป็นต่อการดึงศักยภาพของเครื่องจักรเหล่านั้นมาใช้ จะถูกเตรียมการไว้พร้อมแล้วอย่างสมบูรณ์

3.5 ศักยภาพการประยุกต์ใช้งานในภาคการเงิน (Potential Applications In Finance)

สื่อมักกล่าวถึงเทคโนโลยีการประมวลผลเชิงควอนตัมว่ามีศักยภาพในการพลิกโฉม ภาคการเงิน อย่างไรก็ตาม ในมุมมองทางวิทยาศาสตร์ งานวิจัยเชิงลึก ด้านการเงินเชิงควอนตัมยังคงมีอยู่อย่างจำกัด และกรณีการใช้งานที่ถูกนำเสนอจำนวนมากยังคงอยู่ในระยะเริ่มต้นของการสำรวจ



สิ่งนี้ได้สร้างโอกาสครั้งสำคัญให้กับสถาบันการเงินในการเข้ามามีส่วนร่วมกับงานวิจัยระดับรากฐานอย่างจริงจัง ซึ่งอาจเป็นตัวกำหนดทิศทางการประยุกต์ใช้เทคโนโลยีควอนตัมในภาคการเงินในอนาคต โดยมีกลุ่มงานหลายด้านที่ได้รับการประเมินอย่างกว้างขวางว่ามีศักยภาพสูง [3]:

1. การบริหารความเสี่ยงผ่านการจำลองมอนติคาร์โล (Risk Management via Monte Carlo Simulations): การคำนวณความเสี่ยงทางการเงินจำนวนมากต้องพึ่งพาการจำลองมอนติคาร์โล ซึ่งเป็นการประเมินการแจกแจงความน่าจะเป็น (Probability distribution) ของผลลัพธ์ตลาดที่อาจเกิดขึ้น การจำลองเหล่านี้มีต้นทุนการประมวลผลสูง และมักถูกนำมาใช้เพื่อคำนวณตัวชี้วัด เช่น มูลค่าความเสี่ยง (Value-at-Risk หรือ VaR) ในทางทฤษฎี อัลกอริทึมควอนตัมสำหรับการประเมินค่าแอมพลิจูด (Amplitude estimation) อาจช่วยเร่งความเร็วในการคำนวณมอนติคาร์โลบางประเภท ซึ่งมีศักยภาพในการลดเวลาการคำนวณจากหลายชั่วโมงให้อยู่ในระดับใกล้เคียงเรียลไทม์ แม้ว่าการประเมินที่ตีพิมพ์จะชี้ว่าสิ่งนี้ต้องใช้เครื่อง Fault-tolerant ขนาดใหญ่และเร็วมาก [14] หากสามารถนำไปใช้งานจริงในสเกลขนาดใหญ่ สิ่งนี้จะช่วยยกระดับความเร็วและความรวดเร็วในการตอบสนอง ของระบบประเมินความเสี่ยงได้อย่างมหาศาล

2. การตรวจจับการทุจริต (Fraud Detection): อีกหนึ่งศักยภาพการใช้งานอยู่ที่การเรียนรู้ของเครื่องเชิงควอนตัม (Quantum machine learning หรือ QML) ซึ่งมีการใช้อัลกอริทึมควอนตัมเพื่อวิเคราะห์ชุดข้อมูลขนาดใหญ่และตรวจจับรูปแบบที่มีความซับซ้อน ในระบบการเงิน เทคนิคดังกล่าวอาจช่วยระบุความผิดปกติที่สังเกตได้ยาก ในข้อมูลธุรกรรม ซึ่งอาจเป็นสัญญาณบ่งชี้ถึงพฤติกรรมการทุจริตหรือความเสี่ยงเชิงระบบ แม้ว่าในปัจจุบันจะยังอิงอยู่กับทฤษฎีเป็นส่วนใหญ่ แต่สาขานี้ถือเป็นจุดตัดสำคัญระหว่างวิทยาการข้อมูล ความมั่นคงปลอดภัยทางไซเบอร์ และควอนตัมคอมพิวติง ซึ่งควรค่าแก่การสืบค้นและวิจัยเพิ่มเติม อุปสรรคในทางปฏิบัติคือ การโหลดข้อมูลคลาสสิกปริมาณมากเข้าสู่คอมพิวเตอร์ควอนตัมนั้นช้าในตัวเอง ซึ่งอาจกระทบกับการเร่งความเร็วที่คาดหวังไว้ได้

3. การกำหนดราคาสินทรัพย์ (Asset Pricing): การกำหนดราคาตราสารอนุพันธ์ทางการเงิน ที่มีความซับซ้อน มักต้องอาศัยการแก้ระบบสมการเชิงอนุพันธ์ ขนาดใหญ่ หรือการหาปริพันธ์เชิงตัวเลขในมิติสูง อัลกอริทึมควอนตัมสำหรับระบบสมการเชิงเส้น และการจำลองเชิงควอนตัม (Quantum simulation) อาจนำเสนอแนวทางใหม่ ๆ ในการแก้ปัญหาเหล่านี้ด้วยความแม่นยำเชิงตัวเลข ที่ดียิ่งขึ้น แม้ว่าการสาธิตการใช้งานจริงจะยังคงมีจำกัด แต่ในท้ายที่สุด เทคนิคเหล่านี้ก็อาจช่วยยกระดับความแม่นยำและประสิทธิภาพของแบบจำลองการกำหนดราคาตราสารอนุพันธ์ได้

4. การหาค่าเหมาะสมที่สุดของพอร์ตโฟลิโอ (Portfolio Optimization): ยังคงเป็นหนึ่งในการประยุกต์ใช้งานด้านการเงินของเทคโนโลยีควอนตัมคอมพิวติงที่มีการศึกษาอย่างกว้างขวางที่สุด อย่างไรก็ตาม ความสำคัญของโจทย์ปัญหานี้มีความแตกต่างกันอย่างมากในแต่ละสถาบัน โดยขึ้นอยู่กับกลยุทธ์ทางธุรกิจขององค์กรนั้น ๆ ตัวอย่างเช่นที่ SCBX งานวิจัยของเรามุ่งเน้นไปที่การสร้างพอร์ตโฟลิโอที่คำนึงถึงความเสี่ยงเป็นหลักมากกว่าการหาค่าเหมาะสมที่สุดสำหรับการเทรดความถี่สูง (High-frequency trading optimization) ในบริบทนี้ วัตถุประสงค์จึงอาจไม่ใช่การคำนวณหาผลลัพธ์ให้เร็วกว่าคู่แข่งเสมอไป แต่เป็นการสำรวจว่าข้อมูลเพิ่มเติม เช่น ข้อมูลธุรกรรม หรือสัญญาณอัลฟ่า (Alpha signals) — จะสามารถถูกนำมาบูรณาการเข้ากับกระบวนการหาค่าเหมาะสมที่สุดโดยยังคงรักษาระดับการควบคุมความเสี่ยงไว้ได้อย่างไร ในท้ายที่สุด อัลกอริทึมควอนตัมอาจมอบวิธีการใหม่ ๆ ในการรวบรวมเงื่อนไขข้อจำกัดและสัญญาณเหล่านี้เข้าสู่แบบจำลองการหาค่าเหมาะสมที่สุดในสเกลขนาดใหญ่ได้

โครงการนำร่องในอุตสาหกรรมเมื่อไม่นานมานี้สะท้อนทั้งศักยภาพและความจำเป็นที่ต้องระมัดระวัง ในปี 2025 HSBC และ IBM รายงานว่าเวิร์กโฟลว์ควอนตัมแบบไฮบริดช่วยปรับปรุงการคาดการณ์ว่าคำสั่งซื้อขายหุ้นกู้ภาคเอกชนจะได้รับการจับคู่หรือไม่ โดยใช้ข้อมูลการซื้อขายจริงในสเกลระดับการผลิต [15] ผลลัพธ์เช่นนี้น่ายินดี แต่ก็ยังไม่ได้แสดงให้เห็นว่าสามารถเอาชนะวิธีคลาสสิกที่ดีที่สุดได้โดยทั่วไป

3.6 Quantum AI: ความคาดหวังและความเป็นจริง (Quantum AI: Promise And Reality)

ปัญญาประดิษฐ์ควอนตัม (Quantum AI) กลายเป็นหนึ่งในวลีที่ถูกพูดถึงมากที่สุดในวงการเทคโนโลยี และปัจจุบันปรากฏอยู่ในยุทธศาสตร์ระดับชาติ พันธกิจของศูนย์วิจัย และการเปิดตัวผลิตภัณฑ์ต่าง ๆ รวมถึงในประเทศไทยด้วย (ดูหัวข้อ 6.1–6.2) การแยกแยะแนวคิดสองอย่างที่แตกต่างกันมากซึ่งซ่อนอยู่ภายใต้ป้ายชื่อเดียวกันนี้จะช่วยให้เข้าใจได้ชัดเจนขึ้น แนวคิดแรกคือ ควอนตัมเพื่อ AI (Quantum for AI) หมายถึงการใช้คอมพิวเตอร์ควอนตัมเพื่อเร่งความเร็วหรือยกระดับงาน Machine learning เช่น การจำแนกประเภท การรู้จำรูปแบบ (Generative modelling) และแนวคิดที่สองคือ AI เพื่อควอนตัม (AI for Quantum): หมายถึงการใช้ AI ในปัจจุบันเพื่อช่วยสร้างและควบคุมการทำงานของคอมพิวเตอร์ควอนตัมเอง

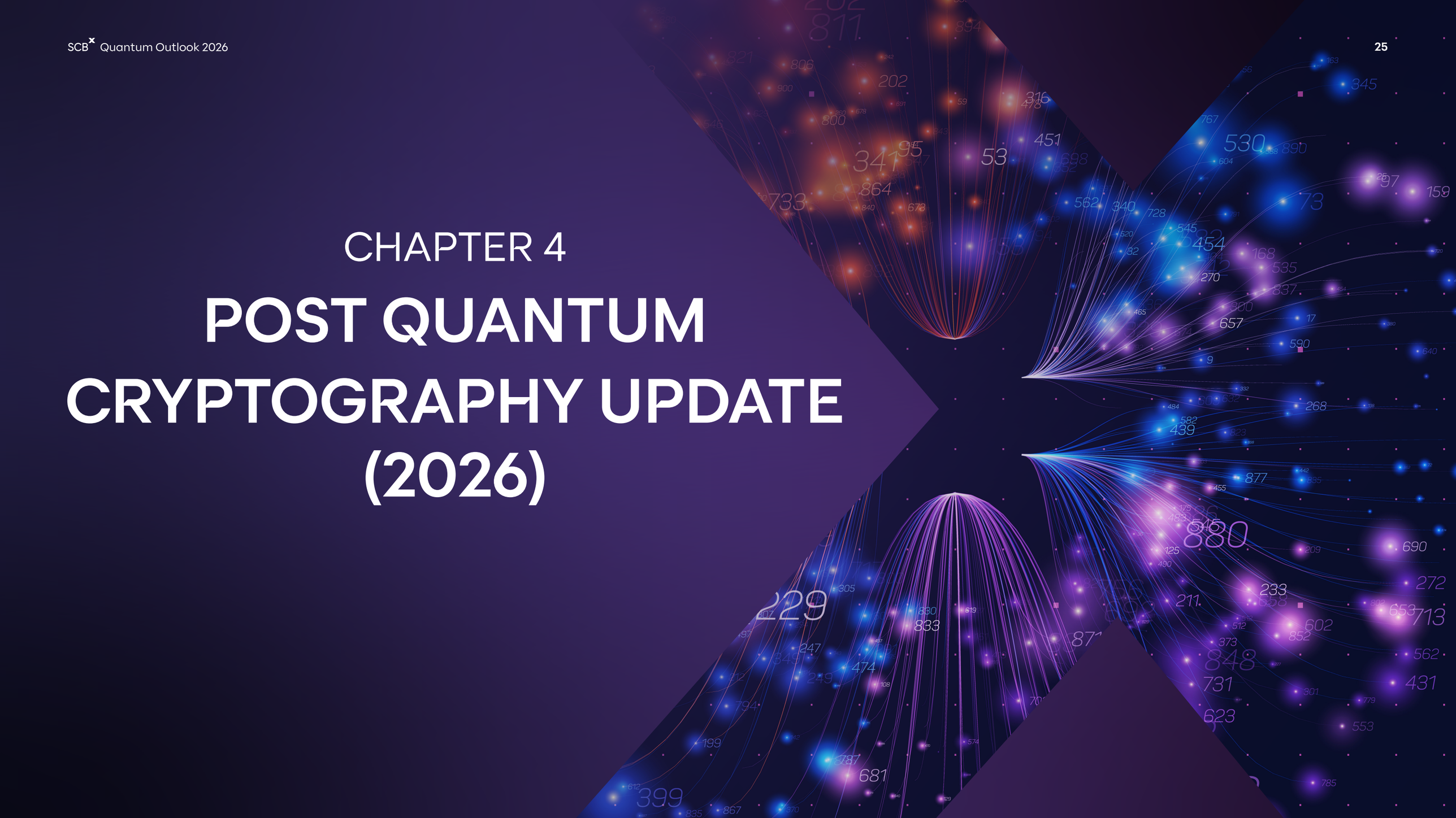
ที่อาจน่าสนใจคือ แนวทางที่สองคือจุดที่มีผลลัพธ์ชัดเจนที่สุดในปัจจุบัน โมเดล AI ถูกนำมาใช้แล้วในการปรับเทียบคิวบิต ช่วยออกแบบชิปและวัสดุ และตรวจจับข้อผิดพลาดแบบเรียลไทม์ ตัวอย่างเช่น AlphaQubit ของ Google DeepMind แสดงให้เห็นว่าโครงข่ายประสาทเทียมสามารถระบุข้อผิดพลาดในโปรเซสเซอร์ควอนตัมได้แม่นยำกว่าวิธีทั่วไป [17] และ Microsoft ระบุว่าได้ใช้เครื่องมือ AI ช่วยออกแบบวัสดุในชิป Majorana 2 ขึ้นใหม่ [18] กล่าวอีกนัยหนึ่ง AI กำลังช่วยเร่งให้คอมพิวเตอร์ควอนตัมที่ใช้งานได้จริงมาถึงเร็วขึ้น ซึ่งเป็นหนึ่งในเหตุผลที่เทคโนโลยีทั้งสองถูกกล่าวถึงควบคู่กันมากขึ้นเรื่อย ๆ

แนวทางแรก (คอมพิวเตอร์ควอนตัมทำให้ AI ดีขึ้น) มีศักยภาพแต่ยังไม่ได้รับการสำรวจในสเกลที่ใช้งานได้จริง อุปสรรคสำคัญมีสองประการ หนึ่งคือ AI ในปัจจุบันทำงานบนข้อมูลคลาสสิกปริมาณมหาศาล และการโหลดข้อมูลเหล่านั้นเข้าสู่คอมพิวเตอร์ควอนตัมนั้นช้าในตัวเอง ซึ่งอาจหักล้างการเร่งความเร็วที่คาดหวังไว้ สองคือ คำกล่าวอ้างในระยะแรกหลายรายการเกี่ยวกับการเร่งความเร็วของ QML ถูกตามทันในภายหลังโดยอัลกอริทึมคลาสสิกอันชาญฉลาดที่หยิบยืมแนวคิดเชิงควอนตัมมาใช้ [19] ดังนั้นคอมพิวเตอร์ควอนตัมจึงไม่สามารถแทนที่ GPU ในการฝึกโมเดลภาษาขนาดใหญ่ได้ บทบาทที่สมจริงกว่าของมันจะแคบกว่านั้น ได้แก่ การทำงานกับโจทย์ที่ข้อมูลมีธรรมชาติเป็นควอนตัมในตัวเอง เช่น โมเลกุลและวัสดุ การสร้างข้อมูลสำหรับฝึกโมเดลที่คอมพิวเตอร์คลาสสิกจำลองได้ยาก หรือการทำหน้าที่เป็นองค์ประกอบเฉพาะทางภายในไปป์ไลน์ AI ขนาดใหญ่ที่ส่วนใหญ่ยังเป็นคลาสสิก ผู้ผลิตฮาร์ดแวร์เริ่มวางตำแหน่งสำหรับเรื่องนี้แล้วตัวอย่างเช่น Quantinuum เปิดตัวระบบ Helios ในปี 2025 โดยมุ่งเน้นสิ่งที่เรียกว่า ‘Generative quantum AI’ [20]

สำหรับ SCBX ประเด็นสำคัญในทางปฏิบัติคือ ควรมอง Quantum AI เป็นพรมแดนการวิจัยมากกว่าผลิตภัณฑ์ในระยะใกล้ งานของเราร่วมกับ SQ[2] เกี่ยวกับแนวทางเชิงควอนตัมสำหรับโจทย์อย่างการตรวจจับการทุจริต (หัวข้อ 3.5) ดำเนินไปในแนวทางนี้ สร้างความเชี่ยวชาญทดสอบแนวคิดอย่างรอบคอบเทียบกับ Baseline แบบคลาสสิกที่แข็งแกร่ง และพร้อมที่จะเดินหน้าอย่างรวดเร็วหากความได้เปรียบที่แท้จริงปรากฏขึ้น

CHAPTER 4

POST QUANTUM CRYPTOGRAPHY UPDATE (2026)



4.1 เหตุใดองค์กรจึงต้องเตรียมพร้อมตั้งแต่วันนี้

บริการดิจิทัลสมัยใหม่พึ่งพาการเข้ารหัสลับ (Cryptography) เพื่อรักษาความลับของข้อมูล ยืนยันตัวตน และยืนยันความถูกต้องของธุรกรรม ความน่าเชื่อถือส่วนสำคัญนี้อาศัยการเข้ารหัสลับแบบกุญแจสาธารณะ (public-key cryptography) ซึ่งใช้ปกป้องการเชื่อมต่อดิจิทัลและสร้างลายมือชื่อดิจิทัล เมื่อคอมพิวเตอร์ควอนตัมมีขีดความสามารถสูงเพียงพอ วิธีการแบบกุญแจสาธารณะบางประเภทที่ใช้อย่างแพร่หลายในปัจจุบันอาจไม่ปลอดภัยอีกต่อไป PQC คือวิธีการเข้ารหัสลับรุ่นใหม่ที่ออกแบบให้ยังคงปลอดภัยต่อความสามารถดังกล่าวในอนาคต [1]

ปัจจุบันยังไม่มีคอมพิวเตอร์ควอนตัมที่เป็นที่ทราบต่อสาธารณะว่าสามารถทำลายวิธีการเหล่านี้ในระดับที่ใช้โจมตีระบบจริงได้ ความท้าทายสำคัญคือ เวลา การเปลี่ยนกลไกการเข้ารหัสลับในองค์กรขนาดใหญ่อาจใช้เวลาหลายปี ขณะที่ข้อมูลอ่อนไหวบางประเภทจำเป็นต้องรักษาความลับต่อเนื่องเป็นเวลานาน ดังนั้น ข้อมูลที่ถูกจัดเก็บหรือดักไว้ในวันนี้อาจยังมีมูลค่า หากในอนาคตสามารถถอดรหัสได้ องค์กรจึงต้องเริ่มเตรียมความพร้อมก่อนที่ภัยคุกคามจะเกิดขึ้นจริง

ประเด็นสำคัญ: **ความเสี่ยงจากควอนตัมมีอยู่จริง แม้ยังไม่ทราบเวลาที่แน่ชัด ขณะที่ระยะเวลาที่ต้องใช้ในการเตรียมความพร้อมสามารถประเมินได้แล้ว**

4.2 กรอบเวลาการเปลี่ยนผ่านชัดเจนขึ้น และใกล้เข้ามา

ความเปลี่ยนแปลงสำคัญในปี 2026 คือ รัฐบาลหลายประเทศเริ่มกำหนดกรอบเวลาการเปลี่ยนผ่าน แม้ยังไม่ทราบว่าคอมพิวเตอร์ควอนตัมที่สามารถทำลายการเข้ารหัสลับจะเกิดขึ้นเมื่อไหร่ก็ตามในสหรัฐฯ คำสั่งฝ่ายบริหาร (Executive Order) 14412 กำหนดให้ระบบของรัฐบาลกลางที่มีความสำคัญหรือมีผลกระทบสูง ใช้วิธีการหลังยุคควอนตัมสำหรับการสร้างกุญแจเข้ารหัสลับภายในสิ้นปี 2030 และสำหรับลายมือชื่อดิจิทัลภายในสิ้นปี 2031 ส่วนแผนดำเนินงานของรัฐบาลกลางที่ออกตามมาได้ขยายกรอบการเปลี่ยนผ่านโดยรวมไปจนถึงปี 2035 [5,6]

คำสั่งฝ่ายบริหาร 14413 ซึ่งออกในช่วงเวลาเดียวกัน มีเป้าหมายเร่งการวิจัยและการนำเทคโนโลยีควอนตัมไปใช้เชิงพาณิชย์ของสหรัฐฯ เมื่อพิจารณาร่วมกัน คำสั่งทั้งสองฉบับสะท้อนทิศทางเชิงนโยบายที่ชัดเจนเดินหน้าพัฒนาขีดความสามารถด้านควอนตัม ควบคู่กับการลดการพึ่งพาวิธีการเข้ารหัสลับที่อาจถูกคุกคามจากระบบควอนตัมในอนาคต [7]

สำหรับองค์กรนอกระบบรัฐบาลกลางสหรัฐฯ ผลกระทบหลักมีแนวโน้มจะเกิดผ่านผู้ให้บริการเทคโนโลยีและแนวปฏิบัติของอุตสาหกรรม มากกว่าการบังคับใช้กฎหมายโดยตรง ผู้ให้บริการคลาวด์ ความมั่นคงปลอดภัย การยืนยันตัวตน เครือข่าย และซอฟต์แวร์ที่ให้บริการแก่ภาครัฐหรือธุรกิจที่อยู่ภายใต้การกำกับ จะต้องรองรับข้อกำหนดหลังยุคควอนตัมมากขึ้น ทิศทางคล้ายกันเกิดขึ้นในประเทศอื่น ตัวอย่างเช่น ประเทศออสเตรเลียที่ตั้งเป้าให้การเปลี่ยนผ่านเสร็จสิ้นภายในสิ้นปี 2030 ขณะที่ประเทศสิงคโปร์กำลังขยับจากแนวทางทั่วไปไปสู่ความคาดหวังด้านความพร้อมที่วัดผลได้สำหรับสถาบันการเงิน [8-10]

สำหรับผู้มีอำนาจตัดสินใจ ปี 2030 กำลังกลายเป็นกรอบเวลาสำคัญสำหรับการวางแผนระบบที่มีความสำคัญสูง อย่างไรก็ตาม ปีดังกล่าวไม่ควรถูกตีความว่าเป็นการคาดการณ์ว่าวิธีการเข้ารหัสลับในปัจจุบันจะล้มเหลวเมื่อใด

4.3 ความเสี่ยงจากควอนตัมมีอยู่จริง แม้ยังไม่ทราบว่าจะเกิดขึ้นเมื่อใด

ปัจจุบันยังไม่มีการรายงานเกี่ยวกับคอมพิวเตอร์ควอนตัมที่สามารถทำลายการเข้ารหัสลับแบบกุญแจสาธารณะได้จริง อย่างไรก็ตาม งานวิจัยล่าสุดชี้ว่า ทรัพยากรที่จำเป็นต้องใช้ในการโจมตีภายในอนาคตอาจต่ำกว่าการประมาณการบางส่วนในอดีต ทว่าข้อมูลนี้ยังไม่สามารถตอบได้ว่าคอมพิวเตอร์ที่ทำลายการเข้ารหัสลับได้จะมาถึงเมื่อใด แต่ก็ทำให้การวางแผนโดยอิงตัวเลขประมาณการทรัพยากรแบบเดิมเชื่อถือได้น้อยลง

ข้อมูลสำคัญจากงานวิจัยเดือนพฤษภาคม 2026 โดย Tian Xue และ Jacob Covey จำลองการโจมตี RSA-2048 ซึ่งเป็นรูปแบบหนึ่งของการเข้ารหัสลับแบบกุญแจสาธารณะที่ใช้กันแพร่หลาย บนคอมพิวเตอร์ควอนตัมแบบโมดูลาร์ที่มีประมาณ 500,000 คิวบิต งานวิจัยนี้ไม่ได้สาธิตการโจมตีจริง และไม่ใช่การคาดการณ์ว่าการโจมตีจะเกิดขึ้นเมื่อไร สิ่งที่งานวิจัยนี้ชี้ให้เห็นคือ ความก้าวหน้าด้านอัลกอริทึมและการออกแบบระบบ สามารถทำให้ระดับเทคโนโลยีที่ต้องใช้ในการโจมตีเปลี่ยนไปจากที่เคยคาดไว้ และอาจทำให้องค์กรมีเวลาเตรียมตัวเปลี่ยนผ่านน้อยลง [3]

แนวคิดสำหรับการวางแผน: **องค์กรไม่ควรรอให้คอมพิวเตอร์ควอนตัมมีคิวบิตถึงจำนวนใดจำนวนหนึ่ง หรือรอวันที่มีคนคาดการณ์ไว้แล้วค่อยเริ่มเปลี่ยนผ่าน แต่ควรวางแผนจากสามเรื่อง คือ ข้อมูลต้องเก็บเป็นความลับไปอีกนานแค่ไหน ระบบนั้นสำคัญเพียงใด และต้องใช้เวลานานเท่าไรในการเปลี่ยนระบบ**



4.4 จากมาตรฐาน สู่การนำไปใช้จริง

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐฯ (National Institute of Standards and Technology: NIST) ได้ประกาศมาตรฐาน PQC ชุดแรกอย่างเป็นทางการแล้ว และยังคงสนับสนุนให้องค์กรต่าง ๆ เริ่มเปลี่ยนไปใช้มาตรฐานใหม่ ความไม่แน่นอนสำคัญข้อหนึ่งจึงหมดไป เพราะตอนนี้มีมาตรฐานที่ใช้งานได้จริงแล้ว ความท้าทายที่เหลืออยู่คือจะนำมาตรฐานเหล่านี้ไปใช้ในระบบจริงอย่างไร โดยไม่กระทบบริการที่ต้องพึ่งพาระบบเหล่านั้น [1]

ในองค์กรขนาดใหญ่ การเข้ารหัสลับกระจายอยู่ในเว็บไซต์ ใบรับรองดิจิทัล ระบบยืนยันตัวตน การเชื่อมต่อที่ปลอดภัย บริการชำระเงิน อุปกรณ์ และแพลตฟอร์มจากผู้ให้บริการภายนอก การเปลี่ยนผ่านจึงไม่ใช่เพียงการเปลี่ยนอัลกอริทึมตัวเดียว องค์กรต้องรู้ว่าการเข้ารหัสที่เสี่ยงต่อคอมพิวเตอร์ควอนตัมถูกใช้อยู่ที่ไหน บริการทางธุรกิจใดต้องพึ่งพาการเข้ารหัสนั้น ผลิตภัณฑ์ใดอัปเกรดได้ และส่วนใดที่ผู้ให้บริการภายนอกเป็นผู้กำหนดกรอบเวลา

นอกจากนี้ องค์กรยังต้องเตรียมตัวให้พร้อมสำหรับการเปลี่ยนแปลงในอนาคต เพราะความคล่องตัวด้านการเข้ารหัสลับ (crypto-agility) หมายถึงความสามารถในการเปลี่ยนวิธีการเข้ารหัสลับโดยไม่ต้องสร้างระบบธุรกิจใหม่ทั้งหมด แนวทางฉบับปรับปรุงของ NIST มองเรื่องนี้เป็นขีดความสามารถด้านสถาปัตยกรรมและการปฏิบัติงาน ไม่ใช่การอัปเกรดเทคโนโลยีเพียงครั้งเดียว ในทางปฏิบัติ ระบบ สัญญา และกระบวนการปฏิบัติงานควรเอื้อต่อการเปลี่ยนวิธีการเข้ารหัสลับในอนาคตได้อย่างบริหารจัดการได้ [2]

4.5 บทเรียนที่ภาคการเงิน เริ่มได้รับจากการนำไปใช้จริง

หลักฐานจากภาคการเงินสนับสนุนมุมมองว่า การเปลี่ยนผ่านเป็นเรื่องของระบบโดยรวม ศูนย์นวัตกรรมของธนาคารเพื่อการชำระหนี้ระหว่างประเทศ (Bank for International Settlements Innovation Hub: BIS Innovation Hub) ได้ทดสอบลายมือชื่อดิจิทัลแบบหลังยุคควอนตัมในสภาพแวดล้อมระบบชำระเงินที่ใช้งานจริงผ่าน Project Leap Phase 2 ซึ่งแสดงให้เห็นว่าบทเรียนสำคัญไม่ได้อยู่ที่อัลกอริทึมเพียงอย่างเดียว ระบบและผลิตภัณฑ์หลายส่วนต้องทำงานร่วมกันอย่างเหมาะสม รวมถึงประสิทธิภาพต้องอยู่ในระดับที่ยอมรับได้ และองค์กรต้องประสานการเปลี่ยนแปลงตลอดทั้งบริการ แนวคิดเดียวกันนี้ยังปรากฏในโครงการต่อมาของ BIS ชื่อ FuSSE ซึ่งเกี่ยวข้องกับโครงสร้างพื้นฐานการชำระราคาในอนาคต โครงการนี้กำหนดให้ความพร้อมรับมือคอมพิวเตอร์ควอนตัมและความสามารถในการเปลี่ยนวิธีการเข้ารหัสได้เมื่อจำเป็น เป็นสิ่งที่ต้องคำนึงถึงตั้งแต่ขั้นออกแบบ [11,12]

สำหรับธนาคารและสถาบันการเงินอื่น ประเด็นนี้ควรให้ความสำคัญเป็นพิเศษ เนื่องจากบริการสำคัญจำนวนมากพึ่งพาผู้ให้บริการภายนอกและโครงสร้างพื้นฐานที่มีอายุการใช้งานยาวนาน ซึ่งผู้ให้บริการเทคโนโลยีอาจระบุโดยรวมว่า “พร้อมรองรับ PQC” แต่ผลิตภัณฑ์บางเวอร์ชัน บริการใบรับรองดิจิทัล หรือองค์ประกอบในระบบชำระเงินอาจยังไม่รองรับ ดังนั้นความพร้อมต้องอาศัยหลักฐานในระดับบริการจริง ไม่ใช่เพียงคำยืนยันจากผู้ให้บริการ

4.6 ทิศทางในภูมิภาคชัดเจนขึ้น

ประเทศสิงคโปร์เป็นตัวอย่างในภูมิภาคที่แสดงให้เห็นว่าการเตรียมความพร้อม กำลังมีโครงสร้างและสามารถวัดผลได้มากขึ้น ในปี 2026 สำนักงานความมั่นคงปลอดภัยไซเบอร์แห่งสิงคโปร์ (Cyber Security Agency of Singapore: CSA), GovTech และ IMDA ได้เผยแพร่ Quantum-Safe Migration Handbook ฉบับสมบูรณ์และ Quantum Readiness Index เพื่อให้องค์กรมีกรอบร่วมในการประเมินความก้าวหน้า Monetary Authority of Singapore (MAS) ซึ่งเป็นหน่วยงานกำกับดูแลภาคการเงินของสิงคโปร์ อีกทั้งยังระบุเป้าหมายให้สถาบันการเงินมีความพร้อมรับมือความเสี่ยงจากควอนตัม (quantum-resilient) กล่าวคือ สามารถรักษาความมั่นคงปลอดภัยได้เมื่อเทคโนโลยีควอนตัมพัฒนาไปให้แล้วเสร็จภายในทศวรรษนี้ [9,10]

กลับมาที่ประเทศไทย เรากำลังอยู่ในระยะต้นของวงจรนโยบาย แต่ก็มองเห็นทิศทางได้ชัดเจนมากขึ้น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เปิดรับฟังความคิดเห็นต่อร่างกรอบการเตรียมความพร้อมสู่ความปลอดภัยเชิงควอนตัม 2026-2035 ระหว่างวันที่ 15-29 กรกฎาคม 2026 ขณะที่ร่างแผนแม่บทการเปลี่ยนผ่านสู่ความปลอดภัยเชิงควอนตัม 2026-2035 โดยเสนอการดำเนินงานเป็นระยะ ได้แก่ การสำรวจความพร้อมและจัดทำบัญชีรายการการเข้ารหัสลับในช่วง 2026-2027 การดำเนินโครงการนำร่องและยืนยันทางเทคนิคในช่วง 2027-2030 และการขยายการเปลี่ยนผ่านในวงกว้างจนถึงปี 2035 หมุดหมายเหล่านี้ยังเป็นข้อเสนอในเอกสารร่างเพื่อพัฒนานโยบาย ไม่ใช่ข้อกำหนดทางกฎหมายหรือข้อบังคับที่มีผลใช้แล้ว [13-15]

ดังนั้น สำหรับสถาบันการเงิน พัฒนาการเหล่านี้ล้วนให้ข้อสรุปในทางปฏิบัติไปในทางเดียวกัน คือความพร้อมรับมือคอมพิวเตอร์ควอนตัมกำลังกลายเป็นส่วนหนึ่งของการบริหารความเสี่ยงด้านเทคโนโลยี ซึ่งหมายความว่าองค์กรต้องรู้ว่าการเข้ารหัสที่เสี่ยงต่อคอมพิวเตอร์ควอนตัมถูกใช้อยู่ที่ไหน ระบบใดสำคัญที่สุด ผู้ให้บริการรองรับการเปลี่ยนผ่านได้หรือไม่ อะไรทดสอบไปแล้วบ้าง และใครเป็นผู้รับผิดชอบการตัดสินใจในขั้นถัดไป

ความพร้อมในวันนี้ไม่ได้วัดกันแค่ว่ารู้ถึงความเสี่ยงหรือไม่ **แต่ต้องมีหลักฐานว่าได้ลงมือทำแล้วใน 5 ด้าน ได้แก่ การรู้ว่าใช้การเข้ารหัสอยู่ที่ไหน การจัดลำดับความสำคัญ ความพร้อมของผู้ให้บริการ การทดสอบ และการมีผู้รับผิดชอบที่ชัดเจน**

4.7 การเตรียมเข้าสู่ระยะนำไปใช้จริง

องค์กรเริ่มเตรียมตัวได้เลยตั้งแต่ตอนนี้ ไม่ต้องรอให้หน่วยงานกำกับดูแลออกกฎฉบับจริงก่อน ในไทยเองก็มีร่างกรอบความปลอดภัยเชิงควอนตัม และร่างแผนแม่บทการเปลี่ยนผ่านออกมาแล้ว โดยวางขั้นตอนไว้แบบเดียวกับที่ต่างประเทศใช้ คือ เริ่มจากสำรวจว่าตอนนี้ใช้อะไรอยู่บ้าง ดูว่าส่วนไหนเสี่ยงที่สุดแล้วจัดการก่อน ทดลองในวงเล็กก่อนค่อยขยาย และเก็บบันทึกความคืบหน้าไว้เป็นหลักฐาน ถึงจะยังเป็นแค่ร่าง แต่เอกสารสองฉบับนี้ก็ช่วยให้เห็นภาพได้ดีว่า ถ้าจะลงมือทำจริงในบริบทของไทย น่าจะต้องทำเป็นขั้นตอนอย่างไร [13,14]

สิ่งแรกที่ควรทำคือ มองให้เห็นภาพรวมก่อนว่าองค์กรมีอะไรอยู่บ้าง ต้องรู้ว่าการเข้ารหัสที่เสี่ยงต่อคอมพิวเตอร์ควอนตัมถูกใช้อยู่ที่ไหน ระบบไหนต้องพึ่งพามัน และใครเป็นเจ้าของระบบนั้น โดยเครื่องมือที่ช่วยเรื่องนี้ได้ คือ บัญชีรายการการเข้ารหัส (Cryptographic Inventory) พูดง่าย ๆ ก็คือรายการที่จดไว้ว่าองค์กรใช้การเข้ารหัส ลายมือชื่อดิจิทัล และกลไกความปลอดภัยอื่น ๆ อยู่ตรงไหนบ้าง รายการนี้ไม่ต้องสมบูรณ์ตั้งแต่วันแรก ขอแค่ดีพอจะบอกได้ว่าส่วนไหนอาจต้องเปลี่ยนเมื่อเห็นภาพแล้ว ก็มาจัดลำดับว่าจะทำอะไรก่อน โดยให้ความสำคัญกับข้อมูลอ่อนไหวที่ต้องเก็บเป็นความลับ ระบบยืนยันตัวตน ระบบชำระเงิน การจัดการกุญแจเข้ารหัส และบริการสำคัญอื่น ๆ พร้อมกับดูด้วยว่าแต่ละระบบเปลี่ยนยากแค่ไหน และต้องพึ่งผู้ให้บริการภายนอกมากน้อยเพียงใด หรือกล่าวได้ว่า เวลาและทรัพยากรมีจำกัด จึงควรเริ่มจากระบบที่ถ้าเปลี่ยนช้าแล้วจะเสี่ยงต่อธุรกิจหรือความปลอดภัยมากที่สุดก่อนเป็นอันดับแรก [13,14]

ต่อมาคือความพร้อมของผู้ให้บริการและการทดสอบในระบบจริง สำหรับธนาคารและองค์กรขนาดใหญ่ควรถามผู้ให้บริการหลักว่า ขณะนี้รองรับ PQC ในระดับใด จะมีการอัปเกรดเมื่อใด และจะรองรับวิธีการเดิมต่อไปอีกนานเท่าใด และก่อนขยายการเปลี่ยนผ่าน องค์กรควรทดสอบบริการจริงตั้งแต่ต้นทางถึงปลายทาง แทนการทดสอบอัลกอริทึมแยกส่วน เพื่อยืนยันว่าแอปพลิเคชัน ใบรับรองดิจิทัล บริการบริหารจัดการกุญแจเข้ารหัสลับ องค์ประกอบเครือข่าย และกระบวนการปฏิบัติงานยังสามารถทำงานร่วมกันได้ด้วยประสิทธิภาพและน่าเชื่อถือ ซึ่ง Project Leap ของ BIS เป็นตัวอย่างที่ชี้ให้เห็นว่าการทดสอบระบบมีความสำคัญเพียงใด [11,14]

ท้ายที่สุด ความพร้อมรับมือคอมพิวเตอร์ควอนตัมควรเป็นส่วนหนึ่งของการบริหารความเสี่ยงด้านเทคโนโลยีที่องค์กรทำอยู่เป็นประจำ หมายความว่าต้องคอยอัปเดตบัญชีรายการการเข้ารหัสอยู่เสมอ ติดตามว่าผู้ให้บริการแต่ละรายไปถึงไหนแล้ว มีคนรับผิดชอบที่ชัดเจน จดไว้ว่ายังเหลือความเสี่ยงอะไรอยู่บ้าง และกลับมาทบทวนความพร้อมเป็นระยะ เป้าหมายที่แท้จริงไม่ใช่การคาดเดาให้ถูกว่าคอมพิวเตอร์ควอนตัมจะเจาะระบบเข้ารหัสได้เมื่อไร แต่อยู่ที่การเปลี่ยนผ่านอย่างมีแผน มีหลักฐานรองรับ และรวดเร็วพอ เพื่อที่วันข้างหน้าองค์กรจะไม่ถูกบีบให้ต้องรีบเปลี่ยนแบบฉุกละหุกจนกระทบการทำงาน

CHAPTER 5

ภูมิทัศน์การลงทุนระดับโลก และความพยายามในการสร้างคอมพิวเตอร์ควอนตัม





5.1 จาก Research Ecosystem สู่ Quantum Supply Chain

ระบบนิเวศควอนตัมระดับโลกกำลังเปลี่ยนผ่านจากยุคที่ขับเคลื่อนด้วยงานวิจัย ไปสู่ระยะเริ่มต้นของการพัฒนาสู่ระดับอุตสาหกรรมเชิงพาณิชย์ ถึงอย่างนั้น ก็ไม่ได้แปลว่าอุตสาหกรรมนี้เติบโตเต็มที่แล้ว เทคโนโลยีควอนตัมส่วนใหญ่ยังอยู่ในช่วงเริ่มต้นของการทำเชิงพาณิชย์ แต่สิ่งที่กำลังเปลี่ยนไปคือโครงสร้างของอุตสาหกรรมจากเดิมที่บริษัทหนึ่งพยายามทำเองทุกอย่าง ตั้งแต่การสร้างฮาร์ดแวร์ในระดับฟิสิกส์ไปจนถึงแอปพลิเคชันที่ผู้ใช้ใช้งานจริง ตอนนี้เริ่มมีการแบ่งงานกันชัดเจนขึ้น โดยมีบริษัทที่เชี่ยวชาญเฉพาะด้านเข้ามาทำในแต่ละขั้นของเทคโนโลยี บทวิเคราะห์หลายฉบับในช่วงหลังเริ่มมีการเปรียบเทียบทิศทางนี้ไว้ตรง ๆ กับเส้นทางที่อุตสาหกรรมเซมิคอนดักเตอร์เคยผ่านมา ซึ่งการขยายตัวในระยะยาวเกิดจากการที่แต่ละบริษัทเชี่ยวชาญในส่วนของตัวเอง ไม่ใช่การที่บริษัทเดียวทำเองครบทุกขั้นตอน [1]

การเปลี่ยนแปลงนี้เห็นได้จากบริษัทใหม่ที่เกิดขึ้น รวมถึงนโยบายภาครัฐและเงินลงทุนที่ไหลเข้ามาด้วย องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) และสำนักงานสิทธิบัตรยุโรป (EPO) รายงานว่ามีมากกว่า 30 ประเทศที่ออกนโยบายด้านควอนตัมโดยเฉพาะแล้ว โดยในจำนวนนี้มี 18 ประเทศสมาชิก OECD ที่มียุทธศาสตร์ระดับชาติอย่างครอบคลุม [4] ในสหราชอาณาจักร รัฐบาลได้ประกาศทุ่มงบประมาณ 2.5 พันล้านปอนด์สำหรับแผนงานวิจัยและนวัตกรรมด้านควอนตัม เป็นระยะเวลา 10 ปี [5] ขณะที่โครงการนำร่องเทคโนโลยีควอนตัม ของคณะกรรมาธิการยุโรป (European Commission) ซึ่งเป็นโครงการริเริ่มระยะเวลา 10 ปี ก็คาดว่าจะได้รับงบประมาณสนับสนุนจากสหภาพยุโรปมากถึง 1 พันล้านยูโร [6] ทางด้านสหรัฐอเมริกา งบประมาณของรัฐบาลกลางด้านการวิจัยและพัฒนาเทคโนโลยีควอนตัมได้เพิ่มสูงขึ้นอย่างมีนัยสำคัญนับตั้งแต่ปี 2019 ภายใต้โครงการริเริ่มด้านควอนตัมแห่งชาติ และในช่วงปลายปี 2025 กระทรวงพลังงานได้ประกาศอัดฉีดเงินอีก 625 ล้านดอลลาร์ เพื่อต่ออายุศูนย์วิจัยวิทยาศาสตร์สารสนเทศควอนตัมแห่งชาติ (National Quantum Information Science Research Centers) ทั้ง 5 แห่ง [7-8] ในปี 2026 จังหวะดังกล่าวยิ่งเร่งตัวขึ้นไปอีก ในเดือนพฤษภาคม กระทรวงพาณิชย์สหรัฐฯ ประกาศมอบเงินสนับสนุน 2 พันล้านดอลลาร์ ให้แก่บริษัทควอนตัม 9 แห่ง เพื่อแลกกับการถือหุ้นส่วนน้อย ในเดือนมิถุนายน ประธานาธิบดีสหรัฐฯ ลงนามคำสั่งฝ่ายบริหารสองฉบับ ฉบับหนึ่งว่าด้วยการเข้ารหัสที่ทนต่อคอมพิวเตอร์ควอนตัม อีกฉบับว่าด้วยนวัตกรรมควอนตัม ในเดือนกันยายน กระทรวงพลังงานเปิดตัวการแข่งขัน ‘Genesis Q’ มูลค่าสูงสุด 215 ล้านดอลลาร์ เพื่อสร้างเครื่องที่มีคิวบิตเชิงตรรกะ 100 ตัวให้ได้ภายในปี 2028 ทางด้านประเทศฝรั่งเศสก็เพิ่มงบอีก 1 พันล้านยูโรให้กับยุทธศาสตร์ควอนตัมแห่งชาติ [16–18][20]

นักลงทุนทั้งภาครัฐและภาคเอกชนต่างก็ยกระดับการลงทุนเช่นกัน จากรายงาน Quantum Technology Monitor 2026 ของ McKinsey เม็ดเงินลงทุนในสตาร์ทอัพด้านเทคโนโลยีควอนตัมพุ่งสูงขึ้นไปสู่ 1.26 หมื่นล้านดอลลาร์ในปี 2025 ประมาณ 6.3 เท่าของปี 2024 โดยกว่า 60% กระจุกตัวอยู่ในดีลที่ใหญ่ที่สุด 10 รายการ [15] ความน่าสนใจอยู่ที่สัดส่วนเงินทุนจากภาครัฐในการระดมทุนของสตาร์ทอัพลดลงจากประมาณหนึ่งในสามในปี 2024 เหลือเพียง 3% ในปี 2025 เนื่องจากการเข้าจดทะเบียนในตลาดหลักทรัพย์และเงินทุนภาคเอกชนเข้ามามีบทบาทแทน ตามมาด้วยการประกาศลงทุนครั้งใหญ่ของภาคธุรกิจในปี 2026 อย่างเช่น IBM ที่ประกาศแผนการลงทุนด้านควอนตัมมากกว่า 1 หมื่นล้านดอลลาร์ภายในห้าปี และ Quantinuum ระดมทุนได้ 1.7 พันล้านดอลลาร์จากการเข้าจดทะเบียนในตลาดหลักทรัพย์ [16][19] อย่างไรก็ตาม บทวิเคราะห์ระบบนิเวศของ OECD (ธันวาคม 2025) ระบุว่าการสนับสนุนจากภาครัฐยังคงมีความสำคัญต่อฐานการวิจัยของสาขานี้อย่างมาก [4]

สำหรับสถาบันการเงิน ประเด็นนี้มีนัยเชิงกลยุทธ์ที่สำคัญ เศรษฐกิจควอนตัมไม่ได้เป็นแค่เรื่องของการมีฮาร์ดแวร์เป็นของตัวเอง แต่กำลังกลายเป็นระบบนิเวศที่แบ่งเป็นชั้น ๆ โดยองค์กรส่วนใหญ่จะเข้ามามีส่วนร่วมในชั้นบน ๆ ที่อยู่ใกล้การใช้งานจริง ผ่านการใช้งานบนระบบคลาวด์ การเชื่อมเข้ากับกระบวนการทำงานที่มีอยู่ การใช้อัลกอริทึมที่ออกแบบมาเฉพาะอุตสาหกรรม และการสร้างความสามารถภายในองค์กร โดยไม่ต้องลงไปผลิตคิวบิตหรือดูแลระบบทำความเย็นจัดด้วยตัวเอง [1] สำหรับห่วงโซ่อุปทานของการประมวลผลควอนตัมแบ่งออกเป็นระดับต่าง ๆ ดังนี้:

Supply Chain Layer	Functional Description	Representative Companies / Leaders
1. Materials and equipment	นี่คือรากฐานทางกายภาพที่ทำให้เทคโนโลยีเกิดขึ้นได้ ระบบทำความเย็นจัด (Cryogenic systems), เลเซอร์, ระบบสุญญากาศ โฟโตนิกส์ อิเล็กทรอนิกส์ควบคุม วัสดุเฉพาะทาง และเครื่องมือการผลิต	Bluefors, Oxford Instruments, Applied Materials และซัพพลายเออร์อื่น ๆ ซึ่งผลิตภัณฑ์มักถูกใช้งานร่วมกับระบบนิเวศเทคโนโลยีขั้นสูง (Deep-tech) และเซมิคอนดักเตอร์ที่ใกล้เคียงกัน
2. Qubit fabrication and hardware	การสร้างโปรเซสเซอร์ทางกายภาพที่ใช้งานจริง ระดับชั้นนี้มีความหลากหลายสูง โดยมีการสำรวจรูปแบบ (Modalities) ทางควอนตัมที่หลากหลายเพื่อลดความเสี่ยงจากเทคโนโลยีที่อาจไปต่อไม่ได้รูปแบบฮาร์ดแวร์ที่แข่งขันกันอยู่ ได้แก่ วงจรตัวนำยวดยิ่ง (Superconducting circuits), ไอออนที่ถูกดักจับ (Trapped ions), อะตอมเป็นกลางโฟโตนิกส์, สปินคิวบิตและระบบที่ใช้พื้นฐานการแอนนีลลิง (Annealing-based systems)	IBM, Google, Atom Computing, IonQ, Pasqal, QuEra, Microsoft, PsiQuantum, และ D-Wave.
3. Middleware and control Systems	ส่วนต่อประสานที่สำคัญระหว่างระบบคลาสสิกและระบบควอนตัม ครอบคลุมถึงซอฟต์แวร์จัดระบบการทำงาน การควบคุมพัลส์ (Pulse control), อิเล็กทรอนิกส์ไมโครเวฟ สแต็กการปรับเทียบ และโครงสร้างพื้นฐานสำหรับการประมวลผลแบบไฮบริด	Quantum Machines, Emergence Quantum, Horizon Quantum, Conductor Quantum, Zurich Instruments, Keysight, Qblox และ NVIDIA (CUDA-Q / NVQLink)
4. Error correction, suppression, and runtime reliability	ระดับชั้นที่ช่วยแปลงคิวบิตทางกายภาพที่มีสัญญาณรบกวน ให้เป็นการดำเนินการเชิงตรรกะที่มีเสถียรภาพมากขึ้น ซึ่งรวมถึงตัวถอดรหัสเครื่องมือยับยั้งข้อผิดพลาด และสถาปัตยกรรมการแก้ไขข้อผิดพลาดที่มีประสิทธิภาพด้านฮาร์ดแวร์	Riverlane, QuEra, Alice & Bob, พร้อมกับความพยายามภายในองค์กรจากผู้เล่นฮาร์ดแวร์หลัก
5. Algorithms and software development	ระดับชั้นนี้ช่วยลดทอนความซับซ้อนของฮาร์ดแวร์ และมุ่งเน้นไปที่วิธีการที่เป็นประโยชน์สำหรับการหาค่าเหมาะสมที่สุด การจำลอง การเรียนรู้ของเครื่อง และการออกแบบกระบวนการทำงาน	Phasecraft, QC Ware, Classiq และ Multiverse Computing
6. Application and cloud access layer	นี่คือจุดที่องค์กรส่วนใหญ่จะเข้ามามีส่วนร่วมเป็นอันดับแรก ผ่านบริการควอนตัม (Quantum-as-a-service) และแพลตฟอร์มคลาวด์แบบไฮบริด ที่เชื่อมต่อระบบประมวลผลประสิทธิภาพสูงคลาสสิก (Classical HPC) และกระบวนการทำงานขององค์กรเข้ากับโปรเซสเซอร์ควอนตัม	IBM Quantum Platform, Amazon Braket, Microsoft Azure Quantum, Google Cloud และ Oracle Cloud (ซึ่งโฮสต์ Helios ของ Quantinuum)[19]

The Quantum Computing Supply Chain Stack



The quantum ecosystem has evolved into specialized abstraction layers. Financial institutions engage primarily at the Application and Cloud Access layers, leveraging the underlying innovations without needing to manage physical hardware.

สำหรับองค์กรอย่าง SCBX โครงสร้างแบบแบ่งลำดับชั้นนี้ ชี้ให้เห็นว่าการลงทุนที่ตอบโจทย์และคุ้มค่าที่สุดไม่ใช่การครอบครองฮาร์ดแวร์ แต่คือการลงทุนในกลุ่มบุคลากรที่มีความเชี่ยวชาญ การสร้างเครือข่ายพันธมิตร การเตรียมความพร้อมด้านข้อมูล การคัดเลือกกรณีการใช้งานที่เหมาะสม การออกแบบกระบวนการทำงานแบบไฮบริด ตลอดจนการสร้างขีดความสามารถภายในองค์กร เพื่อให้สามารถประเมินได้อย่างถ่องแท้ว่า เมื่อใดที่วิธีการทางควอนตัมหรือเทคโนโลยีที่ได้แรงบันดาลใจจากควอนตัมให้ผลลัพธ์ที่เหนือกว่ามาตรฐานของระบบคลาสสิกอย่างแท้จริง ทิศทางดังกล่าวถือเป็นความมุ่งมั่นเชิงกลยุทธ์ ที่มีความเฉพาะเจาะจงและเป็นไปได้จริงในทางปฏิบัติ มากกว่าการพยายามสร้างโครงสร้างระบบควอนตัมทั้งหมด (Building a quantum stack) ขึ้นมาใหม่ตั้งแต่ต้น

5.2 การคาดการณ์ผลกระทบทางเศรษฐกิจ: วิธีตีความตัวเลขอย่างระมัดระวัง (Economic Impact Projections: How To Read The Numbers Carefully)

ข้อควรระวังเมื่อพูดถึงคอมพิวเตอร์ควอนตัมในที่สาธารณะ มักมีการนำตัวเลขหลายประเภทมาปนกัน ซึ่งควรแยกออกจากกันให้ชัด

- **ประการแรก** คือ เงินลงทุนที่ไหลเข้าสู่อุตสาหกรรม เช่น เงินจากกองทุนร่วมลงทุน เงินลงทุนจากบริษัทเอกชน และงบประมาณจากโครงการของรัฐ
- **ประการที่สอง** คือ รายได้ของตลาด หมายถึงเงินที่บริษัทผู้ขายเทคโนโลยีควอนตัมอาจได้รับจากการขายฮาร์ดแวร์ ซอฟต์แวร์ บริการ และโครงสร้างพื้นฐาน
- **ประการที่สาม** คือ มูลค่าทางเศรษฐกิจที่ผู้ใช้งานได้รับ หมายถึงรายได้ที่เพิ่มขึ้น ต้นทุนที่ลดลง ประสิทธิภาพการทำงานที่ดีขึ้น หรือความเสี่ยงที่ลดลง ซึ่งการนำคอมพิวเตอร์ควอนตัมมาใช้ในกระบวนการทำงานอาจสร้างให้กับอุตสาหกรรมต่าง ๆ เช่น การเงิน เคมีภัณฑ์ การแพทย์ และโลจิสติกส์

สิ่งเหล่านี้ไม่ใช่เรื่องเดียวกันและไม่ควรนำมาบวกรวมเข้าด้วยกัน

ทางด้านของ **ขนาดตลาด** McKinsey ประเมินว่าภายในปี 2035 ตลาดเทคโนโลยีควอนตัมโดยรวมอาจมีรายได้ทั่วโลกสูงถึง 9.7 หมื่นล้านดอลลาร์ต่อปี ซึ่งในจำนวนนี้ การประมวลผลควอนตัมอาจมีสัดส่วนประมาณ 2.8-7.2 หมื่นล้านดอลลาร์ การสื่อสารเชิงควอนตัม (Quantum communication) 1.1-1.5 หมื่นล้านดอลลาร์ และการรับรู้เชิงควอนตัม (Quantum sensing) 7 พันล้าน-1 หมื่นล้านดอลลาร์ [10] นอกจากนี้ McKinsey ยังนำเสนอตัวเลขเหล่านี้ในรูปแบบของช่วงความน่าจะเป็นเนื่องจากผลลัพธ์ที่แท้จริงนั้นขึ้นอยู่กับความก้าวหน้าทางเทคโนโลยี ความเร็วในการเปิดรับเทคโนโลยี และสมมติฐานในการขยายสเกล รายงานฉบับปรับปรุงปี 2026 ของ McKinsey ได้ทบทวนมุมมองนี้เป็นประมาณ 6-10 หมื่นล้านดอลลาร์สำหรับตลาดเทคโนโลยีควอนตัมโดยรวมภายในปี 2035 โดยควอนตัมคอมพิวติงมีสัดส่วนราว 4.3-7.1 หมื่นล้านดอลลาร์ [15]

ในฝั่งของ **มูลค่าทางเศรษฐกิจ** ตัวเลขจะสูงกว่ามาก เนื่องจากเป็นการอ้างอิงถึงมูลค่าที่สร้างขึ้นในอุตสาหกรรมปลายน้ำ ไม่ใช่รายได้ของฝั่งซัพพลายเออร์ McKinsey ประเมินว่าการประมวลผลควอนตัมอาจช่วยปลดล็อกมูลค่าทางเศรษฐกิจได้ราว 9 แสนล้าน- 2 ล้านล้านดอลลาร์ ภายในปี 2035 โดยครอบคลุม 4 กลุ่มอุตสาหกรรมหลัก ได้แก่ พลังงานและวัสดุระดับโลก เภสัชภัณฑ์และผลิตภัณฑ์ทางการแพทย์ บริการทางการเงิน และการเดินทางขนส่งและโลจิสติกส์ [11] เมื่อมองลึกลงไปในภาพใหญ่ บทวิเคราะห์ภาคการเงินของ McKinsey ประเมินว่า บริการทางการเงินมีศักยภาพในการสร้างมูลค่าได้ถึง 4-6 แสนล้านดอลลาร์ภายในปี 2035 [12] การวิเคราะห์ยังระบุว่ามีมูลค่า 2-5 แสนล้านดอลลาร์สำหรับภาคเภสัชภัณฑ์ [13] และช่วง 2-5 แสนล้านดอลลาร์เดียวกันสำหรับภาคเคมีภัณฑ์ [14] ตัวเลขเหล่านี้ควรถูกตีความว่าเป็น **มูลค่าทางเศรษฐกิจที่คาดหวังได้ ภายใต้สถานการณ์การเปิดรับเทคโนโลยีที่เอื้ออำนวย** ไม่ใช่ผลลัพธ์ที่มีการการันตีว่าจะเกิดขึ้นอย่างแน่นอน

เหตุผลรองรับของตัวเลขประเมินเหล่านี้ค่อนข้างจะตรงไปตรงมา แม้ว่าตัวเลขที่แน่ชัดจะยังมีความไม่แน่นอน แต่มูลค่าเหล่านี้ไม่ได้เกิดจากการที่การประมวลผลควอนตัมทำงานได้เร็วขึ้นในเชิงนามธรรม แต่มันเกิดจากการให้คำตอบที่ดีกว่าสำหรับปัญหาการคำนวณที่มีต้นทุนสูง ตัวอย่างเช่น การจำลองระดับโมเลกุลที่แม่นยำขึ้น การคำนวณพอร์ตโฟลิโอและความเสี่ยงที่ดีขึ้น การวางเส้นทางและจัดตารางเวลาที่มีประสิทธิภาพยิ่งขึ้น รอบการออกแบบที่รวดเร็วขึ้น และคุณภาพการตัดสินใจที่ดีขึ้นในสถานการณ์ที่แม้แต่การพัฒนาเพียงเปอร์เซ็นต์เล็ก ๆ ก็ส่งผลกระทบทางการเงินอย่างมหาศาล ดังนั้น ข้อสนับสนุนทางเศรษฐกิจที่แข็งแกร่งที่สุดสำหรับควอนตัมคอมพิวติงจึงไม่ใช่การทำระบบอัตโนมัติในวงกว้างแบบครอบจักรวาล แต่เป็น **การยกระดับแบบเจาะจงในปัญหาการตัดสินใจที่มีต้นทุนสูงลิ่ว**

ถึงจะเป็นเช่นนั้น การคาดการณ์เหล่านี้ก็ควรถูกประเมินด้วยความระมัดระวังอย่างยิ่งจากเหตุผลอย่างน้อย 4 ประการ

1. เส้นทางของฮาร์ดแวร์ยังคงมีความไม่แน่นอน: แม้สาขานี้จะมีความก้าวหน้าที่จับต้องได้ แต่การขยายสเกลคิวบิตเชิงตรรกะที่เชื่อถือได้ยังคงเป็นคอขวดที่จุดศูนย์กลาง

2. แอปพลิเคชันธุรกิจในระยะแรกจะเป็นแบบไฮบริด: ซึ่งหมายความว่ามูลค่าทางเศรษฐกิจอาจค่อย ๆ ทยอยเกิดขึ้น มากกว่าจะเกิดจากการปะทุของความได้เปรียบเชิงควอนตัม (Quantum advantage) ขั้นสมบูรณ์ในชั่วข้ามคืน

3. ระบบนิเวศยังไม่เติบโตเต็มที่: และยังคงต้องพึ่งพาเม็ดเงินอุดหนุนจากภาครัฐและการเป็นพันธมิตรเชิงกลยุทธ์ในระดับที่สูงเป็นพิเศษ

4. การประเมินในแต่ละภาคส่วนมักอิงจากการวิเคราะห์ฉากทัศน์: ซึ่งอาจมีความทับซ้อนกันในเชิงคอนเซปต์ ดังนั้นจึงไม่ควรนำตัวเลขเหล่านี้มาบวกสะสมรวมกันโดยปราศจากความระมัดระวัง

สำหรับ SCBX การตีความที่ถูกต้องจึงไม่ใช่การมองว่าการประมวลผลเชิงควอนตัมจะสร้างมูลค่าทันทีภายในปี 2035 แต่มันสะท้อนว่าบทความวิเคราะห์อิสระหลายสำนักต่างจัดให้ภาคการเงินเป็นหนึ่งในภาคส่วนที่มีโอกาสได้รับผลกระทบสูงสุดทั้งในแง่ของโอกาสทางธุรกิจและความเสี่ยงเชิงกลยุทธ์ หากเทคโนโลยีนี้เติบโตจนพร้อมใช้งาน ดังนั้น การรับมือที่เหมาะสมจึงไม่ใช่การทุ่มลงทุนเกินตัวเพื่อเก็งกำไร แต่คือ **การเตรียมความพร้อมอย่างรัดกุม** เพื่อสร้างความเข้าใจภายในองค์กร ระบุกรณีการใช้งานเฉพาะเจาะจงที่มีมูลค่าสูง ดำเนินโครงการนำร่องแบบไฮบริดเมื่อเห็นสมควร และติดตามระบบนิเวศนี้อย่างใกล้ชิดพร้อมที่จะสามารถเปลี่ยนแปลงได้อย่างทันท่วงที เมื่อเทคโนโลยีนี้ก้าวข้ามเส้นแบ่งจากแค่สิ่งที่น่าสนใจ ไปสู่สิ่งที่มีประโยชน์ทางเศรษฐกิจอย่างแท้จริง

CHAPTER 6

THAILAND POSITIONING



6.1 จุดเปลี่ยนเชิงยุทธศาสตร์ระดับชาติ (National Strategic Pivot)

การขับเคลื่อนด้านควอนตัมของไทยในตอนนี้ คือช่วงเริ่มต้นของการสร้างขีดความสามารถด้านควอนตัมของประเทศในหลายระดับ ปัจจุบันไทยมีรากฐานด้านนโยบายอย่างเป็นทางการแล้ว คือแผนที่นำทางเทคโนโลยีควอนตัมของประเทศไทย 2020 - 2029 ซึ่งจัดทำขึ้นภายใต้กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) แผนนี้กำหนดให้เทคโนโลยีควอนตัมทุกด้านเป็นเสาหลักเชิงยุทธศาสตร์ในการพัฒนาประเทศระยะยาว

แผนที่นำทางฉบับนี้เกิดจากการร่วมเขียนและผลักดันโดย QTRic (Quantum Technology Research Initiative Consortium) ซึ่งเป็นเครือข่ายความร่วมมือของกลุ่มนักวิจัยด้านควอนตัมในประเทศไทย ที่มุ่งเน้นการพัฒนาเทคโนโลยีควอนตัมแบบครบวงจร โดยไม่จำกัดเพียงแค่การประมวลผลเชิงควอนตัมเท่านั้น แต่ยังครอบคลุมขยายไปถึงการจำลองสถานการณ์เชิงควอนตัม (Quantum simulation) การสื่อสารเชิงควอนตัม (Quantum communication) รวมถึงการรับรู้และมาตรวิทยาเชิงควอนตัม (Quantum sensing and metrology)

ภายใต้บริบทดังกล่าว เป้าหมายระดับชาติจึงไม่ได้ถูกวางกรอบไว้ที่การพึ่งพาตนเองทางเทคโนโลยีอย่างเบ็ดเสร็จในทันที แต่เป็นการยกระดับขึ้นไปตามห่วงโซ่มูลค่า ในลักษณะค่อยเป็นค่อยไป เริ่มจากการเป็นเพียงผู้ใช้เทคโนโลยีดิจิทัลนำเข้า สู่การสร้างบุคลากรผู้เชี่ยวชาญภายในประเทศ การวางโครงสร้างพื้นฐานด้านการวิจัย และการก้าวขึ้นเป็นเจ้าของเทคโนโลยี ในขอบเขตเฉพาะทางที่ได้รับการคัดสรรแล้ว ซึ่งขณะนี้ นโยบายภาครัฐ หลักสูตรในระดับมหาวิทยาลัย และการเคลื่อนไหวในระยะเริ่มต้นของภาคเอกชน กำลังเริ่มปรับทิศทางให้สอดรับกับเป้าหมายดังกล่าวอย่างเป็นรูปธรรม

แรงขับเคลื่อนได้เร่งตัวขึ้นในปี 2026 เมื่อวันที่ 3 สิงหาคม 2026 กระทรวง อว. กลุ่มซีพี บริษัท ทรู คอร์ปอเรชั่น Arise Ventures, QTRic, และ qBraid แพลตฟอร์มซอฟต์แวร์จากสหรัฐฯ ได้ร่วมกันเปิดตัว Quantum Club Thailand ที่ True Digital Park กรุงเทพมหานคร โดยเป็น 3 โครงการเรือธงที่ประกอบไปด้วย ศูนย์กลางการพัฒนากำลังคน (Quantum Academy Thailand) ห้องปฏิบัติการร่วมระหว่างภาคธุรกิจ นักวิจัย และผู้ให้บริการเทคโนโลยี (Quantum Industry Lab) และเวที Hackathon ระดับชาติ และการจับคู่ธุรกิจ (Quantum Innovation Challenge)[6] แนวทางของประเทศไทยถูกอธิบายว่าเป็นแบบ 'Cloud-first' เข้าถึงคอมพิวเตอร์ควอนตัมชั้นนำผ่านระบบคลาวด์แทนการสร้างขึ้นเองในประเทศ ควบคู่กับการพัฒนาทักษะด้านฮาร์ดแวร์ในประเทศ[7]

6.2 Siam Quantum Square (SQ²)

หมุดหมายสำคัญระดับสถาบันที่เพิ่งเกิดขึ้นเมื่อไม่นานมานี้ คือการเปิดตัว **Siam Quantum Square (SQ²)** ณ จุฬาลงกรณ์มหาวิทยาลัย เมื่อวันที่ 26 มกราคม 2026 ตามวิสัยทัศน์ของมหาวิทยาลัย SQ² ถูกตั้งเป้าให้เป็นศูนย์กลางด้านควอนตัมระดับชาติ (National quantum hub) สำหรับการศึกษาวิจัย การพัฒนาบุคลากร และการทำงานร่วมกันข้ามภาคส่วน

ศูนย์แห่งนี้มุ่งเน้นในหลายสาขา ได้แก่:

- การประมวลผลเชิงควอนตัมและอัลกอริทึมควอนตัม ปัญญาประดิษฐ์เชิงควอนตัม (Quantum AI) หรือที่รู้จักกันในชื่อ การเรียนรู้ของเครื่องเชิงควอนตัม (Quantum machine learning)
- ระบบคิวบิตแบบตัวนำยวดยิ่งและฮาร์ดแวร์ควอนตัมเชิงทดลอง (Superconducting qubit systems and experimental quantum hardware)

การดำเนินกิจกรรมต่าง ๆ ของศูนย์ได้รับการสนับสนุนจากโครงการวิจัยระดับชาติ ซึ่งรวมถึงโครงการพลิกโฉมมหาวิทยาลัย หน่วยบริหารและจัดการทุนด้านการพัฒนากำลังคน และทุนด้านการพัฒนาสถาบันอุดมศึกษาการวิจัยและการสร้างนวัตกรรม (บพค. หรือ PMU-B) ภายใต้กระทรวง อว.[3] ตลอดจนเงินทุนสนับสนุนภายในของจุฬาลงกรณ์มหาวิทยาลัย เช่น CU Power Grant

ความเชี่ยวชาญ (Expertise): SQ² ผสมผสานงานวิจัยพื้นฐานเข้ากับการประยุกต์ใช้จริงเพื่อตอบโจทย์ภาคอุตสาหกรรม

- **ในมิติทางวิทยาศาสตร์:** ศูนย์แห่งนี้ดำเนินการวิจัยเชิงวิชาการอย่างเข้มข้นในด้านฟิสิกส์และคณิตศาสตร์ที่เป็นรากฐานของ Quantum AI รวมถึงอัลกอริทึมควอนตัมกลุ่มใหม่ ๆ ที่มีศักยภาพในการประมวลผลข้อมูลในรูปแบบที่แตกต่างจากการประมวลผลแบบคลาสสิกอย่างสิ้นเชิง
- **ในมิติเชิงทดลอง:** SQ² กำลังพัฒนาความเชี่ยวชาญด้านวัสดุตัวนำยวดยิ่ง และการผลิตฟิล์มบาง เพื่อสนับสนุนงานวิจัยระยะยาวในการสร้างขีดความสามารถด้านฮาร์ดแวร์ควอนตัมภายในประเทศ
- **ที่สำคัญ ศูนย์แห่งนี้ยังถูกจัดโครงสร้างมาเพื่อให้ทำงานร่วมกับภาคอุตสาหกรรมโดยตรง:** ความร่วมมือกับพันธมิตรอย่าง **SCBX** (ซึ่งเป็นทางการผ่านบันทึกข้อตกลงความร่วมมือ (MoU) ในเดือนพฤษภาคม 2026; ดูหัวข้อ 6.3) เปิดโอกาสให้นักวิจัยได้ศึกษาว่าเทคโนโลยีควอนตัมคอมพิวติงจะสามารถทำงานในสภาพแวดล้อมจริงขององค์กรธุรกิจได้อย่างไร และโจทย์ปัญหาทางการเงินหรืออุตสาหกรรมประเภทใดที่จะได้รับประโยชน์สูงสุดจากความได้เปรียบเชิงควอนตัม

นอกจากนี้ SQ² ยังให้บริการคำปรึกษาและโปรแกรมเตรียมความพร้อมสำหรับบริษัทและหน่วยงานภาครัฐที่สนใจเตรียมตัวรับมือกับยุคควอนตัม พร้อมกันนี้ ศูนย์ยังมีแผนที่จะเปิดตัวหลักสูตรควอนตัมระดับบัณฑิตศึกษาสำหรับนักศึกษามหาวิทยาลัยอีกด้วย



วิสัยทัศน์และแนวโน้มในอนาคต (Vision and Future Prospect): ภารกิจระยะยาวของ SQ² ก้าวไกลไปกว่าแค่งานวิจัยเชิงวิชาการ ศูนย์แห่งนี้ตั้งเป้าที่จะเป็นเสาหลักทางยุทธศาสตร์ สำหรับระบบนิเวศควอนตัมที่กำลังเติบโตของประเทศไทย โดยมุ่งเน้นที่วัตถุประสงค์หลักดังต่อไปนี้

- ยกระดับตนเองให้เป็นศูนย์กลางการวิจัยด้านวิทยาศาสตร์และเทคโนโลยีควอนตัมที่เป็นที่ยอมรับในระดับสากล
- สร้างจุดเชื่อมโยงที่แข็งแกร่งระหว่างงานวิจัยเชิงวิชาการและการประยุกต์ใช้ในภาคอุตสาหกรรม
- สนับสนุนองค์กรต่าง ๆ ให้มีความพร้อมด้านควอนตัม ผ่านการฝึกอบรมและการทำงานร่วมกัน
- บ่มเพาะนักวิทยาศาสตร์ วิศวกร และนักพัฒนาด้านควอนตัมรุ่นใหม่
- มีส่วนร่วมในการสร้างระบบนิเวศนวัตกรรมควอนตัมระดับชาติที่ยั่งยืน

ในทางปฏิบัติ สิ่งนี้หมายถึงการสร้างโครงสร้างพื้นฐานที่จำเป็นสำหรับนักวิจัยและวิศวกรชาวไทย เพื่อประยุกต์ความรู้ทางฟิสิกส์ควอนตัมให้กลายเป็นเทคโนโลยีที่นำไปใช้งานได้จริง ผ่านความพยายามเหล่านี้ SQ² มุ่งหวังที่จะเสริมสร้างฐานกำลังคนด้านความคิดและเทคโนโลยีของประเทศไทยโดยการติดอาวุธทักษะขั้นสูงให้กับนักฟิสิกส์ วิศวกร และนักวิทยาศาสตร์ข้อมูล เพื่อให้มีความพร้อมในการเข้าไปมีส่วนร่วมในเศรษฐกิจเทคโนโลยีควอนตัมระดับโลก

การเชื่อมโยงระดับนานาชาติ (International connections): เพื่อรับประกันว่าจะสามารถบูรณาการเข้ากับห่วงโซ่อุปทานควอนตัมระดับโลกที่มีการแบ่งส่วนย่อยอย่างชัดเจนได้อย่างทันท่วงที SQ² จึงได้ผนึกกำลังสร้างพันธมิตรเชิงกลยุทธ์ระดับสูงกับผู้นำด้านเทคโนโลยีระดับนานาชาติ ความร่วมมือกับหน่วยงานต่าง ๆ เช่น IBM Thailand, Western Digital, Qunova Computing จากเกาหลีใต้ และสถาบันวิทยาศาสตร์และเทคโนโลยีอุตสาหกรรมขั้นสูงแห่งชาติของญี่ปุ่น (AIST) เพื่อช่วยให้ระบบนิเวศควอนตัมภายในประเทศของไทยยังคงเชื่อมโยงและก้าวทันพัฒนาการระดับแนวหน้าของโลกอยู่เสมอ ในเดือนกันยายน 2026 ความสัมพันธ์เหล่านี้ได้รับการยกระดับเป็นทางการผ่านบันทึกข้อตกลงความร่วมมือ (MoU) ระยะ 3 ปีกับ Qunova Computing และ MoU ระยะ 5 ปีกับ AIST โดยฉบับหลังรวมถึงการเข้าถึงโครงสร้างพื้นฐานด้านการประมวลผลเชิงควอนตัมของ AIST ด้วย [9][10]

6.3 ผู้ขับเคลื่อนหลักจากภาคธุรกิจอุตสาหกรรม (Key Players From Industrial Sector)

ในภาคเอกชน ผู้เล่นหลักรายหนึ่งคือ Quantum Technology Foundation (Thailand) หรือ QTFT บริษัทที่ปรึกษาในกรุงเทพมหานคร ซึ่งพัฒนาเครื่องมือที่พร้อมรองรับคอมพิวเตอร์ควอนตัม สำหรับสร้างแบบจำลองและหาค่าที่เหมาะสมที่สุดให้กับเครือข่ายที่ซับซ้อนขององค์กร โดยทาง QTFT เน้นการนำค่าที่เหมาะสมที่สุดไปใช้งานจริงและการเตรียมความพร้อมให้องค์กร มากกว่าการพัฒนาฮาร์ดแวร์ จึงเกี่ยวข้องเป็นพิเศษกับอุตสาหกรรมอย่างโลจิสติกส์ พลังงาน และบริการทางการเงิน [2] นอกจากนี้ QTFT ยังมีบทบาทสำคัญในการผลักดันให้ประเทศเปลี่ยนผ่านสู่ยุคควอนตัมได้อย่างปลอดภัยและราบรื่น ด้วยการนำการเข้ารหัสที่ทนต่อคอมพิวเตอร์ควอนตัม เข้าไปใช้ในระบบดิจิทัลของทั้งภาครัฐและภาคธุรกิจในเชิงรุก

องค์กรจากภาคอุตสาหกรรมที่สร้างคุณูปการสำคัญอีกรายคือ **SCBX** ซึ่งได้เริ่มลงทุนในการสำรวจเทคโนโลยีควอนตัม และถือเป็นหนึ่งในองค์กรขนาดใหญ่กลุ่มแรก ๆ ของไทยที่ตื่นตัวในการเตรียมความพร้อมสู่ยุคควอนตัมอย่างจริงจัง SCBX ได้ร่วมมือกับ SQ² เพื่อสืบค้นและประเมิน

ความเป็นไปได้ในการประยุกต์ใช้เทคโนโลยีการประมวลผลควอนตัมในภาคการเงิน ความร่วมมือนี้ครอบคลุมถึงการวิจัยอัลกอริทึมควอนตัมเพื่อแก้โจทย์ปัญหาสำคัญทางการเงิน เช่น การหาค่าเหมาะสมที่สุดของพอร์ตโฟลิโอ และการตรวจจับการทุจริต ตลอดจนการสำรวจในภาพกว้างว่าเทคโนโลยีการประมวลผลควอนตัมจะสามารถเข้ามายกระดับการสร้างแบบจำลองทางการเงินและการวิเคราะห์ความเสี่ยงได้อย่างไร โดยในเดือนพฤษภาคม 2026 SCBX และจุฬาลงกรณ์มหาวิทยาลัยได้ยกระดับความร่วมมือนี้ให้เป็นทางการผ่านบันทึกข้อตกลงความร่วมมือ (MoU) ซึ่งครอบคลุมการวิจัยแนวหน้า กิจกรรมสร้างระบบนิเวศ และการร่วมจัดทำรายงาน SCBX Quantum Outlook ฉบับนี้ [8]

นอกเหนือจากความพยายามด้านการวิจัย SCBX ยังมีส่วนร่วมสำคัญในการพัฒนาระบบนิเวศควอนตัมในภาพรวมของประเทศไทยในมิติของภาคอุตสาหกรรม โดย SCBX กำลังทำงานร่วมกับ QTFT ในการนำ PQC มาประยุกต์ใช้จริง ซึ่งเป็นการตอกย้ำจุดยืนขององค์กรในฐานะกลุ่มผู้เปิดรับเทคโนโลยีระดับผู้บุกเบิก ที่มุ่งเตรียมความพร้อมโครงสร้างพื้นฐานทางการเงินให้แข็งแกร่งสำหรับยุคความมั่นคงปลอดภัยหลังยุคควอนตัม

ซึ่งกลุ่มบริษัทขนาดใหญ่ของไทยก็กำลังก้าวเข้าสู่สาขานี้เช่นกัน กลุ่มซีพีและ ทรู คอร์ปอเรชั่น ได้ร่วมก่อตั้ง Quantum Club Thailand ในปี 2026 และใช้ True Digital Park เป็นศูนย์กลางให้บริษัทในประเทศได้ทดสอบแอปพลิเคชันควอนตัมแบบไฮบริด โดยมีเป้าหมายที่ประกาศไว้ว่าจะวางตำแหน่งประเทศไทยให้เป็นศูนย์กลางควอนตัมของอาเซียน [6]

6.4 ระบบนิเวศการวิจัยด้านควอนตัมของไทยแบบกระจายศูนย์ (A Distributed Thai Quantum Research Ecosystem)

กิจกรรมด้านควอนตัมของประเทศไทยมีการกระจายตัวในเชิงภูมิศาสตร์เช่นกัน แทนที่จะกระจุกตัวขีดความสามารถทั้งหมดไว้ที่สถาบันเพียงแห่งเดียว ระบบนิเวศนี้กำลังพัฒนาผ่านรูปแบบเครือข่าย (Networked model) โดยที่มหาวิทยาลัยแต่ละแห่งจะนำเสนอจุดแข็งที่แตกต่างกัน ซึ่งจะขาดกลไกการประสานงานที่สำคัญในส่วนนี้ไปไม่ได้ คือ QTRic ที่ได้รับการนำเสนอผ่านช่องทางการทูตด้านวิทยาศาสตร์ของไทย ว่าเป็นส่วนหนึ่งของการลงทุนระดับชาติในวงกว้างสำหรับวิทยาศาสตร์ขั้นแนวหน้า [4] สิ่งนี้ได้สร้างระบบนิเวศควอนตัมระดับชาติที่ครอบคลุม ซึ่งภาคอุตสาหกรรมสามารถเข้ามาเชื่อมต่อและใช้ประโยชน์ได้อย่างไร้รอยต่อ:

- **ภาคกลาง (กรุงเทพมหานคร) – จุฬาลงกรณ์มหาวิทยาลัย:** ทำหน้าที่เป็นแกนหลักของเครือข่ายระดับชาติในด้านการประมวลผลเชิงควอนตัม และอัลกอริทึมควอนตัม รวมถึงเป็นที่ตั้งของศูนย์ SQ² ศูนย์กลางแห่งนี้มุ่งเน้นเชิงลึกไปที่ทฤษฎีการประมวลผลเชิงควอนตัม เทคโนโลยีคิวบิตแบบตัวนำยวดยิ่ง (Superconducting qubit), การพัฒนาอัลกอริทึม และวิศวกรรมซอฟต์แวร์ ควบคู่ไปกับการพัฒนาบุคลากรและการจัดการศึกษาสำหรับผู้บริหารในภาคธุรกิจ สำหรับภาคส่วนต่าง ๆ เช่น ภาคการเงิน จุดนี้ทำให้กรุงเทพมหานคร มีความสำคัญมากในฐานะจุดบรรจบที่ขีดความสามารถด้านการวิจัย การฝึกอบรมระดับองค์กร และการพัฒนากรณีการใช้งานในระยะเริ่มต้น สามารถดำเนินการร่วมกันได้

- **ภาคตะวันออกเฉียงเหนือ – มหาวิทยาลัยเทคโนโลยีสุรนารี (SUT):** ในฐานะที่เป็นที่ตั้งของ QTRic มหาวิทยาลัยเทคโนโลยีสุรนารีมีบทบาทสำคัญในเครือข่ายระดับชาติผ่านทั้งกลุ่ม QTRic และผ่านผลงานที่โดดเด่นในด้านการรับรู้เชิงควอนตัม (Quantum sensing) เอกสารเผยแพร่และบันทึกการประชุมของ SUT แสดงให้เห็นถึงกิจกรรมที่เกี่ยวข้องกับการวัดสนามแม่เหล็กด้วย NV-diamond magnetometry และการรับรู้เชิงควอนตัม ซึ่งรวมถึงวิทยานิพนธ์เกี่ยวกับการถ่ายภาพสนามแม่เหล็กด้วยเซนเซอร์เพชรควอนตัม และการจัดประชุมวิชาการเกี่ยวกับเทคโนโลยีเครื่องวัดสนามแม่เหล็กด้วยเพชรควอนตัม สิ่งนี้วางตำแหน่งให้ SUT เป็นศูนย์กลางที่สำคัญยิ่งสำหรับการวิจัยด้านการรับรู้และมาตรวิทยาเชิงควอนตัม (Metrology-oriented quantum research) [5] นอกจากนี้ วิทยาลัยเพื่อการค้นคว้าระดับรากฐาน (IF) – มหาวิทยาลัยนเรศวร ได้เริ่มดำเนินงานด้าน PQC โดยความร่วมมือกับ QTFT

- **ภาคเหนือ – มหาวิทยาลัยเชียงใหม่ (CMU):** เป็นผู้นำระดับชาติในการวิจัยเชิงทดลองด้านการจำลองสถานการณ์เชิงควอนตัม (Experimental Quantum Simulation) CMU ใช้ประโยชน์จากการจัดเตรียมระบบทางกายภาพขั้นสูง เช่น การทดลองการจำลองด้วยอะตอมเป็นกลาง (Neutral atom simulation)—โดยมีเป้าหมายเพื่อสร้างแบบจำลองปฏิกิริยาทางเคมี ชีววิทยา และฟิสิกส์ที่มีความซับซ้อนได้อย่างแม่นยำ แพลตฟอร์มดังกล่าวยังสามารถนำมาใช้เพื่อศึกษาสถานะควอนตัมแบบพิเศษ (Exotic quantum phases) ได้อีกด้วย

- **ภาคใต้ – มหาวิทยาลัยสงขลานครินทร์ (PSU):** รับหน้าที่หลักด้านการวิจัยการสื่อสารเชิงควอนตัมโดย PSU เป็นผู้บุกเบิกการทดลองที่สำคัญเกี่ยวกับโปรโตคอลการกระจายคีย์เชิงควอนตัม (Quantum Key Distribution หรือ QKD) โดย QKD สามารถกระจายกุญแจเข้ารหัสผ่านลิงก์เฉพาะทางได้ ในขณะที่ PQC เป็นเส้นทางที่นำไปใช้งานได้กว้างขวางกว่าในการปกป้องเครือข่ายทางการเงินและภาครัฐจากการโจมตีด้วยควอนตัม

6.5 การขับเคลื่อนไปข้างหน้าร่วมกัน (Moving Forwards Together)

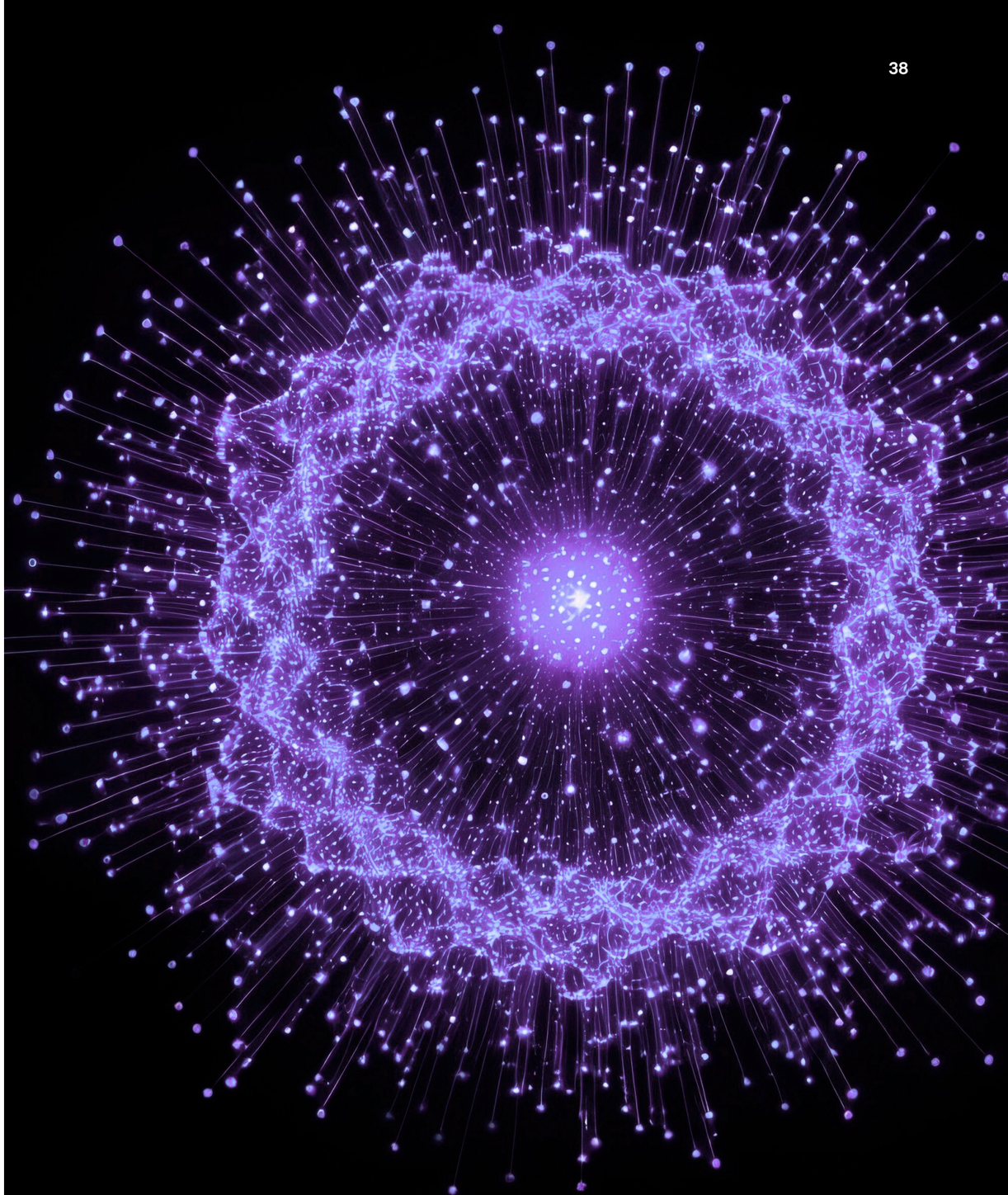
เมื่อพิจารณาในภาพรวม ลักษณะการกระจายตัวของโครงการริเริ่มระดับชาติต่าง ๆ เหล่านี้ สะท้อนให้เห็นถึงกลยุทธ์ที่เน้นผลลัพธ์ในทางปฏิบัติอย่างชัดเจนความได้เปรียบทางการแข่งขัน ของประเทศไทยอาจไม่ได้มาจากการพยายามสร้างโครงสร้างฮาร์ดแวร์ควอนตัมแบบเต็มรูปแบบซึ่งต้องใช้เงินลงทุนมหาศาล เพื่อแข่งกับมหาอำนาจระดับโลก แต่จะมาจากการสร้างระบบนิเวศที่สอดประสานกัน มีความเชี่ยวชาญเฉพาะด้าน และเชื่อมโยงกับเครือข่ายระดับนานาชาติ โมเดลดังกล่าวสอดคล้องโดยตรงกับความเป็นจริงของห่วงโซ่อุปทานที่ได้สรุปไว้ในส่วนที่ 5.1 ประเทศไทยไม่จำเป็นต้องครอบครองห่วงโซ่อุปทานของการประมวลผลควอนตัมทั้งหมด เพื่อที่จะเข้าไปมีบทบาทสำคัญ

ด้วยการมุ่งเน้นไปที่ระดับชั้นโครงสร้าง เฉพาะกลุ่มที่มีมูลค่าสูง เช่น การพัฒนาอัลกอริทึม การบูรณาการซอฟต์แวร์แบบไฮบริด และเทคโนโลยีเฉพาะกลุ่มเชิงยุทธศาสตร์ภายในประเทศ อย่างการรับรู้เชิงควอนตัมประเทศไทยจะสามารถเข้าสู่ตลาดโลกในจุดที่ขีดความสามารถภายในประเทศกำลังฉายแววความโดดเด่น ซึ่งจะช่วยยกระดับอธิปไตยทางเทคโนโลยี และบทบาททางเศรษฐกิจให้ลึกซึ้งยิ่งขึ้นเมื่อเวลาผ่านไป

อย่างไรก็ตาม การขับเคลื่อนกลยุทธ์ด้านความเชี่ยวชาญเฉพาะด้านอย่างชาญฉลาดนี้ จำเป็นต้องอาศัยความร่วมมืออย่างเป็นเอกภาพจากทุกภาคส่วนการแปรเปลี่ยนงานวิจัยเชิงวิชาการให้กลายเป็นมูลค่าทางเศรษฐกิจที่จับต้องได้นั้น เรียกร้องให้ภาคธุรกิจอุตสาหกรรม ผู้มีส่วนได้ส่วนเสียจากภาครัฐ และผู้เชี่ยวชาญด้านควอนตัม ต้องทำงานร่วมกันอย่างสอดประสานเป็นเนื้อเดียวกัน หน่วยงานภาครัฐจะต้องเดินหน้าจัดเตรียมโครงสร้างพื้นฐานทางดิจิทัลและกรอบการสนับสนุนด้านเงินทุนต่อไป ส่วนศูนย์กลางทางวิชาการและการวิจัย เช่น SQ² และ QTRic ต้องยังคงมุ่งเน้นไปที่การขับเคลื่อนวิทยาศาสตร์ประยุกต์และบ่มเพาะบุคลากรให้มีความพร้อมสู่ยุคควอนตัม

ประการสำคัญ ผู้นำภาคอุตสาหกรรมที่มีวิสัยทัศน์ก้าวไกลและองค์กรที่ทำหน้าที่เชื่อมโยงอุตสาหกรรมเช่น SCBX และ QTFT จะต้องสวมบทบาทเป็นตัวเร่งให้เกิดผลลัพธ์ที่จับต้องได้ในเชิงพาณิชย์ ด้วยการกำหนดกรณีการใช้งานทางธุรกิจที่มีมูลค่าสูง การจัดเตรียมภูมิทัศน์ข้อมูลจริงที่มีความซับซ้อนและการริเริ่มโครงการนำร่องสำหรับกระบวนการทำงานแบบไฮบริดตั้งแต่วันนี้ ภาคเอกชนจะเป็นผู้สร้างสัญญาณความต้องการ ที่สำคัญ ซึ่งจะช่วยเร่งการเติบโตของระบบนิเวศระดับชาติทั้งระบบ

ท้ายที่สุดแล้ว การก้าวไปข้างหน้าร่วมกันจะเป็นหลักประกันว่า ประเทศไทยจะไม่เป็นเพียงแค่ผู้รอรับเทคโนโลยีในการปฏิวัติควอนตัมที่กำลังจะมาถึง แต่จะก้าวขึ้นเป็นผู้มีส่วนร่วมที่แข็งแกร่ง บูรณาการเป็นหนึ่งเดียว และสามารถสร้างมูลค่าเพิ่ม ให้กับเทคโนโลยีแห่งอนาคตนี้ได้อย่างแท้จริง



บทสรุปส่งท้าย: ความจำเป็นเร่งด่วนเชิงยุทธศาสตร์ด้านควอนตัม (Ending Remarks: The Quantum Imperative)



การเปลี่ยนผ่านจากระบบประมวลผลแบบคลาสสิกสู่การประมวลผลเชิงควอนตัม ไม่ใช่เพียงแค่การอัปเกรดระบบไอทีทั่วไป แต่มันคือการเปลี่ยนแปลงในระยะยาวต่อวิธีการนำเสนอ จำลองสถานการณ์ หาค่าเหมาะสมที่สุด และประมวลผลโจทย์ปัญหาที่มีความซับซ้อนระดับสูง แม้ว่าคอมพิวเตอร์ควอนตัมแบบสเกลใหญ่ที่ทนทานต่อข้อผิดพลาดเต็มรูปแบบจะยังคงอยู่ระหว่างการพัฒนา แต่ระยะแห่งการเตรียมความพร้อมได้เริ่มต้นขึ้นแล้ว ทั้งในภาคอุตสาหกรรมระดับโลกนโยบายระดับชาติ และทวีความเข้มข้นมากขึ้นในประเทศไทยเอง

สำหรับผู้นำองค์กรและผู้มีส่วนได้ส่วนเสียระดับชาติ ในเชิงปฏิบัติไม่ได้หมายความว่ามูลค่าทางควอนตัม จะการันตีผลลัพธ์ให้ในชั่วข้ามคืน แต่มันหมายความว่า การรอคอยจนกว่าเทคโนโลยีนี้จะกลายเป็นสินค้าที่เข้าถึงได้ทั่วไปอย่างสมบูรณ์อาจก่อให้เกิดช่องว่างทางขีดความสามารถที่มีมูลค่าความสูญเสียมหาศาล ดังนั้น การสร้างความพร้อมด้านควอนตัมตั้งแต่วันนี้ จึงถือเป็นความจำเป็นเร่งด่วนเชิงยุทธศาสตร์

องค์กรที่มีแนวโน้มจะได้รับประโยชน์สูงสุด คือองค์กรที่เริ่มต้นเตรียมตัวตั้งแต่ตอนนี้ และต้องเตรียมตัวอย่างมีแบบแผนด้วยการสร้างความรู้ความเข้าใจทางเทคนิค ระบุกรณีการใช้งานที่เฉพาะเจาะจงแต่มอบมูลค่าสูงเตรียมความพร้อมด้านสถาปัตยกรรมข้อมูลและความปลอดภัย และสร้างเครือข่ายพันธมิตรด้านการวิจัยและอุตสาหกรรมที่เหมาะสม และที่สำคัญเฉกเช่นเดียวกับเทคโนโลยีก้าวกระโดด อื่น ๆ บทลงโทษของการถูกทิ้งไว้ข้างหลังนั้นรุนแรงและมีราคาแพง ความเชี่ยวชาญทางเทคนิคอันซับซ้อนที่จำเป็นต่อการประยุกต์ใช้เทคโนโลยีนี้ หมายความว่าการพยายามไล่ตามคู่แข่งให้ทันในภายหลังจะเป็นกระบวนการที่เชื่องช้าและอาจยากลำบากยิ่งกว่ายุคของการปรับตัวรับเทคโนโลยี AI เสียด้วยซ้ำเมื่อเป็นเรื่องของควอนตัม

ดังนั้น เป้าหมายของประเทศไทยจึงไม่ควรเป็นการลอกเลียนแบบแนวทางของประเทศมหาอำนาจด้านควอนตัมรายใหญ่แบบทุกกระเบียดนิ้ว แต่ควรเป็นการพัฒนาจุดแข็งภายในประเทศที่แข็งแกร่ง เชื่อมโยงจุดแข็งเหล่านั้นเข้ากับเครือข่ายระดับโลก และสร้างความมั่นใจว่า เมื่อเทคโนโลยีควอนตัมกลายเป็นปัจจัยชี้วัดความสำเร็จทางเศรษฐกิจ ในอุตสาหกรรมเป้าหมายประเทศไทยจะไม่ได้เตรียมพร้อมเพียงแค่เพื่อเป็น ผู้รับเทคโนโลยีมาปรับใช้ เท่านั้น แต่ยังพร้อมที่จะก้าวขึ้นเป็นผู้สร้างสรรค์และมีส่วนร่วมต่อนวัตกรรมแห่งอนาคตนี้อย่างเต็มภาคภูมิ

Appendix

ภาคผนวก ก:

อภิธานศัพท์ (Appendix A: Glossary of Terms)

- **คิวบิต (Qubit):** หน่วยพื้นฐานของข้อมูลเชิงควอนตัม ซึ่งแตกต่างจากบิตคลาสสิก (ที่เป็นได้เพียง 0 หรือ 1) เนื่องจากคิวบิตสามารถดำรงอยู่ในสถานะทับซ้อน (Superposition) ซึ่งเป็นการแสดงผลที่รวมทั้งค่า 0 และ 1 เข้าด้วยกันได้ในเวลาเดียวกัน
- **ความพัวพันเชิงควอนตัม (Entanglement):** ปรากฏการณ์ทางควอนตัมที่คิวบิตเกิดการเชื่อมโยงกันในลักษณะที่ผลการวัดของคิวบิตเหล่านั้นมีความสัมพันธ์กัน (Correlated) ในรูปแบบที่ไม่มีสิ่งเทียบเท่าในโลกคลาสสิก ไม่ว่าจะอยู่ห่างไกลกันเพียงใดก็ตาม Entanglement ไม่ได้ส่งข้อมูลในทันที แต่เป็นทรัพยากรที่จำเป็นอย่างยิ่งสำหรับอัลกอริทึมควอนตัมและการแก้ไขข้อผิดพลาด
- **ความได้เปรียบเชิงควอนตัม (Quantum Advantage):** จุดที่คอมพิวเตอร์ควอนตัมสามารถแก้โจทย์ปัญหาที่มีความสำคัญเชิงพาณิชย์ได้รวดเร็วกว่า ถูกกว่า หรือแม่นยำกว่าวิธีคลาสสิกใด ๆ ที่รู้จัก (ระดับ 3 ในหัวข้อ 3.1) สื่อมักใช้คำนี้อย่างหลวมกว่า โดยหมายถึงงานใดก็ตามที่คอมพิวเตอร์ควอนตัมเอาชนะวิธีคลาสสิกได้
- **NISQ (Noisy Intermediate-Scale Quantum):** ยุคปัจจุบันของการพัฒนาฮาร์ดแวร์ควอนตัม ซึ่งโปรเซสเซอร์มีขนาดใหญ่เพียงพอที่จะประมวลผลงานที่ซับซ้อนได้ แต่ยังคงมีความอ่อนไหวต่อ “สัญญาณรบกวน (Noise)” จากสภาพแวดล้อม ซึ่งนำไปสู่การเกิดข้อผิดพลาดในการคำนวณ
- **ความทนทานต่อข้อผิดพลาด (Fault-Tolerance):** ขีดความสามารถของคอมพิวเตอร์ควอนตัมในการทำงานต่อไปได้อย่างถูกต้องแม่นยำ แม้ว่าส่วนประกอบย่อยบางชิ้นจะล้มเหลวหรือเกิดข้อผิดพลาดขึ้นในระบบ โดยบรรลุผลผ่านการใช้รหัสแก้ไขข้อผิดพลาด (Error-correction codes) ที่มีความซับซ้อนสูง
- **Physical Qubit กับ Logical Qubit (Physical vs. Logical Qubit):** Physical qubit คือองค์ประกอบฮาร์ดแวร์หน่วยเดียวที่มีโอกาสเกิดข้อผิดพลาด ส่วน Logical qubit คือคิวบิตที่เชื่อถือได้มากกว่า ซึ่งสร้างขึ้นจากการรวม Physical qubits จำนวนมากเข้าด้วยกันพร้อมการแก้ไขข้อผิดพลาด—เปรียบเสมือนทีมงานที่คอยตรวจสอบงานของกันและกัน
- **การแก้ไขข้อผิดพลาดเชิงควอนตัม (Quantum Error Correction หรือ QEC):** เทคนิคที่กระจายข้อมูลไปยัง Physical qubits จำนวนมาก เพื่อให้สามารถตรวจจับและแก้ไขข้อผิดพลาดได้ระหว่างการคำนวณโดยไม่ทำลายสถานะควอนตัม
- **Magic States / T-gate:** ทรัพยากรพิเศษที่จำเป็นสำหรับการดำเนินการประเภทเดียว (“T-gate”) ซึ่งโครงร่างการแก้ไขข้อผิดพลาดมาตรฐานไม่สามารถป้องกันได้ในต้นทุนต่ำ การผลิตทรัพยากรเหล่านี้อย่างมีประสิทธิภาพเป็นความท้าทายทางวิศวกรรมที่สำคัญ
- **วิทยาการเข้ารหัสลับหลังยุคควอนตัม (Post-Quantum Cryptography หรือ PQC):** วิธีการเข้ารหัสแบบใหม่ที่ได้รับการกำหนดมาตรฐานโดยหน่วยงานอย่าง NIST ซึ่งทำงานบนคอมพิวเตอร์ในปัจจุบัน แต่ถูกออกแบบมาให้ต้านทานการโจมตีจากคอมพิวเตอร์ควอนตัมในอนาคต
- **CRQC / Q-Day:** คอมพิวเตอร์ควอนตัมที่มีนัยสำคัญต่อการเข้ารหัส (Cryptographically relevant quantum computer หรือ CRQC) คือเครื่องที่ทรงพลังพอจะถอดรหัสกุญแจสาธารณะที่ใช้ในปัจจุบันได้ ส่วน “Q-Day” คือวันที่เครื่องดังกล่าวถือกำเนิดขึ้น
- **อัลกอริทึมควอนตัมแบบแปรผัน (Variational Quantum Algorithm หรือ VQA):** แนวทางการประมวลผลแบบไฮบริด ที่ใช้ขุมพลังของทั้งคอมพิวเตอร์ควอนตัมและคอมพิวเตอร์แบบคลาสสิกร่วมกันเพื่อแก้ปัญหาการหาค่าเหมาะสมที่สุด (Optimization problems) ซึ่งถูกใช้อย่างแพร่หลายในการทดลองระยะใกล้ในปัจจุบัน แม้ว่าความสนใจกำลังเปลี่ยนไปสู่อัลกอริทึมที่มีการแก้ไขข้อผิดพลาดในระยะแรก (Early error-corrected algorithms)

ภาคผนวก ข:

เจาะลึกเชิงเทคนิค – งานวิจัยการหาค่าเหมาะสมที่สุดของพอร์ตโฟลิโอโดย SCBX
(Appendix B: Technical Deep-Dive – SCBX Portfolio Optimization Research)

เนื้อหาส่วนนี้อธิบายถึงผลการค้นพบเบื้องต้น (Preliminary finding) จากงานวิจัยที่ดำเนินการภายใต้ความร่วมมือระหว่าง SCBX และจุฬาลงกรณ์มหาวิทยาลัย ในหัวข้อ “การหาค่าเหมาะสมที่สุดของพอร์ตโฟลิโอภายใต้เงื่อนไขข้อจำกัด (Portfolio Optimization with Constraint)”

- **โจทย์ปัญหา: การบังคับใช้เงื่อนไขข้อจำกัด (The Problem: Constraint Enforcement)** ในการสร้างแบบจำลองทางการเงิน (Financial modeling) พอร์ตโฟลิโอจะต้องเป็นไปตามกฎเกณฑ์ที่ถูกกำหนดไว้อย่างเข้มงวด (เช่น “ต้องลงทุนให้ครบ 100% ของงบประมาณพอดี” หรือ “ต้องเลือกสินทรัพย์จำนวน 5 รายการเท่านั้น”) แนวทางปฏิบัติทางควอนตัมแบบมาตรฐาน (Standard quantum approaches) มักจะเสียเวลาไปกับการสำรวจผลลัพธ์ที่ “ไม่ถูกต้องตามเงื่อนไข (Invalid solutions)” ซึ่งทำให้สูญเสียทรัพยากรเวลาในการประมวลผลและลดทอนความแม่นยำของผลลัพธ์ลง
- **ทางออก: วงจรตัวผสมแบบรักษาสถานะ (The Solution: The Preserving Mixer)** งานวิจัยชิ้นนี้ได้นำเสนอสถาปัตยกรรมวงจรควอนตัมแบบเฉพาะทางที่เรียกว่า “Preserving Mixer” สถาปัตยกรรมดังกล่าวใช้หลักการทางคณิตศาสตร์ในการจำกัดพื้นที่การค้นหา (Search space) ของคอมพิวเตอร์ควอนตัม ให้ครอบคลุมเฉพาะกลุ่มพอร์ตโฟลิโอที่ผ่านเกณฑ์และตรงตามเงื่อนไขข้อจำกัดที่กำหนดไว้ล่วงหน้าทั้งหมดเท่านั้น แนวทางนี้ต่อยอดจากกรอบแนวคิด “Quantum Alternating Operator Ansatz” ของ Hadfield และคณะ (2019) ซึ่งเป็นผู้เสนอ Constraint-preserving mixers เป็นครั้งแรก และปรับให้เหมาะกับเงื่อนไขข้อจำกัดของพอร์ตโฟลิโอตามจริง

เกณฑ์มาตรฐานประสิทธิภาพหลัก (Key Performance Benchmarks):

- **ความเสถียรในการฝึกฝนโมเดล (Training Stability):** ระเบียบวิธีวิจัยของเราแสดงให้เห็นถึงอัตราส่วนความน่าจะเป็นสูงสุด (MaxProb ratio) ที่สูงขึ้นอย่างมีนัยสำคัญ ซึ่งหมายความว่าอัลกอริทึมสามารถค้นหาคำตอบที่เหมาะสมที่สุด (Optimal solution) ได้ด้วยระดับความสม่ำเสมอ (Consistency) ที่สูงกว่ามาก (MaxProb วัดว่าอัลกอริทึมมีโอกาสมากเพียงใดที่จะให้ผลลัพธ์เป็นพอร์ตโฟลิโอที่ดีที่สุดเพียงหนึ่งเดียว)
- **ความสามารถในการขยายสเกล (Scalability):** ด้วยการบรรเทาผลกระทบจากปรากฏการณ์บาร์เรนพลาโต หรือ Barren Plateau effect (ภาวะที่สัญญาณการฝึกฝนโมเดลจางหายไปในระบบขนาดใหญ่) แนวทางนี้คาดว่าจะช่วยให้กระบวนการหาค่าเหมาะสมที่สุด (Optimization) ยังคงฝึกฝนได้ (Trainable) เมื่อโจทย์ปัญหาขยายขนาดเกินกว่าการทดลองระดับ 11 คิวบิตที่ดำเนินการมาจนถึงปัจจุบัน — ซึ่งเป็นสัญญาณที่น่าพอใจ แต่ยังต้องได้รับการยืนยันบนโจทย์ที่ใหญ่ขึ้นและบนฮาร์ดแวร์จริง

ภาคผนวก ค:

รายการตรวจสอบความพร้อมสู่ยุคควอนตัม
(Appendix C: The Quantum Readiness Checklist)

องค์กรต่าง ๆ สามารถใช้กรอบการทำงาน (Framework) นี้ เพื่อประเมินสถานะปัจจุบันของตนเอง และเตรียมความพร้อมสำหรับการเปลี่ยนผ่านสู่การดำเนินงานที่ยกระดับด้วยเทคโนโลยีควอนตัม (Quantum-enhanced operations)

1. การระบุเป้าหมายเชิงกลยุทธ์ (Strategic Identification): ระบุโจทย์ปัญหาด้านการหาค่าเหมาะสมที่สุด (Optimization) หรือการจำลองสถานการณ์ (Simulation) ที่ “ยากเกินขีดจำกัดของระบบปัจจุบัน (Intractable)” จำนวน 3 อันดับแรกภายในหน่วยธุรกิจหลักขององค์กร (เช่น การสร้างแบบจำลองความเสี่ยง, การจัดการห่วงโซ่อุปทาน, หรือการค้นคว้าโมเลกุลใหม่)

2. ผู้นำการขับเคลื่อนด้านควอนตัม (Quantum Champion): แต่งตั้งผู้นำทางเทคนิคหรือ “Quantum Champion” เพื่อทำหน้าที่ติดตามความคืบหน้าของหมุดหมายทางฮาร์ดแวร์ และบริหารจัดการแผนที่นำทาง (Roadmap) ขององค์กร

3. สถาปัตยกรรมข้อมูล (Data Architecture): ตรวจสอบให้แน่ใจว่าระบบส่งผ่านข้อมูล (Data pipelines) มีการจัดระเบียบที่ “สะอาด (Clean)” และมีศักยภาพพร้อมที่จะป้อนข้อมูลเข้าสู่กระบวนการทำงานแบบไฮบริดระหว่างระบบคลาสสิกและควอนตัม (Hybrid classical-quantum workflows)

4. การวางแผนผังระบบนิเวศ (Ecosystem Mapping): ระบุเครือข่ายพันธมิตรที่มีศักยภาพทั้งจากภาควิชาการและภาคอุตสาหกรรม (เช่น SQ²) เพื่อร่วมขับเคลื่อนโครงการริเริ่มด้านการวิจัยและพัฒนา (Joint R&D initiatives)

5. การตรวจสอบระบบรักษาความปลอดภัยเชิงรหัสลับ (Cryptography Audit): ประเมินความมั่นคงปลอดภัยของข้อมูลในระยะยาวขององค์กร และเริ่มต้นวางแผนสำหรับการเปลี่ยนผ่านไปสู่ PQC ในเมื่อหน่วยงานกำกับดูแลเริ่มกำหนดเส้นตายที่ชัดเจนแล้ว (เช่น คำสั่งฝ่ายบริหารสหรัฐฯ ฉบับที่ 14412 เมื่อเดือนมิถุนายน 2026) ควรเริ่มต้นจากการจัดทำบัญชีรายการว่ามีการใช้การเข้ารหัสที่เปราะบางอยู่ที่ใดบ้าง

6. การเฝ้าติดตามหมุดหมาย (Milestone Watch): ติดตามรายการสั้น ๆ ของสัญญาณภายนอกที่มีกำหนดเวลาชัดเจน—เช่น โมดูล Kookaburra ของ IBM เครื่อง “Magne” ของ Microsoft และ Atom Computing ระบบ Sol ของ Quantinuum และการตรวจสอบยืนยันโดยอิสระของคำกล่าวอ้างเรื่องความได้เปรียบเชิงควอนตัม—และตกลงกันล่วงหน้าว่าแต่ละสัญญาณจะนำไปสู่การดำเนินการใด

7. การสร้างขุมกำลังบุคลากร (Talent Pipeline): ประเมินเส้นทางการเปลี่ยนผ่านภายในองค์กรจาก “AI สู่ควอนตัม (AI-to-Quantum)” สำหรับทีมนักวิทยาศาสตร์ข้อมูล (Data scientists) และวิศวกรที่มีอยู่ในปัจจุบัน

References:

CHAPTER 1: Summary

[1] https://physics.mit.edu/news/quantum-computing-reality-check-what-business-needs-to-know-now/#:~:text=Credit%3A%20Adam%20Glanzman,Credit%3A%20Adam%20Glanzman

[2] https://www.scbx.com/th/scbx-exclusive/scbx-quantum-outlook/

[Feynman1982] Feynman, R. P. (1982). "Simulating physics with computers." International Journal of Theoretical Physics, 21, 467–488

[PNAS2017] Reiher, M., Wiebe, N., Svore, K. M., Wecker, D., & Troyer, M. (2017). "Elucidating reaction mechanisms on quantum computers." Proceedings of the National Academy of Sciences (PNAS), 114(29), 7555-7560.

[Shor] Shor, P. W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring." Proceedings 35th Annual Symposium on Foundations of Computer Science (IEEE).

[Kempe2006] Kempe, J., Kitaev, A., & Regev, O. (2006). "The Complexity of the Local Hamiltonian Problem." SIAM Journal on Computing, 35(5), 1070–1097. DOI: 10.1137/S0097539704445226.

[Preskill2018] Preskill, J. (2018). "Quantum Computing in the NISQ era and beyond." Quantum, 2, 79.

[WEF1] World Economic Forum in collaboration with Accenture. (January 2025). Embracing the Quantum Economy: A Pathway for Business Leaders.

[WEF2] World Economic Forum in collaboration with Accenture. (October 2025). Quantum Technologies: Key Opportunities for Advanced Manufacturing and Supply Chains.

[WEF3] World Economic Forum in collaboration with Accenture. (December 2025). Quantum Technologies: Strategic Imperatives for Health and Healthcare Leaders.

[WEF4] World Economic Forum in collaboration with Accenture. (July 2025). Quantum Technologies: Key Strategies and Opportunities for Financial Services Leaders.

CHAPTER 2: Quantum Computing for Laypeople

[1] SCBX. (December 2025). SCBX Quantum Outlook: Post-Quantum Cryptography.

[2] Shor, P. W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring." Proceedings 35th Annual Symposium on Foundations of Computer Science (IEEE).

[3] Kitaev, A. Y. (1995). "Quantum measurements and the Abelian Stabilizer Problem." arXiv:quant-ph/9511026.

[4] Harrow, A. W., Hassidim, A., & Lloyd, S. (2009). "Quantum algorithm for linear systems of equations." Physical Review Letters, 103(15), 150502.

[5] Reiher, M., Wiebe, N., Svore, K. M., Wecker, D., & Troyer, M. (2017). "Elucidating reaction mechanisms on quantum computers." Proceedings of the National Academy of Sciences (PNAS), 114(29), 7555-7560.

[6] https://quantumalgorithmzoo.org/

CHAPTER 3: Progress towards quantum advantage

[1] Financial Services & Quantum: Making Big Decisions When Seconds Equal Money, Third Quarter 2023, https://www.vedp.org/news/financial-services-quantum-making-big-decisions-when-seconds-equal-money

[2] https://www.sciencenews.org/article/google-quantum-supremacy-claim-controversy-top-science-stories-2019-yir#:~:text=Google%20claimed%20quantum%20supremacy%20in%202019%20%E2%80%94%20and%20sparked%20controversy

[3] Herman, D. et. al. Quantum computing for finance, Nature Review Physics 2023 https://www.nature.com/articles/s42254-023-00603-1

[4] Arute, F. et al. (2019). "Quantum supremacy using a programmable superconducting processor." Nature, 574, 505–510.

[5] Kim, Y. et al. (2023). "Evidence for the utility of quantum computing before fault tolerance." Nature, 618, 500–505.

[6] IBM Newsroom (30 July 2026). "IBM and The University of Chicago Demonstrate Quantum Advantage, Establishing Trusted Quantum Computation on Logical Circuits."

[7] Replace or supplement with Manabe, H., Gu, H., & Pan, F. (13 August 2026). 'Classical Simulation and Design Frontiers for IBM's Doped Clifford Sampling Experiment.' arXiv:2608.13110.

[8] Lee, J. et al. (2021). "Even more efficient quantum computations of chemistry through tensor hypercontraction." PRX Quantum, 2, 030305.

[9] Gidney, C. (2025). "How to factor 2048 bit RSA integers with less than a million noisy qubits." arXiv:2505.15917.

[10] Webster, P. et al. (2026). "The Pinnacle Architecture: Reducing the cost of breaking RSA-2048 to 100 000 physical qubits using quantum LDPC codes." arXiv:2602.11457.

[11] Babbush, R. & Neven, H., Google Research (31 March 2026). "Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly."

[12] Mosca, M. & Piani, M., Global Risk Institute (March 2026). "Quantum Threat Timeline Report 2025."

[13] Babbush, R. et al. (2021). "Focus beyond quadratic speedups for error-corrected quantum advantage." PRX Quantum, 2, 010103.

[14] Chakrabarti, S. et al. (2021). "A threshold for quantum advantage in derivative pricing." Quantum, 5, 463.

[15] IBM (2025). "Quantum computing shows promising potential in finance." IBM Think.

[16] IBM Corp. Form 8-K (28 May 2026), Regulation FD disclosure on quantum investment.

[17] Bausch, J. et al. (2024). "Learning high-accuracy error decoding for quantum processors." Nature, 635, 834–840.

[18] Microsoft Source (2 June 2026). "Majorana 2, made more reliable with Microsoft Discovery agentic AI."

[19] Tang, E. (2019). "A quantum-inspired classical algorithm for recommendation systems." Proceedings of the 51st ACM Symposium on Theory of Computing (STOC), 217–228.

[20] Quantinuum (5 November 2025). "Quantinuum Announces Commercial Launch of New Helios Quantum Computer That Offers Unprecedented Accuracy to Enable Generative Quantum AI (GenQAI)."

CHAPTER 4: Post Quantum Cryptography Update (2026)

Primary sources and technical research used for the 2025-2026 update

[1] NIST - Post-Quantum Cryptography

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[2] NIST CSWP 39upd1 - Considerations for Achieving Crypto Agility

https://csrc.nist.gov/pubs/cswp/39/upd1/considerations-for-achieving-crypto-agility/final

[3] Xue & Covey - Factoring 2048-bit RSA integers with a half-million-qubit modular atomic processor, 5 May 2026

https://arxiv.org/abs/2605.03951

[4] DARPA - Quantum Benchmarking Initiative update, 10 Mar 2026

https://www.darpa.mil/news/2026/qbi-stage-a-qbit

[5] White House - Executive Order 14412

https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/

[6] OMB M-26-15 - Execution of the Migration to Post-Quantum Cryptography

https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf

[7] White House - Executive Order 14413

https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-next-frontier-of-quantum-innovation/

[8] Australian Signals Directorate - Planning for Post-Quantum Cryptography

https://www.cyber.gov.au/business-government/secure-design/quantum/planning-for-post-quantum-cryptography

[9] Singapore CSA - Quantum-Safe Migration Handbook and Quantum Readiness Index

https://www.csa.gov.sg/resources/publications/quantum-safe-handbook-and-quantum-readiness-index/

[10] MAS - Annual Report 2025/2026 remarks on quantum resilience

https://www.bis.org/speeches/20260817-remarks-mas-annual-report-20252026

[11] BIS Innovation Hub - Project Leap Phase 2

https://www.bis.org/publ/othp107.htm

[12] BIS Innovation Hub - Project FuSSE

https://www.bis.org/publications/project-fusse-exploring-flexible-scalable-and-secure-settlement-engines

[13] NCSA Thailand - Draft Quantum Security Framework 2026-2035, public-consultation revision, 2026

[14] NCSA Thailand - Draft Quantum Security Transition Master Plan 2026-2035, 2026

[15] Replace the URL with https://law.go.th/listeningDetail?survey_id=NzY0OURHQV9MQVdfRlJPTlRFTkQ%3D . Keep the Framework title and 15-29 July 2026 dates. Alternatively relabel the existing URL as the Migration Master Plan and Action Plan consultation, 16-30 July 2026.

Note: The Thai Framework and Master Plan are cited as draft policy-development materials.
They are used to indicate the current direction of policy and implementation planning, not as binding regulatory requirements.

CHAPTER 5: Global Investment Landscape and the Effort to Build Quantum Computers

[1] The emerging quantum supply chain – Riverlane (2025), https://www.riverlane.com/blog/the-emerging-quantum-supply-chain

[3] Quantum 2.0 Market Report 2026: A Global $50 Billion Market https://www.globenewswire.com/news-release/2026/02/16/3238572/0/en/Quantum-2-0-Market-Report-2026-A-Global-50-Billion-Market-by-2036-Seismic-Technological-Shift-Unlocks-New-Capabilities-in-Industries-Like-Finance-Healthcare-and-Defense.html

[4] Mapping the global quantum ecosystem (December 2025): https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/mapping-the-global-quantum-ecosystem_47891dd2/20251217-0001.pdf

[5] Policy Paper on UK National Quantum Strategy (December 2023): https://www.gov.uk/government/publications/national-quantum-strategy/national-quantum-strategy-accessible-webpage

[6] European Quantum Technologies Flagship: https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship

[7] The U.S. National Quantum Initiative Supplement to the President's FY 2025 Budget, National Science & Technology Council (December 2024)

https://www.quantum.gov/wp-content/uploads/2024/12/NQI-Annual-Report-FY2025.pdf

[8] The U.S. Department of Energy https://www.energy.gov/articles/energy-department-announces-625-million-advance-next-phase-national-quantum-information?utm_source=chatgpt.com

[9] McKinsey. The quantum leap in banking: Redefining financial performance – McKinsey (2026), https://www.mckinsey.com/industries/financial-services/our-insights/the-quantum-leap-in-banking-redefining-financial-performance

[10] McKinsey. The Year of Quantum: From concept to reality in 2025 (June 23, 2025 Report) https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025

[11] McKinsey. Quantum Technology Monitor (June 2025) https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20year%20of%20quantum%20from%20concept%20to%20reality%20in%202025/quantum-monitor-2025.pdf

[12] McKinsey. Quantum communications and computing: elevating the banking sector (2026). https://www.mckinsey.com/industries/financial-services/our-insights/quantum-communication-and-computing-elevating-the-banking-sector

[13] McKinsey. The quantum revolution in pharma (2025). https://www.mckinsey.com/industries/life-sciences/our-insights/the-quantum-revolution-in-pharma-faster-smarter-and-more-precise

[14] McKinsey. Solving chemistry's toughest problems: the quantum computing advantages (2026). https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/solving-chemistrys-toughest-problems-the-quantum-computing-advantage?utm_source=chatgpt.com

[15] McKinsey. Quantum Technology Monitor 2026: A commercial tipping point (April 2026). https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/mckinsey-quantum-technology-monitor-2026-a-commercial-tipping-point

[16] IBM Corp. Form 8-K (28 May 2026) and Reuters (28 May 2026), "IBM to invest $10 billion for large-scale quantum computer by 2029."

[17] The White House. Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks" (22 June 2026); Executive Order 14413, "Ushering in the Next Frontier of Quantum Innovation" (22 June 2026).

[18] U.S. Department of Energy (17 September 2026). "DOE Launches Competition to Accelerate Development of World's First Fault-Tolerant Quantum Computer."

[19] Quantinuum Inc. (11 August 2026). "Quantinuum Reports Second Quarter 2026 Results."

[20] WisdomTree (June 2026). "The U.S. government became a quantum investor. Should you?"

CHAPTER 6: Thailand Positioning

[1] NXPO: Roadmap Whitepaper https://www.nxpo.or.th/th/wp-content/uploads/2021/11/TQT-Roadmap-Whitepaper-Rev4-21-Sep-2020.pdf

[2] https://www.qtft.org/

[3] https://www.chula.ac.th/en/news/288469/

[4] https://qtric.sut.ac.th/qtri2025/index.html

[5] https://sutir.sut.ac.th/jspui/handle/123456789/10268

[6] Quantum Computing Report (6 August 2026). "Thailand Launches 'Quantum Club Thailand' at True Digital Park to Build ASEAN Quantum Hub"; The Quantum Insider (5 August 2026).

[7] Quantum Computing Report (September 2026). "Chulalongkorn University and Qunova Computing Execute MoU to Advance Hybrid Quantum Algorithms for Industrial R&D."

[8] SCBX (8 May 2026). "SCBX Partners with Chulalongkorn University to Advance Quantum Technology."

[9] Qunova Computing (7 September 2026). "Chulalongkorn University Signs MoU with Qunova Computing for Cooperation on Quantum Technology & Research."

[10] The Quantum Insider (21 September 2026). "Chulalongkorn University and AIST Sign MoU on Quantum Technology."

Authors



Assistant Professor Thiparat Chotibut, Ph.D.
Tenure-track faculty member
at School of Physical and Mathematical Sciences,
Nanyang Technological University (NTU)



Supanut Thanasilp, Ph.D.
Tenure-track faculty member, Department of Physics,
Faculty of Science, Chulalongkorn University



Poompong Chaiwongkhot, Ph.D.
Co-Founder and Chief Technology Officer, QTFT



Kaweewut Temphuwapat
Chief Innovation Officer, SCBX
Chief Executive Officer, SCB 10X



Tutanon Sinthuprasith, Ph.D.
Head of R&D, SCBX



Nut Chukamphaeng
Senior Research Scientist, SCBX



Koravich Sangkaew
AI Engineer, SCB DataX

This publication was made possible through the collaboration of

SCB X · data X · SIAM QUANTUM SQUARE · Chula Chulalongkorn University · QTFT



www.scbx.com