ธนาคารแห่งประเทศไทย

4 มิถุนายน 2564

เรียน ผู้จัดการ

สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง
ผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ที่มิใช่สถาบันการเงินทุกแห่ง
บริษัทผู้ประกอบธุรกิจบัตรเครดิตที่มิใช่สถาบันการเงินทุกแห่ง
บริษัทผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับที่มิใช่สถาบันการเงินทุกแห่ง
บริษัทผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับที่มิใช่สถาบันการเงินทุกแห่ง

ที่ ธปท.ฝทง. ว. 546 /2564 เรื่อง นำส่งแนวปฏิบัติการใช้เทคโนโลยีบล็อกเชน (Blockchain) ในการให้บริการทางการเงิน

ธนาคารแห่งประเทศไทย (ธปท.) ได้ออกแนวปฏิบัติการใช้เทคโนโลยีบล็อกเชน (Blockchain) ในการให้บริการทางการเงิน โดยมีวัตถุประสงค์เพื่อให้ผู้ให้บริการทางการเงินที่มีการนำเทคโนโลยีบล็อกเชนมาใช้ในการให้บริการทางการเงินใช้อ้างอิงในการปฏิบัติ และเพื่อให้มั่นใจว่าผู้ให้บริการทางการเงินมีการบริหารจัดการในการนำเทคโนโลยีบล็อกเชนมาใช้อย่างเหมาะสม มั่นคงปลอดภัย น่าเชื่อถือ และสอดคล้องกับหลักการที่ได้รับการยอมรับในระดับสากล สร้างความเชื่อมั่นในการใช้บริการให้กับประชาชน และเป็นมาตรฐานในการพัฒนาระบบโครงสร้างทางการเงินของประเทศต่อไป

แนวปฏิบัตินี้ครอบคลุมหลักการพึงปฏิบัติที่สำคัญในการใช้เทคโนโลยีบล็อกเชนในการให้บริการทางการเงิน โดยเน้นตั้งแต่การมีความรู้ความเข้าใจในเทคโนโลยี การมีแนวทางการกำกับดูแลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติตามกฎหมายที่เกี่ยวข้อง โดย ธปท. ได้จัดทำแนวปฏิบัตินี้ขึ้นโดยอ้างอิงจากมาตรฐานสากลและแนวทางการกำกับดูแลที่เกี่ยวข้องกับเทคโนโลยีบล็อกเชน รวมถึงการประเมินโครงการที่ใช้เทคโนโลยีบล็อกเชนภายใต้ Regulatory Sandbox

ธปท. ขอให้ผู้ให้บริการทางการเงินที่ประสงค์จะนำเทคโนโลยีบล็อกเชนมาใช้ในการให้บริการทางการเงิน ถือปฏิบัติตามแนวปฏิบัติฉบับนี้อย่างครบถ้วน โดยคำนึงถึงการรักษาความปลอดภัยของข้อมูลลูกค้า และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง รวมถึงต้องปฏิบัติตามแนวทางดังนี้

1. ผู้ให้บริการทางการเงินที่มีความประสงค์จะประยุกต์ใช้เทคโนโลยี Blockchain แบบ Private Blockchain Network ให้ดำเนินการดังนี้

1.1 โครงการที่มีลักษณะเป็นโครงสร้างพื้นฐานทางการเงินให้ดำเนินการทดสอบภายใต้ Regulatory Sandbox รวมถึงต้องปฏิบัติตามเงื่อนไขการทดสอบที่กำหนดโดยครบถ้วนและได้รับอนุญาตจาก ธปท. ก่อนให้บริการในวงกว้าง

1.2 โครงการร่วมกับพันธมิตรทางธุรกิจให้ดำเนินการตามกรอบ Own Sandbox รวมถึงต้องปฏิบัติตามเงื่อนไขการทดสอบที่กำหนดโดยครบถ้วนก่อนให้บริการในวงกว้าง

2. ผู้ให้บริการทางการเงินที่มีความประสงค์จะประยุกต์ใช้เทคโนโลยี Blockchain แบบ Public Blockchain Network ให้ผู้ให้บริการทางการเงินหารือ ธปท. เป็นรายกรณีก่อนดำเนินการ

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายรณดล นุ่มนนท์)
รองผู้ว่าการ ด้านเสถียรภาพสถาบันการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย แนวปฏิบัติการใช้เทคโนโลยีบล็อกเชน (Blockchain) ในการให้บริการทางการเงิน

ฝ่ายเทคโนโลยีทางการเงิน
โทรศัพท์ 0 2283 6924, 0 2283 6892
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 5827

หมายเหตุ [ ] ธนาคารแห่งประเทศไทยจะจัดให้มีการประชุมชี้แจงในวันที่ ..... ณ .....
[x] ไม่มีการจัดประชุมชี้แจง

แนวปฏิบัติ
การใช้เทคโนโลยีบล็อกเชน (Blockchain) ในการให้บริการทางการเงิน

4 มิถุนายน 2564

ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายเทคโนโลยีทางการเงิน

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน

ธนาคารแห่งประเทศไทย

โทรศัพท์ 0 2283 6892

0 2283 5705

e-mail: FinTechDept@bot.or.th

สารบัญ

หัวข้อ **หน้า**

บทสรุปผู้บริหาร (Executive Summary) 3

1. เหตุผลในการออกแนวปฏิบัติ 5

2. ขอบเขตการใช้แนวปฏิบัติ 6

3. คำจำกัดความ 6

4. ภาพรวมเทคโนโลยี Blockchain 8

4.1 หลักการทำงานของเทคโนโลยี Blockchain 8

4.2 ประเภทของเทคโนโลยี Blockchain 8

4.3 ความเสี่ยงสำคัญด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับเทคโนโลยี Blockchain 9

5. หลักการที่พึงปฏิบัติสำหรับผู้ให้บริการทางการเงิน 12

หลักการที่ 1 การประยุกต์ใช้เทคโนโลยี Blockchain ในการประกอบธุรกิจ 13

หลักการที่ 2 การกำกับดูแลการใช้เทคโนโลยี Blockchain 15

หลักการที่ 3 การบริหารจัดการความเสี่ยงด้าน IT สำหรับเทคโนโลยี Blockchain 19

หลักการที่ 4 การบริหารความเสี่ยงทางกฎหมายกับการใช้เทคโนโลยี Blockchain 21

ภาคผนวก 1 ความรู้พื้นฐานเกี่ยวกับเทคโนโลยี – Blockchain 23

เอกสารอ้างอิง 25

บทสรุปผู้บริหาร (Executive Summary)

ธนาคารแห่งประเทศไทย (ธปท.) เห็นความสำคัญและโอกาสของการนำเทคโนโลยีบล็อกเชน (Blockchain) มาใช้เพิ่มประสิทธิภาพในการให้บริการ ตลอดจนพัฒนานวัตกรรมทางการเงินและระบบการเงินของประเทศไทย จึงได้ออกแนวปฏิบัติฉบับนี้เพื่อให้ผู้ประกอบธุรกิจในภาคการเงินใช้อ้างอิงในการนำเทคโนโลยีดังกล่าวไปใช้ประโยชน์ โดยยังมีการดูแลความเสี่ยงของเทคโนโลยีอย่างรัดกุม เพื่อสร้างความเชื่อมั่นและความปลอดภัยแก่ประชาชนผู้ใช้บริการทางการเงิน

ขอบเขตของแนวปฏิบัติฉบับนี้ครอบคลุมผู้ให้บริการทางการเงินที่อยู่ภายใต้การกำกับดูแลของ ธปท. ได้แก่ สถาบันการเงิน และบริษัทในกลุ่มธุรกิจทางการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ผู้ประกอบธุรกิจที่ไม่ใช่สถาบันการเงินที่อยู่ภายใต้การกำกับของ ธปท. ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน ซึ่งประยุกต์ใช้เทคโนโลยี Blockchain แบบ Private Blockchain Network ในการให้บริการธุรกรรมทางการเงินทั้งในกรณีที่เป็นสมาชิกและผู้ดูแลเครือข่าย Blockchain

แนวปฏิบัติฯ มีสาระสำคัญ 4 ส่วน ประกอบด้วย

1. **การประยุกต์ใช้เทคโนโลยี Blockchain ในทางธุรกิจ** เพื่อให้ผู้ให้บริการทางการเงินมีกระบวนการประเมินประกอบการตัดสินใจนำเทคโนโลยี Blockchain มาประยุกต์ใช้ให้เกิดประโยชน์ต่อธุรกิจ โดยต้องคำนึงถึงต้นทุนและความคุ้มค่าของการนำเทคโนโลยี Blockchain มาใช้ รวมทั้งการคัดเลือก platform ที่เหมาะสมกับรูปแบบธุรกิจ
2. **การกำกับดูแลการใช้เทคโนโลยี Blockchain** เพื่อให้ผู้ให้บริการทางการเงินมีแนวทางกำกับดูแลโครงการที่ใช้เทคโนโลยี Blockchain อย่างมีประสิทธิภาพ โดยครอบคลุม 2 กรณี ประกอบด้วย
   2.1 <u>กรณีเป็นผู้ใช้หรือเข้าร่วมเป็นสมาชิกในเครือข่าย Blockchain</u> ต้องให้เกิดความแน่ใจว่าโครงการ Blockchain สอดคล้องกับลักษณะธุรกิจ พร้อมมีการบริหารความเสี่ยงที่เหมาะสมด้วยการกำหนดผู้รับผิดชอบโครงการ มีการปรับปรุงนโยบายและกระบวนการทำงานอย่างต่อเนื่อง รวมทั้งมีการควบคุม ติดตาม และสอบทานการรักษาความมั่นคงและปลอดภัย โดยเฉพาะการเชื่อมโยงกับระบบอื่น ๆ ตลอดจนการบริหารจัดการความเสี่ยงจากบุคคลภายนอก
   2.2 <u>กรณีเป็นผู้ดูแลเครือข่ายหรือโครงการ Blockchain ที่เป็นโครงสร้างพื้นฐานทางการเงิน</u> ต้องกำหนดบทบาทหน้าที่ของผู้ดูแลเครือข่าย พร้อมทั้งการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีให้เป็นไปตามมาตรฐานที่กำหนดไว้
3. **การบริหารจัดการความเสี่ยงด้าน IT สำหรับเทคโนโลยี Blockchain** เพื่อให้ผู้ให้บริการทางการเงินมีกระบวนการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลเพื่อสร้างความเชื่อมั่นต่อผู้ใช้บริการ โดยต้องมีการออกแบบและพัฒนาระบบ Blockchain อย่างปลอดภัย ควบคุมการเข้าถึงระบบและกุญแจเข้ารหัสอย่างรัดกุม มีการรักษาความปลอดภัยข้อมูลทั้ง On-chain

และ Off-chain รวมถึงการสอบทานความถูกต้องของข้อมูลและติดตามรายการธุรกรรมจาก Log ให้สอดคล้องกับลักษณะธุรกิจ ตลอดจนมีการทดสอบการรักษาความปลอดภัยอย่างน้อยปีละ 1 ครั้งและเมื่อเปลี่ยนแปลงอย่างมีนัยสำคัญ

นอกจากนี้ ต้องมีการทดสอบประสิทธิภาพและความพร้อมใช้ รวมทั้งปรับปรุงให้ระบบพร้อมรองรับธุรกรรมที่คาดว่าจะเพิ่มขึ้นได้อย่างต่อเนื่อง และมีการสำรองข้อมูลใน Blockchain ให้มีความพร้อมใช้งานอย่างต่อเนื่อง รวมถึงมี Business Continuity Plan และ IT Disaster Recovery Plan รองรับระบบ Blockchain

4. **การบริหารความเสี่ยงทางกฎหมายกับการใช้เทคโนโลยี Blockchain** เพื่อให้การใช้เทคโนโลยี Blockchain มีการปฏิบัติตามกฎหมายที่เกี่ยวข้องและคุ้มครองข้อมูลส่วนบุคคล โดยต้องมีข้อตกลงร่วมกันระหว่างสมาชิกและผู้ที่เกี่ยวข้องในเครือข่าย Blockchain และข้อตกลงเกี่ยวกับ Smart Contract รวมถึงมีการประเมิน Data Protection Impact Assessment และการประเมินความเสี่ยงที่จะกระทบสิทธิเจ้าของข้อมูลส่วนบุคคล โดยควรเก็บรักษาข้อมูลส่วนบุคคลแบบ Off-chain ทั้งนี้ ต้องปฏิบัติตามหลักเกณฑ์ต่าง ๆ ของ ธปท. ตลอดจนกฎหมายอื่นที่เกี่ยวข้อง

แนวปฏิบัติการใช้เทคโนโลยีบล็อกเชน (Blockchain) ในการให้บริการทางการเงิน

(Guideline for Blockchain Technology Adoption in Financial Services)

1. เหตุผลในการออกแนวปฏิบัติ

ปัจจุบันภาคการเงินได้นำเทคโนโลยีบล็อกเชน (Blockchain) เข้ามาช่วยเพิ่มประสิทธิภาพการให้บริการทางการเงินมากขึ้น เช่น การโอนเงินระหว่างประเทศ ด้วยคุณสมบัติเรื่องการกระจายข้อมูลจัดเก็บ การเข้ารหัสข้อมูล การเชื่อมต่อกันโดยอ้างอิงจากข้อมูลก่อนหน้า รวมถึงการมีส่วนร่วมในการตรวจสอบและลงความเห็นของสมาชิกในเครือข่าย Blockchain ในกรณีที่มีการเปลี่ยนแปลงแก้ไขข้อมูล ทำให้การบริหารจัดการข้อมูลในเครือข่าย Blockchain มีความปลอดภัย น่าเชื่อถือ และข้อมูลใน Blockchain ถูกปลอมแปลงแก้ไขได้ยาก ส่งผลให้ต้นทุนการตรวจสอบความถูกต้องของข้อมูลต่ำลงและทำให้ประสิทธิภาพการดำเนินงานสูงขึ้น ก่อให้เกิดรูปแบบธุรกิจใหม่ ๆ รวมถึงการพัฒนาโครงสร้างพื้นฐานทางการเงินต่าง ๆ

อย่างไรก็ตาม การนำเทคโนโลยี Blockchain มาประยุกต์ใช้ในการให้บริการทางเงิน อาจก่อให้เกิดความเสี่ยงทั้งจากตัวเทคโนโลยีเอง ความเสี่ยงจากการเชื่อมต่อกับระบบโครงสร้างพื้นฐานเดิม และความเสี่ยงจากความเข้าใจในเทคโนโลยีไม่เพียงพอ ดังนั้น การตระหนักถึงข้อดี ข้อเสีย และความเสี่ยงต่าง ๆ รวมถึงการวางโครงสร้างการกำกับดูแลการใช้งานเทคโนโลยีอย่างรัดกุม มีนโยบายและระเบียบวิธีปฏิบัติอย่างเพียงพอเหมาะสมจึงเป็นสิ่งสำคัญ

ธนาคารแห่งประเทศไทย (ธปท.) เห็นความสำคัญและโอกาสของการนำเทคโนโลยี Blockchain มาใช้ในการพัฒนาระบบการเงินของประเทศไทย จึงได้กำหนดแนวทางในการนำเทคโนโลยีนี้มาใช้ในภาคการเงินควบคู่กันกับการควบคุมความเสี่ยงผ่านกลไก Regulatory Sandbox หรือ Own Sandbox ซึ่งเป็นการทดสอบการนำเทคโนโลยี Blockchain มาใช้พัฒนาบริการและนวัตกรรมทางการเงินในวงจำกัด โดยได้มีการประเมินผลการทดสอบและกำกับดูแลอย่างใกล้ชิด เพื่อให้ผู้ให้บริการทางการเงินมีการควบคุมดูแลความเสี่ยงที่รัดกุมและมีแนวทางคุ้มครองผู้ใช้บริการที่เหมาะสม

ในการนี้ เพื่อยกระดับการกำกับดูแลการใช้เทคโนโลยี Blockchain ในการให้บริการทางการเงิน ธปท. จึงได้ออกแนวปฏิบัตินี้ให้ผู้ให้บริการทางการเงิน ทั้งในกรณีที่เป็นผู้ดูแลและเป็นสมาชิกในเครือข่าย Blockchain ใช้อ้างอิงในการปฏิบัติ และให้มั่นใจว่าผู้ให้บริการทางการเงินมีการบริหารจัดการในการนำเทคโนโลยี Blockchain มาใช้อย่างเหมาะสม มั่นคงปลอดภัย น่าเชื่อถือ และสอดคล้องกับหลักการที่ได้รับการยอมรับในระดับสากล สร้างความเชื่อมั่นในการใช้บริการให้กับประชาชนและเป็นมาตรฐานในการพัฒนาระบบโครงสร้างทางการเงินของประเทศต่อไป ทั้งนี้ ผู้ให้บริการทางการเงินยังต้องปฏิบัติตามหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ และหลักเกณฑ์กำกับดูแลด้านอื่นของ ธปท. ตลอดจนกฎหมายที่เกี่ยวข้อง

2. ขอบเขตการใช้แนวปฏิบัติ

แนวปฏิบัติฉบับนี้ให้ใช้กับผู้ให้บริการทางการเงินที่อยู่ภายใต้การกำกับดูแลของ ธปท. ได้แก่ สถาบันการเงิน และบริษัทในกลุ่มธุรกิจทางการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ผู้ประกอบธุรกิจที่ไม่ใช่สถาบันการเงินที่อยู่ภายใต้การกำกับของ ธปท. ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน มีการประยุกต์ใช้เทคโนโลยี Blockchain แบบ Private Blockchain Network ในการให้บริการธุรกรรมทางการเงินทั้งในกรณีที่เป็นผู้ดูแลเครือข่าย Blockchain และกรณีที่เป็นสมาชิกในเครือข่าย Blockchain

สำหรับกรณีที่ผู้ให้บริการทางการเงินมีการประยุกต์ใช้เทคโนโลยี Blockchain แบบ Public Blockchain Network นั้น ให้ผู้ให้บริการทางการเงินหารือ ธปท. เป็นรายกรณีก่อนดำเนินการ

3. คำจำกัดความ

ในแนวปฏิบัติฉบับนี้

Blockchain หมายถึง เทคโนโลยีการประมวลผลและจัดเก็บข้อมูลแบบกระจายศูนย์ Distributed Ledger Technology (DLT) เป็นรูปแบบการบันทึกข้อมูลที่ใช้หลักการ Cryptography ร่วมกับกลไก Consensus ทำให้ข้อมูลที่ถูกบันทึกไปแล้วสามารถเปลี่ยนแปลงหรือแก้ไขได้ยาก เพิ่มความถูกต้องและเชื่อถือได้ของข้อมูล

เครือข่าย Blockchain หมายถึง เครือข่ายประมวลผลแบบกระจายศูนย์ที่เชื่อมต่อ Node ของสมาชิกเข้าด้วยกันเป็นเครือข่าย มีกลไกตรวจสอบและแลกเปลี่ยนข้อมูลระหว่างกันด้วยเทคโนโลยี Blockchain

ผู้ดูแลเครือข่าย Blockchain หมายถึง ผู้ที่เป็นคนกลางทำหน้าที่บริหารจัดการสมาชิกในเครือข่าย Blockchain ระบบและการเชื่อมต่อกับเครือข่าย Blockchain

สมาชิกในเครือข่าย Blockchain หมายถึง ผู้ที่ได้รับอนุญาตให้เชื่อมต่อและใช้งานเครือข่าย Blockchain โดยผู้ดูแลเครือข่าย Blockchain ซึ่งอาจเชื่อมต่อผ่าน Node หรือเรียกใช้งานผ่าน API

Private Blockchain Network หมายถึง เครือข่าย Blockchain ที่ควบคุมสิทธิในการเข้าถึงเครือข่าย Blockchain และข้อมูล และมีการกำกับดูแลโดยองค์กรที่อาจมีลักษณะทางธุรกิจเหมือนกันหรือแตกต่างกันได้

Public Blockchain Network หมายถึง เครือข่าย Blockchain ที่เปิดให้ทุกคนมีสิทธิ์ในการเข้าถึงเครือข่าย Blockchain และข้อมูลได้อย่างอิสระโดยไม่จำเป็นต้องขออนุญาต

Consensus หมายถึง กลไกที่ควบคุมความถูกต้องของข้อมูลในทุก Node ผ่าน Algorithm ต่าง ๆ เพื่อให้ข้อมูลมีความถูกต้อง เที่ยงตรงและเป็นข้อมูลชุดเดียวกัน รวมทั้งข้อมูลมีการจัดเก็บที่สอดคล้องและมีลำดับการจัดเก็บตรงกัน ผ่านการกำหนดข้อตกลงและความเห็นชอบร่วมกันระหว่างสมาชิกในเครือข่าย Blockchain ซึ่งสมาชิกต้องยอมรับกฎระเบียบร่วมกัน ทั้งนี้ กระบวนการ Consensus มีอยู่ด้วยกันหลายวิธี โดยการเลือกใช้ Consensus วิธีใดนั้นขึ้นอยู่กับความเหมาะสมของ Blockchain ในแต่ละประเภท

Smart Contract หมายถึง รูปแบบโปรแกรมหรือชุดคำสั่งคอมพิวเตอร์ที่จัดเก็บเงื่อนไขหรือข้อตกลงของสัญญาต่าง ๆ ซึ่งจะถูกจัดเก็บและดำเนินการ (Execute) ในเครือข่าย Blockchain โดยจะดำเนินการอัตโนมัติเมื่อเป็นไปตามเงื่อนไขที่กำหนด

Node หมายถึง เครื่องประมวลผลที่จัดเก็บข้อมูลในเครือข่าย Blockchain เช่น คอมพิวเตอร์หรือเครื่อง Server ซึ่งเชื่อมต่อและรับส่งข้อมูลระหว่างกันภายในเครือข่าย Blockchain

On-chain หมายถึง รูปแบบการจัดเก็บข้อมูลในเครือข่าย Blockchain

Off-chain หมายถึง รูปแบบการจัดเก็บข้อมูลนอกเครือข่าย Blockchain เช่น จัดเก็บในระบบฐานข้อมูลภายในองค์กร เป็นต้น

4. ภาพรวมเทคโนโลยี Blockchain

4.1 หลักการทำงานของเทคโนโลยี Blockchain

เทคโนโลยี Blockchain เป็นเทคโนโลยีการประมวลผลและจัดเก็บข้อมูลแบบกระจายศูนย์ (Distributed Ledger Technology: DLT) กระจายข้อมูลที่จัดเก็บไปยังแต่ละ Node ซึ่งเป็นเครื่องคอมพิวเตอร์หลายเครื่อง ที่เชื่อมโยงกันในเครือข่าย Blockchain โดยกลุ่มข้อมูล (Block) ที่จัดเก็บจะเชื่อมต่อกันเป็นห่วงโซ่ (Chain) ด้วยกระบวนการเข้ารหัส ซึ่งข้อมูลแต่ละ Block จะมีค่าทางคณิตศาสตร์ (Hash) ของ Block ก่อนหน้าเพื่อใช้สอบทานความถูกต้อง จึงทำให้การจัดเก็บข้อมูลสามารถมีข้อมูลเพียงชุดเดียวที่กระจายจัดเก็บอยู่ใน Node ต่าง ๆ โดยไม่จำเป็นต้องมีตัวกลางในการจัดเก็บหรือควบคุม ซึ่งจะเป็นการลดความเสี่ยงจากการถูกปลอมแปลงข้อมูล นอกจากนี้ ยังช่วยให้สามารถทำธุรกรรมแบบอัตโนมัติผ่านกลไก Smart Contract โดยเมื่อมีการส่งคำสั่งทำธุรกรรม หรือคำสั่งเปลี่ยนแปลงแก้ไขข้อมูลธุรกรรมหรือเงื่อนไขของการทำธุรกรรม คำสั่งนั้นจะต้องได้รับการตรวจสอบและลงความเห็นจากสมาชิกในเครือข่าย Blockchain เรียกว่า การทำ Consensus ส่งผลให้การบริหารจัดการข้อมูลในเครือข่าย Blockchain มีความปลอดภัย น่าเชื่อถือ และยากต่อการแก้ไขหากไม่ได้รับอนุญาต[1]

4.2 ประเภทของเทคโนโลยี Blockchain

หากพิจารณาในด้านลักษณะและแนวทางการพัฒนาเทคโนโลยี จะสามารถแบ่งการนำเทคโนโลยี Blockchain มาใช้ ออกเป็น 2 รูปแบบ ได้แก่ Private Blockchain Network และ Public Blockchain Network ซึ่งมีคุณลักษณะและรูปแบบการใช้งานแตกต่างกัน ดังนี้

ตารางที่ 1 การเปรียบเทียบรูปแบบของการนำเทคโนโลยี Blockchain มาใช้

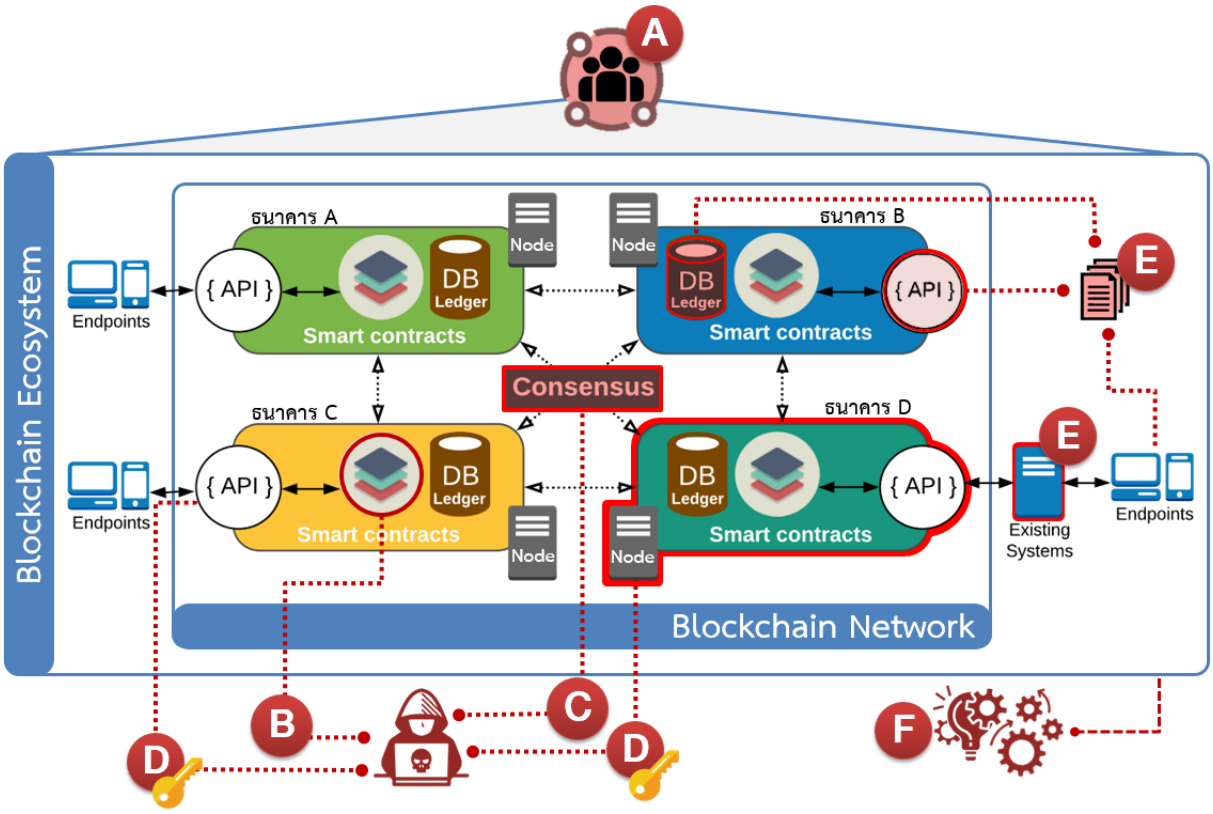
	Private Blockchain Network	Public Blockchain Network
การบริหารจัดการเครือข่าย	- บริหารจัดการโดยองค์กรใดองค์กรหนึ่งหรือมีข้อตกลงร่วมกันระหว่างองค์กร - บริหารจัดการโดยคณะกรรมการที่ได้รับการแต่งตั้งมีกฎเกณฑ์ร่วมกัน (Business Rules)	บริหารจัดการผ่านกระบวนการ Consensus และกลไกการให้รางวัล (Incentive Mechanism)
ลักษณะเครือข่าย	- วงปิด ใช้งานเฉพาะกลุ่มธุรกิจหรือองค์กรสมาชิก - เปิดให้ภายนอกเข้าร่วมในลักษณะวงจำกัด (Permissioned) หรือจำกัดจำนวนสมาชิก - มีกระบวนการพิจารณารับและยกเลิกสมาชิก - มีเป้าหมายทางธุรกิจร่วมกันที่ชัดเจน	- เปิดกว้างให้องค์กรหรือบุคคลภายนอกเข้าร่วมเครือข่ายได้อย่างอิสระ (Permissionless) - ไม่มีการจำกัดจำนวนสมาชิก

[1] กระบวนการทำงานและคุณลักษณะสำคัญของเทคโนโลยี Blockchain สามารถศึกษาเพิ่มเติมได้ใน ภาคผนวก 1 – ความรู้พื้นฐานเกี่ยวกับเทคโนโลยี Blockchain

	Private Blockchain Network	Public Blockchain Network
แนวทางการพัฒนาเทคโนโลยี	- กรณี Open source: เปิดกว้างให้กลุ่มนักพัฒนาระบบในวงกว้าง (Developer Community) - กรณี Proprietary: นักพัฒนาระบบของบริษัทผู้ให้บริการเทคโนโลยีเป็นผู้พัฒนา	กรณี Open source: เปิดกว้างให้กลุ่มนักพัฒนาระบบในวงกว้าง (Developer Community)
ลักษณะเสี่ยงด้านความปลอดภัย	ความเสี่ยงในวงจำกัดเฉพาะสมาชิก หรือบริษัทคู่ค้า	ความเสี่ยงในวงกว้าง (เทียบเท่าระบบอินเตอร์เน็ตสาธารณะ)
ความเป็นส่วนบุคคลของข้อมูล	ข้อมูลมีความเป็นส่วนบุคคล เข้าถึงได้เฉพาะผู้ที่เกี่ยวข้อง	ข้อมูลที่ได้รับการเปิดเผยแบบสาธารณะ ไม่มีความเป็นส่วนตัว หรือมีความเป็นส่วนตัวบางส่วน ทั้งนี้ ขึ้นอยู่กับการออกแบบ

4.3 ความเสี่ยงสำคัญด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับเทคโนโลยี Blockchain

การใช้เทคโนโลยี Blockchain มีจุดที่ควรพิจารณาให้ความสำคัญตามระดับความเสี่ยงของรูปแบบในการนำเทคโนโลยี Blockchain มาใช้ ซึ่งมีความเสี่ยงเฉพาะจากการนำเทคโนโลยีดังกล่าวมาใช้และความเสี่ยงพื้นฐานด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ โดยมีรายละเอียด ดังนี้



ความเสี่ยงเฉพาะจากการใช้เทคโนโลยี Blockchain

- A การกำกับดูแลเครือข่าย Blockchain ไม่ครอบคลุมเพียงพอ
- B Smart Contract ทำงานไม่ถูกต้องและไม่ปลอดภัย
- C การโจมตีกลไก Consensus
- D การบริหารจัดการกุญแจเข้ารหัสที่ไม่รัดกุมเพียงพอ

ความเสี่ยงพื้นฐานด้าน IT และภัยคุกคามทางไซเบอร์

- E ความเสี่ยงจากการเชื่อมต่อระบบโครงสร้างพื้นฐานเดิมกับเครือข่าย Blockchain
- F ความเสี่ยงจากการเปลี่ยนแปลงของเทคโนโลยี

(1) ความเสี่ยงเฉพาะจากการใช้เทคโนโลยี Blockchain

(1.1) การกำกับดูแลเครือข่าย Blockchain ไม่ครอบคลุมเพียงพอ เนื่องจากเครือข่าย Blockchain ประกอบด้วยสมาชิกที่มีรูปแบบธุรกิจที่หลากหลายประเภท จึงทำให้สมาชิกในเครือข่าย Blockchain มีมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบ Blockchain ที่แตกต่างกัน ซึ่งอาจมีช่องโหว่จากการเชื่อมต่อที่ไม่ปลอดภัยจาก Attack Surface ที่มากขึ้นกว่าระบบแบบรวมศูนย์ จึงมีโอกาสที่ผู้ไม่ประสงค์ดีอาจเข้าถึงข้อมูลที่จัดเก็บแบบกระจายศูนย์ในระบบ Blockchain ผ่าน Node Endpoint และจุดเชื่อมต่อจำนวนมาก

(1.2) Smart Contract ทำงานไม่ถูกต้องและไม่ปลอดภัย เนื่องจาก Smart Contract เป็นโปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่สามารถดำเนินการตามข้อตกลงโดยอัตโนมัติ จึงมีโอกาสเกิดข้อบกพร่องจากการพัฒนาโปรแกรมหรือจากการตรวจสอบเงื่อนไขการทำงานไม่ครบถ้วน นอกจากนี้ อาจเกิดช่องโหว่ด้านความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของ Smart Contract ซึ่งส่งผลกระทบต่อกระบวนการประมวลผลธุรกรรมแบบอัตโนมัติและการดำเนินธุรกิจได้

(1.3) การโจมตีกลไก Consensus เนื่องจากกลไก Consensus ทำหน้าที่ให้ทุก Node มีข้อมูลที่ถูกต้องเชื่อถือได้ หากมีช่องโหว่ในชุดคำสั่งหรือ Algorithm ของกลไก Consensus ที่ไม่ปลอดภัย อาจทำให้ข้อมูลถูกเพิ่มหรือแก้ไขได้โดยไม่ต้องผ่านความเห็นชอบจากสมาชิกในเครือข่าย Blockchain และส่งผลให้ข้อมูลในระบบ Blockchain ได้รับความเสียหายและขาดความน่าเชื่อถือได้ นอกจากนี้ หาก Node ที่รับหน้าที่ทำ Consensus มีการรักษาความมั่นคงปลอดภัยไม่ครอบคลุมเพียงพอ อาจถูกโจมตีจากภัยคุกคามทางไซเบอร์ได้

(1.4) การบริหารจัดการกุญแจเข้ารหัสที่ไม่รัดกุมเพียงพอ อาจทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงกุญแจเข้ารหัส และใช้เข้าถึงจุดเชื่อมต่อที่สำคัญโดยไม่ได้รับอนุญาต เช่น ผู้ไม่ประสงค์ดีอาจเข้าควบคุม Node หรือเข้าถึง API พร้อมทั้งสร้างความเสียหายต่อระบบและข้อมูลได้

(2) ความเสี่ยงพื้นฐานด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์

(2.1) ความเสี่ยงจากการเชื่อมต่อระบบโครงสร้างพื้นฐานเดิม (Existing IT Infrastructure) กับเครือข่าย Blockchain หากโครงสร้างพื้นฐานเดิมที่เชื่อมต่อกับเครือข่าย Blockchain มีการรักษาความมั่นคงปลอดภัยของระบบที่ไม่รัดกุมเพียงพอ อาจส่งผลกระทบทางอ้อมกับเครือข่าย Blockchain และข้อมูลของสมาชิกในเครือข่าย Blockchain ทั้งในด้านการรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability) เช่น กรณีระบบงานภายใน API และจุดเชื่อมต่อต่าง ๆ ที่มีการรักษาความมั่นคงปลอดภัยไม่เพียงพอ ถูกโจมตีทางไซเบอร์ อาจทำให้ข้อมูลที่จัดเก็บในรูปแบบ Off-chain อาจรั่วไหลได้

(2.2) ความเสี่ยงจากการเปลี่ยนแปลงของเทคโนโลยี เนื่องจากเทคโนโลยี Blockchain เป็นเทคโนโลยีที่ถูกพัฒนาเปลี่ยนแปลงอย่างต่อเนื่องและรวดเร็ว (Emerging Technology) อีกทั้งแต่ละ

Blockchain Platform มีแนวทางออกแบบพัฒนาและประเด็นความเสี่ยงที่ควรคำนึงถึงที่แตกต่างกัน ส่งผลให้การกำกับดูแล การบริหารจัดการความเสี่ยง และการรักษาความมั่นคงปลอดภัยอาจไม่เท่าทันต่อความเสี่ยงที่เปลี่ยนแปลงอย่างต่อเนื่อง

5. หลักการที่พึงปฏิบัติสำหรับผู้ให้บริการทางการเงิน

แนวปฏิบัติฉบับนี้ประกอบด้วย 4 หลักการ โดยมีรายละเอียดภาพรวม ดังนี้

Blockchain Business Application

มีความเข้าใจ Blockchain ในแง่มุมรูปแบบธุรกิจ ประโยชน์ และข้อจำกัดของเทคโนโลยี

- วิเคราะห์ Feasibility Assessment
- กำหนดกลยุทธ์การนำ Blockchain มาใช้ในธุรกิจ
- ประเมินต้นทุนและความคุ้มค่าของการใช้ Blockchain
- คัดเลือก Blockchain Platform ให้เหมาะสมกับรูปแบบธุรกิจ

Blockchain Governance

มีแนวทางกำกับดูแล Blockchain อย่างมีประสิทธิภาพ

กรณีเป็นสมาชิกในเครือข่าย Blockchain

- กำกับดูแลโครงการ Blockchain ให้สอดคล้องกับลักษณะธุรกิจและความเสี่ยง
- เฝ้าระวังเหตุการณ์ทุจริต
- บริหารความเสี่ยงโดยครอบคลุม 3rd Party

กรณีเป็นผู้ดูแลเครือข่าย Blockchain

- กำหนดบทบาทหน้าที่ของผู้ดูแลเครือข่าย
- มีมาตรฐานการรักษาความปลอดภัย
- มีมาตรฐานการบริหารจัดการสมาชิก
- มีแผนรับมือภัยคุกคามไซเบอร์

IT Risk Management

บริหารจัดการความเสี่ยงด้าน IT ที่เกี่ยวกับ Blockchain อย่างรัดกุม

- ออกแบบและพัฒนา Blockchain ให้ปลอดภัย
- ทดสอบความปลอดภัยของ Blockchain อย่างสม่ำเสมอ
- ควบคุมการเข้าถึง Blockchain อย่างรัดกุม
- รักษาความลับและสำรองข้อมูล On-chain และ Off-chain ตามระดับความสำคัญ
- ดูแลกุญแจเข้ารหัสใน Blockchain
- ติดตามรายการธุรกรรมและ Log
- มีแผน BCP และ IT DRP รองรับ

Legal Risk Management

ดูแลข้อมูลส่วนบุคคลบน Blockchain โดยคำนึงถึงสิทธิและความเป็นส่วนตัว

- มีข้อตกลงร่วมกันระหว่างสมาชิกและผู้ที่เกี่ยวข้องในเครือข่าย
- เก็บรักษาข้อมูลส่วนบุคคลแบบ Off-chain
- ประเมิน Data Protection Impact Assessment
- การปฏิบัติตามกฎหมายที่เกี่ยวข้อง เช่น AML/CFT PDPA

หลักการที่ 1 การประยุกต์ใช้เทคโนโลยี Blockchain ในการประกอบธุรกิจ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินควรมีความรู้ความเข้าใจในเทคโนโลยี Blockchain ทั้งในแง่มุมรูปแบบธุรกิจ ประโยชน์และข้อจำกัดของเทคโนโลยี รวมถึงมีการคัดเลือก Blockchain Platform ที่เหมาะสมกับลักษณะธุรกิจ ก่อให้เกิดประโยชน์ต่อการดำเนินธุรกิจและมีความคุ้มค่าต่อการลงทุน เนื่องจากปัจจุบันเทคโนโลยี Blockchain มีพัฒนาการหลากหลายรูปแบบ โดยแต่ละแบบต่างมีจุดแข็ง จุดอ่อน และข้อจำกัดทางเทคโนโลยีที่แตกต่างกัน

แนวทางที่พึงปฏิบัติ

(1) พิจารณาการนำเทคโนโลยี Blockchain มาใช้ให้ตรงกับความจำเป็นหรือความต้องการทางธุรกิจขององค์กร โดยมีการใช้แนวทางการพิจารณาตัดสินใจใช้เทคโนโลยี Blockchain โดยอ้างอิงแนวทางที่มีความน่าเชื่อถือ[2] หรือมีการประเมินความเป็นไปได้ (Feasibility Assessment) ในการนำเทคโนโลยี Blockchain มาปรับในการประกอบธุรกิจขององค์กร โดยการศึกษาและประเมินความเป็นไปได้ดังกล่าวควรได้รับความยินยอมจากผู้บริหารหรือผู้มีหน้าที่รับผิดชอบในการนำเทคโนโลยี Blockchain มาใช้ในองค์กร

(2) วิเคราะห์กลยุทธ์สำหรับการนำเทคโนโลยี Blockchain มาใช้กับธุรกิจในมิติต่าง ๆ เช่น กลุ่มลูกค้าเป้าหมายและความต้องการหรือปัญหาของลูกค้าที่สามารถนำเทคโนโลยี Blockchain มาแก้ปัญหาได้ คู่แข่งทางธุรกิจ ศักยภาพขององค์กร ข้อจำกัดของเทคโนโลยี Blockchain เป็นต้น

(3) ประเมินต้นทุนและความคุ้มค่าของการนำเทคโนโลยี Blockchain มาใช้กับกระบวนการทางธุรกิจปัจจุบัน รวมถึงการเปรียบเทียบเทคโนโลยี Blockchain กับเทคโนโลยีอื่นที่สามารถตอบสนองความต้องการทางธุรกิจได้เช่นเดียวกัน โดยคำนึงถึงปัจจัยต่าง ๆ อย่างรอบด้าน เช่น

(3.1) ค่าใช้จ่ายในการพัฒนาระบบ ซึ่งอาจมีการเปรียบเทียบต้นทุนในการพัฒนาด้วย In-house Development กับการใช้บริการจากผู้ให้บริการภายนอก (Outsourcing)

(3.2) การบริหารจัดการโครงการ เช่น การจ้างที่ปรึกษาหรือผู้เชี่ยวชาญ

(3.3) ต้นทุนการดำเนินงานต่าง ๆ (Operation Cost) เช่น ค่าใช้บริการ Cloud Services

(4) คัดเลือกเทคโนโลยี Blockchain Platform ให้เหมาะสมกับรูปแบบธุรกิจ โดยมีการประเมินตามปัจจัย ดังต่อไปนี้

(4.1) ประเภทของเทคโนโลยี Blockchain ที่สอดคล้องกับความต้องการขององค์กรและรูปแบบธุรกิจ โดยพิจารณาในประเด็นต่าง ๆ ได้แก่ การรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ความสามารถในการรองรับปริมาณธุรกรรม (Performance) ทั้งในปัจจุบันและอนาคต รูปแบบการกำกับดูแลเครือข่าย (Network Governance) ลักษณะของผู้ร่วมในเครือข่าย (Participants)

---

[2] เช่น แนวทางของ World Economic Forum – Blockchain Beyond the Hype A Practical Framework for Business Leaders แนวทางของ IEEE Spectrum – Do You Need A Blockchain? แนวทางของ NISTIR 8202 - Blockchain Technology Overview

(4.2) รูปแบบสถาปัตยกรรม โดยพิจารณาความสามารถของ Blockchain Platform ในรายละเอียด ดังต่อไปนี้

(4.2.1) การเชื่อมต่อ (Interoperability) กับระบบงานต่าง ๆ ขององค์กรด้วยรูปแบบต่าง ๆ เช่น API Standard เพื่อรองรับความเปลี่ยนแปลงของธุรกิจและกฎหมายที่เกี่ยวข้อง

(4.2.2) ความน่าเชื่อถือและความมั่นคงปลอดภัยของกลไก Consensus ของ Blockchain Platform โดยครอบคลุมการประเมินข้อดี ข้อจำกัดของ Consensus Algorithm ที่เหมาะสมกับธุรกรรมแต่ละประเภท รวมถึงความสามารถในการขยายระบบ (Scalability) เพื่อรองรับปริมาณธุรกรรมในอนาคต

(4.2.3) การดูแลข้อมูลที่อยู่ในระบบ Blockchain รวมถึงการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนการออกแบบระบบ (Privacy by Design) หรือใช้มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งมาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ร่วมกัน ในการบริหารจัดการเพื่อคุ้มครองข้อมูลส่วนบุคคล

(4.3) พัฒนาการของเทคโนโลยี โดยประเมินความพร้อมและการสนับสนุนของ Technology Provider/Blockchain Platform โดยพิจารณาในรายละเอียด ดังนี้

(4.3.1) การสนับสนุนด้านเทคนิค (Technical Support) จากผู้ให้บริการภายนอก ความพร้อมของเอกสารที่เกี่ยวข้อง (Documentation) และการสนับสนุนจากนักพัฒนาระบบ (Community/Developer)

(4.3.2) แนวทางการพัฒนาเทคโนโลยี Blockchain ในอนาคต (Technology Roadmap)

(4.3.3) ฐานลูกค้าหรือจำนวนโครงการที่มีการนำ Blockchain Platform ไปใช้งาน (Active Project)

หลักการที่ 2 การกำกับดูแลการใช้เทคโนโลยี Blockchain

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีแนวทางในการกำกับดูแลโครงการที่ใช้เทคโนโลยี Blockchain อย่างมีประสิทธิภาพ โดยครอบคลุมการกำหนดบทบาทหน้าที่ที่จำเป็น การบริหารความเสี่ยงด้านปฏิบัติการ การรักษาความมั่นคงปลอดภัย และการกำกับและตรวจสอบผู้ให้บริการภายนอก นอกจากนี้ ผู้ประกอบธุรกิจที่เป็นผู้ดูแลเครือข่าย Blockchain ก็อาจนำหลักการนี้ไปประยุกต์ใช้ในการบริหารจัดการสมาชิกในเครือข่าย Blockchain ทั้งที่เป็นผู้ให้บริการทางการเงิน หน่วยงานภาครัฐ หรือบริษัทเอกชนจากภาคอุตสาหกรรมอื่น ๆ ซึ่งจะส่งผลต่อความน่าเชื่อถือของโครงการ รวมถึงโอกาสในการขยายการนำเทคโนโลยี Blockchain ไปใช้ในวงกว้างมากยิ่งขึ้น

แนวทางที่พึงปฏิบัติ

2.1 <u>กรณีการใช้เทคโนโลยี Blockchain หรือการเข้าร่วมเป็นสมาชิกในเครือข่าย Blockchain</u>

(1) ควรกำกับดูแลโครงการที่ใช้เทคโนโลยี Blockchain ให้สอดคล้องตามหลักเกณฑ์ของ ธปท. ว่าด้วยการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ให้สอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมถึงอยู่บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า

(2) ควรกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในระดับต่าง ๆ ในโครงการที่ใช้เทคโนโลยี Blockchain เช่น การกำหนดให้มีผู้บริหารระดับสูงหรือคณะทำงานเพื่อรับผิดชอบการกำหนดกลยุทธ์ นโยบาย ระเบียบ วิธีปฏิบัติ กระบวนการทำงาน การรายงานความคืบหน้าของโครงการ

(3) ควรทบทวนหรือปรับปรุงนโยบายและกระบวนการทำงานให้สามารถรองรับการใช้เทคโนโลยี Blockchain สำหรับใช้ปฏิบัติงานภายในองค์กร เช่น นโยบายการรักษาความมั่นคงปลอดภัยของระบบและข้อมูล กระบวนการปฏิบัติงาน (Business Process) ที่เกี่ยวข้อง

(4) ควรจัดให้มีการควบคุมดูแลความเสี่ยงจากเหตุการณ์ทุจริตที่อาจเกิดขึ้นจากการกระทำของบุคคลภายในองค์กรและบุคคลภายนอกองค์กร (Internal and External Fraud) เช่น การทำธุรกรรมโดยไม่รับอนุญาต การลักลอบใช้บัญชีผู้อื่น การยักยอกทรัพย์ การปลอมเป็นบุคคลอื่น การนำข้อมูลความลับไปขายหรือส่งต่อ และการลักลอบนำข้อมูลของลูกค้าไปทำทุจริตต่าง ๆ

(5) ควรมีการควบคุม ติดตาม และสอบทานการปฏิบัติตามการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการเชื่อมต่อระบบกับเครือข่าย Blockchain อย่างเหมาะสมตามข้อกำหนดของผู้ดูแลเครือข่าย Blockchain และรายงานการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงที่เกี่ยวข้องอย่างสม่ำเสมอ เช่น คณะกรรมการภายในองค์กร และผู้ดูแลเครือข่าย Blockchain

(6) ควรมีการประเมินความเสี่ยงและจัดให้มีการควบคุมให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) โดยพิจารณาครอบคลุมข้อดี ข้อจำกัด และประเด็นด้านความมั่นคงปลอดภัยของเทคโนโลยี

Blockchain และกลไก Consensus ที่ใช้งาน รวมถึงกระบวนการทำธุรกรรมที่เกี่ยวข้อง อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

(7) ควรจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอกอย่างรัดกุมต่อเนื่อง โดยครอบคลุมตั้งแต่การใช้บริการ Cloud Computing จากผู้ให้บริการภายนอก จนถึงการเชื่อมต่อระบบกับพันธมิตรทางธุรกิจเพื่อให้บริการร่วมกัน เช่น การเชื่อมต่อกับเครือข่าย Blockchain โดยมีเนื้อหาครอบคลุมในเรื่องดังต่อไปนี้

(7.1) มีการประเมินและบริหารความเสี่ยงอันเกิดจากบุคคลภายนอก เช่น การรักษาความลับการดูแลข้อมูลของลูกค้ารวมถึงการคุ้มครองข้อมูลส่วนบุคคล การเปลี่ยนแปลงหรือยกเลิกบริการได้ยาก (Vendor Lock-in) การกระจุกตัวของทรัพยากรที่สำคัญ (Concentration Risk) เป็นต้น

(7.2) มีมาตรฐานการรักษาความมั่นคงปลอดภัยระบบและข้อมูลขั้นต่ำที่บุคคลภายนอกต้องถือปฏิบัติ

(7.3) มีการตรวจสอบและติดตามการรักษาความมั่นคงปลอดภัยระบบและข้อมูลของบุคคลภายนอกอย่างต่อเนื่อง ทั้งนี้ กรณีที่ไม่สามารถเข้าตรวจสอบได้อาจสอบทานจากรายงานตรวจสอบจากผู้ตรวจสอบหรือผู้เชี่ยวชาญภายนอกที่มีมาตรฐานเป็นที่ยอมรับ เช่น ผลการตรวจสอบตามมาตรฐาน SSAE 18 (SOC 2 Type 2 Report)

ทั้งนี้ แนวทางการบริหารจัดการความเสี่ยงบุคคลภายนอกเป็นไปตามแนวปฏิบัติของธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Implementation Guideline) โดยให้ผู้ให้บริการทางการเงินนำไปปรับใช้ให้เหมาะสมและสอดคล้องตามระดับความเสี่ยงและความมีนัยสำคัญของแต่ละการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

2.2 <u>กรณีเป็นผู้ดูแลเครือข่าย Blockchain หรือโครงการ Blockchain ที่มีลักษณะเป็นโครงสร้างพื้นฐานทางการเงิน (Financial Infrastructure)</u> ที่มีผลกระทบต่อการให้บริการทางการเงินในวงกว้าง ควรมีแนวทางการกำกับดูแลเพิ่มเติม ดังนี้

(1) ผู้ดูแลเครือข่าย Blockchain ควรกำหนดบทบาทหน้าที่ความรับผิดชอบของตน โดยครอบคลุมหน้าที่ ดังต่อไปนี้

(1.1) การดูแลภาพรวม การกำหนดกลยุทธ์ ทิศทางการดำเนินธุรกิจ การกำหนดกฎเกณฑ์ทางธุรกิจ (Business Rule) ของเครือข่าย Blockchain

(1.2) การเข้าร่วมเป็นสมาชิก (On-boarding) การสื่อสารกับสมาชิกในเครือข่าย Blockchain การปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้อง

(1.3) การดูแลเทคโนโลยีและสถาปัตยกรรมระบบ Blockchain การดูแลเสถียรภาพของระบบ IT Infrastructure รวมถึงการติดตามเรื่องความปลอดภัยและความพร้อมใช้ของระบบ

(2) ควรจัดให้มีมาตรฐานหรือคู่มือการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของเครือข่าย Blockchain ให้กับสมาชิกในเครือข่าย Blockchain อย่างเป็นลายลักษณ์อักษร รวมทั้งผู้ดูแลเครือข่าย Blockchain ควรควบคุม ติดตาม รายงาน และนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงที่เกี่ยวข้องอย่างสม่ำเสมอ เช่น คณะกรรมการภายในองค์กร โดยมีเนื้อหาครอบคลุมในเรื่องต่อไปนี้

(2.1) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับสมาชิกในการเชื่อมต่อกับเครือข่าย Blockchain เช่น การบริหารจัดการกุญแจเข้ารหัส การควบคุมการเข้าถึง การติดตาม ดูแล จัดเก็บข้อมูลบันทึกเหตุการณ์ของระบบ รวมถึง Security Baseline

(2.2) การออกแบบและเชื่อมต่อระบบ เช่น แนวทางการตั้งค่าจุดเชื่อมต่อและ Node ที่เหมาะสม รูปแบบการวางระบบที่เหมาะสม (Recommended Architecture)

(2.3) การบริหารจัดการการเปลี่ยนแปลง (Change Management) การบริหารจัดการ patch (Patch Management) ของเครือข่าย Blockchain และตลอดวงจรชีวิตของ Smart Contract

(2.4) การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศและการบริหารความต่อเนื่องทางธุรกิจ (IT Incident Management and Business Continuity Management) ของเครือข่าย Blockchain

(3) ควรจัดให้มีมาตรฐานการบริหารจัดการสมาชิกในเครือข่าย Blockchain ทั้งสมาชิกใหม่และสมาชิกปัจจุบันในเครือข่าย Blockchain อย่างเป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมในเรื่องต่อไปนี้

(3.1) หลักเกณฑ์การสื่อสารกับสมาชิก เพื่อให้สมาชิกรับทราบข้อมูลขั้นพื้นฐานอย่างเท่าเทียมกันและมีความโปร่งใส เช่น ข้อมูลพื้นฐานด้านเทคโนโลยีสารสนเทศ แนวทางแก้ไขปัญหาการตั้งค่าระบบและสถานะความปลอดภัยของเครือข่าย

(3.2) กระบวนการเข้าร่วมเป็นสมาชิก (On-boarding Process) เช่น กำหนดให้สมาชิกและผู้ใช้งานต้องมีการบริหารความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศตามเกณฑ์ที่กำหนด

(3.3) กระบวนการเปลี่ยนแปลงและยกเลิกการเป็นสมาชิก (Off-boarding Process) เช่น มีอำนาจในการยกเลิก หากมีการทำผิดข้อตกลง กฎหมาย หรือไม่ผ่านเกณฑ์ขั้นพื้นฐานตามที่ระบุไว้ในกระบวนการการเข้าร่วม ตลอดจนกระบวนการยกเลิกการเข้าถึงข้อมูลและเครือข่ายของสมาชิก

(3.4) กระบวนการบริหารจัดการสิทธิการใช้งานของสมาชิก เช่น ให้สิทธิเฉพาะเท่าที่จำเป็น แบ่งกลุ่มสมาชิกที่สามารถและไม่สามารถทำธุรกรรมได้ กำหนดสิทธิในทรัพย์สินทางปัญญาและขอบเขตในการอนุญาตให้ใช้สิทธิดังกล่าว

(3.5) กำหนดข้อตกลงการให้บริการ (Service Level Agreement: SLA) ที่สอดคล้องกับระดับความต้องการทางธุรกิจ

(3.6) กำหนดแนวทางหรือมาตรฐานการเชื่อมต่อกับเครือข่ายของสมาชิก เช่น มาตรการตัดการเชื่อมต่อชั่วคราว กรณี Node ของสมาชิกส่งคำสั่งธุรกรรมที่ผิดพลาดอย่างต่อเนื่อง เพื่อป้องกันไม่ให้เกิดผลกระทบด้านประสิทธิภาพในวงกว้าง

(4) ควรกำกับดูแลเครือข่ายและสมาชิกในเครือข่าย Blockchain ให้ครอบคลุมความเสี่ยงด้านไซเบอร์ เช่น ประเมินและควบคุมความเสี่ยงด้านไซเบอร์ รวมถึงจัดทำแผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ที่สำคัญ

ทั้งนี้ ผู้ให้บริการทางการเงินควรพิจารณาเข้าร่วมเป็นสมาชิกในเครือข่าย Blockchain ที่ผู้ดูแลเครือข่าย Blockchain ปฏิบัติตามแนวทางการกำกับดูแลในข้อ 2.2

หลักการที่ 3 การบริหารจัดการความเสี่ยงด้าน IT สำหรับเทคโนโลยี Blockchain

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีการบริหารจัดการความเสี่ยงด้าน IT ในการนำเทคโนโลยี Blockchain มาใช้ ครอบคลุมตั้งแต่ระบบ Blockchain จุดเชื่อมต่อกับเครือข่าย Blockchain และภายในเครือข่าย Blockchain สอดคล้องตามมาตรฐาน แนวปฏิบัติที่เป็นสากล และหลักเกณฑ์ของ ธปท. ว่าด้วยการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ (1) การรักษาความลับของระบบและข้อมูล (Confidentiality) (2) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และ (3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability) ตามระดับความเสี่ยงของธุรกรรม เพื่อให้ผู้ที่เกี่ยวข้องมีความเชื่อมั่น และมั่นใจว่าระบบและจุดเชื่อมต่อกับเครือข่าย Blockchain ของสมาชิกแต่ละราย ทั้งในภาคการเงินและอุตสาหกรรมอื่น ๆ ที่ร่วมอยู่ในเครือข่าย Blockchain มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นมาตรฐานเดียวกัน

แนวทางที่พึงปฏิบัติ

(1) กำหนด Security Baseline ของระบบ Blockchain จุดเชื่อมต่อกับเครือข่าย Blockchain และภายในเครือข่าย Blockchain ให้มีการตั้งค่าตามระดับความเสี่ยงที่เหมาะสม โดยอ้างอิงมาตรฐานสากล หรือตามคำแนะนำในทางปฏิบัติ (Best Practices) ของเจ้าของผลิตภัณฑ์หรือผู้ให้บริการ (Vendor)

(2) ออกแบบ พัฒนา และทดสอบระบบอย่างปลอดภัย (Secure Software Development) โดยครอบคลุมภาษาชุดคำสั่งและเครื่องมือที่ใช้พัฒนาโปรแกรมแบบกระจายศูนย์ของระบบ Blockchain จุดเชื่อมต่อกับเครือข่าย Blockchain และภายในเครือข่าย Blockchain เช่น การพัฒนา Smart Contract ที่กำหนดการทำธุรกรรมแบบอัตโนมัติ ควรดำเนินการเพื่อให้มั่นใจว่าโปรแกรมสามารถทำงานได้อย่างถูกต้องตลอดกระบวนการทำธุรกรรม รวมทั้งมีการสอบทานคำสั่ง (Source Code Review) ของ Smart Contract ทั้งในด้านความมั่นคงปลอดภัย และความครอบคลุมของเงื่อนไข ทุกครั้งที่มีการพัฒนาหรือเปลี่ยนแปลง

(3) ทดสอบประสิทธิภาพและความพร้อมใช้ เช่น Performance Testing และ Stress Testing แบบ End-to-End เพื่อให้มั่นใจได้ว่าระบบมีความเสถียรเพียงพอรองรับการใช้งานจำนวนมาก รวมทั้งจัดให้มีการติดตามและปรับปรับปรุงประสิทธิภาพ เพื่อให้มั่นใจว่าระบบมีความพร้อมใช้สามารถรองรับธุรกรรมที่คาดว่าจะเพิ่มขึ้นได้อย่างต่อเนื่อง

(4) ทดสอบการรักษาความมั่นคงปลอดภัย (Security Testing) ระบบที่ใช้เทคโนโลยี Blockchain อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยครอบคลุมการประเมินช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test) ของระบบ Blockchain จุดเชื่อมต่อกับเครือข่าย Blockchain และภายในเครือข่าย Blockchain ตามระดับความเสี่ยง เช่น API และระบบโครงสร้างพื้นฐานที่เชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (Internet Facing) รวมถึงพิจารณาประเมินช่องโหว่และทดสอบเจาะระบบตามระดับความเสี่ยงของ Smart Contract ที่ใช้ภาษาชุดคำสั่งเฉพาะทางสำหรับทำงานแบบกระจายศูนย์ โดยผู้เชี่ยวชาญที่มีความอิสระ

(5) ควบคุมการเข้าถึง (Access Control) ให้ครอบคลุม ดังนี้

(5.1) ผู้ใช้งานที่เกี่ยวข้องบนระบบ Blockchain เช่น สมาชิกในเครือข่าย Blockchain และพนักงานภายในองค์กร

(5.2) ระบบ Blockchain จุดเชื่อมต่อกับเครือข่าย Blockchain และภายในเครือข่าย Blockchain เช่น Node ของสมาชิกในเครือข่าย Blockchain และ Node ตัวกลางที่รับหน้าที่ทำ Consensus รวมถึงจุดเชื่อมต่อทั้ง API Server และ Web Portal

(5.3) ข้อมูลที่จัดเก็บทั้ง On-chain และ Off-chain

(6) รักษาความมั่นคงปลอดภัยของข้อมูล (Information Security) ทั้ง On-chain และ Off-chain เช่น จัดชั้นความลับ และข้อมูลที่มีระดับชั้นความลับสูงควรจัดเก็บแบบ Off-chain หรือเข้ารหัสข้อมูล

(7) บริหารจัดการการเข้ารหัสข้อมูล (Cryptography) และบริหารจัดการกุญแจเข้ารหัส (Key Management) ของระบบ Blockchain จุดเชื่อมต่อกับเครือข่าย Blockchain และภายในเครือข่าย Blockchain ที่รัดกุมตามมาตรฐานสากล ตั้งแต่กระบวนการสร้าง จัดเก็บ ต่ออายุ เปลี่ยน และทำลายกุญแจเข้ารหัส

(8) ติดตามรายการธุรกรรม (Transaction Monitoring) จัดเก็บบันทึกเหตุการณ์การเข้าถึง (Access Log) และบันทึกการดำเนินงาน (Activity Log) ของระบบ Blockchain จุดเชื่อมต่อกับเครือข่าย Blockchain และภายในเครือข่าย Blockchain เช่น ติดตามและเฝ้าระวังธุรกรรมผิดปกติที่อาจนำไปสู่การทำธุรกรรมโดยทุจริต (Fraud) หรือผลการทำ Consensus ที่ล้มเหลว รวมถึงเฝ้าระวังการเข้าถึง Node และการใช้งาน API ที่ผิดปกติ

(9) ควรจัดให้มีการสอบทานความถูกต้องของข้อมูล และขั้นตอนการทำธุรกรรมตลอดกระบวนการ (End-to-End) โดยพิจารณาดำเนินการให้สอดคล้องกับลักษณะธุรกิจและระดับความเสี่ยงของผู้ดูแลเครือข่ายและสมาชิกในเครือข่าย Blockchain เช่น จัดให้มีการสอบทานความถูกต้องของข้อมูลระหว่าง On-chain และ Off-chain เพื่อให้มั่นใจว่าการทำธุรกรรมตั้งแต่การส่งคำสั่งของลูกค้าจนถึงการประมวลผลในระบบ Blockchain และเครือข่าย Blockchain ข้อมูลคำสั่งหรือค่าตัวแปรไม่ได้ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(10) สำรองข้อมูล (Data Backup) เพื่อให้มีข้อมูล On-chain และ Off-chain พร้อมใช้เป็นหลักฐานหากข้อมูลดังกล่าวได้รับความเสียหาย ทั้งนี้ กรณีใช้บริการ Cloud Services จากผู้ให้บริการภายนอก ควรมีกระบวนการสำรองข้อมูลธุรกรรมที่มีความสำคัญหรืออาจส่งผลกระทบต่อการให้บริการในวงกว้างให้มีความพร้อมใช้งานอย่างต่อเนื่อง

(11) บริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศและการบริหารความต่อเนื่องทางธุรกิจ (IT Incident Management and Business Continuity Management) รองรับระบบงานที่ใช้เทคโนโลยี Blockchain โดยสอดคล้องตามระดับความสำคัญของระบบงาน

หลักการที่ 4 การบริหารความเสี่ยงทางกฎหมายกับการใช้เทคโนโลยี Blockchain

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินต้องปฏิบัติตามกฎหมายที่เกี่ยวข้อง และมีแนวทางในการจัดการกับข้อมูลของผู้ใช้บริการซึ่งเก็บอยู่ในเครือข่าย Blockchain ที่มั่นคงปลอดภัย โดยคำนึงถึงความมีผลผูกพันและการบังคับใช้ตามกฎหมาย ตลอดจนมีการคุ้มครองสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูล รวมถึงการคุ้มครองข้อมูลส่วนบุคคล เพื่อการบริหารจัดการความเสี่ยงทางกฎหมายที่มีประสิทธิภาพและการคุ้มครองดูแลผู้ให้บริการและผู้ที่เกี่ยวข้องอย่างเหมาะสม

แนวทางที่พึงปฏิบัติ

(1) กรณีเป็นผู้ดูแลเครือข่าย Blockchain ควรจัดให้มีข้อตกลงร่วมกันระหว่างสมาชิกในเครือข่าย Blockchain และผู้ที่เกี่ยวข้องในเครือข่าย Blockchain เช่น การกำหนดรูปแบบและเงื่อนไขเกี่ยวกับผู้ที่มีบทบาทหน้าที่ในการทำ Consensus แนวปฏิบัติและความถี่การสำรองข้อมูลและสอบทานความถูกต้องของข้อมูล และรูปแบบกระบวนการทำธุรกรรมและเวลา Timeout ของระบบ Blockchain เพื่อกำหนดผู้รับผิดชอบที่ชัดเจน สร้างความเข้าใจที่ตรงกัน และลดข้อโต้แย้งระหว่างสมาชิก

(2) ควรจัดให้มีข้อตกลงเกี่ยวกับ Smart Contract ในเครือข่าย Blockchain ระหว่างผู้ที่เกี่ยวข้อง เช่น ความมีผลทางกฎหมายของธุรกรรม ความมีผลสมบูรณ์ของธุรกรรม (Finality) สิทธิหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้อง กระบวนการจัดการข้อผิดพลาดหรือข้อโต้แย้ง เป็นต้น รวมทั้ง ควรจัดให้มีการทบทวนเนื้อหาและกระบวนการตาม Smart Contract ให้สอดคล้องกับข้อตกลงดังกล่าว กฎหมายและนโยบายของผู้ให้บริการทางการเงินที่เปลี่ยนแปลงไป

(3) กรณีที่การใช้เทคโนโลยี Blockchain หรือการเข้าร่วมเครือข่าย Blockchain มีข้อมูลส่วนบุคคลเข้ามาเกี่ยวข้อง ผู้ให้บริการทางการเงินควรประเมินความเสี่ยงที่อาจจะกระทบกับสิทธิของเจ้าของข้อมูลส่วนบุคคล และหากประเมินแล้วพบว่ามีความเสี่ยงสูง ผู้ให้บริการทางการเงินควรเก็บรักษาข้อมูลส่วนบุคคลแบบ Off-chain หรือพิจารณาใช้เทคโนโลยีหรือวิธีการอื่นที่ทำให้การควบคุมดูแลข้อมูลเป็นไปตามกฎหมายที่เกี่ยวข้องหรือมาตรการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ ผู้ให้บริการทางการเงินควรจัดให้มีกระบวนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลร่วมด้วย[3] หากมีการเปลี่ยนแปลงการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับระบบหรือเครือข่าย Blockchain อย่างมีนัยสำคัญ ผู้ให้บริการทางการเงินควรทบทวนการประเมินดังกล่าว

(4) จัดให้มีกระบวนการพิจารณาและทบทวนข้อมูลที่อยู่ในเครือข่าย Blockchain อย่างสม่ำเสมอว่าเป็นข้อมูลที่สามารถระบุตัวบุคคลไม่ว่าโดยทางตรงหรือทางอ้อม เพื่อประเมินลักษณะที่อาจเข้าข่ายเป็นข้อมูลส่วนบุคคล[4] หากเข้าข่ายว่าเป็นข้อมูลส่วนบุคคล นอกจากการปฏิบัติตามแนวปฏิบัติ ธปท. ว่าด้วยการกำกับดูแล

---

[3] การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment) สามารถอ้างอิงได้จากแนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

[4] การประเมินความสามารถของข้อมูลในการเชื่อมโยงไปยังตัวบุคคล สามารถอ้างอิงได้จากปัจจัยตามที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล รวมถึงหลักเกณฑ์และแนวปฏิบัติของหน่วยงานที่เกี่ยวข้อง

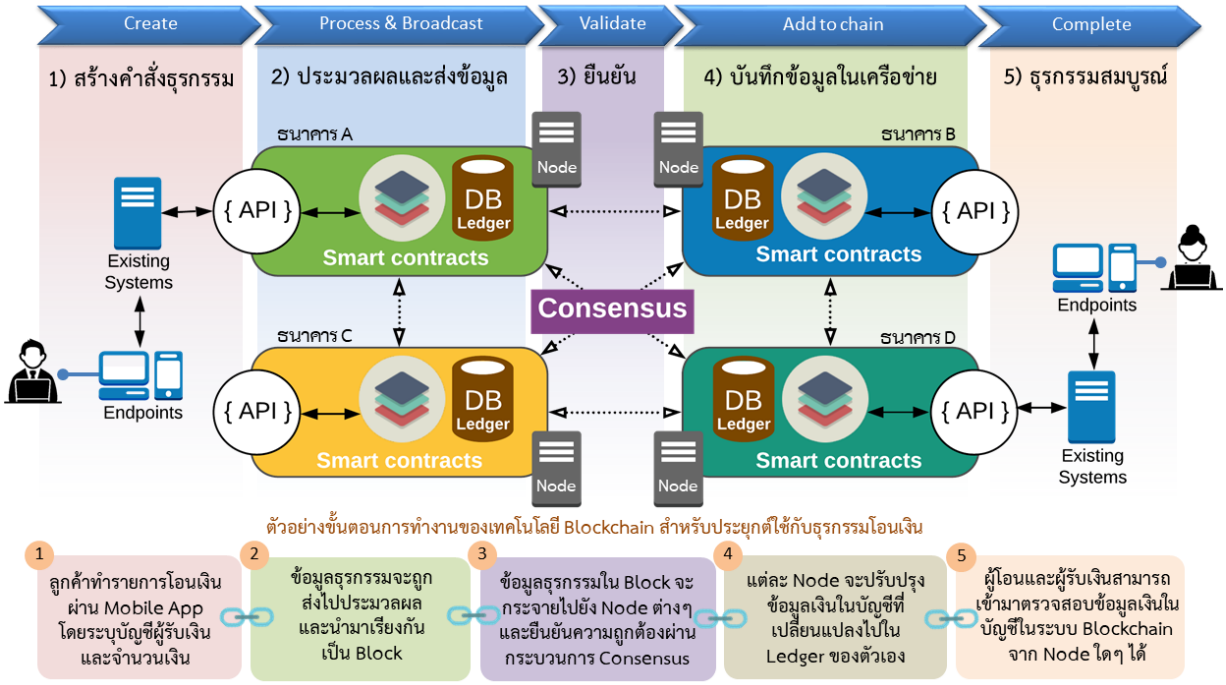
ข้อมูล (Data Governance) แล้ว ผู้ให้บริการทางการเงินต้องคำนึงอย่างที่สุดในการคุ้มครองสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล และปฏิบัติตามกฎหมายที่เกี่ยวข้อง

(5) ผู้ให้บริการทางการเงินที่นำเทคโนโลยี Blockchain มาใช้ ต้องปฏิบัติตามกฎหมายและหลักเกณฑ์การกำกับดูแลของ ธปท. และกฎหมายอื่นที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล

(6) จัดให้มีกระบวนการให้ความรู้แก่ผู้ใช้บริการและผู้ที่เกี่ยวข้องเกี่ยวกับการนำเทคโนโลยี Blockchain มาใช้กับผลิตภัณฑ์และบริการทางการเงิน เพื่อให้ผู้ใช้บริการและผู้ที่เกี่ยวข้องเข้าใจถึงประโยชน์และผลกระทบที่อาจเกิดขึ้นจากการใช้เทคโนโลยี Blockchain

ภาคผนวก 1 – ความรู้พื้นฐานเกี่ยวกับเทคโนโลยี Blockchain

1. **กระบวนการทำงานของเทคโนโลยี Blockchain** ประกอบด้วย 5 ขั้นตอนหลัก ดังนี้



(1) สร้างคำสั่งธุรกรรม (Create) สำหรับส่งข้อมูลและส่งคำสั่งเพื่อทำธุรกรรมที่เกี่ยวข้อง เช่น การโอนเงิน การซื้อขายพันธบัตร โดยส่งผ่านอุปกรณ์ (Endpoint) และจุดเชื่อมต่อที่เป็นระบบโครงสร้างพื้นฐานเดิม ผ่าน API[5] ไปประมวลผลด้วยกลไก Smart Contract ภายใน Node

(2) ประมวลผลและส่งต่อข้อมูล (Process and Broadcast) เพื่อให้ Node ที่เชื่อมต่อในเครือข่าย Blockchain ที่เกี่ยวข้องกับคำสั่งธุรกรรม ทำการบันทึกข้อมูลลงใน Block โดยอาจประมวลผลพร้อมทั้งตรวจสอบข้อมูลร่วมกันด้วย

(3) ยืนยันและตรวจสอบข้อมูล (Validate) โดยผ่านการลงความเห็นจากสมาชิกในเครือข่าย Blockchain ที่ได้รับมอบหมาย เป็นไปตามรูปแบบของ Consensus ของเครือข่าย Blockchain ตามขั้นตอนและกติกาที่ได้กำหนดไว้

(4) บันทึกข้อมูลในเครือข่าย Blockchain (Add to chain) เมื่อมีการ Consensus สำเร็จ ระบบจะสร้าง Block ขึ้นใหม่ โดยนำ Block ที่สร้างขึ้นใหม่มาเชื่อมต่อกับ Block ก่อนหน้าในรูปแบบ Chain หรือเป็นไปตามการออกแบบในแต่ละประเภทของ Blockchain Platform

(5) ธุรกรรมสมบูรณ์ (Complete) ข้อมูลที่ถูกบันทึกไว้ในระบบที่ถูกจัดเก็บแบบกระจายศูนย์ มีความน่าเชื่อถือ ยากต่อการเปลี่ยนแปลง และสามารถใช้อ้างอิงเป็นหลักฐานในการทำธุรกรรมต่อไป

[5] API ย่อมาจาก Application Programming Interface เป็น Software ตัวกลางสำหรับเชื่อมต่อระบบเข้าด้วยกัน

2. คุณลักษณะสำคัญของเทคโนโลยี Blockchain

Blockchain เป็นเทคโนโลยีเนกประสงค์ (General Purpose Technology) เนื่องจากสามารถนำไปประยุกต์กับรูปแบบธุรกิจได้หลากหลาย มีการพัฒนาการของเทคโนโลยีอย่างต่อเนื่อง และสามารถสร้างนวัตกรรมต่อยอดรูปแบบธุรกิจเดิมได้หลากหลาย มีโอกาสที่สร้างประโยชน์แก่ระบบเศรษฐกิจ รวมถึงการเปลี่ยนแปลงต่อสังคม

เทคโนโลยี Blockchain มีคุณลักษณะที่สำคัญ 5 ประการ ดังนี้

(1) ฐานข้อมูลแบบกระจายศูนย์ (Distributed Database) โดยสมาชิกในเครือข่าย Blockchain จะมีข้อมูลชุดเดียวกัน[2]

(2) การสื่อสารโดยตรงระหว่างสมาชิก (Peer-to-Peer Transmission) โดยสมาชิกในเครือข่าย Blockchain จะแลกเปลี่ยนข้อมูลกันโดยตรงด้วยรูปแบบการแลกเปลี่ยนข้อมูล (Protocol)

(3) ข้อมูลธุรกรรมมีความโปร่งใส (Transparency) โดยสมาชิกในเครือข่าย Blockchain จะสามารถเข้าถึงข้อมูลชุดเดียวกันจาก Node ใด ๆ ได้[6] ซึ่งยากต่อการปลอมแปลงข้อมูลที่ Node ที่ใดที่หนึ่ง

(4) ข้อมูลย้อนกลับไปแก้ไขไม่ได้ (Irreversibility) โดยชุดข้อมูลในแต่ละ Block จะมีการระบุค่าทางคณิตศาสตร์ (Hash) ของ Block ก่อนหน้าเชื่อมโยงกัน ทำให้การแก้ไขข้อมูลใน Block ใด ๆ จะส่งผลกระทบต่อข้อมูลของ Block ที่เชื่อมโยงในภายหลังตลอดทั้งชุดข้อมูล

(5) สามารถตั้งโปรแกรมให้ทำงานอัตโนมัติ (Computational Logic) โดยนักพัฒนาระบบสามารถเขียนโปรแกรมเพื่อเพิ่มข้อมูลในระบบ Blockchain เช่น Smart Contract ซึ่งข้อมูลใน Blockchain จะดำเนินการตามเงื่อนไขที่กำหนดไว้ในโปรแกรม

[6] ในบาง Blockchain Platform สามารถออกแบบให้สมาชิกแต่ละรายสามารถเก็บข้อมูลที่แตกต่างกันได้ตามวัตถุประสงค์ รวมถึงมีความสามารถปรับเทคโนโลยีให้สมาชิกเห็นข้อมูลเฉพาะที่เกี่ยวข้องได้ ซึ่งขึ้นอยู่กับการออกแบบความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิง

- Blockchain Preparation Audit Program ของ Information Systems Audit and Control Association (ISACA)
- Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector ของ The European Union Agency for Network and Information Security (ENISA)
- Distributed Ledger Technology: Principles for Industry-Wide Acceptance ของ International Securities Services Association (ISSA)
- Distributed Ledger Technology: Implications of Blockchain for the Securities Industry ของ Financial Industry Regulatory Authority (FINRA)
- Distributed Ledger Technology: Feedback Statement on Discussion Paper ของ Financial Conduct Authority (FCA)
- Inclusive Deployment of Blockchain for Supply Chains: Part 5 – A Framework for Blockchain Cybersecurity ของ The World Economic Forum (WEF)
- Proposals for a DLT Regulatory Framework ของ Gibraltar Finance – HM Government of Gibraltar
- Whitepaper 2.0 on Distributed Ledger Technology ของ Hong Kong Monetary Authority (HKMA)
- Project Ubin Phase 2 ของ Monetary Authority of Singapore (MAS)
- Governing DLT Networks – Distributed Ledger Technology Governance for Private Permissioned Networks ของ Depository Trust & Clearing Corporation (DTCC)
- Blockchain Technology Overview ของ National Institute of Standards and Technology (NIST)
- Blockchain for Government Services ของ Digital Government Development Agency (DGA)
- Blockchain/Distributed Ledger Working Group Glossary ของ Cloud Security Alliance
- Distributed Ledger Technology: Risk functions need to play an active role in shaping Blockchain strategy ของ Deloitte
- Realizing Blockchain’s potential ของ KPMG
- Assessing Blockchain risks ของ KPMG
- Auditing Blockchain solutions ของ KPMG

- Global Blockchain benchmarking study ของ Cambridge – Centre for Alternative Finance
- Guide to General Data Protection Regulation ของ UK Information Commissioner's Office
- Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law? ของ European Parliamentary Research Service
- A Thematic Report – Blockchain and the GDPR ของ EU Blockchain Observatory and Forum
- Technical Report ISO/TR 23244:2020 - Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations
- NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- Solutions for a responsible use of the Blockchain in the context of personal data ของ Commission Nationale de l'Informatique et des Libertés
- How Blockchain Applications will move beyond finance ของ Harvard Business Review
- Blockchain Beyond the Hype A Practical Framework for Business Leaders ของ World Economic Forum
- Do You Need A Blockchain? ของ IEEE Spectrum
- Thailand Data Protection Guidelines 2.0 ของ ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- พ.ร.ก. การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561